**Глава 5: Маршрутизация между VLAN**

**Введение**

Из предыдущих глав мы узнали о том, что использование сетей VLAN для сегментации коммутируемой сети повышает производительность, управляемость и безопасность сети. Транковые каналы служат для передачи между устройствами трафика сразу нескольких VLAN. Однако ввиду того, что VLAN делят сеть на сегменты, для передачи трафика между сегментами требуется процесс 3-го уровня.

Процесс маршрутизации на 3-м уровне можно осуществлять с помощью маршрутизатора или коммутатора 3-го уровня. Использование устройства 3-го уровня обеспечивает возможность управления передачей трафика между сегментами сети, в том числе сегментами, которые были созданы с помощью VLAN.

В данной главе подробно рассматриваются методы реализации маршрутизации между VLAN, а также приводятся настройки маршрутизатора и коммутатора 3-го уровня. Кроме того, в главе описываются проблемы, возникающие в процессе реализации маршрутизации между виртуальными локальными сетями, и стандартные методы поиска и устранения неполадок.

**Переход на локальные сетевые каналы**

**Переход на локальные сетевые каналы**

Вы работаете на предприятии малого или среднего бизнеса. Как сетевой администратор вы несёте ответственность за обеспечение эффективной и безопасной работы сети.

Несколько лет назад вы создали сети VLAN на одном коммутаторе для двух отделов — бухгалтерии и отдела продаж. По мере роста компании стало очевидно, что иногда этим отделам требуется общий доступ к корпоративным файлам и сетевым ресурсам.

Вы обсуждаете этот сценарий с сетевыми администраторами в филиалах вашей компании. Они рекомендуют вам использовать маршрутизацию между VLAN.

Изучите концепцию маршрутизации между VLAN.

Создайте простую презентацию, чтобы показать менеджерам, как использование маршрутизации между VLAN позволит оставить бухгалтерию и отдел продаж изолированными, но при этом открыть доступ к корпоративным файлам и сетевым ресурсам.

[Работа в аудитории. Переход на локальные сетевые каналы. Инструкции](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/5.0.1.2%20Switching%20to%20Local%20Network%20Channels%20Instructions.pdf)

# Что такое маршрутизация между VLAN?

Сети VLAN используются для сегментации коммутируемых сетей. Сетевой специалист может настроить коммутаторы 2-го уровня, например Catalyst 2960, на работу с более чем 4 тысячами сетей. Однако возможности протоколов IPv4 и IPv6 на коммутаторах 2-го уровня весьма ограничены, т. е. устройства не могут выполнять функцию маршрутизации. Несмотря на то, что возможности коммутаторов 2-го уровня расширяются, например, они могут выполнять статическую маршрутизацию, их функционала по-прежнему недостаточно для динамической маршрутизации. Для работы большого количества сетей VLAN, которые возможно настроить на коммутаторе, статической маршрутизации недостаточно.

Сеть VLAN — это домен широковещательной рассылки, поэтому компьютеры в разных сетях VLAN не могут обмениваться данными без помощи устройства маршрутизации. Любое устройство, поддерживающее маршрутизацию 3-го уровня, например маршрутизатор или многоуровневый коммутатор, можно использовать для выполнения основных функций маршрутизации. Независимо от используемого устройства, процесс пересылки сетевого трафика из одной VLAN в другую с использованием маршрутизации называют маршрутизацией между VLAN.

# Устаревшие методы маршрутизации между VLAN

Исторически первым решением для маршрутизации между VLAN стало использование маршрутизаторов с несколькими физическими интерфейсами. Каждый интерфейс должен был быть подключён к отдельной сети и настроен с определённой подсетью.

При таком устаревшем подходе маршрутизация между VLAN выполняется путём подключения различных физических интерфейсов маршрутизатора к разным физическим портам коммутатора. Порты коммутатора, подключённые к маршрутизатору, переводятся в режим доступа, а каждый физический интерфейс назначается отдельной VLAN. Каждый интерфейс маршрутизатора может принимать трафик из VLAN, связанной с интерфейсом коммутатора, к которому она подключена, и трафик можно направлять в другие VLAN, подключённые к другим интерфейсам.

**Примечание**. В топологии используются параллельные каналы для создания транков между коммутаторами в целях агрегации и резервирования каналов. Однако резервные каналы усложняют топологию и без должного управления могут привести к проблемам с подключением. Для управления резервными каналами необходимо реализовать такие протоколы и технологии, как связующее дерево (протокол STP) и EtherChannel. В рамках главы данные технологии не рассматриваются.

На рисунке нажмите кнопку Воспроизведение, чтобы просмотреть анимацию, демонстрирующую устаревший метод маршрутизации между VLAN.

Как видно из анимации:

1. Компьютер PC1 из сети VLAN 10 обменивается данными с компьютером PC3 из сети VLAN 30 через маршрутизатор R1.

2. Компьютеры PC1 и PC3 находятся в разных сетях VLAN, а их IP-адреса находятся в разных подсетях.

3. На маршрутизаторе R1 для каждой VLAN настроен отдельный интерфейс.

4. Компьютер PC1 отправляет на коммутатор S2 в сети VLAN 10 одноадресный трафик, предназначенный для компьютера PC3. Оттуда трафик пересылается по транковому интерфейсу на коммутатор S1.

5. Затем коммутатор S1 пересылает одноадресный трафик на интерфейс G0/0 маршрутизатора R1.

6. Маршрутизатор отправляет одноадресный трафик со своего интерфейса G0/1, который подключён к сети VLAN 30.

7. Маршрутизатор пересылает одноадресный трафик на коммутатор S1 в сети VLAN 30.

8. Затем коммутатор S1 пересылает одноадресный трафик на коммутатор S2 через активный транковый канал. После этого коммутатор S2 может переслать этот одноадресный трафик на компьютер PC3 в сети VLAN 30.

В этом примере для взаимодействия с разными VLAN и выполнения маршрутизации на маршрутизаторе были настроены два отдельных физических интерфейса.

**Примечание**. Этот метод маршрутизации между VLAN не является эффективным и теперь реже реализуется в коммутируемых сетях. В данном курсе пример приведён в образовательных целях.

# Маршрутизация между VLAN с использованием конфигурации router-on-a-stick

В отличие от традиционного метода маршрутизации между VLAN, который задействует несколько физических интерфейсов на маршрутизаторе и коммутаторе, более распространённый и современный метод маршрутизации между VLAN этого не требует. Вместо этого на некоторых маршрутизаторах ПО позволяет настраивать интерфейс маршрутизатора в качестве транка. Это означает, что для маршрутизации пакетов между несколькими VLAN на маршрутизаторе и коммутаторе требуется только один физический интерфейс.

Метод «router-on-a-stick» — это такой тип конфигурации маршрутизатора, при котором один физический интерфейс маршрутизирует трафик между несколькими VLAN. Как видно на рисунке, маршрутизатор подключён к коммутатору S1 с помощью одного физического сетевого подключения (транка).

Интерфейс маршрутизатора настраивается для работы в качестве транкового канала и подключается к порту коммутатора, который настроен в режиме транка. Маршрутизатор выполняет маршрутизацию между VLAN, принимая на транковом интерфейсе трафик с меткой VLAN, поступающий от смежного коммутатора, и затем с помощью подынтерфейсов маршрутизируя его между VLAN. Затем уже смаршрутизированный трафик посылается с этого же физического интерфейса с меткой VLAN, соответствующей VLAN назначения.

Подынтерфейсы — это программные виртуальные интерфейсы, связанные с одним физическим интерфейсом. Подынтерфейсы настраиваются в программном обеспечении маршрутизатора, и каждому подынтерфейсу назначаются IP-адрес и VLAN. Для облегчения логической маршрутизации подынтерфейсы настраиваются для различных подсетей, соответствующих назначенным им VLAN. После принятия решения о маршрутизации на основе сети назначения VLAN кадрам данных присваиваются метки VLAN, после чего они отправляются обратно на физический интерфейс.

На рисунке нажмите кнопку Воспроизведение, чтобы просмотреть анимацию, демонстрирующую функцию маршрутизации с использованием метода router-on-a-stick.

Как видно из анимации:

1. Компьютер PC1 в сети VLAN 10 обменивается данными с компьютером PC3 в сети VLAN 30 через маршрутизатор R1, используя один физический интерфейс маршрутизатора.

2. Компьютер PC1 отправляет одноадресный трафик на коммутатор S2.

3. Затем коммутатор S2 маркирует этот трафик как полученный из сети VLAN 10 и пересылает его через транк на коммутатор S1.

4. Коммутатор S1 пересылает помеченный трафик с транка на порту F0/5 на интерфейс маршрутизатора R1.

5. Маршрутизатор R1 принимает помеченный одноадресный трафик в сети VLAN 10 и направляет его в сеть VLAN 30 с помощью своих настроенных подынтерфейсов.

6. Одноадресному трафику присваивается метка VLAN 30 при отправке с интерфейса маршрутизатора на коммутатор S1.

7. Коммутатор S1 пересылает помеченный одноадресный трафик через транк на коммутатор S2.

8. Коммутатор S2 удаляет из одноадресного кадра метку сети VLAN и пересылает кадр на порт F0/6 компьютера PC3.

**Примечание**. Маршрутизация между VLAN с использованием метода router-on-a-stick не масштабируется при работе более 50 сетей VLAN.

# Маршрутизация между VLAN через многоуровневый коммутатор

Реализация маршрутизации между VLAN с использованием метода router-on-a-stick требует только одного физического интерфейса на маршрутизаторе и одного интерфейса на коммутаторе, что упрощает проведение кабелей для маршрутизатора. Однако в других реализациях маршрутизации между VLAN для этого не требуется дополнительно задействовать маршрутизатор.

Многоуровневые коммутаторы могут работать как на 2-м, так и на 3-м уровне, благодаря чему для выполнения базовой маршрутизации не требуется дополнительно задействовать маршрутизаторы. Многоуровневые коммутаторы поддерживают динамическую маршрутизацию и маршрутизацию между VLAN.

На рисунке нажмите кнопку «Воспроизведение», чтобы просмотреть анимацию, демонстрирующую маршрутизацию между VLAN с помощью коммутатора.

Как видно из анимации:

1. Компьютер PC1 в сети VLAN 10 обменивается данными с компьютером PC3 в сети VLAN 30 с помощью коммутатора S1, который использует интерфейсы VLAN, настроенные для каждой VLAN.

2. Компьютер PC1 отправляет одноадресный трафик на коммутатор S2.

3. Коммутатор S2, пересылая трафик через транк на коммутатор S1, маркирует его как принадлежащий VLAN 10.

4. Коммутатор S1 удаляет метки сети VLAN и пересылает одноадресный трафик на интерфейс сети VLAN 10.

5. Коммутатор S1 направляет одноадресный трафик на свой интерфейс сети VLAN 30.

6. Затем коммутатор S1 заново присваивает метки VLAN 30 одноадресному трафику и пересылает трафик из транкового канала на коммутатор S2.

7. Коммутатор S2 удаляет из одноадресного кадра метку сети VLAN и пересылает кадр на порт F0/6 компьютера PC3.

Чтобы многоуровневый коммутатор выполнял функции маршрутизации, на нём нужно включить функцию IP-маршрутизации.

Многоуровневая коммутация масштабируется лучше, чем любая другая реализация маршрутизации между VLAN. Это связано с тем, что маршрутизаторы оснащены ограниченным количеством портов для подключения к сетям. Кроме того, интерфейс, настроенный в качестве транка, имеет ограниченную пропускную способность.

При использовании многоуровнего коммутатора трафик маршрутизируется внутри коммутатора, и его не надо передавать по одному транку туда и обратно, чтобы перенести из одного VLAN в другой. Однако многоуровневый коммутатор не может выполнять все функции маршрутизатора. Маршрутизаторы поддерживают множество дополнительных функций, например позволяют реализовывать больше возможностей для обеспечения безопасности. Скорее, многоуровневый коммутатор можно рассматривать в качестве устройства 2-го уровня, в которое добавили некоторые возможности маршрутизации.

**Примечание**. В рамках этого курса настройка маршрутизации между VLAN на коммутаторе ограничивается настройкой статических маршрутов на коммутаторе 2960 — это единственная функция маршрутизации, поддерживаемая на коммутаторах 2960. Коммутатор 2960 поддерживает до шестнадцати статических маршрутов (включая маршруты, заданные пользователем, и маршрут по умолчанию) и любое количество напрямую подключенных маршрутов, а также маршрут по умолчанию для интерфейса управления. Полнофункциональные и относительно недорогие многоуровневые коммутаторы Cisco Catalyst серии 3560 поддерживают протоколы маршрутизации EIGRP, OSPF и BGP.

# Настройка маршрутизации между VLAN с использованием устаревшего метода: подготовка

Для реализации устаревшего метода маршрутизации между VLAN маршрутизаторы должны иметь несколько физических интерфейсов. Для маршрутизации каждый физический интерфейс маршрутизатора должен быть подключён к отдельной VLAN. Кроме того, на каждом интерфейсе настраивается IP-адрес из той подсети, которая соответствует подключенной к нему VLAN. Благодаря настройке IP-адресов на физических интерфейсах, сетевые устройства, подключённые к каждой из VLAN, могут обмениваться данными с маршрутизатором с помощью физического интерфейса, подключённого к той же VLAN. В этой конфигурации сетевые устройства могут использовать маршрутизатор в качестве шлюза для доступа к устройствам, подключённым к другим VLAN.

В процессе отправки сообщения устройство-источник должно определить, находится ли адресат в локальной или же в удалённой сети. Для этого устройство сравнивает IP-адреса источника и назначения, применяя к ним маску подсети. Установив, что IP-адрес назначения находится в удалённой сети, устройство-источник должно определить, куда оно должно переслать пакет для достижения адреса назначения. Устройство-источник проверяет локальную таблицу маршрутизации, чтобы определить, куда следует отправить данные. Устройства используют свой шлюз по умолчанию в качестве адреса назначения на втором уровне для всего трафика, который должен покинуть локальную подсеть. Шлюз по умолчанию — это маршрут, который устройство использует, когда у него нет явно определённого маршрута до сети назначения. IP-адрес интерфейса маршрутизатора в локальной подсети работает в качестве шлюза по умолчанию для устройства-отправителя.

После того как устройство-источник определило, что пакет должен пройти через локальный интерфейс маршрутизатора в подключённой сети VLAN, оно отправляет ARP-запрос, чтобы определить МАС-адрес интерфейса локального маршрутизатора. После отправки маршрутизатором ARP-ответа устройству-источнику оно может использовать МАС-адрес маршрутизатора для формирования кадра перед его отправкой в сеть.

Поскольку в Ethernet-кадре в качестве MAC-адреса назначения указан адрес интерфейса маршрутизатора, коммутатор точно знает, на какой порт нужно отправить трафик, чтобы он достиг интерфейса маршрутизатора в данной VLAN. Когда маршрутизатор получает кадр, он удаляет МАС-адреса источника и назначения, чтобы проверить IP-адрес назначения пакета. Маршрутизатор сравнивает адрес назначения с записями в своей таблице маршрутизации, чтобы определить, куда ему следует переслать данные, чтобы они достигли своего пункта назначения. Если маршрутизатор определяет, что сеть назначения является локально подключённой сетью, как в случае с маршрутизацией между VLAN, маршрутизатор отправляет ARP-запрос с того интерфейса, который физически подключён к VLAN назначения. В ответ устройство назначения отправляет маршрутизатору свой МАС-адрес, который маршрутизатор впоследствии использует для формирования кадра. Затем маршрутизатор отправляет одноадресный трафик на коммутатор, который пересылает его на тот порт, к которому подключено устройство назначения.

На рисунке нажмите кнопку Воспроизведение, чтобы просмотреть выполнение маршрутизации между VLAN.

Несмотря на то что маршрутизация между VLAN происходит за несколько шагов, на самом деле обмен данными между двумя устройствами из разных VLAN через маршрутизатор занимает долю секунды.

# Настройка коммутатора при использовании устаревшего метода маршрутизации между VLAN

Настройку при использовании устаревшего метода маршрутизации между VLAN следует начинать с настройки коммутатора.

Как показано на рисунке, маршрутизатор R1 подключён к портам коммутатора F0/4 и F0/5, которые настроены для VLAN 10 и 30 соответственно.

Для создания сетей VLAN используйте команду режима глобальной конфигурации **vlan** *vlan\_id*. В этом примере сети VLAN 10 и 30 были созданы на коммутаторе S1.

После создания сетей VLAN порты коммутатора назначаются соответствующим VLAN. Для каждого интерфейса, к которому подключается маршрутизатор, из режима конфигурации интерфейса выполняется команда **switchport access vlan** *vlan\_id*.

В этом примере интерфейсы F0/4 и F0/11 были назначены сети VLAN 10 с помощью команды **switchport access vlan 10**. Таким же образом интерфейсы F0/5 и F0/6 на коммутаторе S1 были назначены сети VLAN 30.

Наконец, чтобы конфигурация не была потеряна после перезагрузки коммутатора, выполняется команда **copy running-config startup-config**. После этого текущая конфигурация сохраняется в загрузочную конфигурацию.

# Настройка интерфейса маршрутизатора при использовании устаревшего метода маршрутизации между VLAN

Следующим этапом является настройка маршрутизатора.

Интерфейсы маршрутизатора настраиваются аналогично тому, как интерфейсы VLAN настраиваются на коммутаторах. Чтобы настроить конкретный интерфейс, из режима глобальной конфигурации перейдите в режим конфигурации интерфейса.

Как показано на рис. 1, каждому интерфейсу присваивается IP-адрес с помощью команды **ip address** *ip\_address subnet\_mask* в режиме конфигурации интерфейса.

В данном примере интерфейс G0/0 настраивается с IP-адресом 172.17.10.1 и маской подсети 255.255.255.0 с помощью команды **ip address 172.17.10.1 255.255.255.0**.

Интерфейсы маршрутизатора отключены по умолчанию, поэтому перед использованием их нужно включить с помощью команды **no shutdown**. После выполнения команды режима конфигурации интерфейса **no shutdown** появляется уведомление о том, что состояние интерфейса изменилось на up (Вкл.). Это указывает на то, что интерфейс включён.

Процедуру включения следует повторить для всех интерфейсов маршрутизатора. Для осуществления маршрутизации каждый интерфейс маршрутизатора должен быть в своей подсети. В этом примере другой интерфейс маршрутизатора, G0/1, был настроен для использования IP-адреса 172.17.30.1, который находится в другой подсети, нежели интерфейс G0/0.

После назначения IP-адресов физическим интерфейсам и активации интерфейсов маршрутизатор готов для выполнения маршрутизации между VLAN.

Для просмотра таблицы маршрутизации используется команда **show ip route**.

На рис. 2 в таблице маршрутизации отображены два маршрута. Один маршрут ведёт к подсети 172.17.10.0, которая подключена к локальному интерфейсу G0/0. Другой маршрут ведёт к подсети 172.17.30.0, которая подключена к локальному интерфейсу G0/1. Маршрутизатор использует эту таблицу маршрутизации, чтобы определить, куда отправлять получаемый трафик. Например, если маршрутизатор получает на интерфейсе G0/0 пакет, который предназначен для узла из подсети 172.17.30.0, маршрутизатор определит, что для достижения узлов в подсети 172.17.30.0 ему нужно отправить пакет из интерфейса G0/1.

Обратите внимание на букву **С** слева от каждой из записей маршрутов для сетей VLAN. Данная буква указывает, что данный маршрут является локальным маршрутом для подключённого интерфейса, что также указано в записи маршрута. Используя выходные данные из этого примера, маршрутизатор пересылает из интерфейса G0/1 трафик, предназначенный для подсети 172.17.30.0.

# Лабораторная работа. Настройка маршрутизации между VLAN для каждого интерфейса

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

* Часть 1. Создание сети и настройка базовых параметров устройства
* Часть 2. Настройка VLAN и транков на коммутаторах
* Часть 3. Проверка работы транков, VLAN, маршрутизации и связи

[Лабораторная работа. Настройка маршрутизации между VLAN для каждого интерфейса](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/5.1.2.4%20Lab%20-%20Configuring%20Per-Interface%20Inter-VLAN%20Routing.pdf)

# Настройка конфигурации router-on-a-stick: подготовка

Устаревший метод маршрутизации между VLAN, использующий физические интерфейсы, имеет большие ограничения. Маршрутизаторы оснащены ограниченным количеством физических интерфейсов для подключения к разным VLAN. По мере возрастания количества VLAN в сети, требующих по одному физическому интерфейсу на каждую VLAN, количество свободных интерфейсов маршрутизатора быстро уменьшается. Именно поэтому в больших сетях часто используются транковые каналы и подынтерфейсы. Создание транка позволяет одному физическому интерфейсу маршрутизировать трафик между несколькими VLAN. Подобный метод маршрутизации называется router-on-a-stick. Его суть заключается в использовании виртуальных подынтерфейсов для преодоления ограничений в количестве интерфейсов маршрутизатора.

Подынтерфейсы — это программные виртуальные интерфейсы, назначаемые физическим интерфейсам. Каждому подынтерфейсу назначается уникальный IP-адрес и маска подсети. Это позволяет одному физическому интерфейсу работать одновременно в нескольких логических сетях.

При настройке маршрутизации между VLAN с использованием метода router-on-a-stick физический интерфейс маршрутизатора должен быть подключен к транковому каналу смежного коммутатора. На маршрутизаторе подынтерфейсы создаются для каждой отдельной сети VLAN. Каждому подынтерфейсу назначается IP-адрес в соответствии с его подсетью или сетью VLAN. Кроме того, на подынтерфейсах настраивается, метку какой сети VLAN они будут присваивать кадрам. Таким образом, маршрутизатор может отделять трафик из каждого подынтерфейса по мере его прохождения по транковому каналу обратно в коммутатор.

С функциональной точки зрения, метод router-on-a-stick мало чем отличается от работы маршрутизации между VLAN по устаревшему методу. Отличие заключается в том, что при использовании метода router-on-a-stick вместо физических интерфейсов используются подынтерфейсы одного физического интерфейса.

На рисунке компьютер PC1 планирует обмен данными с компьютером PC3. PC1 находится в сети VLAN 10, а PC3 — в сети VLAN 30. Для обмена данными между PC1 и PC3 данные компьютера PC1 должны быть направлены через маршрутизатор R1 с помощью подынтерфейсов.

На рисунке нажмите кнопку Воспроизведение, чтобы увидеть, каким образом подынтерфейсы используются для маршрутизации данных между VLAN. Когда анимация остановится, прочитайте текст, расположенный слева от схемы топологии. Затем продолжите просмотр анимации, снова нажав Воспроизведение.

Использование транковых каналов и подынтерфейсов снижает количество используемых портов маршрутизаторов и коммутаторов. Это позволяет не только сэкономить финансовые средства, но и упростить процесс настройки. В результате возможности подынтерфейсов маршрутизатора позволяют использовать гораздо большее количество сетей VLAN, чем при конфигурации с одним физическим интерфейсом на каждую VLAN.

# Маршрутизация с методом Router-on-a-Stick: настройка коммутатора

Для того чтобы включить маршрутизацию между VLAN с использованием метода router-on-a-stick, необходимо активировать транковую связь на порте коммутатора, подключённом к маршрутизатору.

На этом рисунке маршрутизатор R1 подключён к коммутатору S1 через транковый порт F0/5. На коммутаторе S1 добавляются VLAN 10 и 30.

Поскольку порт коммутатора F0/5 настроен в качестве транкового порта, он не требует назначения какой-либо сети VLAN. Для того чтобы настроить порт коммутатора F0/5 в качестве транкового порта, выполните команду **switchport mode trunk** в режиме конфигурации интерфейса для порта F0/5.

**Примечание**. Маршрутизатор не поддерживает протокол динамического создания транкового канала (DTP), который используется коммутаторами, поэтому команды **switchport mode dynamic auto** или **switchport mode dynamic desirable** использовать нельзя.

Теперь маршрутизатор можно настроить для выполнения маршрутизации между VLAN.

# Метод router-on-a-stick: настройка подынтерфейса маршрутизатора

Процедура настройки маршрутизатора отличается при использовании метода router-on-a-stick и устаревшего метода маршрутизации между VLAN. На рисунке показано, что настраивается несколько подынтерфейсов.

Каждый подынтерфейс создаётся с помощью команды режима глобальной конфигурации **interface** *interface\_id subinterface\_id*. Синтаксис для подынтерфейсов таков: сначала указывается физический интерфейс, в данном случае **g0/0**, затем точка и номер подынтерфейса. Номер подынтерфейса можно сделать любым, но чаще всего он соответствует номеру VLAN. В примере в качестве номеров подынтерфейсов используются **10** и **30**, чтобы было проще запомнить, в каких VLAN они находятся. Подынтерфейс GigabitEthernet0/0.10 создаётся с помощью команды режима глобальной конфигурации **interface g0/0.10**.

Перед назначением подынтерфейсу IP-адреса подынтерфейс необходимо настроить для работы в конкретной сети VLAN с помощью команды **encapsulation dot1q** *vlan\_id.* В данном примере подынтерфейс G0/0.10 назначен сети VLAN 10.

**Примечание**. Для настройки сети native VLAN стандарта IEEE 802.1Q к этой команде можно добавить ключевой параметр **native**. В рассматриваемом примере ключевое слово **native** не использовалось, чтобы в качестве native VLAN использовалась сеть VLAN 1 (настройка по умолчанию).

Далее следует назначить IP-адрес подынтерфейсу с помощью команды режима конфигурации подынтерфейса **ip address** *ip\_address subnet\_mask*. В данном примере подынтерфейсу G0/0.10 назначен IP-адрес 172.17.10.1 с помощью команды **ip address 172.17.10.1 255.255.255.0**.

Процедуру следует повторить для всех подынтерфейсов маршрутизатора, необходимых для маршрутизации между сетями VLAN, настроенными в сети. Для осуществления маршрутизации каждому подынтерфейсу маршрутизатора необходимо назначить IP-адрес в своей подсети. Например, другой подынтерфейс маршрутизатора, G0/0.30, был настроен для использования IP-адреса 172.17.30.1, который находится в другой подсети, нежели интерфейс G0/0.10.

После настройки подынтерфейсы нужно включить.

В отличие от физических интерфейсов, подынтерфейсы нельзя включить с помощью команды **no shutdown** на уровне режима конфигурации подынтерфейса программного обеспечения Cisco IOS. Ввод команды **no shutdown** на уровне подынтерфейса ни к чему не приведёт. Все настроенные подынтерфейсы активируются, когда физический интерфейс включается с помощью команды **no shutdown**. Соответственно, если отключить физический интерфейс, то все подынтерфейсы также отключаются. В этом примере команда **no shutdown** введена в режиме настройки для интерфейса G0/0, что приводит к включению всех настроенных подынтерфейсов.

Администратор может отключить отдельные подынтерфейсы с помощью команды **shutdown**.

# Метод router-on-a-stick: проверка подынтерфейсов

По умолчанию маршрутизаторы Cisco настроены для маршрутизации трафика между локальными подынтерфейсами. В связи с этим функцию маршрутизации не нужно активировать индивидуально.

На рис. 1 команда **show vlans** служит для вывода информации о подынтерфейсах с VLAN в Cisco IOS. В выходных данных ниже отображается информация о двух подынтерфейсах с VLAN: GigabitEthernet0/0.10 и GigabitEthernet0/0.30.

Далее просмотрите таблицу маршрутизации с помощью команды **show ip route** (рис. 2). Указанные в таблице маршруты связаны с определёнными подынтерфейсами, а не отдельными физическими интерфейсами. Таблица маршрутизации содержит два маршрута. Один маршрут ведёт к подсети 172.17.10.0, которая подключена к локальному подынтерфейсу G0/0.10. Другой маршрут ведёт к подсети 172.17.30.0, которая подключена к локальному подынтерфейсу G0/0.30. Маршрутизатор использует эту таблицу маршрутизации, чтобы определить, куда отправлять получаемый трафик. Например, если на подынтерфейсе G0/0.10 маршрутизатор получил пакет, предназначенный для подсети 172.17.30.0, маршрутизатор определит, что для достижения узлов в сети 172.17.30.0 ему нужно отправить пакет из подынтерфейса G0/0.30.

На рис. 3 используйте инструмент проверки синтаксиса, чтобы настроить и проверить метод router-on-a-stick на маршрутизаторе R1.

# Метод router-on-a-stick: проверка маршрутизации

Следующий шаг после настройки маршрутизатора и коммутатора для маршрутизации между VLAN — проверка соединения между узлами. Возможность доступа к устройствам в удалённых VLAN можно протестировать с помощью команды **ping**.

В примере, показанном на рисунке, от компьютера PC1 к адресу назначения компьютера PC3 выполняются команды **ping** и **tracert**.

**Проверка эхо-запросов**

Команда **ping** отправляет эхо-запрос протокола ICMP на адрес назначения. Когда узел получает эхо-запрос ICMP, он отправляет эхо-ответ ICMP, чтобы подтвердить получение эхо-запроса ICMP. Команда **ping** вычисляет время, которое прошло между отправкой эхо-запроса и получением эхо-ответа. Полученное значение используется для определения задержки соединения. Успешное получение ответа подтверждает наличие пути между устройством-отправителем и принимающим устройством.

**Проверка маршрута командой tracert**

Команда tracert — это полезный инструмент для подтверждения существования пути между двумя устройствами. В системах UNIX подобная команда называется **traceroute**. Tracert также использует протокол ICMP для определения используемого пути, но при этом используются эхо-запросы ICMP со значениями предписанного времени жизни, определяемыми в кадре.

Значение времени жизни определяет точное количество переходов до маршрутизатора, которое может выполнить эхо-запрос ICMP. Первый эхо-запрос ICMP отправляется с таким значением времени жизни (TTL), чтобы оно закончилось на первом маршрутизаторе по пути к устройству назначения.

Когда время жизни ICMP эхо-запроса истекает, от маршрутизатора на устройство-источник отправляется ICMP-сообщение. Устройство записывает ответ от маршрутизатора и отправляет другой эхо-запрос ICMP, однако с увеличенным значением времени жизни. Это позволяет эхо-запросу ICMP пройти первый маршрутизатор и достичь второго устройства на пути до устройства назначения. Далее эта процедура повторяется рекурсивно, пока эхо-запрос ICMP не пройдёт весь путь до устройства назначения. После выполнения команды **tracert** отображается список входящих интерфейсов маршрутизатора, до которых эхо-запрос ICMP достиг по пути до пункта назначения.

В примере операция **ping** смогла отправить эхо-запрос ICMP на IP-адрес компьютера PC3. Кроме того, команда **tracert** подтверждает, что путь до компьютера PC3 проходит через IP-адрес подынтерфейса 172.17.10.1 маршрутизатора R1.

# Packet Tracer. Настройка маршрутизации между VLAN с использованием метода router-on-a-stick

В данном упражнении необходимо предварительно проверить подключения, чтобы приступить к реализации маршрутизации между VLAN. Далее вам предстоит настроить сети VLAN и маршрутизацию между VLAN. В завершение необходимо активировать транковую связь и проверить соединение между сетями VLAN.

[Packet Tracer. Настройка маршрутизации между VLAN с использованием метода router-on-a-stick. Инструкции](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/5.1.3.6%20Packet%20Tracer%20-%20Configuring%20Router-on-a-Stick%20Inter-VLAN%20Routing%20Instructions.pdf)

[Packet Tracer. Настройка маршрутизации между VLAN с использованием метода router-on-a-stick. РКА](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/5.1.3.6%20Packet%20Tracer%20-%20Configuring%20Router-on-a-Stick%20Inter-VLAN%20Routing.pka)

**Лабораторная работа. Настройка маршрутизации между VLAN на основе стандарта 801.2Q и транкового канала**

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

* Часть 1. Создание сети и базовая настройка устройств
* Часть 2. Настройка VLAN и транков на коммутаторах
* Часть 3. Настройка маршрутизации между VLAN с помощью транкового канала

[Лабораторная работа. Настройка маршрутизации между VLAN на основе стандарта 802.1Q и транкового канала](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/5.1.3.7%20Lab%20-%20Configuring%20802.1Q%20Trunk-Based%20Inter-VLAN%20Routing.pdf)

# Неполадки в работе порта коммутатора

Существует несколько распространённых ошибок в конфигурации коммутатора, которые могут возникнуть при настройке маршрутизации между несколькими VLAN.

При реализации маршрутизации между VLAN устаревшим методом убедитесь, что порты коммутатора, подключённые к интерфейсам маршрутизатора, настроены с соответствующими VLAN. Если порт коммутатора настроен для неверной VLAN, то устройства, настроенные в этой VLAN, не смогут подключиться к интерфейсу маршрутизатора; таким образом, эти устройства не смогут отправлять данные в другие VLAN.

Как показано в топологии на рис. 1, компьютер PC1 и интерфейс G0/0 маршрутизатора R1 настроены для одной и той же логической подсети, как видно из назначенных им IP-адресов. Однако порт коммутатора F0/4, подключённый к интерфейсу G0/0 маршрутизатора R1, не был настроен и остаётся в сети VLAN по умолчанию. Поскольку маршрутизатор R1 находится в другой сети VLAN, нежели компьютер PC1, они не могут обмениваться данными.

Для того чтобы исправить эту проблему, на порте F0/4 коммутатора S1 выполните команду режима глобальной конфигурации **switchport access vlan 10**. Когда порт коммутатора настроен для верной сети VLAN, компьютер PC1 может обмениваться данными с интерфейсом G0/0 маршрутизатора R1, который обеспечивает доступ к другим VLAN, подключённым к маршрутизатору R1.

В топологии на рис. 2 показана модель маршрутизации с использованием метода router-on-a-stick. Однако интерфейс F0/5 коммутатора S1 не настроен в качестве транкового канала и остаётся в сети VLAN по умолчанию для порта. В результате маршрутизатор не может передавать данные между VLAN, поскольку каждый из настроенных подынтерфейсов не может отправлять или принимать трафик с метками VLAN.

Для того чтобы исправить эту проблему, на порте F0/5 коммутатора S1 выполните команду режима глобального интерфейса **switchport mode trunk**. Это позволяет преобразовать интерфейс в транковый порт, благодаря чему между маршрутизатором R1 и коммутатором S1 устанавливается транковый канал. После успешной установки транкового канала устройства, подключённые к каждой из VLAN, могут обмениваться данными с подынтерфейсом, назначенным их VLAN, что делает возможной маршрутизацию между VLAN.

В топологии на рис. 3 показано, что транковый канал между коммутаторами S1 и S2 не работает. Поскольку между устройствами нет резервного соединения или пути, все устройства, подключённые к коммутатору S2, не могут получить доступ к маршрутизатору R1. В результате все устройства, подключённые к коммутатору S2, не могут направлять данные в другие VLAN через маршрутизатор R1.

Для того чтобы снизить вероятность нарушения маршрутизации между VLAN из-за плохой работы канала между коммутаторами, в сетевое проектирование необходимо включить резервные каналы и альтернативные пути.

# Проверка конфигурации коммутатора

В настройках коммутатора могут присутствовать проблемы, поэтому рекомендуется использовать специальные команды для проверки конфигурации и определения неполадок.

В выходных данных на рис. 1 показаны результаты выполнения команды **show interfaces** *interface-id* **switchport**. Предположим, что команды были выполнены из соображений, что сеть VLAN 10 не была назначена порту F0/4 коммутатора S1. Из верхней выделенной области видно, что порт F0/4 коммутатора S1 находится в режиме доступа, но нет данных о том, был ли он напрямую назначен сети VLAN 10. Данные в нижней выделенной области подтверждают, что порт F0/4 по-прежнему настроен для сети VLAN по умолчанию. Для того чтобы определить назначение VLAN и выявить неполадки в конфигурации порта, рекомендуется выполнить команды **show running-config** и **show interfaces** *interface-id* **switchport**.

На рис. 2 показано, что после изменения настроек обмен данными между маршрутизатором R1 и коммутатором S1 приостановился. Канал между маршрутизатором и коммутатором должен быть транковым. На экране выходных данных показаны результаты выполнения команд **show interfaces** *interface\_id* **switchport** и **show running-config**. Данные в верхней выделенной области свидетельствуют о том, что порт F0/4 на коммутаторе S1 находится в режиме доступа, а не в режиме транка. Данными в нижней выделенной области также подтверждается, что порт F0/4 настроен на работу в режиме доступа.

# Неполадки в работе интерфейса

Одной из самых распространённых ошибок при включении маршрутизации между VLAN на маршрутизаторе является подключение физического интерфейса маршрутизатора к неверному порту коммутатора. В результате этой ошибки интерфейс маршрутизатора оказывается в неверной сети VLAN и не может получить доступ к другим устройствам в той же сети.

Как показано на рисунке, интерфейс G0/0 маршрутизатора R1 подключён к порту F0/9 коммутатора S1. Порт коммутатора F0/9 настроен для сети VLAN по умолчанию, а не для сети VLAN 10. Из-за этого компьютер PC1 не может обмениваться данными с интерфейсом маршрутизатора и, как следствие, направлять данные в сеть VLAN 30.

Для того чтобы исправить данную ошибку, требуется физическое подключение интерфейса G0/0 маршрутизатора R1 к порту F0/4 коммутатора S1. Благодаря внесённым корректировкам интерфейс маршрутизатора окажется в верной VLAN, что сделает маршрутизацию между VLAN возможной. Кроме того, нужно назначить порт коммутатора F0/9 сети VLAN 10. Это решение также позволит компьютеру PC1 обмениваться данными с интерфейсом G0/0 маршрутизатора R1.

# Проверка настроек маршрутизатора

Основная проблема с методом router-on-a-stick заключается в неверном назначении подынтерфейсу идентификатора VLAN.

Как показано на рис. 1, маршрутизатор R1 был настроен с неверной сетью VLAN на подынтерфейсе G0/0.10, из-за чего устройства, настроенные в сети VLAN 10, не могут обмениваться данными с подынтерфейсом G0/0.10. Вследствие этого устройства не могут отправлять данные другим VLAN, находящимся в сети.

Как показано на рисунке, для решения подобной проблемы следует использовать команды **show interfaces** и **show running-config**.

На рис. 2 команда **show interfaces** выводит большой объём выходных данных, что усложняет определение проблемы. Однако в верхней выделенной области видно, что подынтерфейс G0/0.10 на маршрутизаторе R1 использует VLAN 100.

Команда **show running-config** подтверждает, что подынтерфейс G0/0.10 на маршрутизаторе R1 разрешает доступ для трафика сети VLAN 100, но не сети VLAN 10.

Для того чтобы исправить эту проблему, следует настроить подынтерфейс G0/0.10, чтобы он входил в нужную (правильную) VLAN, используя команду режима конфигурации подынтерфейса **encapsulation dot1q 10**. При назначении подынтерфейса верной сети VLAN он становится доступным для устройств в этой VLAN, а маршрутизатор может осуществлять маршрутизацию между VLAN.

При проведении тщательной проверки специалист может быстро найти неполадки в конфигурации маршрутизатора и наладить работу маршрутизации между VLAN.

**Ошибки в IP-адресах и масках подсети**

Сети VLAN соответствуют уникальным подсетям в сети. Для работы маршрутизации между VLAN маршрутизатор должен быть подключён ко всем VLAN через физические интерфейсы или подынтерфейсы. Каждому интерфейсу или подынтерфейсу необходимо назначить IP-адрес, соответствующий подсети, к которой он подключён. Это позволяет устройствам в сети VLAN обмениваться данными с интерфейсом маршрутизатора и осуществлять маршрутизацию трафика в другие VLAN, подключённые к маршрутизатору.

Приведём список распространённых ошибок в IP-адресации:

* Как показано на рис. 1, маршрутизатор R1 был настроен с неверным IP-адресом на интерфейсе G0/0. Из-за этого компьютер PC1 не может обмениваться данными с маршрутизатором R1 в VLAN 10. Чтобы устранить эту проблему, интерфейсу G0/0 маршрутизатора R1 следует назначить верный IP-адрес с помощью команды **ip address 172.17.10.1 255.255.255.0**. После назначения интерфейсу маршрутизатора верного IP-адреса компьютер PC1 может использовать интерфейс маршрутизатора в качестве шлюза по умолчанию для доступа к другим VLAN.
* На рис. 2 компьютер PC1 был настроен с неверным IP-адресом для подсети, связанной с сетью VLAN 10. Из-за этого компьютер PC1 не может обмениваться данными с маршрутизатором R1 в VLAN 10. Чтобы устранить эту проблему, компьютеру PC1 следует назначить верный IP-адрес. Детали конфигурации могут отличаться в зависимости от типа используемого ПК.
* На рис. 3 компьютер PC1 был настроен с неверной маской подсети. В соответствии с маской подсети, настроенной для компьютера PC1, он находится в сети 172.17.0.0. В результате компьютер PC1 вычисляет, что компьютер PC3 с IP-адресом 172.17.30.23 находится в той же подсети, что и PC1. Компьютер PC1 не пересылает трафик, предназначенный для PC3, на интерфейс G0/0 маршрутизатора R1. Поэтому трафик никогда не достигнет компьютера PC3. Чтобы исправить эту проблему, следует изменить маску подсети компьютера PC1 на 255.255.255.0. Детали конфигурации могут отличаться в зависимости от типа используемого ПК.

# Ошибки при настройке IP-адреса и маски подсети

Каждому интерфейсу или подынтерфейсу необходимо назначить IP-адрес, соответствующий подсети, к которой он подключён. Одной из распространённых ошибок является неверная настройка IP-адреса для подынтерфейса. На рис. 1 показаны выходные данные команды **show running-config**. В выделенной области показано, что подынтерфейс G0/0.10 на маршрутизаторе R1 имеет IP-адрес 172.17.20.1. Сеть VLAN для этого подынтерфейса должна поддерживать трафик сети VLAN 10. Параметры IP-адреса были настроены неверно. В этом следует применить команду **show ip interface**. Во второй выделенной области показан неверный IP-адрес.

Нередкими являются случаи, когда неправильно настроено именно устройство конечного пользователя, например ПК. На рис. 2 показаны параметры IP-конфигурации компьютера PC1. IP-адрес равен 172.17.20.21, а маска подсети — 255.255.255.0. Однако в данном сценарии компьютер PC1 должен находиться в сети VLAN 10 с адресом 172.17.10.21 и маской подсети 255.255.255.0.

**Примечание**. Настройка идентификаторов подынтерфейсов таким образом, чтобы они совпадали с номером VLAN, облегчает управление конфигурацией маршрутизации между VLAN, но не является обязательным условием. При поиске и устранении неполадок в адресации убедитесь, что подынтерфейс настроен с верным адресом для этой VLAN.

# Packet Tracer. Поиск и устранение неполадок маршрутизации между VLAN

В этом упражнении необходимо найти и устранить неполадки подключения, вызванные неверной конфигурацией VLAN и маршрутизации между VLAN.

[Packet Tracer. Поиск и устранение неполадок маршрутизации между VLAN. Инструкции](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/5.2.2.4%20Packet%20Tracer%20-%20Troubleshooting%20Inter-VLAN%20Routing%20Instructions.pdf)

[Packet Tracer. Поиск и устранение неполадок маршрутизации между VLAN. PKA](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/5.2.2.4%20Packet%20Tracer%20-%20Troubleshooting%20Inter-VLAN%20Routing.pka)

**Введение в основы коммутации 3-го уровня**

Реализация метода router-on-a-stick не представляет сложности, поскольку маршрутизаторы доступны практически в каждой сети. Как показано на рисунке, в большинстве корпоративных сетей используются многоуровневые коммутаторы, обеспечивающие высокую скорость обработки пакетов с помощью аппаратной коммутации. Как правило, полоса пропускания коммутаторов 3-го уровня позволяет передавать миллионы пакетов в секунду (pps), в то время как стандартные маршрутизаторы поддерживают скорость коммутации от 100 тысяч до 1 миллиона пакетов в секунду.

Все многоуровневые коммутаторы Catalyst поддерживают следующие типы интерфейсов 3-го уровня:

* **Маршрутизируемый порт** — простой интерфейс 3-го уровня, аналогичный физическому интерфейсу на маршрутизаторе Cisco IOS.
* **Виртуальный интерфейс коммутатора (SVI)** — виртуальный интерфейс сети VLAN для маршрутизации между VLAN. Другими словами, интерфейсы SVI — это виртуально маршрутизируемые интерфейсы VLAN.

Высокопроизводительные коммутаторы, например Catalyst 6500 и Catalyst 4500, выполняют практически любые функции, начиная с 3-го уровня модели OSI и выше, используя аппаратную коммутацию на основе Cisco Express Forwarding.

Все коммутаторы Cisco Catalyst 3-го уровня поддерживают протоколы маршрутизации, но некоторые модели коммутаторов Cisco Catalyst требуют ПО с расширенными возможностями для активации отдельных функций и протоколов маршрутизации. Коммутаторы серии Catalyst 2960 под управлением IOS 12.2(55) или более поздней версии поддерживают статическую маршрутизацию.

На коммутаторах Catalyst могут быть различные настройки по умолчанию для интерфейсов. Все модели коммутаторов семейств Catalyst 3560 и 4500 по умолчанию используют интерфейсы 2-го уровня. Все коммутаторы семейства Catalyst 6500 под управлением Cisco IOS по умолчанию используют интерфейсы 3-го уровня. Настройки интерфейса по умолчанию не отображаются в текущей или загрузочной конфигурации. В зависимости от используемой модели коммутатора семейства Catalyst, в файлах текущей или загрузочной конфигурации могут присутствовать команды **switchport** или **no switchport**.

# Маршрутизация между VLAN через виртуальные интерфейсы коммутатора

На первых порах развития коммутационных сетей коммутация была быстрой (часто не отставала от скорости работы аппаратного оборудования, т. е. скорость совпадала со временем, которое требовалось для получения и пересылки кадров в другие порты), а маршрутизация была медленной (маршрутизации была реализована программно). Поэтому проектировщики сетей старались сделать максимально большой коммутируемую часть сети. Уровни доступа, распределения и ядра часто настраивались для обмена данными на 2-м уровне. Это создавало проблемы с возникновением циклов. Для решения этой проблемы и предотвращения циклов использовался протокол STP, что позволяло сохранить гибкость и возможность добавления резервных соединений между коммутаторами.

Однако с развитием сетевых технологий маршрутизация стала быстрее и дешевле. Сегодня маршрутизация осуществляется на скорости аппаратного обеспечения. Следствием подобной эволюции стала возможность перехода маршрутизации на уровни ядра и распределения без негативного воздействия на производительность сети.

Многие пользователи находятся в отдельных VLAN, а каждая сеть VLAN, как правило, является отдельной подсетью. В связи с этим, логично настраивать коммутаторы распределения в качестве шлюзов 3-го уровня для пользователей каждой VLAN на коммутаторе доступа. Это означает, что каждый коммутатор распределения должен содержать IP-адреса, соответствующие каждой сети VLAN на коммутаторе доступа.

Между уровнями ядра и распределения, как правило, используются порты 3-го уровня (маршрутизируемые).

Данная сетевая архитектура не зависит от работы STP, поскольку у той части топологии, которая использует 2-й уровень, нет физических петель.

**Маршрутизация между VLAN через виртуальные интерфейсы коммутаторов (продолжение)**

Как показано на рисунке, SVI — это виртуальный интерфейс, настраиваемый в многоуровневом коммутаторе. Интерфейс SVI можно создать для любой сети VLAN, существующей на коммутаторе. Интерфейс SVI считается виртуальным, поскольку он не имеет выделенных физических портов. Он может выполнять те же функции для сети VLAN, что и интерфейс маршрутизатора. Кроме того, его можно настраивать практически так же, как интерфейс маршрутизатора (т.е. с IP-адресом, входящими и исходящими списками ACL и т.д.). Интерфейс SVI для сети VLAN обеспечивает обработку пакетов 3-го уровня по направлению к или из портов коммутатора, связанных с этой VLAN.

По умолчанию интерфейс SVI создаётся для сети VLAN по умолчанию (VLAN 10) для возможности удалённого управления коммутатором. Дополнительные интерфейсы SVI необходимо создавать отдельно. Интерфейсы SVI создаются при первом входе в режим конфигурации интерфейса сети VLAN для SVI конкретной VLAN, например, когда вводится команда **interface vlan 10**. Используемый номер сети VLAN соответствует метке VLAN, связанной с кадрами данных в инкапсулированном транке 802.1Q, или идентификатору VLAN (VID), настроенному для порта доступа. При создании интерфейса SVI в качестве шлюза для сети VLAN 10 присвойте интерфейсу SVI имя VLAN 10. Настройте и назначьте IP-адреса для каждого интерфейса SVI сети VLAN.

При создании интерфейса SVI убедитесь, что в базе данных VLAN существует данная сеть VLAN. На рисунке база данных VLAN коммутатора должна содержать сети VLAN 10 и VLAN 20. В противном случае интерфейс SVI останется выключенным.

Ниже приводится несколько причин необходимости настройки интерфейса SVI:

* Обеспечение шлюза для сети VLAN с целью маршрутизации трафика по направлению к или из этой VLAN
* Обеспечение на коммутаторе IP-соединения 3-го уровня
* Поддержка конфигураций протокола маршрутизации и режима моста

Далее приведены некоторые из преимуществ интерфейсов SVI (единственный недостаток заключается в высокой стоимости многоуровневых коммутаторов):

* Данный вид маршрутизации гораздо быстрее маршрутизации с использованием метода router-on-a-stick, поскольку процессы коммутации и маршрутизации осуществляются на базе аппаратных средств.
* Для маршрутизации не требуются внешние каналы от коммутатора к маршрутизатору.
* Нет ограничения в один канал. Для повышения пропускной способности между коммутаторами можно использовать каналы EtherChannel 2-го уровня.
* Задержки намного меньше, поскольку трафик обрабатывается внутри коммутатора.

**Маршрутизация между VLAN через маршрутизируемые порты**

**Маршрутизируемые порты и порты доступа на коммутаторе**

Маршрутизируемый порт является физическим портом, работающим аналогично интерфейсу маршрутизатора. В отличие от порта доступа маршрутизируемый порт не связан с определённой VLAN. Маршрутизируемый порт функционирует как обычный интерфейс маршрутизатора. Кроме того, поскольку функциональные возможности 2-го уровня были удалены, протоколы 2-го уровня, например STP, не действуют на маршрутизируемом интерфейсе. Однако на 3-м уровне работают такие протоколы, как EtherChannel и LACP (протокол управления агрегацией канала).

В отличие от маршрутизаторов Cisco IOS, маршрутизируемые порты на коммутаторе Cisco IOS не поддерживают подынтерфейсы.

Маршрутизируемые порты используются для соединений типа «точка-точка» (p2p). Маршрутизируемые порты могут также использоваться для подключения маршрутизаторов глобальной сети и устройств безопасности. В коммутируемой сети маршрутизируемые порты в основном устанавливаются между коммутаторами на уровнях ядра и распределения. На рисунке показаны примеры маршрутизируемых портов в коммутируемой сети кампусного типа.

Для настройки маршрутизируемых портов используйте команду конфигурации интерфейса **no switchport** на соответствующих портах. Например, по умолчанию на коммутаторах Catalyst 3560 интерфейсы настроены как интерфейсы 2-го уровня, поэтому их необходимо вручную настроить в качестве маршрутизируемых портов. Кроме того, для них необходимо назначить IP-адрес и другие параметры 3-го уровня. После назначения IP-адреса убедитесь, что IP-маршрутизация включена глобально и настроены соответствующие протоколы маршрутизации.

Ниже приводятся некоторые преимущества маршрутизируемых портов:

* В одном многоуровневом коммутаторе могут функционировать как интерфейс SVI, так и маршрутизируемые порты.
* Многоуровневые коммутаторы пересылают трафик 2-го или 3-го уровня, способствуя более быстрой маршрутизации.

**Примечание**. Маршрутизируемые порты не поддерживаются на коммутаторах серии Catalyst 2960.

# Настройка статических маршрутов на коммутаторе Catalyst 2960

Коммутатор Catalyst 2960 может функционировать в качестве устройства 3-го уровня и маршрутизировать данные между сетями VLAN и ограниченным количеством статических маршрутов.

Диспетчер базы данных коммутатора Cisco (Switch Database Manager, SDM) содержит несколько шаблонов для коммутатора 2960. Шаблоны можно применять для выполнения определённых функций в зависимости от того, как коммутатор используется в сети. Например, шаблон SDM lanbase-routing можно включить, чтобы разрешить коммутатору маршрутизировать данные между сетями VLAN, а также разрешить поддержку статической маршрутизации.

На рис. 1 команда **show sdm prefer** введена на коммутаторе S1, применён шаблон по умолчанию. Шаблон по умолчанию — это заводская настройка по умолчанию для коммутатора Catalyst 2960. Шаблон по умолчанию не поддерживает статическую маршрутизацию. При включённой IPv6-адресации шаблоном по умолчанию будет dual-ipv4-and-ipv6.

Используемый шаблон SDM можно изменить в режиме глобальной конфигурации с помощью команды **sdm prefer**.

**Примечание**. На рис. 2, 4, 6 и 7 используется команда **do** для выполнения команд пользовательского и привилегированных режимов из других режимов конфигурации маршрутизатора.

На рис. 2 параметры шаблона SDM отображаются с помощью команды **sdm prefer ?** . Используемый шаблон SDM изменён на шаблон lanbase-routing. Для того чтобы новый шаблон начал работать, коммутатор необходимо перезагрузить.

На рис. 3 шаблон lanbase-routing используется на коммутаторе S1. С этим шаблоном статическая маршрутизация поддерживается для 750 статических маршрутов.

На рис. 4 интерфейс F0/6 на коммутаторе S1 назначен сети VLAN 2. Интерфейсы SVI для VLAN 1 и 2 настроены с IP-адресами 192.168.1.1/24 и 192.168.2.1/24 соответственно. IP-маршрутизация активируется с помощью команды режима глобальной конфигурации **ip routing**.

**Примечание**. Команда **ip routing** автоматически включена на маршрутизаторах Cisco. Однако соответствующая команда для IPv6 **ipv6 unicast-routing** на маршрутизаторах и коммутаторах Cisco выключена по умолчанию.

На рис. 5 для маршрутизатора R1 настроены две IPv4-сети: IP-адрес интерфейса G0/1 равен 192.168.1.10/24, а IP-адрес loopback-интерфейса Lo0 равен 209.165.200.225/27. Выходные данные команды **show ip route** показаны на рисунке.

На рис. 6 на коммутаторе S1 настроен маршрут по умолчанию. Выходные данные команды **show ip route** показаны на рисунке.

На рис. 7 на маршрутизаторе R1 настроен статический маршрут до удалённой сети 192.168.2.0/24 (VLAN 2). Выходные данные команды **show ip route** показаны на рисунке.

На рис. 8 компьютер PC-A настроен с IP-адресом 192.168.2.2/24 в сети VLAN 2, а компьютер PC-B настроен с IP-адресом 192.168.1.2/24 в сети VLAN 1. Компьютер PC-B может отправить эхо-запрос как на компьютер PC-B, так и на интерфейс loopback маршрутизатора R1.

Для настройки статической маршрутизации на коммутаторе S1 используйте инструмент проверки синтаксиса на рис. 9.

**Неполадки в настройках коммутатора 3-го уровня**

Проблемы, которые часто встречаются при маршрутизации между VLAN с использованием устаревшего метода или метода router-on-a-stick, описываются в контексте коммутации уровня 3. Для устранения неполадок коммутации 3-го уровня следует проверить следующие пункты:

* **Сети VLAN** — VLAN должны быть определены для всех коммутаторов. Сети VLAN должны быть включены на транковых портах. Порты должны находиться в верных сетях VLAN.
* **Интерфейсы SVI** — интерфейс SVI должен быть настроен с правильным IP-адресом или маской подсети. Интерфейс SVI должен быть включён. Интерфейс SVI должен совпадать с номером сети VLAN.
* **Маршрутизация** — функция маршрутизации должна быть включена. Каждый интерфейс или сеть должны быть добавлены в протокол маршрутизации.
* **Узлы** — узлы должны иметь верные IP-адреса или маски подсети. Шлюзы по умолчанию узлов должны быть связаны с интерфейсом SVI или маршрутизируемым портом.

Для устранения неполадок в коммутации 3-го уровня необходимо хорошо знать принципы реализации и проектирования топологии.

**Пример устранения неполадок в коммутации 3-го уровня**

Компания АБВ добавляет в сеть новый этаж — пятый. В связи с этим необходимо наладить соединение между сотрудниками пятого этажа и остальными сотрудниками. В настоящее время сотрудники пятого этажа не могут обмениваться данными с сотрудниками других этажей. Далее представлен план реализации новой сети VLAN для сотрудников пятого этажа и настройки маршрутизации между новой VLAN и остальными сетями VLAN.

Реализация новой VLAN осуществляется в четыре шага:

**Шаг 1.** Создание новой VLAN с номером 500 на коммутаторе пятого этажа и коммутаторах распределения. Присвоение имени данной сети VLAN.

**Шаг 2.** Определение портов, необходимых для пользователей и коммутаторов. Настройка команды **switchport access vlan** с параметром **500** и проверка настроек транкового канала между коммутаторами и доступности сети VLAN 500 на транке.

**Шаг 3.** Создание интерфейса SVI на коммутаторах распределения и проверка назначения IP-адресов.

**Шаг 4.** Проверка связности.

План проверки включает в себя следующие пункты:

**Шаг 1.** Убедитесь, что все необходимые VLAN (были) созданы.

* Были ли сети VLAN созданы на всех коммутаторах?
* Данный тип проверки проводится с помощью команды **show vlan**.

**Шаг 2.** Необходимо убедиться, что порты находятся в верной сети VLAN, а транковая связь работает ожидаемым образом.

* Была ли команда **switchport access VLAN 500** добавлена на всех портах доступа?
* Нужно ли добавить какие-либо другие порты? Если да, то выполните соответствующие действия.
* Использовались ли эти порты ранее? Если да, то убедитесь, что на этих портах не были выполнены какие-либо дополнительные команды, которые могли повлечь за собой конфликты. Если нет, проверьте, включён ли порт.
* Настроены ли какие-либо пользовательские порты на транковых каналах? Если да, выполните команду **switchport mode access**.
* Настроены ли транковые порты в режиме транка?
* Настроено ли ручное отсечение VLAN? Если да, то убедитесь, что на транковых каналах, необходимых для передачи трафика сети VLAN 500, разрешён доступ VLAN.

**Шаг 3.** Проверка конфигурации интерфейса SVI (при необходимости):

* Создан ли интерфейс SVI с верным IP-адресом и маской подсети?
* Включён ли он?
* Включена ли функция маршрутизации?
* Добавлен ли интерфейс SVI в протокол маршрутизации?

**Шаг 4.** Проверка связности:

* Все ли каналы между коммутаторами находятся в режиме транковой связи?
* Разрешена ли сеть VLAN 500 на всех транковых каналах?
* Блокирует ли протокол STP какие-либо каналы?
* Включены ли порты?
* Назначены ли для узлов верные шлюзы по умолчанию?
* В случае необходимости убедитесь, что включён маршрут по умолчанию или какой-либо протокол маршрутизации.

**Лабораторная работа. Поиск и устранение неполадок маршрутизации между VLAN**

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

* Часть 1. Построение сети и загрузка конфигурации устройств
* Часть 2. Поиск и устранение неполадок в настройках маршрутизации между VLAN
* Часть 3: Проверка конфигурации сети VLAN, назначение портов и транковых каналов
* Часть 4. Проверка подключения 3-го уровня

[Лабораторная работа. Поиск и устранение неполадок маршрутизации между VLAN](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/5.3.2.4%20Lab%20-%20Troubleshooting%20Inter-VLAN%20Routing.pdf)

# Кратчайший путь

**Кратчайший путь**

Ваша компания только что приобрела 3-этажное здание. Вы являетесь сетевым администратором и должны разработать схему маршрутизации между VLAN для передачи данных между сотрудниками каждого этажа.

На первом этаже расположен отдел кадров, на втором — отдел ИТ, а третий этаж занимает отдел продаж. Все отделы должны иметь возможность обмениваться данными друг с другом, но в то же время иметь изолированные сети.

Для реализации сети в новом здании у вас есть три коммутатора Cisco 2960 и маршрутизатор Cisco 1941 из старого офиса. Приобретение дополнительного оборудования не рассматривается.

Для дальнейших инструкций см. файл PDF для этого упражнения.

[Работа в аудитории. Кратчайший путь. Инструкции](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/5.4.1.1%20The%20Inside%20Track%20Instructions.pdf)

# Packet Tracer. Отработка практических навыков

В рамках задания вам предстоит продемонстрировать и закрепить навыки реализации маршрутизации между VLAN, включая настройку IP-адресов, сетей VLAN, создание транковых каналов и подынтерфейсов.

[Packet Tracer. Отработка практических навыков. Инструкции](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/5.4.1.2%20Packet%20Tracer%20-%20Skills%20Integration%20Challenge%20Instructions.pdf)

[Packet Tracer. Отработка практических навыков. РКА](https://static-course-assets.s3.amazonaws.com/RSE503/ru/course/files/5.4.1.2%20Packet%20Tracer%20-%20Skills%20Integration%20Challenge.pka)

# Резюме

Маршрутизация между VLAN — это процесс маршрутизации трафика между сетями VLAN с использованием выделенного маршрутизатора или многоуровневого коммутатора. Маршрутизация между VLAN упрощает обмен данными между устройствами, изолированными границами VLAN.

Устаревший метод маршрутизации между VLAN обусловлен доступностью физического порта коммутатора для каждой настроенной VLAN. Данный метод был заменён на топологию router-on-a-stick, которая полагается на внешний маршрутизатор с подынтерфейсами, подключёнными через транковые каналы к коммутатору 2-го уровня. При использовании метода router-on-a-stick на каждом логическом подынтерфейсе необходимо настроить соответствующие IP-адреса и параметры VLAN. Необходимо настроить транк и инкапсуляцию на маршрутизаторе и на соответствующем порту коммутатора.

Другой способ реализации маршрутизации между VLAN — многоуровневая маршрутизация с использованием коммутации 3-го уровня. Коммутация 3-го уровня использует интерфейсы SVI и маршрутизируемые порты. Коммутация 3-го уровня обычно настраивается на уровне распределения и ядра. Коммутация 3-го уровня с интерфейсами SVI — это форма маршрутизации между VLAN. Маршрутизируемый порт является физическим портом, работающим аналогично интерфейсу маршрутизатора. В отличие от порта доступа маршрутизируемый порт не связан с определённой VLAN.

Коммутаторы Catalyst 2960 могут использоваться в многоуровневой маршрутизации VLAN. Эти коммутаторы поддерживают статическую маршрутизацию, но не поддерживают протоколы динамической маршрутизации. Шаблоны SDM требуются для включения IP-маршрутизации на коммутаторах 2960.

Для поиска и устранения неполадок маршрутизации между VLAN на маршрутизаторе и коммутаторе 3-го уровня используются аналогичные процедуры. В большинстве случаев ошибки возникают в конфигурациях сетей VLAN, транкового канала, интерфейса 3-го уровня и IP-адреса.