



МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«МИРЭА – Российский технологический университет»
РТУ МИРЭА

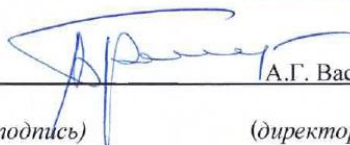
ЛЕКЦИОННЫЕ МАТЕРИАЛЫ

Основы сетевых технологий

| | |
|---------------------------|---|
| Уровень | <u>бакалавриат</u> |
| Форма обучения | <u>очная</u> |
| Направление подготовки | <u>11.03.02 Инфокоммуникационные технологии и системы связи</u> <u>«Инфокоммуникационные системы и сети»</u> |
| Институт | <u>Радиоэлектроники и информатики</u> |
| Кафедра | <u>Телекоммуникаций</u> |
| Лектор | <u>ст. преподаватель Тулинов С.В.</u> |

Используются в данной редакции с учебного года 2021/22

Проверено и согласовано «24» 03 2022г.


(подпись) А.Г. Васильев
(директор ИРИ)

Москва 2022

Оглавление

| | |
|---|-----|
| 1. Концепция коммутации..... | 3 |
| 2. Введение в коммутируемые сети..... | 16 |
| 3. Виртуальные локальные сети | 35 |
| 4. Концепция маршрутизации..... | 64 |
| 5. Принципы STP..... | 82 |
| 6. ETHERCHANNEL | 95 |
| 7. DHCPV4 | 106 |
| 8. SLAAC И DHCPV6 | 107 |
| 9. Основные понятия FHRP..... | 114 |
| 10. Принципы обеспечения безопасности сети..... | 118 |
| СПИСОК ЛИТЕРАТУРЫ..... | 123 |

1. Концепция коммутации

По мере развития и расширения предприятия возрастают и требования к сети. Решение критически важных задач тесно сопряжено с сетевой инфраструктурой предприятия. Отказы сети могут привести к сокращению прибыли и потере заказчиков. Разработчики сети должны спроектировать и реализовать корпоративную сеть с высоким уровнем масштабируемости и доступности.

В данной главе вы изучите стратегии, которые могут использоваться для системного проектирования многофункциональной сети (например иерархическая модель сети), корпоративную архитектуру Cisco (Cisco Enterprise Architecture) и рекомендации по выбору необходимых устройств. Архитектура сети предназначена для ограничения количества устройств, подверженных воздействию в случае сбоя отдельного устройства в сети, обеспечения плана и возможностей расширения, а также создания надежной бесперебойной сети.

Сеть по проекту

Ваш работодатель открывает новый филиал.

Вас перевели на новый объект в должности сетевого администратора. В ваши задачи входят проектирование и обслуживание сети нового филиала.

При проектировании сетей администраторы других филиалов использовали трехуровневую иерархическую модель Cisco. Вы решили использовать аналогичный метод.

Чтобы получить представление о преимуществах иерархической модели в рамках проектирования сети, вам необходимо изучить данную тему.

Организации все больше полагаются на свои сети, предоставляющие критически важные сервисы. По мере роста и развития предприятия, его штат увеличивается, открываются новые филиалы и компания расширяется на мировых рынках. Все эти изменения напрямую влияют на требования, предъявляемые к сети. Масштабная бизнес-среда, включающая большое количество пользователей, объектов и систем, называется корпорацией. Сеть, которая используется для поддержки деятельности корпорации, называется корпоративной.

Корпоративная сеть должна поддерживать обмен различными типами сетевого трафика, среди которых файлы данных, электронная почта, IP-телефония и видеоприложения, для нескольких отделов организации. Все корпоративные сети должны:

поддерживать работу критически важных приложений;

поддерживать трафик в объединенных сетях;

соответствовать различным требованиям бизнес-сектора;

обеспечивать возможность централизованного административного управления.

Корпоративные сети (как, например, на данном рисунке) должны работать 99,999% времени практически без сбоев. Нарушения в работе корпоративной сети препятствуют деятельности предприятия, что может привести к снижению дохода, потере заказчиков, данных и новых возможностей.

Для достижения оптимального уровня надёжности в корпоративных сетях часто устанавливают оборудование корпоративного класса. Оборудование корпоративного класса отвечает за передачу больших объемов сетевого трафика, поэтому оно проектируется и производится в соответствии с более высокими требованиями, чем устройства более низкого класса.

Оборудование корпоративного класса отличается надёжностью, которая обеспечивается благодаря дополнительным резервным источникам питания и возможностям переключения при отказе. Благодаря этим возможностям устройство переключается с неработающего модуля, сервиса или устройства на исправный компонент с незначительными перебоями в обслуживании или совсем без них.

Приобретение и установка оборудования корпоративного класса не означает, что сеть можно спроектировать неправильно.

Для оптимизации пропускной способности корпоративной сети необходимо организовать ее таким образом, чтобы обеспечить локализацию трафика и предотвратить его распространение в областях сети, где данный трафик не требуется. Для организации сети используется трехуровневая иерархическая модель.

Данная модель подразумевает разделение функций сети на три отдельных уровня.

Уровень доступа

Уровень распределения

Уровень ядра

Каждый уровень выполняет свои функции.

Уровень доступа обеспечивает возможность подключения пользователей. Уровень распределения используется для пересылки трафика из одной локальной сети в другую. И наконец, центральный уровень, уровень ядра, представляет собой высокоскоростную магистраль между распределенными сетями. Пользовательский трафик создается на уровне доступа и проходит через другие уровни, если для передачи необходимы функции этих уровней.

Хотя иерархическая модель имеет три уровня, некоторые небольшие корпоративные сети могут использовать и двухуровневую иерархическую модель. В двухуровневой иерархической модели уровни ядра и распределения сведены в единый уровень, что позволяет снизить затраты и упростить сеть ввиду меньшего количества устройств.

Корпоративная архитектура Cisco разделяет сети на функциональные компоненты, сохраняя уровни доступа, распределения и ядра. Как показано на рисунке, к основным модулям корпоративной архитектуры Cisco относятся:

Комплекс зданий предприятия

Границы предприятия

Границы поставщика услуг

Удаленный

Комплекс зданий предприятия

Модуль Enterprise Campus (Комплекс зданий предприятия) охватывает всю инфраструктуру комплекса (уровни доступа, распределения и ядра). Модуль уровня доступа содержит коммутаторы 2 и 3 уровней, обеспечивающие необходимую плотность портов. Здесь осуществляется реализация сетей VLAN и транковых каналов к уровню распределения. Важно предусмотреть избыточные каналы к коммутаторам уровня распределения здания. Модуль уровня распределения объединяет уровни доступа здания с помощью устройств 3 уровня. На этом уровне осуществляются маршрутизация, контроль доступа и работы службы QoS. Модуль уровня ядра обеспечивает высокоскоростное соединение между модулями уровня распределения, серверными фермами в ЦОД и границей корпорации. При проектировании данного модуля особое внимание уделяется резервным каналам, быстрой сходимости и отказоустойчивости.

Помимо этих модулей Enterprise Campus может включать другие подмодули, например:

Серверная ферма и центр обработки данных. Данная область обеспечивает возможность высокоскоростного подключения и защиту для

серверов. Критически важно обеспечить безопасность, избыточность и отказоустойчивость. Системы управления сетями отслеживают производительность с помощью специального устройства и доступности сети.

Сервисный модуль. Данная область обеспечивает доступ ко всем сервисам (например, службы IP-телефонии, беспроводной контроллер и объединенные сервисы).

Границы предприятия

Enterprise Edge (Граница корпорации) включает в себя модули для подключения к Интернету и сетям VPN и WAN, которые обеспечивают подключение предприятия к сети поставщика услуг. Данный модуль предоставляет корпоративные услуги на удаленные площадки и позволяет корпорации использовать Интернет и партнерские ресурсы. Он обеспечивает работу служб QoS, соблюдение политики, уровни обслуживания и безопасность.

Границы поставщика услуг

Модуль Service Provider Edge (Граница поставщика услуг) предоставляет службы для доступа к Интернету, коммутируемой телефонной сети (PSTN) и сети WAN.

Все входящие и исходящие данные в модели составной корпоративной сети (ECNM) проходят через пограничное устройство. На этом этапе система может проверить все пакеты и принять решение об их допуске в корпоративную сеть. Кроме того, на границе предприятия можно настроить системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS) для защиты от вредоносных действий.

Качественно спроектированная сеть не только контролирует трафик, но и ограничивает размер доменов возникновения ошибки. Домен сбоя представляет собой область сети, на которую влияют сбои в работе критически важного устройства или сетевой службы.

Назначение отказавшего устройства определяет характер и размер домена сбоя. Например, неисправный коммутатор в сетевом сегменте, как правило, воздействует только на узлы данного сегмента. Однако, если отказывает маршрутизатор, соединяющий сегмент с другими сегментами, степень воздействия будет гораздо выше.

Использование резервных каналов и надежных устройств корпоративного класса сводит к минимуму вероятность прерывания работы

сети. Небольшие домены, содержащие ошибки, уменьшают степень воздействия неполадок на работу компании. Кроме того, при этом также упрощается процесс поиска и устранения неполадок и снижается коэффициент простоя для всех пользователей.

Сокращение размера доменов сбоя

Поскольку сбой на уровне ядра сети может привести к серьезным последствиям, проектировщики сети нередко уделяют особое внимание предотвращению сбоев. Меры по предотвращению сбоев могут в значительной мере увеличить затраты на реализацию сети. Иерархическая модель архитектуры обеспечивает самый простой и дешевый метод контроля размера домена сбоя на уровне распределения. На уровне распределения можно ограничить ошибки сети областью меньшего размера, благодаря чему они будут затрагивать меньшее количество пользователей. При использовании устройств 3 уровня на уровне распределения каждый маршрутизатор выступает в качестве шлюза для ограниченного количества пользователей уровня доступа.

Развертывание блока коммутации

Маршрутизаторы или многоуровневые коммутаторы обычно развертываются парами, при этом коммутаторы уровня доступа распределяются между ними равномерно. Данная конфигурация называется блоком коммутации здания или отдела. Каждый блок коммутации функционирует независимо от других. Поэтому в случае отказа отдельного устройства сеть будет продолжать работать. Даже сбой всего блока коммутации отражается лишь на незначительном количестве конечных пользователей.

В целях поддержки корпоративной сети проектировщик сети должен разработать стратегию, обеспечивающую доступность сети и ее эффективное и простое масштабирование. Базовая стратегия проектирования сети включает в себя следующие рекомендации:

Следует использовать расширяемое модульное оборудование или кластерные устройства, которые можно легко модернизировать для увеличения их возможностей. Модули устройств можно добавить в существующее оборудование в целях поддержки новых функций и устройств без необходимости полного обновления оборудования. Некоторые устройства можно интегрировать в кластер, чтобы они работали как одно устройство. Это упрощает управление и настройку.

Иерархическую сеть следует проектировать с учетом возможностей добавления, обновления и изменения модулей в случае необходимости, не

затрагивая при этом схему других функциональных областей сети. Например, создание отдельного уровня доступа, который можно расширить, не затрагивает уровни распределения и ядра сети комплекса зданий.

Создайте иерархическую стратегию адресов IPv4 или IPv6. При тщательном планировании IPv4-адресов исключается необходимость повторной адресации сети для поддержки дополнительных пользователей и сервисов.

Выберите маршрутизаторы или многоуровневые коммутаторы, чтобы ограничить широковещательные рассылки и отфильтровать нежелательный трафик из сети. Используйте устройства 3 уровня для фильтрации и сокращения объема трафика к ядру сети.

Как показано на рисунке, к дополнительным требованиям в отношении проектирования сети относятся следующие:

- реализация избыточных каналов в сети между критически важными устройствами, а также между устройствами уровня доступа и уровня ядра;

- реализация нескольких каналов между различными устройствами с использованием функций агрегирования каналов (EtherChannel) или распределением нагрузки в соответствии с равной стоимостью в целях увеличения пропускной способности; объединение нескольких каналов Ethernet в единую конфигурацию EtherChannel с распределенной нагрузкой позволяет увеличить доступную пропускную способность; технологию EtherChannel можно использовать в том случае, если в связи с ограничениями бюджета невозможно приобрести высокоскоростные интерфейсы и оптоволоконные кабели;

- реализация беспроводного подключения для поддержки мобильности и расширения;

- использование масштабируемого протокола маршрутизации и реализация в этом протоколе маршрутизации функций, позволяющих изолировать обновления маршрутизации и минимизировать размер таблицы маршрутизации.

Реализация избыточности

Во многих компаниях обеспечение потребностей бизнеса во многом зависит от доступности сети. Избыточность является важной частью проектирования сети и позволяет предотвращать перебои в работе сетевых служб за счёт устранения единой точки отказа. Одним из способов реализации избыточности является установка запасного оборудования и обеспечение отказоустойчивых сервисов для критически важных устройств.

Другим способом реализации избыточности является использование избыточных путей, как показано на рисунке. Избыточные пути предоставляют альтернативные физические пути передачи данных по сети. Избыточные пути в коммутируемой сети поддерживают высокую доступность. Тем не менее, ввиду принципа работы коммутаторов резервные пути в коммутируемой сети Ethernet могут стать причиной возникновения логических петель 2 уровня. По этой причине требуется использование протокола spanning-tree (STP).

Протокол STP обеспечивает избыточность, необходимую для надёжности, и при этом устраняет логические петли. Это обеспечивается за счёт механизма отключения резервных путей в коммутируемой сети до тех пор, пока этот путь не потребуется (например, в случае сбоя). STP основывается на открытых стандартах и используется для создания логической топологии без петель коммутации.

Дополнительные сведения о резервировании сетей LAN и работе протокола STP представлены в главе «Избыточность LAN».

Реализация EtherChannel

В иерархической модели сети в некоторых каналах между коммутаторами доступа и коммутаторами распределения может потребоваться обработка большего объема трафика, чем в других каналах. Поскольку трафик из нескольких каналов объединяется в одном исходящем канале, такой канал может стать «узким местом». Агрегирование каналов позволяет администратору увеличить объем полосы пропускания между устройствами за счёт создания единого логического канала, состоящего из нескольких физических каналов. EtherChannel представляет собой метод агрегирования каналов, используемый в коммутируемых сетях, как показано на рисунке.

EtherChannel использует существующие порты коммутатора. Таким образом, исключены дополнительные затраты на модернизацию канала с помощью более скоростного и дорогостоящего подключения. EtherChannel можно рассматривать как единый логический канал, использующий интерфейс EtherChannel. Большинство задач конфигурации выполняется на интерфейсе EtherChannel, а не на отдельных портах. Это обеспечивает согласованную конфигурацию на всех каналах. Наконец, конфигурация EtherChannel использует преимущества распределения нагрузки между каналами, которые относятся к одному каналу EtherChannel. В зависимости от аппаратной платформы может применяться один или несколько методов распределения нагрузки.

Принцип работы и настройка EtherChannel подробно рассматриваются в главе «Агрегирование каналов».

Реализация беспроводного подключения

Сеть должна быть спроектирована таким образом, чтобы при необходимости доступ к сети мог расширяться для пользователей и устройств. Все более важное значение приобретает расширение возможностей подключения на уровне доступа посредством беспроводного подключения. Беспроводное подключение обладает множеством преимуществ, среди которых повышенная гибкость, снижение затрат и возможность роста и адаптации в соответствии с изменением требований сети и бизнеса.

Для беспроводного обмена данными оконечным устройствам требуется беспроводной сетевой адаптер со встроенным радиопередатчиком/радиоприемником, а также драйвер, необходимый для работы адаптера. Кроме того, для подключения пользователей требуется беспроводной маршрутизатор и точка беспроводного доступа (AP), как показано на рисунке.

При реализации беспроводной сети необходимо учитывать множество факторов, в том числе типы используемых беспроводных устройств, требования к зоне покрытия беспроводной сети, возможные помехи и требования безопасности.

Принцип действия и реализация беспроводного подключения подробно рассматриваются в главе «Беспроводные сети».

Управление маршрутизируемой сетью

Корпоративные сети и интернет-провайдеры часто используют более сложные протоколы, например протоколы маршрутизации по состоянию канала, поскольку они обладают иерархической структурой и предоставляют возможность масштабирования для больших сетей.

Протоколы маршрутизации по состоянию канала (например, протокол OSPF – алгоритм выбора кратчайшего пути), показанный на рис. 1, эффективен для больших иерархических сетей, где нужна быстрая сходимость. Маршрутизаторы OSPF устанавливают и поддерживают соседские отношения, или отношения смежности, с другими маршрутизаторами OSPF, подключенными к сети. При установлении маршрутизаторами отношений смежности с соседними маршрутизаторами начинается обмен обновлениями о состоянии каналов. Маршрутизаторы достигают состояния смежности FULL (полная смежность) после синхронизации данных в своих базах данных состояний каналов. При использовании протоколов OSPF обновления о состоянии каналов рассылаются при каких-либо изменениях в сети.

OSPF — это популярный протокол маршрутизации по состоянию каналов, который поддерживает точную настройку различными способами. В главе «Настройка и отладка OSPF для одной области» рассматриваются некоторые расширенные функции настройки, поиска и устранения неполадок в работе OSPF.

Кроме того, OSPF поддерживает двухуровневую иерархическую модель (или OSPF для нескольких областей), как показано на рис. 2. Все сети OSPF начинаются с области 0, также называемой магистральной областью. По мере расширения сети можно создавать другие области, не являющиеся магистральными. Все немагистральные области должны быть подключены к области 0 напрямую. В главе «OSPF для нескольких областей» демонстрируются преимущества, принцип работы и способы настройки OSPF для нескольких областей.

Другим распространенным протоколом маршрутизации для больших сетей является усовершенствованный протокол внутренней маршрутизации между шлюзами (EIGRP). Протокол EIGRP, разработанный компанией Cisco, является расширенным проприетарным (запатентованным) протоколом маршрутизации на базе векторов расстояния. Несмотря на простоту настройки, протокол EIGRP оснащен расширенным набором встроенных функций и параметров. Например, как показано на рис. 3, протокол EIGRP использует несколько таблиц для управления процессом маршрутизации. Он предлагает множество функциональных возможностей, ранее не доступных ни в одном другом протоколе маршрутизации. Данный протокол является оптимальным выбором для больших многопротокольных сетей, где используются в основном устройства Cisco.

В главе «EIGRP» описываются принцип работы и настройка протокола маршрутизации EIGRP. В главе «Конфигурации и устранение неполадок расширенного EIGRP» приводятся некоторые дополнительные параметры настройки EIGRP.

Команды проверки коммутатора

| Задача | Команды IOS |
|--|---|
| Отобразите состояние и конфигурацию интерфейса. | S1# show interfaces [interface-id] |
| Отобразите текущую загрузочную конфигурацию. | S1# show startup-config |
| Отобразите текущую конфигурацию. | S1# show running-config |
| Отобразите данные о файловой системе флеш-памяти. | S1# show flash |
| Отобразите состояние системного оборудования и программного обеспечения. | S1# show version |
| Отобразите историю введенных команд. | S1# show history |
| Отобразите данные IP для интерфейса. | S1# show ip interface [interface-id] ИЛИ S1# show ipv6 interface [interface-id] |
| Отобразите таблицу MAC-адресов. | S1# show mac-address-table ИЛИ S1# show mac address-table |

Проверка конфигурации портов коммутатора

Для проверки правильности настройки коммутатора можно использовать команду **show running-config**. Из выборки сокращенного вывода по S1 на рисунке показана некоторая важная информация:

Интерфейс Fast Ethernet 0/18 настроен с сетью управления VLAN 99.

VLAN 99 назначен IPv4-адрес 172.17.99.11 с маской подсети 255.255.255.0.

Задайте шлюз по умолчанию 172.17.99.1.

Команда **show interfaces** является ещё одной распространённой командой, которая выводит данные о состоянии и статистике сетевых интерфейсов коммутатора. Команда **show interfaces** часто используется при настройке и мониторинге сетевых устройств.

На рисунке показаны выходные данные команды **show interfaces fastEthernet 0/18**. Первая строка на рисунке ниже указывает, что интерфейс FastEthernet 0/18 находится в состоянии up/up, т.е. в рабочем состоянии. Выходные данные ниже показывают, что включён полнодуплексный режим, а скорость настроена на 100 Мбит/с.

Проблемы на уровне сетевого доступа

Результат команды **show interfaces** можно использовать для обнаружения типичных проблем среды передачи данных. Важнейшие составляющие этих выходных данных отображают состояние протокола канального уровня и протокола канала передачи данных. На рисунке показана итоговая строка для проверки состояния интерфейса.

Первый параметр (FastEthernet0/1 is up) относится к аппаратному уровню и, по сути, указывает, получен ли интерфейсом сигнал обнаружения несущей от другого оконечного устройства. Второй параметр (line protocol is up) относится к канальному уровню. Он указывает, принимаются ли keepalive сообщения протокола канального уровня.

Используя результат команды **show interfaces**, можно устранить возможные проблемы следующим образом.

Если интерфейс включен, а канальный протокол не функционирует, существует проблема. Возможно несоответствие в типе инкапсуляции, интерфейс на другом конце мог быть выключен в результате сбоя или могли возникнуть проблемы с аппаратным обеспечением.

В случае если протокол канального уровня (Line protocol) и интерфейс отключены, возможно, не подключён кабель или существуют другие проблемы с интерфейсом. Например, при соединении двух устройств напрямую мог быть отключен интерфейс на другом конце.

Если интерфейс отключён администратором, он был отключён вручную (с помощью команды **shutdown**) в активной конфигурации.

Выходные данные команды **show interfaces** отображают счетчики и статистику для интерфейса FastEthernet0/18, как показано на рисунке.

Некоторые ошибки носителя недостаточно серьезны, чтобы привести к сбою цепи, но вызывают проблемы с производительностью сети. В таблице объясняются некоторые из этих распространенных ошибок, которые можно обнаружить с помощью команды **show interface**.

| Тип ошибки | Описание |
|--|---|
| Ошибки ввода | Общее количество ошибок. Включает «карликовые» и «гигантские» кадры, отсутствие буфера, CRC, ошибки в кадрах, переполнение и проигнорированные пакеты. |
| Runts (ошибки типа «карликовый кадр») | Пакеты, отброшенные из-за того, что они меньше минимального размера пакета для среды. Например, любой кадр Ethernet размером менее 64 байтов считается карликовым (runt). |
| Гигантские кадры (giant) | Пакеты, которые отброшены из-за превышения максимального размера пакета для среды. Например, любой кадр Ethernet размером более 1 518 байтов считается слишком большим (giant). |
| CRC | Ошибки CRC создаются, когда рассчитанная контрольная сумма не соответствует полученной контрольной сумме. |
| Ошибки вывода | Сумма всех ошибок, которые мешали окончательной передаче дейтаграмм из анализируемого интерфейса. |
| Коллизии | Количество сообщений, повторно переданных из-за коллизий Ethernet. |
| Поздние коллизии | Коллизия, которая случается после передачи 512 бит кадра. |

Ошибки ввода вывода

«Ошибки ввода» — это сумма всех ошибок в датаграммах, которые были получены при анализе интерфейса. Они включают в себя карликовые (runts) и гигантские (giants) кадры, ошибки CRC, отсутствие буфера, кадр, переполнение и проигнорированные пакеты. К ошибкам ввода, которые можно обнаружить с помощью команды `show interfaces`, относятся следующие:

Карликовые кадры (runt frames) — кадры Ethernet, размер которых не превышает минимально разрешённые 64 байта. Карликовые кадры чаще всего бывают вызваны неисправностью сетевой платы, но могут быть обусловлены и другими причинами, например чрезмерно высоким числом коллизий.

Гигантские кадры (giants) — кадры Ethernet, размер которых превышает максимальную длину кадра. Наличие гигантских кадров вызвано теми же причинами, что и наличие карликовых.

Ошибки CRC — в Ethernet и последовательных интерфейсах ошибки CRC обычно свидетельствуют о неполадках в среде передачи или кабеле. Частыми причинами ошибок являются электрические наводки, плохо закреплённые или повреждённые разъемы, а также неверно выбранный тип кабеля. Большое количество ошибок CRC приводит к шуму на канале, поэтому следует проверить кабель на повреждения и допустимую длину. Также по возможности следует найти и устранить источники шума.

«Ошибки вывода» — это сумма всех ошибок, которые препятствовали успешной передаче датаграмм из проверяемого интерфейса. К ошибкам ввода,

которые можно обнаружить с помощью команды **show interfaces**, относятся следующие:

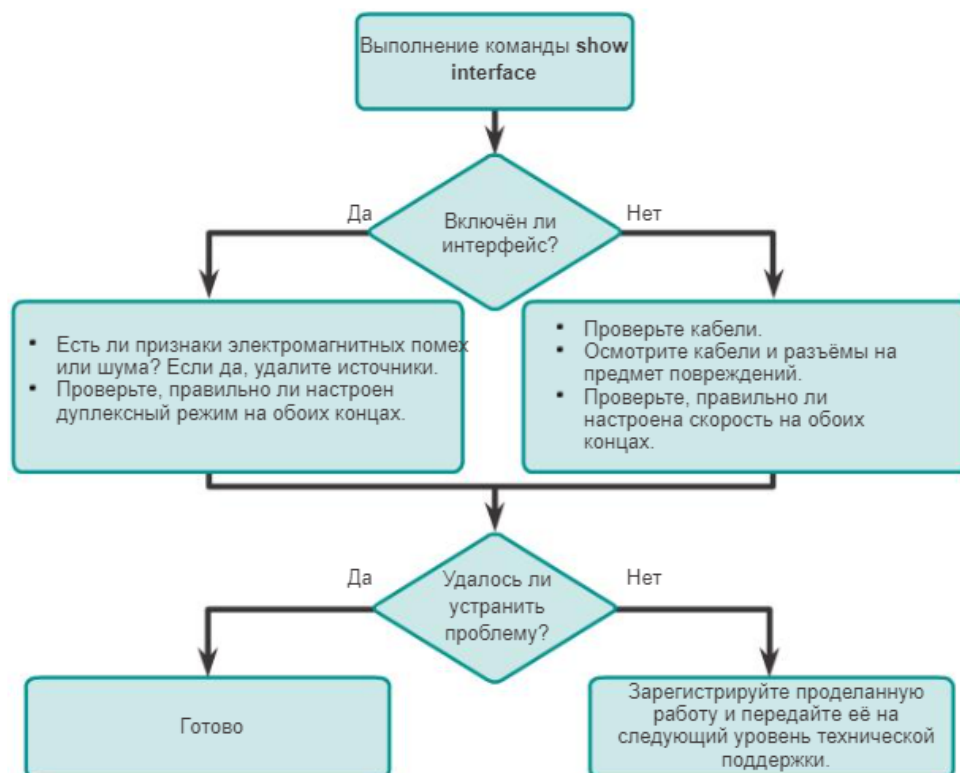
Коллизии — коллизии в полудуплексном режиме являются нормой, поэтому о них не стоит беспокоиться до тех пор, пока работа полудуплексного режима вас устраивает. Однако в правильно спроектированной и настроенной сети с использованием полнодуплексной связи коллизий быть не должно. Мы настоятельно рекомендуем использовать полнодуплексную связь, за исключением случаев, когда вы работаете с устаревшим оборудованием, требующим использования полудуплексного режима.

Поздние коллизии — это коллизии, которые происходят после передачи 512 бит кадра (преамбулы). Наиболее распространённая причина поздних коллизий — превышение допустимой длины кабеля. Неправильная настройка дуплексной связи также может вызывать поздние коллизии, например, в случае, когда один конец соединения настроен на полнодуплексный режим, а другой конец — на полудуплексный режим. Вы обнаружите поздние коллизии на интерфейсе, настроенном на полудуплексный режим. Для решения данной проблемы необходимо настроить один и тот же дуплексный режим на обоих концах соединения. В правильно спроектированной и настроенной сети поздние коллизии возникать не должны.

Поиск и устранение неполадок на уровне сетевого доступа

Для поиска и устранения неполадок при отсутствии или плохом качестве соединения коммутатора с другим устройством следуйте данному алгоритму действий:

Проблемы с поиском и устранением неполадок коммутатора



1.1 Удаленный защищенный доступ

2. Введение в коммутируемые сети

Избыточность сети — ключ к обеспечению надёжности сети. Избыточные маршруты обеспечиваются за счёт нескольких физических каналов между устройствами. Таким образом, сеть может продолжать работу даже в случае сбоя одного канала или порта. Также по избыточным каналам можно распределить нагрузку трафика, что позволяет увеличить емкость.

Во избежание возникновения петель 2 уровня требуется управление несколькими маршрутами. Выбираются оптимальные маршруты, и альтернативный маршрут должен быть незамедлительно доступен в случае сбоя основного маршрута. Протоколы STP используются для управления избыточностью 2 уровня.

Избыточные устройства, например, многоуровневые коммутаторы или маршрутизаторы, предоставляют клиентам возможность использования альтернативного шлюза по умолчанию в случае сбоя основного шлюза по умолчанию. Таким образом клиент сможет использовать несколько путей к нескольким возможным шлюзам по умолчанию. Протоколы обеспечения избыточности на первом хопе (FHRP) используются для управления назначением клиенту шлюза по умолчанию, а также для предоставления

возможности использования альтернативного шлюза по умолчанию в случае сбоя основного шлюза по умолчанию.

Штормовой трафик

Сегодня ваш первый рабочий день в должности сетевого администратора на предприятии малого или среднего бизнеса. Специалист, занимавший эту должность до вас, уволился сразу после обновления сети предприятия.

В результате обновления в сеть был добавлен новый коммутатор. После обновления от сотрудников поступало много жалоб на проблему доступа к Интернету и серверам сети. Если быть точнее, многим из них не удается получить доступ к сети. Руководитель компании попросил вас незамедлительно провести проверку и определить причины проблем подключения и задержек,

поэтому вы принимаетесь за изучение сетевого оборудования в главном распределительном узле здания. По результатам проверки выясняется, что топология сети не содержит ошибок, кабели подключены правильно, маршрутизаторы и коммутаторы включены и исправно работают, при этом коммутаторы соединены друг с другом для обеспечения отказоустойчивости или избыточности.

Однако вы обращаете внимание на то, что индикаторы состояния на всех коммутаторах мигают так быстро, что может показаться, будто они не мигают, а непрерывно горят. Кажется, вы поняли, в чем заключается причина проблем подключения.

Используйте Интернет для изучения STP. В процессе изучения делайте записи и описывайте:

- широковещательный шторм;

- петли коммутации;

- предназначение STP;

- типы STP.

Трехуровневая иерархическая модель сети, которая использует уровни ядра, распределения и доступа с избыточностью, призвана устранить единую точку отказа в сети. Использование нескольких физически подключенных каналов между коммутаторами обеспечивает физическую избыточность в коммутируемой сети. Это повышает надёжность и доступность сети. Наличие альтернативных физических каналов для передачи данных по сети позволяет пользователям получить доступ к сетевым ресурсам даже в случае сбоя одного из каналов.

Нажмите кнопку «Воспроизведение» на рис. 1, чтобы просмотреть анимацию, демонстрирующую избыточность.

1. PC1 взаимодействует с PC4 через избыточную топологию сети.
2. Когда в сетевом канале между S1 и S2 происходит сбой, путь между PC1 и PC4 автоматически корректируется, чтобы компенсировать сбой.
3. Если сетевое соединение между S1 и S2 восстановлено, путь повторно корректируется для маршрутизации трафика непосредственно от S2 к S1 для его доставки на PC4.

Для многих организаций доступность сети является важнейшим фактором обеспечения соответствия требованиям бизнеса. Таким образом, модель инфраструктуры сети является критически важным для бизнеса компонентом. Избыточность маршрута предоставляет решение, обеспечивающее необходимую доступность нескольких сетевых служб за счёт устранения потенциальной единой точки отказа.

Примечание. Избыточность на 1 уровне модели OSI демонстрируется с использованием нескольких каналов и устройств, однако для настройки сети требуется нечто большее, чем просто физическое планирование. Для систематической работы избыточности также необходимо использовать протоколы 2 уровня OSI (например STP).

Важной частью иерархической архитектуры является избыточность, использование которой позволяет предотвратить перебои в обслуживании конечных пользователей. Для работы избыточных сетей требуются физические маршруты, однако и логическая избыточность также должна быть частью архитектуры. Тем не менее, избыточные маршруты в коммутируемой сети Ethernet могут привести к возникновению физических и логических петель 2 уровня.

Нестабильность базы данных MAC-адресов

В отличие от IP-пакетов, кадры Ethernet не содержат атрибут «время жизни» (TTL). Как результат, если не используется механизм блокирования постоянного распространения этих кадров в коммутируемой сети, кадры продолжают распространяться между коммутаторами бесконечно или до тех пор, пока не произойдет сбой канала, в результате чего петля будет прервана. Такое постоянное распространение между коммутаторами может привести к нестабильности базы данных MAC-адресов. Это может произойти вследствие пересылки широковещательных кадров.

Широковещательные кадры пересылаются из всех портов коммутатора, за исключением исходного входного порта. Это гарантирует, что все устройства в домене широковещательной рассылки могут получить кадр. При наличии нескольких путей для пересылки кадров может возникнуть бесконечная петля. В случае возникновения петли таблица MAC-адресов на коммутаторе может постоянно изменяться за счёт обновлений от широковещательных кадров, что приводит к нестабильности базы данных MAC-адресов.

Для просмотра анимации нажмите кнопку «Воспроизведение» на рисунке. Когда анимация остановится, прочитайте текст, расположенный слева от схемы топологии. Анимация продолжится после короткой паузы.

Содержание анимации:

1. PC1 отправляет широковещательный кадр на S2. S2 принимает широковещательный кадр на интерфейс F0/11. Когда S2 принимает широковещательный кадр, он обновляет свою таблицу MAC-адресов, чтобы зарегистрировать доступность PC1 на порте F0/11.

2. Поскольку этот кадр — широковещательный, S2 пересылает кадр из всех портов, включая Магистраль 1 и Магистраль 2. Когда широковещательный кадр поступает на S3 и S1, их таблицы MAC-адресов обновляются относительно PC1, который доступен на порту F0/1 на S1 и на порту F0/2 на S3.

3. Поскольку этот кадр является широковещательным, S3 и S1 пересылают кадр из всех портов, за исключением исходного входного порта. S3 отправляет широковещательный кадр с PC1 на S1. S1 отправляет широковещательный кадр с PC1 на S3. Все коммутаторы обновляют свою таблицу MAC-адресов с учетом неправильного порта PC1.

4. Все коммутаторы снова пересылают широковещательный кадр из всех портов, за исключением входного порта. Это приводит к тому, что оба коммутатора пересылают кадр на S2.

5. Когда S2 получает широковещательные кадры от S3 и S1, таблица MAC-адресов снова обновляется, в этот раз с учетом последней записи, полученной от двух других коммутаторов.

Этот процесс повторяется до тех пор, пока петля не будет прервана путем физического отключения соединений, вызывающих ее, или отключения

питания одного из коммутаторов в петле. При этом создается высокая нагрузка на ЦП на всех коммутаторах, участвующих в петле. Поскольку между всеми коммутаторами в петле постоянно передаются одни и те же кадры, ЦП коммутатора приходится обрабатывать большой объем данных. При этом снижается производительность коммутатора при поступлении допустимого трафика.

Узел, участвующий в сетевой петле, недоступен для других узлов в сети. Кроме того, вследствие постоянных изменений в таблице MAC-адресов коммутатор не знает, из какого порта следует пересылать кадры одноадресной рассылки. В вышеуказанном примере для PC1 перечислены неправильные порты. Любой кадр одноадресной рассылки, предназначенный для PC1, участвует в петле, как и кадры широковещательной рассылки. Из-за возрастающего числа кадров, циклически распространяемых в сети, постепенно создается широковещательный шторм.

Широковещательный шторм

Широковещательный шторм возникает в случае, когда в петлю на 2 уровне попадает столько кадров широковещательной рассылки, что при этом потребляется вся доступная полоса пропускания. Соответственно, для легитимного трафика нет доступной полосы пропускания, и сеть становится недоступной для обмена данными. Описанная ситуация — эффективный отказ в обслуживании.

Широковещательный шторм неизбежен в сети, где возникла петля. По мере того, как все больше устройств отправляют широковещательные рассылки по сети, все больше трафика попадает в петлю и потребляет ресурсы. В конечном счете это создает широковещательный шторм, что приводит к сбоям в сети.

Широковещательные штормы также имеют и ряд других последствий. Поскольку трафик широковещательной рассылки пересылается из всех портов коммутатора, все подключенные устройства должны обрабатывать трафик широковещательной рассылки, лавинная рассылка которого выполняется бесконечно по сети, в которой возникла петля. Из-за этого могут возникать сбои в работе оконечного устройства ввиду высоких требований к обработке в целях поддержания высокой нагрузки трафика на сетевом адаптере.

1. PC1 передает кадр широковещательной рассылки в сеть, где возникла петля.

2. Кадр широковещательной рассылки циклически передается между всеми соединенными друг с другом коммутаторами в сети.

3. PC4 тоже отправляет кадр широковещательной рассылки в сеть, где возникла петля.

4. Кадр широковещательной рассылки PC4 также попадает в петлю между всеми соединенными друг с другом коммутаторами, как и кадр широковещательной рассылки PC1.

5. По мере того, как все больше устройств отправляют широковещательные рассылки по сети, все больше трафика попадает в петлю и потребляет ресурсы. В конечном счете это создает широковещательный шторм, что приводит к сбоям в сети.

6. Когда сеть полностью насыщена трафиком широковещательной рассылки, который циклически передается между коммутаторами, новый трафик отбрасывается коммутатором, поскольку он не в состоянии его обработать.

Поскольку устройства, подключенные к сети, регулярно отправляют кадры широковещательной рассылки, например, ARP-запросы, широковещательный шторм может возникать за считанные секунды. В результате при возникновении петли коммутируемая сеть быстро выходит из строя.

Множественная передача кадров

Кадры широковещательной рассылки являются не единственным типом кадров, на которые влияет возникновение петель. Кадры одноадресной рассылки, отправленные в сеть, где возникла петля, могут стать причиной дублирования кадров, поступающих на устройство назначения.

1. PC1 отправляет кадр одноадресной рассылки, предназначенный для PC4.

2. S2 не содержит в своей таблице MAC-адресов записи для PC4, поэтому выполняет лавинную рассылку этого кадра из всех портов коммутатора, пытаясь найти PC4.

3. Кадр поступает на коммутаторы S1 и S3.

4. S1 содержит в таблице MAC-адресов записи для PC4, поэтому он отправляет кадр на PC4.

5. S3 также содержит в таблице MAC-адресов запись для PC4, поэтому отправляет кадр одноадресной рассылки из порта Магистраль 3 на S1.

6. S1 принимает дублированный кадр и отправляет его на PC4.

7. Таким образом, PC4 принимает два одинаковых кадра.

Большинство протоколов верхнего уровня не предназначены для распознавания или устранения проблемы дублированной передачи. Как правило, протоколы, использующие механизм нумерации последовательности, предполагают, что произошел сбой передачи, и номер последовательности переходит в другой сеанс обмена данными. Остальные протоколы пытаются передать дублированные данные соответствующему протоколу верхнего уровня для обработки и, возможно, отбрасывания.

Протоколы LAN 2 уровня, например Ethernet, не поддерживают механизмы распознавания и предотвращения бесконечных циклических кадров. Некоторые протоколы 3 уровня используют механизмы времени жизни (TTL), которые ограничивают количество попыток повторной передачи пакетов сетевыми устройствами 3 уровня. В отсутствие такого механизма устройства 2 уровня будут производить трафик в бесконечном цикле. Механизм предотвращения петли 2 уровня (STP) разработан как раз для решения данных проблем.

Во избежание подобных проблем в сети с избыточностью, на коммутаторах должны быть включены определённые типы протокола spanning-tree. Протокол spanning-tree по умолчанию включено на коммутаторах Cisco, предотвращая, таким образом, возникновение петель 2 уровня.

Избыточность повышает доступность топологии сети посредством защиты сети от единой точки отказа — например, неисправного сетевого кабеля или коммутатора. При реализации в проектировании физической избыточности возникают петли и дублирование кадров. Петли и дублированные кадры являются причиной серьезных неполадок в коммутируемой сети. Протокол STP разработан для решения подобных проблем.

Протокол STP обеспечивает наличие только одного логического пути между всеми узлами назначения в сети путем намеренного блокирования резервных путей, которые могли бы вызвать петлю. Порт считается заблокированным, когда заблокирована отправка и прием данных на этот порт. К таким данным не относятся кадры BPDU, которые используются протоколом STP для предотвращения петель. Для предотвращения петель в сети чрезвычайно важно блокировать избыточные пути. Физические пути по-прежнему используются для обеспечения избыточности, однако эти пути отключены в целях предотвращения петель. Если путь потребуется для компенсации неисправности сетевого кабеля или коммутатора, протокол STP

повторно рассчитывает пути и снимает блокировку с требуемых портов, чтобы разрешить активацию избыточного пути.

В рассматриваемом примере протокол STP включен на всех коммутаторах:

1. PC1 отправляет широковещательную рассылку в сеть.

2. S2 настроен с использованием протокола STP, и для порта Магистраль 2 задано состояние блокировки. Состояние блокировки запрещает использование портов для пересылки данных пользователей, предотвращая, таким образом, возникновение петли. S2 пересылает кадр широковещательной рассылки из всех портов коммутатора, за исключением порта источника PC1 и порта для Магистраль 2.

3. S1 принимает кадр широковещательной рассылки и пересылает его из всех портов коммутатора, откуда он поступает на PC4 и S3. S3 пересылает кадр из порта для Магистраль 2, и S2 пропускает этот кадр. Возникновение петли 2 уровня предотвращено.

В приведённом примере:

1. PC1 отправляет широковещательную рассылку в сеть.

2. После этого широковещательная рассылка пересылается по сети, как показано в предыдущей анимации.

3. Возникает сбой в транковом канале между S2 и S1, что приводит к прерыванию предыдущего пути.

4. S2 снимает блокировку с предварительно заблокированного порта для Магистраль 2 и разрешает передачу трафика широковещательной сети по альтернативному пути, обеспечивая дальнейший обмен данными. Если этот канал снова работает, выполняется повторное схождение протокола STP, а порт на S2 снова блокируется.

Протокол STP предотвращает возникновение петель за счёт настройки беспетлевого пути в сети с использованием портов, стратегически настроенных на заблокированное состояние. Коммутаторы, использующие протокол STP, могут компенсировать сбои за счёт динамической разблокировки ранее заблокированных портов и разрешения передачи трафика по альтернативным путям.

До сих пор использовался термин Spanning Tree Protocol (протокол spanning-tree) и аббревиатура STP. Однако использование этого термина и этой аббревиатуры может быть двусмысленным. Многие специалисты используют данный термин и аббревиатуру для обозначения различных

реализаций протокола spanning-tree, например протокола Rapid Spanning Tree Protocol (RSTP) и протокола Multiple Spanning Tree Protocol (MSTP). Чтобы правильно объяснять принципы протокола spanning-tree, важно понимать, о какой конкретно реализации или стандарте идет речь в данном контексте. В новейшей версии документации IEEE по протоколу spanning-tree (IEEE-802-1D-2004) говорится: «Протокол STP в настоящее время заменен протоколом Rapid Spanning Tree Protocol (RSTP)»; можно заметить, что в IEEE термин «STP» используется для обозначения исходной реализации протокола spanning-tree, а «RSTP» — для описания версии протокола spanning-tree, указанной в IEEE-802.1D-2004. В рамках данной программы, если в контексте обсуждения речь идет об исходном протоколе STP, то во избежание расхождений используется фраза: «исходный протокол spanning-tree 802.1D».

Примечание. Протокол STP основан на алгоритме, изобретенном компанией Radia Perlman в ходе работы над проектом Digital Equipment Corporation. Алгоритм опубликован в 1985 году в документе «Алгоритм распределенного вычисления протокола spanning-tree в расширенной сети LAN».

IEEE 802.1D STP использует алгоритм протокола spanning-tree (STA), чтобы определить, какие порты коммутаторов в сети должны быть переведены в состояние блокировки во избежание возникновения петель. STA назначает один из коммутаторов в качестве корневого моста и использует его как точку привязки для расчёта всех путей. На рисунке корневой мост (коммутатор S1) выбран с помощью специального процесса выбора. Все коммутаторы, участвующие в STP, обмениваются кадрами BPDU, чтобы определить, какой коммутатор имеет самое низкое значение идентификатора моста (BID) в сети. Коммутатор с наименьшим значением BID автоматически становится корневым мостом для расчётов STA.

Примечание. Чтобы упростить задачу, предположим (пока не указано иное), что все порты на всех коммутаторах назначены сети VLAN 1. У каждого коммутатора есть уникальный MAC-адрес, связанный с сетью VLAN 1.

BPDU представляет собой кадр обмена сообщениями, которым обмениваются коммутаторы для STP. Каждый BPDU содержит идентификатор BID, который определяет коммутатор, отправивший BPDU. Идентификатор BID содержит значение приоритета, MAC-адрес отправляющего коммутатора и дополнительный расширенный идентификатор системы. Самое низкое значение BID определяется комбинацией значений в этих трех полях.

После определения корневого моста STA рассчитывает кратчайший путь до него. Все коммутаторы используют STA для определения портов, подлежащих блокировке. Пока STA определяет оптимальные пути до корневого моста для всех портов коммутатора в домене широковещательной рассылки, пересылка трафика по сети заблокирована. При определении портов, подлежащих блокировке, STA учитывает стоимость как пути, так и порта. Стоимость портов рассчитывается с помощью значений стоимости порта, зависящей от скорости каждого порта коммутатора на данном маршруте. Сумма значений стоимости порта определяет общую стоимость пути до корневого моста. Если для выбора доступно несколько путей, STA выбирает путь с наименьшей стоимостью.

Определив наиболее предпочтительные пути для каждого коммутатора, алгоритм STA назначает роли участвующим портам коммутаторов. Роли портов описывают их связь с корневым мостом в сети, а также указывают, разрешена ли для них пересылка трафика:

Корневые порты – порты коммутатора, находящиеся максимально близко к корневному мосту. На рисунке корневой порт на S2 — порт F0/1, настроенный для транкового канала между S2 и S1. Корневой порт на S3 — порт F0/1, настроенный для транкового канала между S3 и S1. Корневые порты выбираются для каждого коммутатора отдельно.

Назначенные порты — все некорневые порты, которым, тем не менее, разрешено пересылать трафик по сети. На рисунке порты коммутатора S1 (F0/1 и F0/2) являются назначенными портами. На коммутаторе S2 порт F0/2 также настроен в качестве назначенного порта. Назначенные порты выбираются для каждого транкового канала отдельно. Если на одном конце транка находится корневой порт, то на другом — назначенный. Все порты на корневом мосте являются назначенными портами.

Альтернативные и резервные порты – альтернативные и резервные порты настраиваются в состояние блокировки во избежание возникновения петель. На рисунке STA настроил порт F0/2 на коммутаторе S3 в роли альтернативного порта. Порт F0/2 на коммутаторе S3 находится в состоянии блокировки. Альтернативные порты выбираются только на транковых каналах, где ни один из концов не является корневым портом. Обратите внимание, что на рисунке заблокирован только один из концов транка. Это обеспечивает более быстрый переход в состояние пересылки в случае необходимости. (Заблокированные порты используются только в том случае, когда два порта на одном коммутаторе соединены друг с другом посредством коммутатора или одного кабеля).

Отключенные порты – отключенным называется порт коммутатора, питание которого отключено.

Алгоритм протокола spanning-tree зависит от обмена кадрами BPDU, выполняемого для определения корневого моста. Кадр BPDU содержит 12 отдельных полей, которые содержат сведения о пути и приоритете, используемые для определения корневого моста и путей к нему.

В первых четырех полях указаны протокол, версия, тип сообщения и флаги состояния.

Следующие четыре поля используются для определения корневого моста и стоимости пути к нему.

Последние четыре поля являются полями таймера, которые определяют интервал отправки сообщений BPDU и продолжительность хранения данных, полученных посредством процесса BPDU (см. следующий раздел).

На рис. 2 показан кадр BPDU, полученный с помощью программы Wireshark. В этом примере кадр BPDU содержит большее количество полей, чем описано выше. Сообщение BPDU при передаче по сети инкапсулируется в кадр Ethernet. Заголовок 802.3 указывает адреса источника и назначения кадра BPDU. Кадр содержит MAC-адрес назначения 01:80:C2:00:00:00, который является адресом групповой рассылки для группы протокола spanning-tree. При адресации кадра с использованием этого MAC-адреса все коммутаторы, настроенные для протокола spanning-tree, принимают и считывают данные из кадра. Все остальные устройства в сети игнорируют кадр.

В этом примере идентификатор корневого моста в полученном кадре BPDU совпадает с идентификатором BID. Это указывает на то, что кадр получен из корневого моста. Все таймеры настроены с использованием значений по умолчанию.

С момента создания исходного стандарта IEEE 802.1D было разработано несколько разновидностей протоколов STP.

К разновидностям протоколов STP относятся следующие:

STP: исходная версия IEEE 802.1D (802.1D-1998 и более ранние), в рамках которой предоставляется беспетлевая топология в сети с избыточными каналами. Общий протокол spanning-tree (CST): предполагает использование только одного экземпляра протокола spanning-tree для всей сети с мостовым соединением независимо от количества сетей VLAN.

PVST+ является усовершенствованным протоколом компании Cisco, в котором для каждого отдельного VLAN используется отдельный экземпляр RSTP. Рассматриваемый вариант протокола spanning-tree поддерживает PortFast, UplinkFast, BackboneFast, BPDU guard, BPDU filter, root guard и loop guard.

802.1D-2004: обновленная версия стандарта STP, в которую входит IEEE 802.1w.

Быстрый протокол STP (RSTP) или IEEE 802.1w: доработанный протокол STP, который обеспечивает более быстрое схождение, чем протокол STP.

Rapid PVST+: усовершенствованный корпорацией Cisco протокол RSTP, который использует PVST+. Rapid PVST+ предоставляет отдельный экземпляр 802.1w для каждой сети VLAN. Рассматриваемый вариант протокола spanning-tree поддерживает PortFast, BPDU guard, BPDU filter, root guard и loop guard.

Протокол MSTP (несколько протоколов spanning-tree) (MSTP): стандарт IEEE на базе ранее существующей собственной реализации Multiple Instance STP (MISTP) корпорации Cisco. MSTP сопоставляет несколько сетей VLAN в пределах одного экземпляра протокола spanning-tree. Реализация Cisco протокола MSTP, которая обеспечивает до 16 экземпляров протокола RSTP и объединяет множество сетей VLAN с идентичной физической и логической топологией в один общий экземпляр RSTP. Каждая реализация поддерживает функции PortFast, BPDU guard, BPDU filter, root guard и loop guard.

Сетевому специалисту, который отвечает за администрирование коммутаторов, может потребоваться принять решение относительно того, какой тип протокола STP необходимо реализовать.

Примечание. Устаревшие проприетарные функции Cisco UplinkFast и BackboneFast в рамках данного курса не рассматриваются. Эти функции заменены реализацией протокола Rapid PVST+, в которую данные функции включены как часть реализации стандарта RSTP.

Далее представлены характеристики различных протоколов STP. Выделенные курсивом слова указывают, является ли конкретный протокол STP собственным протоколом Cisco или стандартной реализацией IEEE:

STP: использует один экземпляр протокола spanning-tree IEEE 802.1D для всей коммутируемой сети независимо от количества сетей VLAN. Поскольку используется только один экземпляр, требования к ЦП и памяти для этой версии ниже, чем в отношении других протоколов. Однако, поскольку используется только один экземпляр, существует только один корневой мост

и одно дерево. Трафик для всех сетей VLAN проходит по одному и тому же пути, что может привести к образованию неоптимальных потоков трафика. Ввиду ограничений 802.1D данная версия обеспечивает медленное схождение.

PVST+: усовершенствованный корпорацией Cisco протокол STP, который предоставляет отдельный экземпляр реализации 802.1D корпорации Cisco для каждой сети VLAN, настроенной в сети. Рассматриваемый вариант протокола spanning-tree поддерживает PortFast, UplinkFast, BackboneFast, BPDU guard, BPDU filter, root guard и loop guard. При создании экземпляра для каждой сети VLAN увеличиваются требования к ЦП и памяти, однако таким образом обеспечивается возможность использования корневых мостов отдельно для каждой сети VLAN. Такая модель позволяет оптимизировать протокол spanning-tree для трафика каждой сети VLAN. Сходимость этой версии аналогична сходимости 802.1D. Однако сходимость осуществляется отдельно для каждой сети VLAN.

RSTP (или IEEE 802.1w): быстрый протокол spanning-tree, обеспечивающий более быстрое схождение, чем исходная реализация 802.1D. В этой версии устранены многие проблемы со сходимостью, но, поскольку в ней все равно предоставляется один экземпляр STP, проблема неоптимальных потоков трафика по-прежнему остается нерешенной. В целях обеспечения более быстрого схождения требования к ЦП и памяти в этой версии несколько выше, чем для CST, но не такие высокие, как для RSTP+.

Rapid PVST+: усовершенствованный корпорацией Cisco протокол RSTP, который использует PVST+. Предоставляет отдельный экземпляр 802.1w для каждой сети VLAN. Рассматриваемый вариант протокола spanning-tree поддерживает PortFast, BPDU guard, BPDU filter, root guard и loop guard. В этой версии решена проблема сходимости и образования неоптимальных потоков трафика. Однако в этой версии предъявляются самые высокие требования к ЦП и памяти.

MSTP: стандарт IEEE 802.1s, созданный на основе предыдущей собственной реализации протокола MSTP компании Cisco. Чтобы уменьшить число требуемых экземпляров STP, MSTP сопоставляет несколько сетей VLAN, в отношении которых действуют одинаковые требования к потоку трафика, в пределах одного экземпляра протокола spanning-tree.

MST: реализация Cisco протокола MSTP, которая обеспечивает до 16 экземпляров протокола RSTP (802.1w) и объединяет множество сетей VLAN с идентичной физической и логической топологиями в один общий экземпляр RSTP. Каждая реализация поддерживает функции PortFast, BPDU guard, BPDU filter, root guard и loop guard. Требования к ЦП и памяти для этой версии ниже,

чем аналогичные требования в отношении протокола Rapid PVST+, но выше, чем для протокола RSTP.

Для коммутаторов Cisco Catalyst по умолчанию используется режим протокола spanning-tree PVST+, включенный на всех портах. PVST+ характеризуется существенно более медленным сходимением после изменения топологии, чем Rapid PVST+.

Примечание. Важно отличать устаревший стандарт IEEE 802.1D-1998 (и более ранние версии) от стандарта IEEE 802.1D-2004. IEEE 802.1D-2004 включает в себя функцию RSTP, а стандартом IEEE 802.1D-1998 называется исходная реализация алгоритма протокола spanning-tree. Более поздние модели коммутаторов Cisco, на которых работают новые версии IOS (например коммутаторы Catalyst 2960 с IOS 15.0), по умолчанию используют PVST+, однако содержат многие характеристики стандарта IEEE 802.1D-1998 в этом режиме (например, альтернативные порты вместо бывших неназначенных портов). Однако для использования быстрого протокола spanning-tree на таком коммутаторе его необходимо явно настроить для работы в режиме быстрого протокола spanning-tree.

Исходный стандарт 802.1D определяет протокол общего spanning-tree (CST), который подразумевает использование только одного экземпляра протокола spanning-tree во всей коммутируемой сети независимо от количества VLAN. Сеть, использующая CST, имеет следующие характеристики:

Распределение нагрузки не поддерживается. Один восходящий канал должен блокировать все сети VLAN.

Ресурсы ЦП используются экономно. Требуется вычисление только одного экземпляра протокола spanning-tree.

Корпорация Cisco разработала протокол PVST+ таким образом, чтобы сеть могла использовать независимый экземпляр реализации стандарта IEEE 802.1D для каждой сети VLAN в пределах сети. PVST+ позволяет одному транковому порту на коммутаторе блокировать отдельную сеть VLAN, не блокируя при этом остальные сети VLAN. PVST+ можно использовать для распределения нагрузки на 2 уровне. Поскольку все сети VLAN используют отдельный экземпляр STP, коммутаторам в среде PVST+ требуется больший объем ресурсов ЦП и полосы пропускания BPDU, чем в стандартной реализации CST протокола STP.

В среде PVST+ параметры протокола spanning-tree можно настроить таким образом, чтобы половина сетей VLAN выполняла пересылку по всем транковым каналам. На рисунке порт F0/3 на коммутаторе S2 является портом, обеспечивающим передачу данных для сети VLAN 20, а порт F0/2 на коммутаторе S2 — является портом, обеспечивающим передачу данных для сети VLAN 10. Для этого нужно настроить коммутаторы таким образом, чтобы один был выбран в качестве корневого моста для половины сетей VLAN в пределах сети, а второй — в качестве корневого моста для оставшихся сетей VLAN. На рисунке коммутатор S3 является корневым мостом для сети VLAN 20, а S1 является корневым мостом для сети VLAN 10. Несколько корневых мостов STP в одной сети VLAN позволяют увеличить объём избыточности в сети.

Сети под управлением PVST+ имеют следующие характеристики:

Поддерживается оптимальное распределение нагрузки.

Поддержка одного экземпляра протокола spanning-tree для каждой сети VLAN может привести к значительному необоснованному потреблению ресурсов ЦП для всех коммутаторов в сети (помимо ресурсов полосы пропускания, используемых для отправки собственных кадров BPDU каждым из экземпляров). Это нежелательно только в том случае, если настроено большое количество сетей VLAN.

Протокол STP упрощает создание логического беспетлевого пути по домену широковещательной рассылки. Протокол spanning-tree определяется с помощью данных, полученных в процессе обмена кадрами BPDU между соединенными друг с другом коммутаторами. Чтобы упростить процесс получения логического протокола spanning-tree, каждый порт коммутатора проходит через пять возможных состояний порта и три таймера BPDU.

Сразу после загрузки коммутатора начинается построение протокола spanning-tree. Если порт коммутатора переходит непосредственно из состояния блокировки в состояние пересылки, не используя во время перехода данные о полной топологии, порт может временно создавать петлю данных. Именно поэтому протокол STP использует пять состояний портов. На рисунке представлены состояния портов, обеспечивающих отсутствие петель, при формировании логического протокола spanning-tree:

Блокирование: порт является альтернативным и не участвует в пересылке кадров. Порт принимает кадры BPDU, чтобы определить местоположение и идентификатор корневого моста, а также роли порта, выполняемые каждым из портов коммутатора в конечной активной топологии STP.

Прослушивание: прослушивание пути к корневому мосту. Протокол STP определил, что порт может участвовать в пересылке кадров в соответствии с кадрами BPDU, которые коммутатор принял до этого момента. На этом этапе порт коммутатора не только принимает кадры BPDU, но также передает свои собственные кадры BPDU и сообщает смежным коммутаторам о том, что порт коммутатора готовится к участию в активной топологии.

Изучение: изучение MAC-адресов. На этапе подготовки к пересылке кадров порт начинает заполнять таблицу MAC-адресов.

Пересылка: порт считается частью активной топологии. Он пересылает кадры данных, отправляет и принимает кадры BPDU.

Отключенный: порт 2 уровня не участвует в протоколе spanning-tree и не пересылает кадры. Отключенное состояние устанавливается в том случае, если порт коммутатора отключен администратором.

Обратите внимание, что число портов в каждом из состояний (блокирование, прослушивание, получение данных или пересылка) можно отобразить с помощью команды `show spanning-tree summary`.

Для обеспечения логической беспетлевой топологии сети для каждой сети VLAN в коммутируемой сети протокол PVST+ выполняет четыре действия:

1. Выбор одного корневого моста: только один коммутатор может выступать в роли корневого моста (для данной сети VLAN). Корневой мост — это коммутатор с наименьшим значением идентификатора моста. Все порты на корневом мосту являются назначенными (в частности, отсутствуют корневые порты).

2. Выбор корневого порта на каждом некорневом мосту: протокол STP устанавливает один корневой порт на каждом некорневом мосту. Корневой порт является путем с наименьшей стоимостью от некорневого моста к корневому мосту, указывая оптимальный путь к корневому мосту. Как правило, корневые порты находятся в режиме пересылки.

3. Выбор назначенного порта в каждом сегменте: в каждом канале протокол STP устанавливает один выделенный порт. Назначенный порт выбирается на коммутаторе, который предоставляет маршрут с наименьшей стоимостью к корневому мосту. Как правило, назначенные порты находятся в режиме пересылки и выполняют пересылку трафика для сегмента.

4. Остальные порты в коммутируемой сети являются альтернативными: альтернативные порты, как правило, остаются в состоянии блокировки, что позволяет логически разорвать петлевую топологию. Когда порт находится в

состоянии блокировки, он не пересылает трафик, но по-прежнему может обрабатывать полученные сообщения BPDU.

RSTP (IEEE 802.1w) является развитием исходного стандарт 802.1D; он включен в стандарт IEEE 802.1D-2004. Терминология, относящаяся к STP 802.1w, остается в основном той же, что и для исходного стандарта STP IEEE 802.1D. Большинство параметров остаются прежними, поэтому пользователи, знакомые с STP, смогут без проблем настроить новый протокол. Rapid PVST+ — это просто реализация RSTP корпорации Cisco для каждой отдельной сети VLAN. В Rapid PVST+ для каждой сети VLAN запускается самостоятельный экземпляр протокола RSTP.

На рисунке показана сеть под управлением RSTP. S1 является корневым мостом с двумя назначенными портами в состоянии пересылки. RSTP поддерживает новый тип порта: порт F0/3 на коммутаторе S2 является альтернативным портом в состоянии отбрасывания. Обратите внимание, что отсутствуют порты, работающие в режиме блокирования. В протоколе RSTP нет состояния блокирования порта. Протокол RSTP определяет следующие состояния портов: отбрасывание, изучение или пересылка.

Протокол RSTP ускоряет повторный расчёт протокола spanning-tree в случае изменения топологии сети 2 уровня. В правильно настроенной сети RSTP может достичь состояния сходимости гораздо быстрее, иногда всего за несколько сот миллисекунд. Протокол RSTP повторно определяет типы портов и их состояния. Если порт настроен в качестве альтернативного или резервного, он может немедленно перейти в состояние пересылки, не дожидаясь схождения сети. Далее представлено краткое описание характеристик RSTP.

RSTP является предпочтительным протоколом, позволяющим избежать возникновения петель 2 уровня в коммутируемой сети. Многие различия обусловлены проприетарными усовершенствованиями Cisco исходного стандарта 802.1D. Такие усовершенствования, как кадры BPDU, которые содержат и отправляют данные о ролях портов только соседним коммутаторам, не требуют дополнительной настройки и, как правило, работают лучше, чем более ранние проприетарные версии Cisco. Теперь они прозрачны и интегрированы в стандартную работу протокола.

Проприетарные усовершенствования Cisco для исходного стандарта 802.1D, например, функции UplinkFast и BackboneFast, не совместимы с протоколом RSTP.

Протокол RSTP (802.1w) заменяет собой исходный стандарт 802.1D, поддерживая при этом функции обратной совместимости. Сохраняется

большая часть терминологии, относящейся к исходному стандарту 802.1D, и большинство параметров остаются неизменными. Кроме того, 802.1w поддерживает возврат к более ранней версии 802.1D, обеспечивающей взаимодействие с предыдущими моделями коммутаторов на отдельных портах. Например, алгоритм протокола spanning-tree RSTP выбирает корневой мост точно так же, как и исходная версия 802.1D.

RSTP сохраняет те же форматы BPDU, что и исходный IEEE 802.1D, за исключением того, что в поле версии установлено значение 2, что указывает на протокол RSTP, а поле флагов задействует все 8 бит.

Протокол RSTP может активно подтвердить возможность безопасного перехода порта в состояние пересылки, не полагаясь на конфигурацию таймера.

Тип канала позволяет распределить по категориям каждый порт, участвующий в RSTP на основе дуплексного режима порта. В зависимости от того, какие устройства подключены к каждому из портов, можно выделить два различных типа каналов:

Точка-точка: порт, работающий в полнодуплексном режиме; как правило, соединяет два коммутатора и является кандидатом на быстрый переход в состояние пересылки.

Общий: порт, работающий в полудуплексном режиме; соединяет коммутатор с концентратором, объединяющим несколько устройств.

Тип канала позволяет определить, может ли порт сразу перейти в состояние пересылки при условии выполнения определённых условий. Для граничных и неграничных портов требуются разные условия. Неграничные порты распределяются по категориям в двух типах каналов («точка-точка» и «общий»). Тип канала определяется автоматически, но его можно переопределить с помощью явной конфигурации порта, используя команду `spanning-tree link-type parameter`.

Подключения к граничному порту и соединения «точка-точка» претендуют на быстрый переход в состояние пересылки. Тем не менее, прежде чем рассматривать параметр типа канала, RSTP должен определить роль порта. К характеристикам ролей порта с учетом типов канала относятся следующие:

корневые порты не используют параметр типа канала; корневые порты могут осуществлять быстрый переход в состояние пересылки после синхронизации порта;

альтернативные и резервные порты в большинстве случаев не используют параметр типа канала;

назначенные порты максимально эффективно используют параметр типа канала. Быстрый переход в состояние пересылки для назначенного порта выполняется только в том случае, если для параметра типа канала установлено значение point-to-point.

К проблемам, которые могут возникать в связи с избыточной сетью 2 уровня, можно отнести ширококвещательные штормы, нестабильность базы данных MAC-адресов и дублирование кадров одноадресной рассылки. Протокол STP является протоколом 2 уровня, который обеспечивает наличие единственного логического пути между всеми адресами назначения в сети за счёт намеренного блокирования избыточных путей, которые могут вызвать образование петли.

Протокол STP отправляет кадры BPDU для обмена данными между коммутаторами. Для каждого экземпляра протокола spanning-tree в качестве корневого моста выбирается один коммутатор. Администратор может контролировать такой выбор путем изменения приоритета моста. Чтобы настроить распределение нагрузки протокола spanning-tree по сети VLAN или по группе сетей VLAN в зависимости от используемого протокола STP, можно настроить корневые мосты. Затем STP назначает роль порта каждому участвующему порту, используя значение стоимости пути. Стоимость пути равна сумме всех значений стоимости порта по пути к корневому мосту. Стоимость порта автоматически назначается каждому порту. Тем не менее, это значение можно также настроить вручную. Пути с наименьшей стоимостью становятся предпочтительными, а все остальные избыточные пути блокируются.

PVST+ представляет собой конфигурацию IEEE 802.1D по умолчанию на коммутаторах Cisco. Этот протокол запускает один экземпляр STP для каждой сети VLAN. На коммутаторах Cisco для каждой отдельной сети VLAN можно реализовать новую версию протокола STP с более быстрой сходимостью (RSTP) в виде протокола Rapid PVST+. Протокол MST (Multiple Spanning Tree) является реализацией протокола MSTP корпорации Cisco, где один экземпляр протокола spanning-tree используется для определённой группы сетей VLAN. Такие функции, как PortFast и BPDU guard, гарантируют, что узлы в коммутируемой среде будут иметь немедленный доступ к сети без нарушения работы протокола spanning-tree.

Такие протоколы обеспечения избыточности на первом хопе, как HSRP, VRRP и GLBP, предоставляют альтернативные шлюзы по умолчанию для узлов в среде, где используется резервный маршрутизатор или среда с многоуровневой коммутацией. Несколько маршрутизаторов совместно используют виртуальный IP-адрес и MAC-адрес, который выступает в роли

шлюза по умолчанию на клиенте. Это гарантирует, что узлы будут поддерживать подключение в случае сбоя одного из устройств, выступающих в роли шлюза по умолчанию для сети VLAN или группы сетей VLAN. При использовании HSRP или VRRP один маршрутизатор является активным или пересылающим маршрутизатором для конкретной группы, а остальные находятся в режиме ожидания. Помимо автоматического переключения между шлюзами в случае сбоя, GLBP позволяет также одновременно использовать несколько шлюзов.

Снижение перегрузки сети

Коммутаторы используют таблицу MAC-адресов и полнодуплексный режим для устранения конфликтов и предотвращения перегрузки. Функции коммутатора, облегчающие перегрузку, заключаются в следующем:

| Протокол | Функция |
|--------------------------------------|--|
| Быстрая скорость портов | В зависимости от модели коммутаторы могут иметь скорость порта до 100 Гбит/с. |
| Быстрая внутренняя коммутация | Коммутатор использует быструю внутреннюю шину или общую память для повышения производительности. |
| Большие буферы кадров | Это расширяет место для временного хранения при обработке большого количества кадров. |
| Высокая плотность портов | Это обеспечивает увеличение числа портов для устройств, подключенных к локальной сети с меньшими затратами. Это также позволяет увеличить местный трафик с меньшими затратами. |

3. Виртуальные локальные сети

Обзор виртуальных локальных сетей Определение сети VLAN

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

Сети VLAN позволяют администратору производить сегментацию по функциям, проектным группам или областям применения, вне зависимости от физического расположения пользователя или устройства. Устройства в пределах сети VLAN работают таким образом, будто находятся в собственной

независимой сети, даже если делят одну общую инфраструктуру с другими VLAN. Любой порт коммутатора может принадлежать сети VLAN.

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

Определение сети VLAN

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

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

Преимущества использования VLAN

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

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

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

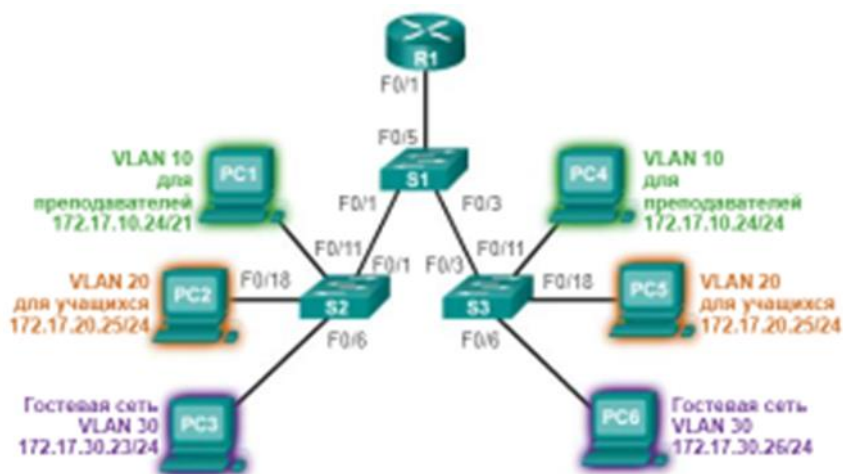
Повышение производительности: разделение однородных сетей 2-го уровня на несколько логических рабочих групп (широковещательных доменов) уменьшает количество лишнего сетевого трафика и повышает производительность.

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

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

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

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



3.1.3 Типы сетей VLAN

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

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

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

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

VLAN 1

| Switch# show vlan brief | | | |
|-------------------------|--------------------|-----------|---|
| VLAN | Name | Status | Ports |
| 1 | default | active | Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gi0/1, Gi0/2 |
| 1002 | fdi-default | act/unsup | |
| 1003 | token-ring-default | act/unsup | |
| 1004 | fdinet-default | act/unsup | |
| 1005 | trnet-default | act/unsup | |

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

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.

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 — это любая сеть VLAN, настроенная для доступа к функциям управления коммутатора. Сеть VLAN 1 по умолчанию является

управляющей VLAN. Для создания управляющей VLAN интерфейсу SVI коммутатора данной VLAN назначаются IP-адрес и маска подсети, благодаря чему коммутатором можно управлять через протоколы HTTP, Telnet, SSH или SNMP. Поскольку в исходной настройке коммутатора Cisco VLAN 1 является сетью VLAN по умолчанию, VLAN 1 не следует использовать в качестве управляющей VLAN.

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

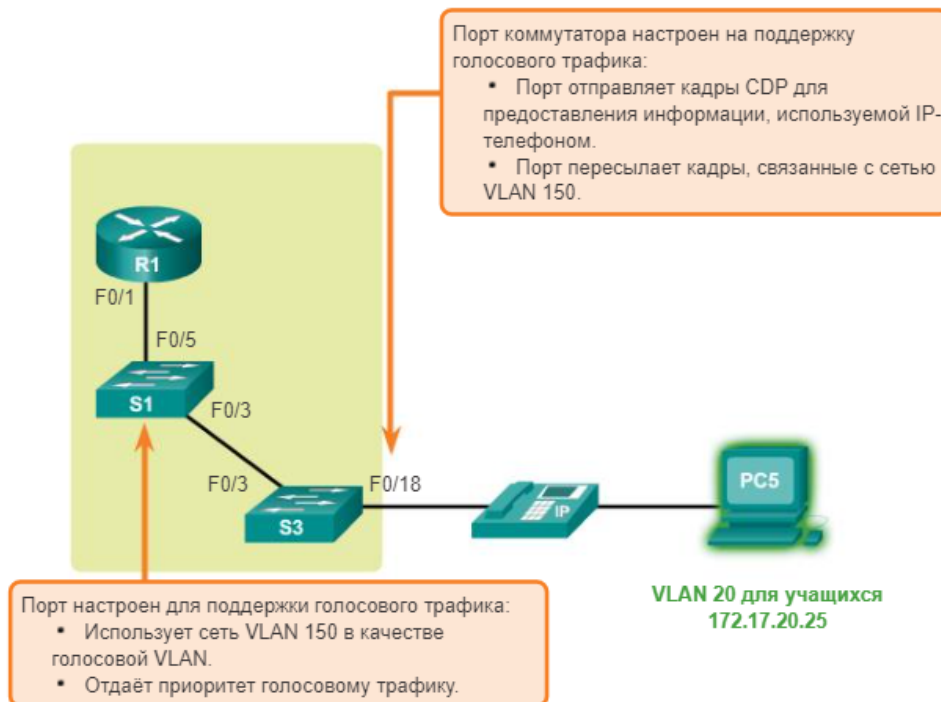
На рисунке из слада 7 все порты назначены сети VLAN 1 по умолчанию. Ни одна native VLAN не назначена явно, и ни одна другая сеть VLAN не является активной. Таким образом, сети native VLAN и управляющая VLAN совпадают. Подобная настройка считается угрозой безопасности.

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

- гарантированная пропускная способность;
- высокий приоритет QoS;
- возможность избежать заторов;
- задержка менее 150 мс от источника к месту назначения.

Вся сеть должна быть спроектирована для поддержки голосовой связи.

Голосовая сеть VLAN



Сети VLAN в среде с несколькими коммутаторами
Магистрالی сетей VLAN

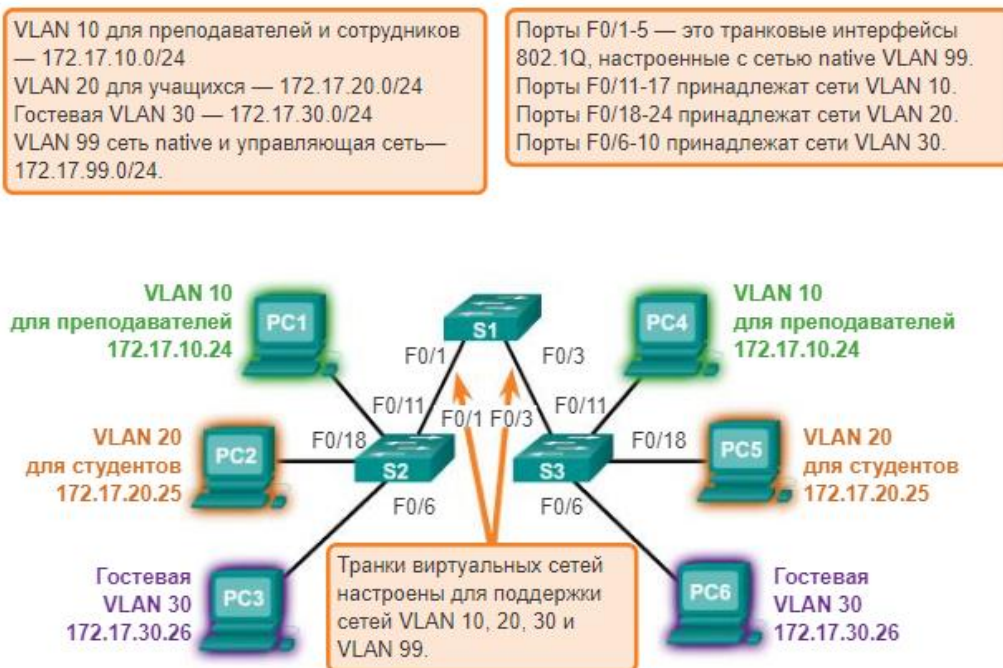
Транк — это канал типа «точка-точка» между двумя сетевыми устройствами, который поддерживает более одной сети VLAN. Транк виртуальных сетей расширяет сети VLAN по всей сети. Cisco поддерживает стандарт IEEE 802.1Q для координации транков в интерфейсах Fast Ethernet, Gigabit Ethernet и 10-Gigabit Ethernet.

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

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.

Транки виртуальных сетей



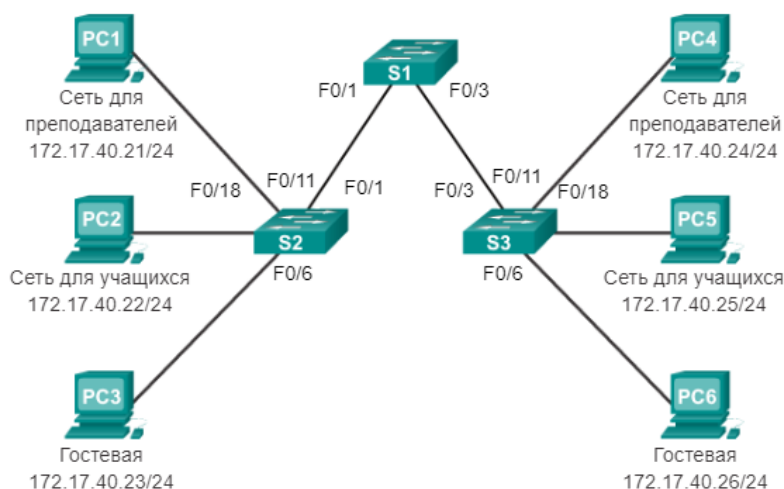
Сети без VLAN

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

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

Без сегментации сети VLAN

Компьютер PC1 отправляет локальную широковещательную рассылку 2-го уровня. Коммутаторы пересылают широковещательный кадр из всех доступных портов.



Сети с VLAN

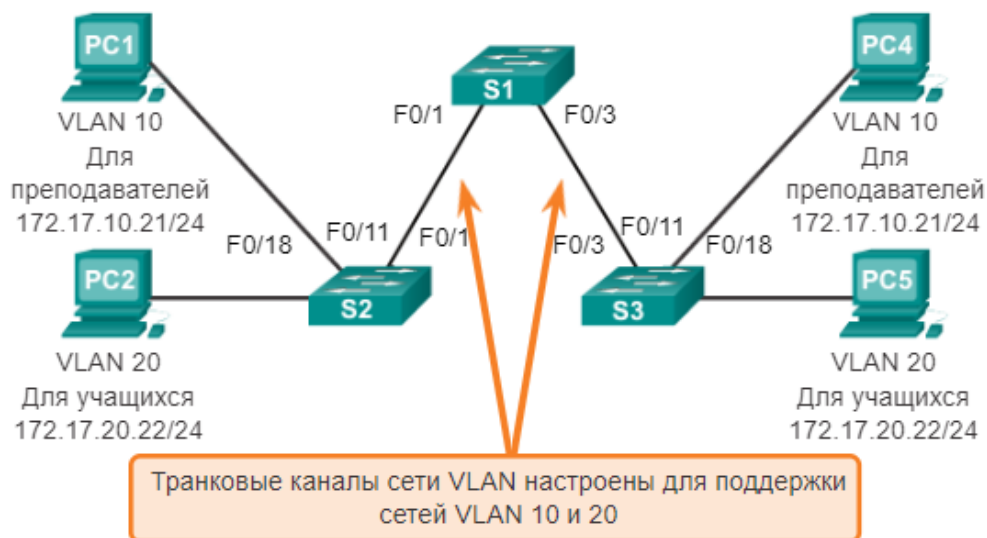
Как показано на рисунке, сеть была разделена на сегменты с помощью двух VLAN. Устройства для преподавателей были назначены сети VLAN 10, а устройства учащихся — сети VLAN 20. Когда из компьютера преподавателя (PC1) отправляется широковещательный кадр на коммутатор S2, коммутатор пересылает кадр только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

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

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

С сегментацией сети VLAN

Компьютер PC1 отправляет локальную широковещательную рассылку 2-го уровня. Коммутаторы пересылают кадр широковещательной рассылки только из портов, настроенных для VLAN 10.



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.

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.

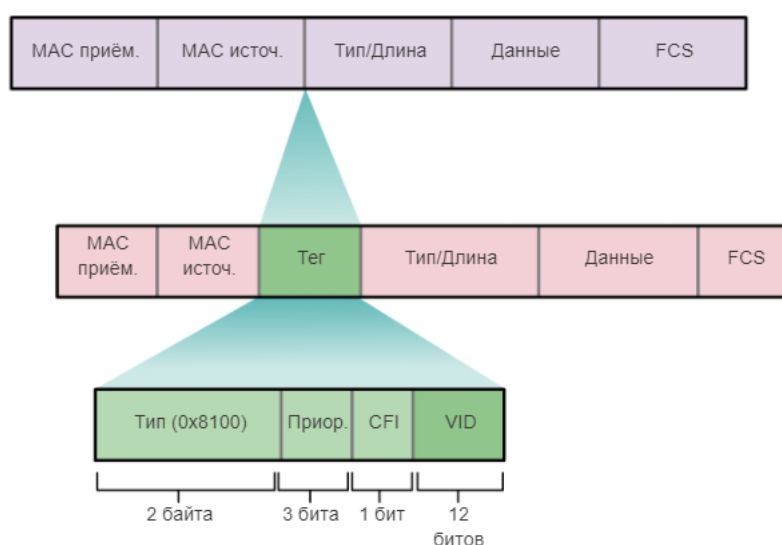
Приоритет пользователя — это 3-битовое значение, которое поддерживает реализацию уровня или сервиса.

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.

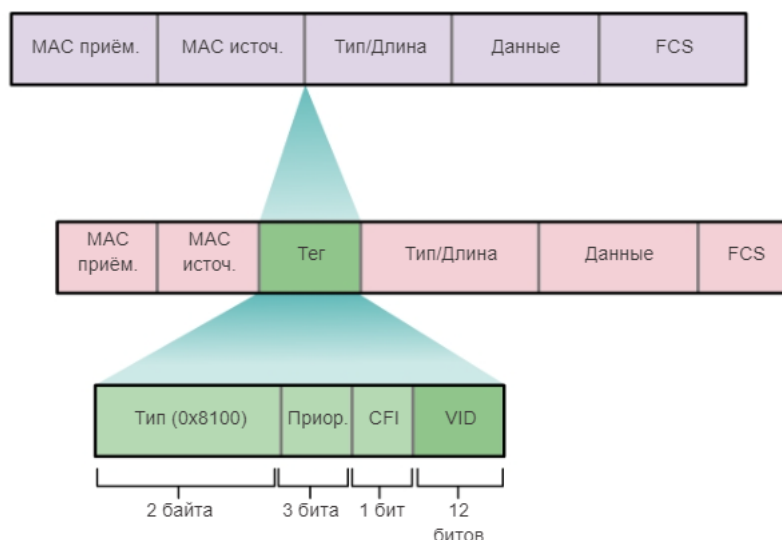
Поля в кадре Ethernet 802.1Q



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.

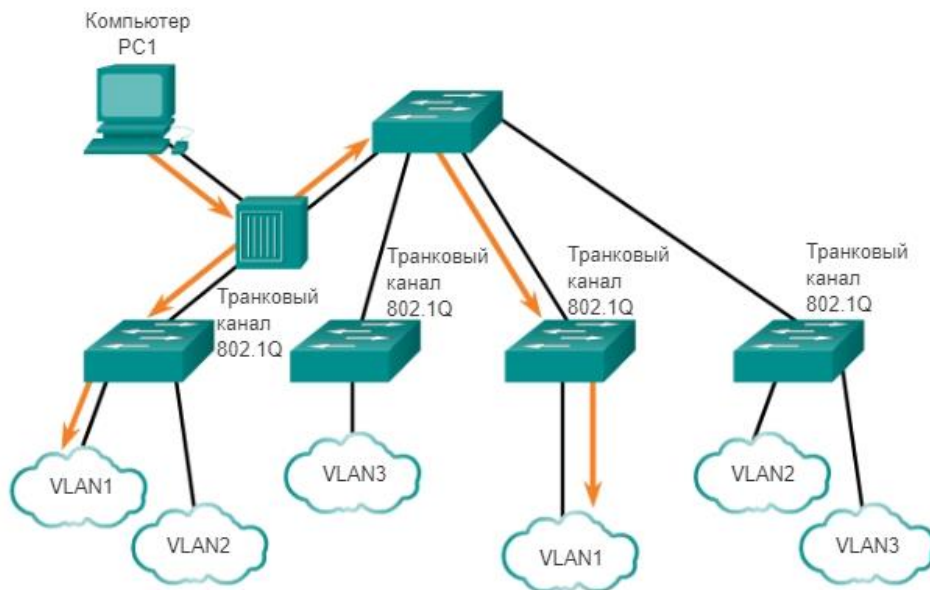
Поля в кадре Ethernet 802.1Q



3.2.5 VLAN с нетегированным трафиком и тегирование по протоколу 802.1Q

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

Сеть native VLAN на транковом канале 802.1Q



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

Тегирование голосовой сети VLAN

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

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

- порт 1 подключается к коммутатору или другому устройству VoIP;

- порт 2 является внутренним интерфейсом 10/100, через который передаётся трафик IP-телефона;
- порт 3 (порт доступа) подключается к ПК или другому устройству.

Тегирование голосовой VLAN



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

- в голосовой VLAN, тегированной значением приоритета класса обслуживания (CoS) уровня 2;
- в VLAN доступа, тегированной значением приоритета CoS уровня 2;
- в нетегированной VLAN доступа (без значения приоритета CoS уровня 2).

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

На рисунке приведён пример выходных данных. В рамках данной темы не рассматриваются команды Cisco IOS голосовой связи, но в выделенных областях в примере выходных данных показан интерфейс F0/18, настроенный

с сетью VLAN для данных (VLAN 20) и сетью VLAN для голосовой связи (VLAN 150).

```
S1# show interfaces fa0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 20 (student)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 150 (voice)
```

Конфигурация VLAN
Диапазоны VLAN на коммутаторах Catalyst

Виртуальные локальные сети стандартного диапазона

Используются в малых и средних сетях предприятий и организаций.

Определяются идентификатором VLAN от 1 до 1005.

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

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

Конфигурации хранятся в файле базы данных VLAN под именем vlan.dat. Файл vlan.dat расположен во флеш-памяти коммутатора.

Протокол VTP (транковый протокол VLAN), помогающий управлять конфигурациями VLAN между коммутаторами, может распознавать и хранить только сети VLAN стандартного диапазона.

```
Switch# show vlan brief
```

| VLAN | Name | Status | Ports |
|------|--------------------|--------|---|
| 1 | default | active | Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gi0/1, Gi0/2 |
| 1002 | fddi-default | | act/unsup |
| 1003 | token-ring-default | | act/unsup |
| 1004 | fddinet-default | | act/unsup |
| 1005 | trnet-default | | act/unsup |

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.

Команды создания VLAN

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

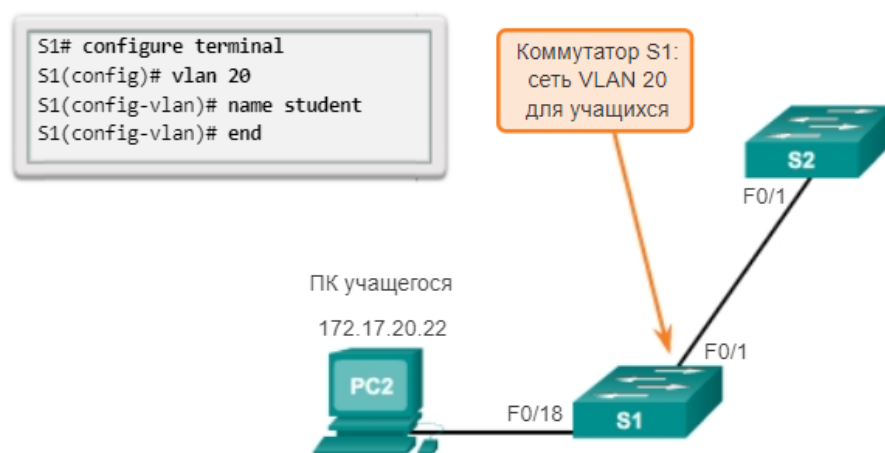
| Задача | Команда IOS |
|---|--|
| Войдите в режим глобальной настройки. | Switch# configure terminal |
| Создайте сеть VLAN с допустимым номером идентификатора. | Switch(config)# vlan vlan-id |
| Укажите уникальное имя для идентификации сети VLAN. | Switch(config-vlan)# name vlan-name |
| Вернитесь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

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

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

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

Пример конфигурации



3.3.3 Команды назначения портов 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 рисунке показан синтаксис для определения порта в качестве порта доступа и назначения его сети VLAN. Выполнять команду **switchport mode access** необязательно, но настоятельно рекомендуется в целях обеспечения безопасности. С помощью этой команды интерфейс переходит в режим постоянного доступа.

Примечание. Используйте команду **interface range**, чтобы одновременно настроить несколько интерфейсов.

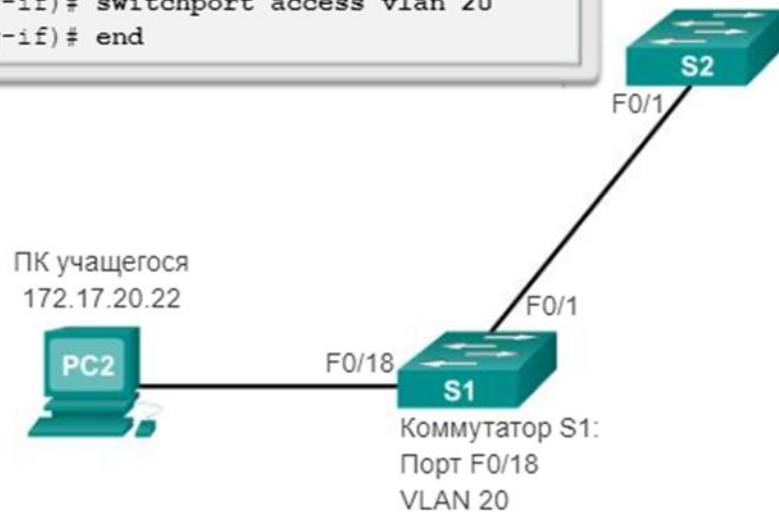
| Задача | Команда |
|--|--|
| Войдите в режим глобальной настройки. | Switch# configure terminal |
| Войдите в режим конфигурации интерфейса. | Switch(config)# interface interface-id |
| Переведите порт в режим доступа. | Switch(config-if)# switchport mode access |
| Назначьте порт сети VLAN. | Switch(config-if)#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

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

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:

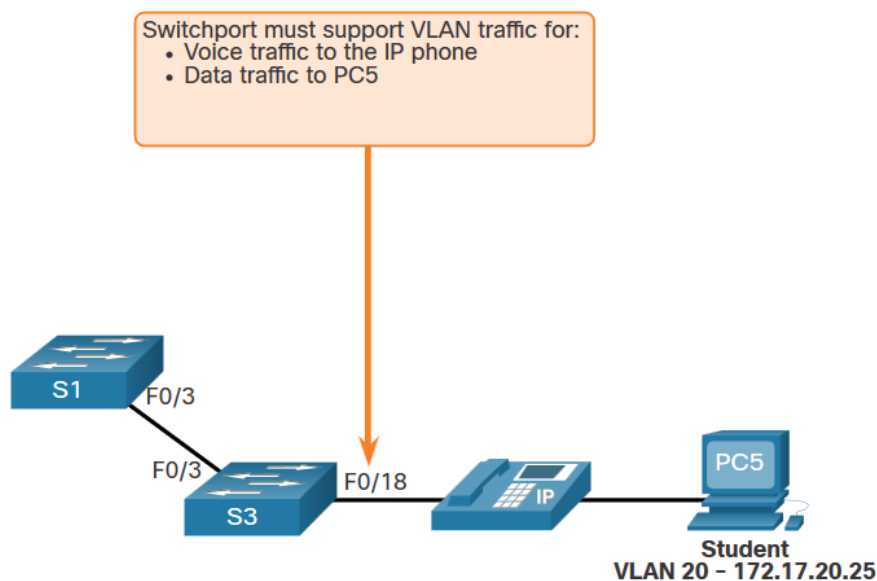
```
% Access VLAN does not exist. Creating vlan 30
```

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



Данные конфигурации VLAN и голосовые VLAN

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



Данные конфигурации VLAN и голосовые VLAN

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

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

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

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

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

Использование команды **show vlan** Полный синтаксис:

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

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

Изменение назначения порта VLAN

Существует несколько способов изменить членство в VLAN:

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

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

```

S1(config)# interface fa0/18
S1(config-if)# no switchport access vlan
S1(config-if)# end
S1#
S1# show vlan brief

```

| VLAN | Name | Status | Ports |
|------|--------------------|-----------|---|
| 1 | default | active | Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gi0/1, Gi0/2 |
| 20 | student | active | |
| 1002 | fddi-default | act/unsup | |
| 1003 | token-ring-default | act/unsup | |
| 1004 | fddinet-default | act/unsup | |
| 1005 | trnet-default | act/unsup | |

```

S1# show interfaces fa0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)

```

Удаление VLAN

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

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

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

Перезагрузите коммутатор после удалении всех VLAN.

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

| | | |
|-----------------------------|------|------|
| Магистрالی | сети | VLAN |
| Команды конфигурации транка | | |

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

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

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

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

Команды конфигурации транка

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

К каждой VLAN относятся следующие подсети:

VLAN 10 - Faculty/Staff - 172.17.10.0/24

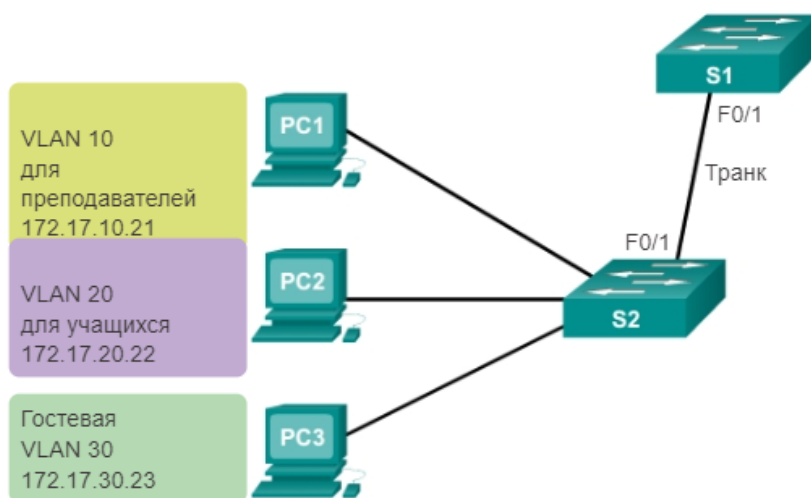
VLAN 20 - Students - 172.17.20.0/24

VLAN 30 - Guests - 172.17.30.0/24

VLAN 99 - Native - 172.17.99.0/24

Порт F0/1 на S1 настроен как магистральный порт.

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



Проверка настроек транка

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

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

```

S1(config)# interface fa0/1
S1(config-if)# switchport mode trunk
S1(config-if)# no switchport trunk native vlan 99
S1(config-if)# end
S1# show interfaces fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (VLAN0099)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
(output omitted)

```

Сброс магистральной в состояние по умолчанию

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

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

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

```
S1# show interfaces fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
(output omitted)
```

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

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# end
S1# show interfaces fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
(output omitted)
```

Протокол динамического транкинга (DTP) Общие сведения о DTP

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

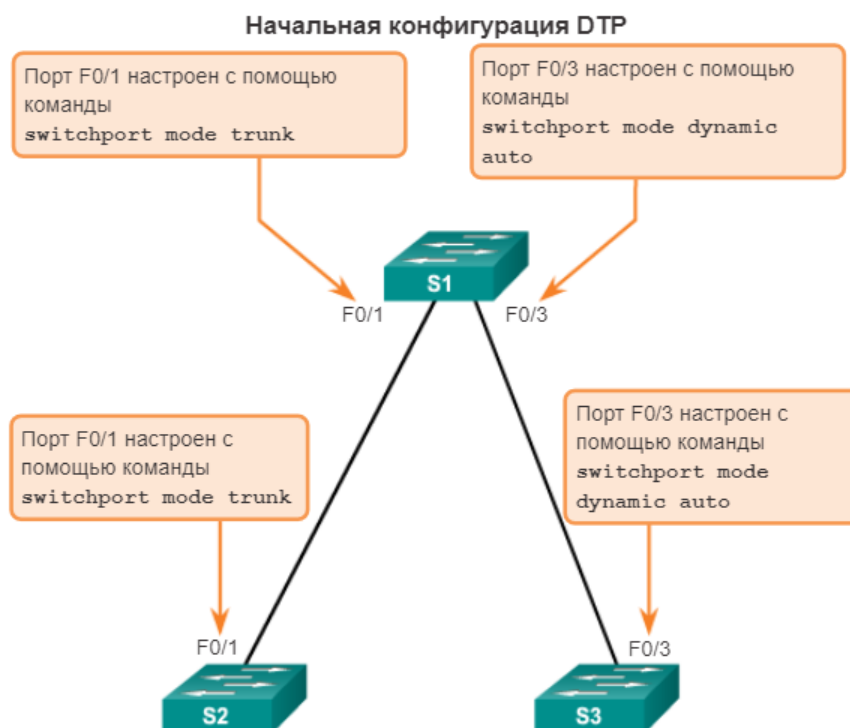
Протокол DTP — это запатентованный протокол Cisco, который автоматически включён на коммутаторах Catalyst 2960 и Catalyst 3560. Коммутаторы других производителей не поддерживают DTP. DTP управляет транковым согласованием только в случае, если порт соседнего коммутатора настроен в режиме транка, который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

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

Общие сведения о DTP

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

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



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

Результаты взаимодействия DTP



Режимы интерфейса для согласования

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

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

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

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

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

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

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

Варианты конфигурации DTP являются следующими:

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

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

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

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

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

4. Концепция маршрутизации

Беспроводные сети обеспечивают мобильность клиента, его способность подключаться к сети из любого места и в любое время, а также возможность перемещения без потери соединения. Беспроводная сеть LAN (WLAN) относится к беспроводным сетям, которые обычно используются в домашних, офисных и корпоративных средах. Хотя беспроводная сеть использует радиочастоты вместо кабелей, она обычно реализована в коммутируемой сети, а формат кадра аналогичен тому, что используется в Ethernet.

Сегодня корпоративные сети развиваются быстрыми темпами, обеспечивая поддержку пользователей, которые постоянно находятся в разъездах. Пользователи могут подключаться, используя различные устройства, включая компьютеры, ноутбуки, планшетные компьютеры и смартфоны. В рамках данной концепции мобильности пользователи могут подключаться к сети, находясь в движении.

Подобную мобильность обеспечивают различные инфраструктуры (проводные сети LAN, сети интернет-провайдеров), однако самой важной составляющей корпоративной среды является беспроводная сеть LAN (WLAN).

Производительность труда больше не ограничивается стационарным рабочим местом или определённым периодом времени. Теперь пользователи рассчитывают на возможность подключения в любое время и из любого места: от офиса до аэропорта или дома. В деловых поездках сотрудникам

приходилось оплачивать телефонную связь между рейсами для проверки сообщений и выполнения нескольких звонков. Теперь сотрудники могут проверять электронную и голосовую почту, а также следить за состоянием проектов со своих смартфонов.

Современные пользователи рассчитывают на возможность повсеместного использования роуминга беспроводной сети. Роуминг обеспечивает доступ беспроводных устройств к Интернету без потери соединения.

Беспроводная связь используется в различных профессиональных областях.

Хотя диапазон беспроводных технологий постоянно расширяется, основным предметом рассмотрения в данном случае являются беспроводные сети, обеспечивающие мобильность пользователей. Беспроводные сети в целом можно разделить на следующие категории:

Беспроводная персональная сеть (WPAN). Радиус действия данной сети составляет несколько метров. В сетях WPAN используются устройства с поддержкой Bluetooth или Wi-Fi Direct.

Беспроводные сети LAN (WLAN). Сети данного типа работают в диапазоне нескольких сотен метров (например, в комнате, в доме, в офисе и даже в сетях комплекса зданий).

Глобальные сети (WWAN). Эти сети действуют в радиусе нескольких километров (например, в муниципальной сети, сети сотовой связи или даже в каналах междугородней связи посредством СВЧ-реле).

Нажмите на компоненты на рисунке, чтобы отобразить дополнительные сведения о различных беспроводных технологиях, поддерживающих подключение устройств к описанным выше беспроводным сетям:

Bluetooth. Изначально является стандартом WPAN IEEE 802.15, который использует процесс сопряжения устройств для обмена данными на расстояниях до 100 метров (0,1 км). Более поздние версии Bluetooth стандартизированы в соответствии с Bluetooth Special Interest Group (<https://www.bluetooth.org/>).

Wi-Fi (wireless fidelity, беспроводная достоверность). Стандарт сетей WLAN IEEE 802.11, обычно развертываемых в целях предоставления доступа к сети для пользователей домашней и корпоративной сети (включая передачу данных, голоса и видео) на расстояниях до 300 м (0,18 мили).

WiMAX (протокол широкополосной радиосвязи). Стандарт сетей WWAN IEEE 802.16, который обеспечивает беспроводной широкополосный доступ на расстояниях до 50 км (30 миль). WiMAX является альтернативой кабельному и широкополосному DSL-подключению. В 2005 году в стандарт WiMax были добавлены мобильные функции, благодаря чему этот стандарт могут использовать операторы связи для предоставления сотового широкополосного доступа.

Сотовый широкополосный доступ. Состоит из нескольких корпоративных, государственных и международных организаций, использующих сотовый доступ к сети оператора связи в целях предоставления широкополосного мобильного подключения к сети. Впервые использован для сотовых телефонов 2-го поколения в 1991 году (2G). В 2001 и 2006 гг. в рамках технологий мобильной связи третьего (3G) и четвертого (4G) поколений стали доступный более высокие скорости.

Спутниковый широкополосный доступ. Предоставляет сетевой доступ к удалённым объектам за счёт использования направленной спутниковой антенны, отрегулированной по геостационарному спутнику (GEO). Как правило, эта технология отличается более высокой стоимостью и к тому же требует обеспечения прямой видимости.

Доступно множество различных типов беспроводных технологий. Однако в этой главе основное внимание уделяется сетям WLAN стандарта 802.11.

Все беспроводные устройства работают в диапазоне радиоволн электромагнитного спектра. За регулирование выделения радиочастотного (РЧ) спектра отвечает Международный союз электросвязи, сектор стандартизации электросвязи (ITU-R). Для различных целей предусмотрены частотные диапазоны, которые называют полосами. Некоторые полосы в электромагнитном спектре жестко регулируются и используются в таких областях, как контроль трафика и сети связи аварийно-спасательных служб. Другие полосы не подлежат лицензированию (например, промышленные, научные и медицинские частотные диапазоны, а также частотные диапазоны национальной информационной инфраструктуры).

Примечание. Сети WLAN работают в диапазоне промышленных, научных и медицинских частотных полос 2,4 ГГц, а также в диапазоне полосы национальной информационной инфраструктуры на частоте 5 ГГц.

Как показано на рисунке, беспроводная связь осуществляется в диапазоне радиоволн (т. е. 3–300 ГГц) электромагнитного спектра. Диапазон радиоволн

разделяется на сектор радиочастот и сектор СВЧ. Обратите внимание, что сети WLAN, Bluetooth, сотовой связи и спутниковой связи работают в диапазонах УВЧ, СВЧ и КВЧ.

Устройства беспроводной сети LAN оснащены передатчиками и приемниками, настроенными на конкретные частоты диапазона радиоволн. В частности, для беспроводных LAN стандарта 802.11 выделяются следующие частотные полосы:

2,4 ГГц (УВЧ): 802.11b/g/n/ad

5 ГГц (СВЧ): 802.11a/n/ac/ad

60 ГГц (КВЧ): 802.11ad

Стандарт сети WLAN IEEE 802.11 определяет, каким образом радиочастоты в нелицензируемых частотных полосах промышленного, научного и медицинского диапазонов используются для физического уровня и подуровня MAC беспроводных каналов.

За прошедшие годы разработан ряд реализаций стандарта IEEE 802.11. Ниже рассмотрим эти стандарты подробнее.

802.11. Разработан в 1997 году, теперь считается устаревшим. Это исходная спецификация сети WLAN, которая работает в частотной полосе 2,4 ГГц и обеспечивает скорости до 2 Мбит/с. На момент создания этого стандарта проводные сети LAN обеспечивали скорости на уровне 10 Мбит/с, поэтому новые беспроводные технологии не получили признания на начальном этапе. Беспроводные устройства оснащены одной антенной для передачи и приема беспроводных сигналов.

IEEE 802.11a. Разработан в 1999 году. Работает в менее загруженной частотной полосе 5 ГГц и обеспечивает скорости до 54 Мбит/с. Поскольку этот стандарт работает на более высоких частотах, он имеет меньшую зону покрытия и менее эффективен внутри зданий. Беспроводные устройства оснащены одной антенной для передачи и приема беспроводных сигналов. Устройства, работающие в соответствии с данным стандартом, несовместимы со стандартами 802.11b и 802.11g.

IEEE 802.11b. Разработан в 1999 году. Работает в частотной полосе 2,4 ГГц и обеспечивает скорости до 11 Мбит/с. Устройства, работающие в соответствии с этими стандартами, имеют больший диапазон и демонстрируют более высокую эффективность при использовании внутри зданий по сравнению с устройствами стандарта 802.11a. Беспроводные устройства оснащены одной антенной для передачи и приема беспроводных сигналов.

IEEE 802.11g. Разработан в 2003 году. Работает в частотной полосе 2,4 ГГц и обеспечивает скорости до 54 Мбит/с. Устройства, работающие в соответствии с этим стандартом, работают с той же радиочастотой и диапазоном, что и устройства со стандартом 802.11b, но имеют пропускную способность стандарта 802.11a. Беспроводные устройства оснащены одной антенной для передачи и приема беспроводных сигналов. Этот стандарт совместим со стандартом 802.11b. Однако при работе с клиентами стандарта 802.11b общая пропускная способность снижается.

IEEE 802.11n. Разработан в 2009 году. Работает в частотных полосах 2,4 ГГц и 5 ГГц, известен как двухполосное устройство. Стандартные скорости передачи данных — 150–600 Мбит/с; диапазон действия — до 70 м. Тем не менее, чтобы обеспечить более высокие скорости, точкам доступа и беспроводным клиентам требуется несколько антенн, использующих технологию многоканального входа — многоканального выхода (MIMO). Технология MIMO использует несколько антенн в качестве передатчика и приемника, что позволяет повысить производительность обмена данными. Технология поддерживает до четырех антенн. Стандарт 802.11n поддерживает обратную совместимость с устройствами 802.11a/b/g. Однако поддержка смешанной среды ограничивает скорость передачи данных.

IEEE 802.11ac. Разработан в 2013 году, работает в частотной полосе 5 ГГц, обеспечивая скорость передачи данных в диапазоне от 450 Мбит/с до 1,3 Гбит/с (1300 Мбит/с). Данный стандарт использует технологию MIMO для повышения производительности обмена данными. Для данного стандарта поддерживается до восьми антенн. Стандарт 802.11ac поддерживает обратную совместимость с устройствами 802.11a/n, но поддержка смешанных сред ограничивает предполагаемую скорость передачи данных.

IEEE 802.11ad. Выпуск запланирован на 2014 год. Этот стандарт также называют WiGig. Он использует решение для трехполосного Wi-Fi, в котором задействованы частотные полосы 2,4 ГГц, 5 ГГц и 60 ГГц. Стандарт теоретически обеспечивает скорость передачи данных до 7 Гбит/с. Тем не менее, полоса 60 ГГц — это технология, для работы которой требуется прямая видимость, следовательно, проходить сквозь стены сигнал не сможет. В роуминге устройства пользователей коммутируются на полосы 2,4 ГГц и 5 ГГц с более низкой частотой. Стандарт поддерживает обратную совместимость с существующими устройствами Wi-Fi. Однако поддержка смешанной среды ограничивает скорость передачи данных.

Данные стандарты обеспечивают совместимость устройств, изготовленных различными производителями. Существуют три международные организации, определяющие стандарты сетей WLAN:

Сектор радиосвязи ITU-R регулирует распределение спектра радиочастот и спутниковых орбит.

IEEE определяет, каким образом радиочастоты модулируются для переноса данных. Эта организация обслуживает стандарты локальных и городских сетей (MAN), относящихся к группе стандартов сетей LAN/MAN IEEE 802. Стандарты 802.3 Ethernet и 802.11 WLAN являются основными в группе стандартов IEEE 802. Хотя IEEE определяет стандарты для устройств радиочастотной модуляции, эта организация не определяет стандарты производства. Следовательно, интерпретации стандартов 802.11 различными поставщиками могут препятствовать совместимости устройств.

Wi-Fi Alliance. Wi-Fi Alliance® (<http://www.wi-fi.org>) является глобальной некоммерческой ассоциацией промышленной торговли, задача которой — способствовать развитию и внедрению сетей WLAN. В эту ассоциацию вошли поставщики, ориентированные на повышение совместимости продуктов стандарта 802.11 путем сертификации поставщиков на соответствие отраслевым нормам и стандартам.

Wi-Fi Alliance сертифицирует сети Wi-Fi и следующие виды совместимости:

Совместимость с IEEE 802.11a/b/g/n/ac/ad

Безопасное использование WPA2™ и расширяемого протокола аутентификации (EAP) в рамках IEEE 802.11i

Функция Wi-Fi Protected Setup (WPS), которая упрощает соединения устройств

Wi-Fi Direct для совместного использования среды устройствами

Wi-Fi Passpoint для обеспечения более простого и безопасного подключения к сети точек доступа Wi-Fi

Wi-Fi Miracast для передачи и отображения видео между устройствами без проблем

Примечание. Доступны также другие продукты сертификации Wi-Fi (например WMM® (Wi-Fi Multimedia™), Tunneled Direct Link Setup (TDLS) и WMM-Power Save.

Сети WLAN имеют такое же происхождение, что и локальные сети Ethernet. IEEE приняла портфель стандартов архитектуры иерархических сетей 802 LAN/MAN. Двумя основными рабочими группами являются 802: 802.3 Ethernet и 802.11 WLAN. Тем не менее, между этими двумя группами есть значительные различия.

На физическом уровне и MAC-подуровне уровня канала передачи данных сети WLAN используют радиочастоты вместо кабелей. Между кабелями и радиочастотами наблюдаются следующие различия:

Радиочастоты не имеют таких ограничений, как, например, кабели, защищенные оболочкой. Поэтому кадры данных могут передаваться по радиочастотным каналам в целях предоставления к ним доступа для всех, кто может принимать радиочастотный сигнал.

Радиочастоты не защищены от внешних сигналов, в то время как кабель защищен экранирующей оболочкой. Радиочастоты функционируют независимо друг от друга в пределах одной географической области, однако при работе на одной и той же или схожей частоте могут возникать помехи.

Передача радиочастот сопряжена с теми же проблемами, которые свойственны любой волновой технологии, например, радио. Например, по мере отдаления радиосигнала от источника, радиостанции могут накладываться друг на друга, что повышает уровень статических помех. В конечном итоге сигнал полностью теряется. В проводных сетях LAN используются кабели соответствующей длины, обеспечивающие надлежащую мощность сигнала.

В различных странах радиочастотные полосы настраиваются по-разному. В отношении использования сетей WLAN действуют дополнительные правила и наборы стандартов, которые не применимы к проводным сетям LAN.

Сети WLAN также имеют следующие отличия от проводных сетей LAN:

Сети WLAN служат для подключения клиентов к сети посредством точки беспроводного доступа (ТД) или беспроводного маршрутизатора, а не посредством коммутатора Ethernet.

Сети WLAN используются для подключения мобильных устройств, которые зачастую работают от аккумулятора в отличие от устройств локальных сетей, подключенных к розетке. Использование беспроводных сетевых адаптеров сокращает время работы мобильного устройства от аккумулятора.

Сети WLAN поддерживают узлы, конкурирующие в доступе к РЧ-носителям (частотным полосам). Стандарт 802.11 предписывает использование технологий предотвращения коллизий (CSMA/CA) вместо технологий обнаружения коллизий (CSMA/CD) для доступа к среде передачи данных, что позволяет эффективно предотвращать коллизии в пределах той или иной среды.

В беспроводных локальных сетях и проводных локальных сетях Ethernet используются разные форматы кадров. Для беспроводных локальных сетей в заголовок кадра 2 уровня необходимо добавить дополнительную информацию.

В отношении сетей WLAN возникает больше проблем, связанных с конфиденциальностью, поскольку радиочастоты могут выходить за пределы объекта.

Для создания простейшей беспроводной сети требуется не менее двух устройств. Каждое из устройств должно содержать радиопередатчик и радиоприемник, настроенные на одинаковые частоты.

Однако для большинства беспроводных развертываний требуются:

Оконечные устройства, оснащённые беспроводными сетевыми адаптерами

Устройство инфраструктуры (например, беспроводной маршрутизатор или точка беспроводного доступа)

Для беспроводного обмена данными оконечным устройствам требуется беспроводной сетевой адаптер со встроенным радиопередатчиком/радиоприемником, а также драйвер, необходимый для работы адаптера. Все современные ноутбуки, планшетные компьютеры и смартфоны оснащены интегрированными беспроводными сетевыми адаптерами. Однако, если в устройстве нет интегрированного беспроводного сетевого адаптера, можно использовать беспроводной USB-адаптер.

Тип устройства инфраструктуры, на котором оконечное устройство выполняет ассоциацию и аутентификацию, варьируется в зависимости от размера и требований сети WLAN.

Например, пользователь домашней сети обычно подключает беспроводные устройства друг к другу с помощью небольшого интегрированного беспроводного маршрутизатора. Такие небольшие маршрутизаторы с интеграцией сервисов выполняют следующие функции:

Точка доступа — предоставляет беспроводной доступ 802.11a/b/g/n/ac.

Коммутатор — предоставляет коммутатор Ethernet 10/100/1000 с четырьмя портами и полнодуплексным режимом для подключения проводных устройств.

Маршрутизатор — предоставляет шлюз по умолчанию для связи с другими сетевыми инфраструктурами.

Например, маршрутизатор Cisco Linksys EA6500, представленный на рис. 1, обычно реализуется в качестве устройства беспроводного доступа к корпоративной сети малого предприятия или домашней сети. Беспроводной маршрутизатор подключается к DSL-модему и объявляет свои службы путем отправки сигналов, содержащих общий идентификатор набора услуг (SSID). Внутренние устройства выполняют беспроводное обнаружение идентификатора маршрутизатора SSID и пытаются выполнить ассоциацию и аутентификацию на маршрутизаторе для получения доступа к сети Интернет.

Предполагаемая нагрузка на маршрутизатор Linksys EA6500 в этой среде достаточно низка. Таким образом, маршрутизатор может управлять обеспечением доступа к сети WLAN, 802.3 Ethernet и подключением к сети интернет-провайдера. Маршрутизатор также предоставляет ряд дополнительных функций, среди которых высокоскоростной доступ, оптимизация для поддержки передачи потокового видео, поддержка IPv6, служба качества обслуживания (QoS), упрощённая установка и настройка с помощью Wi-Fi WPS, USB-порты для подключения принтеров или портативных накопителей.

Кроме того, пользователи домашней сети, которым требуется расширить набор сетевых услуг как в проводной, так и в беспроводной сети, могут воспользоваться беспроводными адаптерами Powerline. С помощью этих адаптеров устройство может напрямую подключиться к сети через розетки электропитания, что идеально подходит для передачи потокового HD-видео и трансляции онлайн-игр. Эти устройства просты в установке: просто подключитесь к розетке электропитания или сетевому фильтру и подключите устройства простым нажатием кнопки.

Организациям, предоставляющим подключение к беспроводной сети для своих пользователей, требуется инфраструктура сети WLAN, обеспечивающая дополнительные возможности подключения.

Примечание. В рамках стандарта IEEE 802.11 беспроводной клиент называется станцией (STA). В данной главе термин «беспроводной клиент» обозначает любое устройство, поддерживающее подключение к беспроводной сети.

Сеть малого предприятия, показанная на рис. 1, является сетью LAN стандарта 802.3 Ethernet LAN. Каждый клиент (например PC1 и PC2) подключается к коммутатору через сетевой кабель. Коммутатор является той точкой, где клиент получает доступ к сети. Обратите внимание, что точка беспроводного доступа также подключена к коммутатору. В этом примере для подключения к беспроводной сети может использоваться точка доступа Cisco WAP4410N или WAP131.

Беспроводные клиенты используют свои беспроводные сетевые адаптеры для обнаружения ближайших точек доступа, объявивших свой идентификатор SSID. После этого клиенты пытаются выполнить ассоциацию и аутентификацию на точке доступа, как показано на рис. 2. После прохождения аутентификации пользователи беспроводной сети получают доступ к ресурсам сети.

Примечание. Небольшие компании предъявляют к ресурсам беспроводной иные требования, нежели крупные компании. Большие беспроводные сети требуют дополнительного беспроводного оборудования в целях упрощения установки и управления беспроводной сетью.

Точки доступа могут быть автономными и управляемыми контроллером.

Автономные точки доступа

Автономные точки доступа, которые иногда называют «тяжелыми», представляют собой автономные устройства, настраиваемые с помощью графического интерфейса пользователя или интерфейса командной строки (CLI) Cisco. Автономные точки доступа рекомендуется использовать в тех случаях, когда в сети требуется не более двух точек доступа. Как вариант, управление несколькими точками доступа может осуществляться посредством служб беспроводного домена (WDS) и CiscoWorks Wireless LAN Solution Engine (WLSE).

Примечание. Домашний маршрутизатор — пример автономной точки доступа, поскольку вся конфигурация точки доступа хранится на устройстве.

Точки доступа, управляемые контроллером

Точки доступа, управляемые контроллером, являются независимыми от сервера устройствами, для которых не требуется начальная настройка. Cisco предлагает два беспроводных решения с использованием контроллера. Точки доступа, управляемые контроллером, рекомендуется использовать в случаях, когда в сети требуется много точек доступа. По мере добавления дополнительных точек доступа настройка и управление каждой из них осуществляется контроллером WLAN автоматически.

Примечание. Некоторые точки доступа могут работать как в автономном режиме, так и в режиме точки доступа, управляемой контроллером.

Для небольших беспроводных сетей Cisco предлагает следующие решения в виде беспроводных автономных точек доступа.

Точка доступа Cisco WAP4410N. Эта точка доступа идеально подходит для небольших компаний, которым требуются две точки доступа и поддержка небольшой группы пользователей.

Точки доступа Cisco WAP121 и WAP321. Эти точки доступа идеально подходят для небольших компаний, которым требуется упростить беспроводную сеть за счёт использования нескольких точек доступа.

Точка доступа Cisco AP541N. Эта точка доступа идеально подходит для небольших и средних компаний, которым требуется надежный и простой в управлении кластер точек доступа.

Примечание. Большинство точек доступа корпоративного уровня поддерживает PoE.

Именно поэтому точки доступа WAP121, WAP321 и AP541N поддерживают кластеризацию точек доступа без использования контроллера. Кластер предоставляет единую точку администрирования и позволяет администратору просматривать развертывание точек доступа как одну беспроводную сеть, а не как набор отдельных беспроводных устройств. Кластеризация позволяет легко осуществлять установку, настройку и управление растущей беспроводной сетью. Несколько точек доступа можно развернуть и настроить с одной конфигурацией на всех устройствах в пределах кластера. При этом управление беспроводной сетью осуществляется как единой системой, и нет необходимости беспокоиться о взаимных помехах между точками доступа или настраивать каждую точку доступа отдельно.

В частности, точки доступа WAP121 и WAP321 поддерживают единую точку настройки (Single Point Setup, SPS), что обеспечивает более быстрое и простое развертывание точки доступа, как показано на рис. 3. SPS позволяет включить для сети LAN возможность масштабирования до четырех точек доступа WAP121 и до восьми точек доступа WAP321, что обеспечивает большее покрытие и поддержку дополнительных пользователей по мере роста и изменения бизнес-требований. Точка доступа Cisco AP541N способна объединить в кластер до 10 точек доступа и поддерживает несколько кластеров.

Существует возможность создания кластера с использованием двух точек доступа. Для этого необходимо соблюдать следующие условия:

На точках доступа включен режим кластеризации.

Точки доступа, входящие в кластер, имеют одно имя кластера.

Точки доступа подключены к одному сегменту сети.

Точки доступа используют один режим радиосвязи (т. е. оба модуля радиосвязи относятся к стандарту 802.11n).

Компании, которым требуется кластеризация нескольких точек доступа, нуждаются в более надежном и масштабируемом решении. Для крупных компаний, использующих большое число точек доступа, Cisco предоставляет управляемые решения на основе контроллера, включая управляемую облачную архитектуру Cisco Meraki и архитектуру беспроводной сети Cisco Unified.

Примечание. Доступны и другие решения на основе контроллера, например, контроллеры, использующие режим Flex. Для получения дополнительных сведений перейдите на веб-сайт <http://www.cisco.com>.

Управляемая облачная архитектура Cisco Meraki

Облачная архитектура Cisco Meraki представляет собой решение для управления, которое позволяет упростить развертывание беспроводной сети. Благодаря этой архитектуре управление точками доступа осуществляется централизованно из контроллера в облаке, как показано на рис. 1. Облачные сети и управление обеспечивают централизованное управление, видимость и контроль без использования дорогостоящих и сложных контроллеров и программного обеспечения для администрирования оверлейной нагрузки.

Этот процесс позволяет сократить затраты и снизить уровень сложности. Контроллер передает настройки управления (например, обновления микропрограммного обеспечения), настройки безопасности, настройки беспроводной сети и идентификатор SSID на точки доступа Meraki.

Примечание. Через облачную инфраструктуру Meraki проходят только потоки управляющих данных. Пользовательский трафик не проходит через центры обработки данных Meraki. Таким образом, если Cisco Meraki не имеет доступа к облаку, сеть продолжает функционировать без сбоев. Это означает, что пользователи могут по-прежнему проходить аутентификацию, действуют правила межсетевого экрана, а потоки трафика передаются на полной линейной скорости. Лишь функции управления перестают работать (например, инструменты создания отчетов и настройки).

Для управляемой облачной архитектуры Cisco Meraki требуются следующие компоненты:

Точки беспроводного доступа под облачным управлением Cisco. Для различных беспроводных сетей существуют различные модели.

Облачный контроллер Meraki (МСС). Контроллер МСС предоставляет для системы беспроводной локальной сети Meraki функции

централизованного управления, оптимизации и мониторинга. МСС — это не устройство, которое нужно приобрести и установить для управления точками беспроводного доступа. МСС, скорее, представляет собой облачный сервис, который постоянно выполняет мониторинг, оптимизацию и создание отчетов о поведении сети.

Веб-панель управления. Веб-панель управления Meraki Dashboard выполняет удалённую настройку и диагностику.

Унифицированная архитектура беспроводной сети Cisco Unified

Решение для архитектуры беспроводной сети Cisco Unified, использующее отдельные MAC-адреса, осуществляет контроль точек доступа с помощью контроллера WLAN (WLC) и также может управляться посредством систем контроля беспроводной сети Cisco Wireless Control Systems (WCS). «Легкие» точки доступа осуществляют обмен данными с контроллером WLAN, используя для этого протокол Lightweight Access Control Point Protocol (LWAPP). Контроллер обладает всеми высокочастотными функциями, необходимыми для обмена данными, а точка доступа является «немой» терминалом, который просто обрабатывает пакеты.

Архитектура беспроводной сети Cisco Unified требует наличия следующих устройств:

«Легкие» точки доступа. Точки беспроводного доступа моделей Cisco Aironet 1600, 2600 и 3600 обеспечивают надежный сетевой доступ для узлов.

Контроллеры для предприятий малого и среднего бизнеса. Беспроводные контроллеры Cisco серии 2500, виртуальный контроллер беспроводной сети Cisco или модуль контроллера беспроводной сети Cisco для Cisco ISR G2 предоставляют возможность развертывания корпоративных сетей WLAN базового уровня для предприятий малого или среднего бизнеса с целью беспроводной передачи данных.

Также доступны другие контроллеры сети WLAN больших производительных возможностей. Например, контроллер беспроводной сети Cisco 5760 и контроллер Cisco серии 8500 разработаны для экономичного управления, обеспечения безопасности и оптимизации производительности масштабируемых беспроводных сетей (например, сетей операторов связи и крупных развертываний в комплексе зданий).

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.

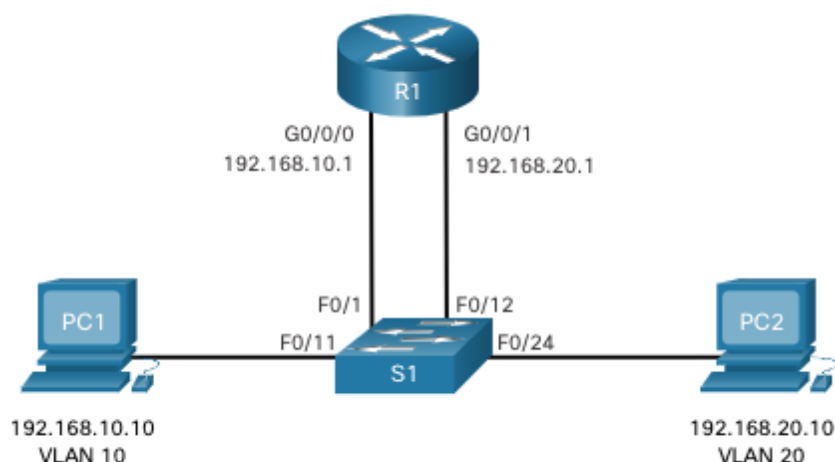
Сеть VLAN — это домен широковещательной рассылки, поэтому компьютеры в разных сетях VLAN не могут обмениваться данными без помощи устройства маршрутизации. Любое устройство, поддерживающее маршрутизацию 3-го уровня, например маршрутизатор или многоуровневый коммутатор, можно использовать для выполнения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

Устаревший метод маршрутизации между сетями VLAN

Первое решение маршрутизации между VLAN основывалось на использовании маршрутизатора с несколькими интерфейсами Ethernet. Каждый интерфейс маршрутизатора был подключен к порту коммутатора в разных VLAN. Интерфейсы маршрутизатора служат шлюзами по умолчанию для локальных узлов в подсети VLAN.

Устаревший метод маршрутизации между VLAN, использующий физические интерфейсы, имеет большие ограничения. Он не является достаточно масштабируемым, поскольку маршрутизаторы имеют ограниченное количество физических интерфейсов. По мере возрастания количества VLAN в сети, требующих по одному физическому интерфейсу на каждую VLAN, количество свободных интерфейсов маршрутизатора быстро уменьшается.

Этот метод маршрутизации между VLAN больше не реализован в коммутируемых сетях и включен только для пояснений.



Маршрутизация между сетями VLAN с помощью метода 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.

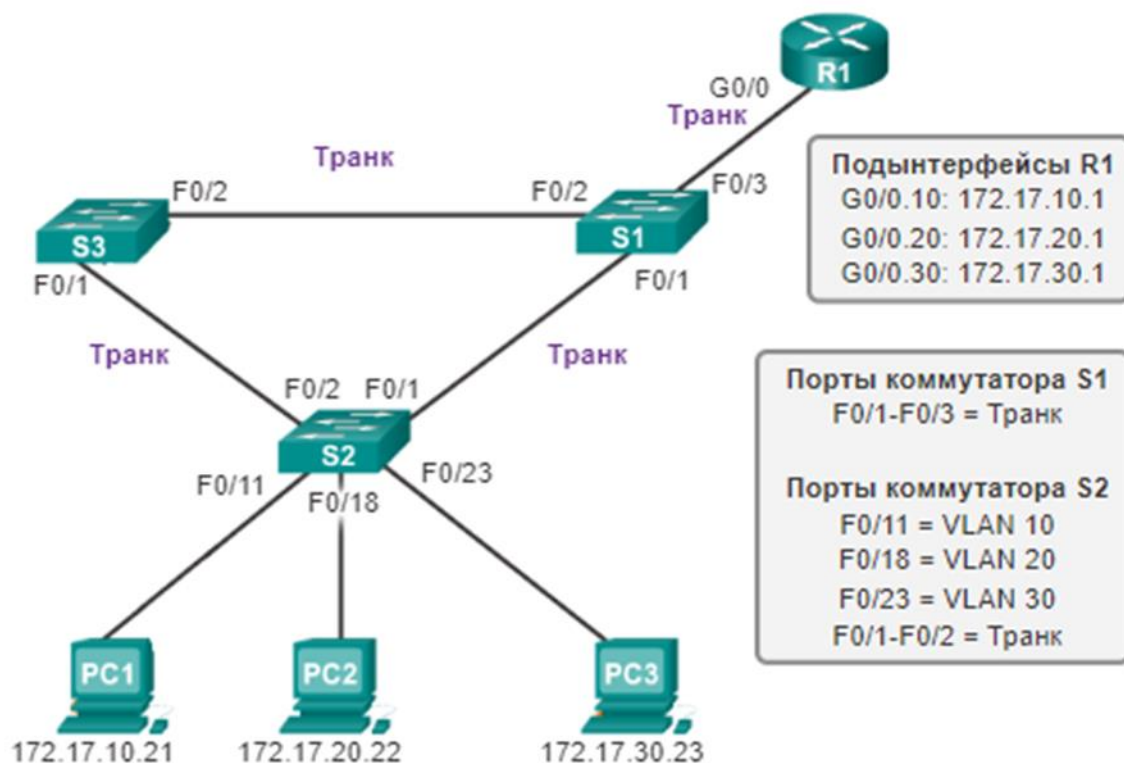
Метод **«router-on-a-stick»** — это такой тип конфигурации маршрутизатора, при котором один физический интерфейс маршрутизирует трафик между несколькими VLAN. Как видно на рисунке, маршрутизатор подключён к коммутатору S1 с помощью одного физического сетевого подключения (транка).

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.

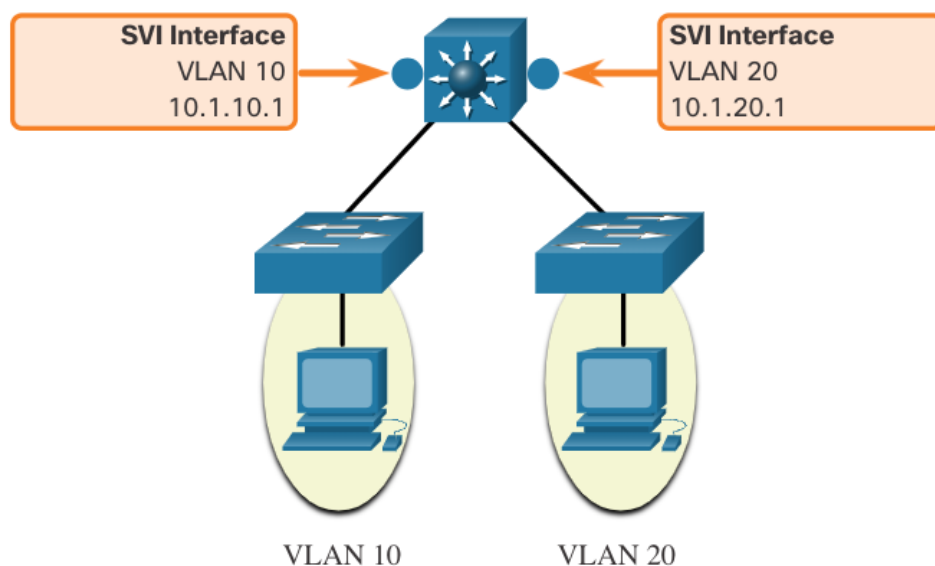
Примечание. Маршрутизация между VLAN с использованием метода router-on-a-stick не масштабируется при работе более 50 сетей VLAN.



Маршрутизация между VLAN на коммутаторе уровня 3

Современный способ выполнения маршрутизации между VLAN заключается в использовании коммутаторов уровня 3 и коммутируемых виртуальных интерфейсов (SVI). Как показано на рисунке, SVI — это виртуальный интерфейс, настраиваемый в многоуровневом коммутаторе.

Примечание. Коммутатор уровня 3 также называется многоуровневым коммутатором, поскольку он работает на уровнях 2 и 3.



SVI Inter-VLAN создаются так же, как и интерфейс VLAN управления. Интерфейс SVI можно создать для любой сети VLAN, существующей на коммутаторе. Несмотря на то, что SVI является виртуальным, он выполняет те же функции для VLAN, что и интерфейс маршрутизатора. В частности, он обеспечивает обработку на уровне 3 для пакетов, которые отправляются на или из всех портов коммутатора, связанных с этой VLAN.

Ниже приведены преимущества использования коммутаторов уровня 3 для маршрутизации между VLAN:

- это более быстрая маршрутизация, чем конфигурация router-on-stick, поскольку и коммутация, и маршрутизация выполняются аппаратно;
- для маршрутизации не требуются внешние каналы от коммутатора к маршрутизатору;
- они не ограничиваются одним каналом, поскольку EtherChannel уровня 2 можно использовать в качестве магистральных каналов между коммутаторами для увеличения пропускной способности;
- задержка намного короче, поскольку для маршрутизации в другую сеть данным не нужно покидать коммутатор;
- они чаще развертываются в локальной сети кампуса, чем маршрутизаторы.

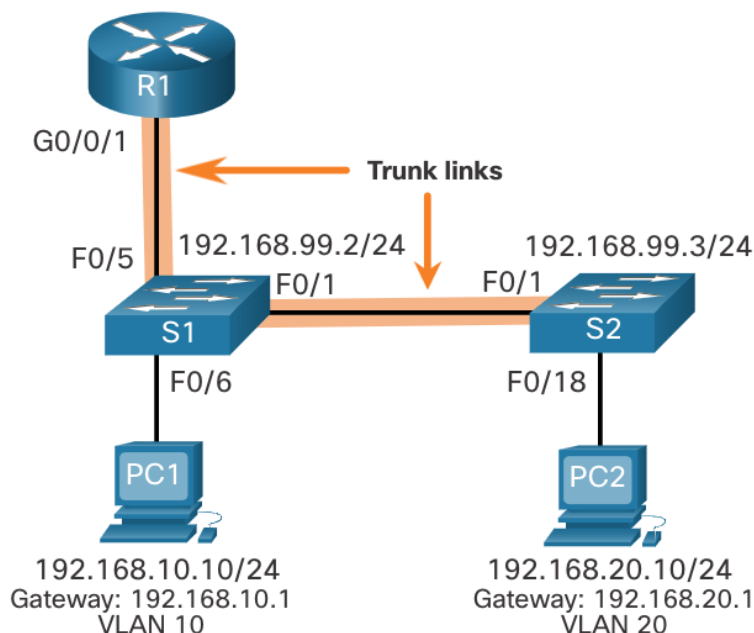
Единственным недостатком является то, что коммутаторы уровня 3 дороже.

Маршрутизация с помощью метода Router-on-a-Stick. Рассмотрение основной топологии

На рисунке интерфейс R1 GigabitEthernet 0/0/1 подключен к порту S1 FastEthernet 0/5. Порт S1 FastEthernet 0/1 подключен к порту S2 FastEthernet 0/1. Это магистральные каналы, которые необходимы для пересылки трафика внутри VLAN и между ними.

Для маршрутизации между VLAN интерфейс R1 GigabitEthernet 0/0/1 логически разделен на три подынтерфейса, как показано в таблице. В таблице также показаны три VLAN, которые будут настроены на коммутаторах.

Предположим, что R1, S1 и S2 имеют начальные базовые конфигурации. В настоящее время PC1 и PC2 не могут выполнять эхо-запрос друг с другом, поскольку они находятся в разных сетях. Только S1 и S2 могут пинговать друг друга, но они недоступны для PC1 или PC2, потому что они также находятся в разных сетях.



| Подынтерфейс | VLAN | IP-адрес |
|--------------|------|-----------------|
| G0/0/1.10 | 10 | 192.168.10.1/24 |
| G0/0/1.20 | 20 | 192.168.20.1/24 |
| G0/0/1.30 | 99 | 192.168.99.1/24 |

4.2.1 Рассмотрение основной топологии

Чтобы устройства могли выполнять эхо-запрос друг с другом, коммутаторы должны быть настроены с помощью VLAN и магистрали, а маршрутизатор должен быть настроен для маршрутизации между VLAN.

Выполните следующие шаги для настройки S1 с VLAN и транковым каналом:

Шаг 1. Создайте сети VLAN и присвойте им имена.

Шаг 2. Создайте интерфейс управления.

Шаг 3. Настройка портов доступа

Шаг 4. Настройте транковые порты.

Настройка на R1 подынтерфейсов

Для использования метода Router-on-a-Stick требуется настроить подынтерфейсы для каждой маршрутизируемой сети VLAN. Подынтерфейс создается с помощью команды режима глобальной конфигурации **interface interface_id.subinterface_id**. Синтаксис для подынтерфейсов следующий: сначала указывается физический интерфейс, в данном случае g0/0, затем точка и номер подынтерфейса. Хотя это не требуется, обычно сопоставляют номер подынтерфейса с номером VLAN.

Затем каждый субинтерфейс настраивается с помощью следующих двух команд:

encapsulation dot1q vlan_id [native] - эта команда настраивает подынтерфейс для соответствия на инкапсулированный трафик 802.1Q из указанного идентификатора **vlan-id**. Параметр **native** ключевого слова добавляется только для установки собственной VLAN на что-то отличное от VLAN 1.

ip address ваш ip-address subnet-mask - эта команда настраивает IPv4-адрес подынтерфейса. Этот адрес обычно служит шлюзом по умолчанию для идентифицированных VLAN.

Повторите процесс для каждой маршрутизируемой VLAN. Для осуществления маршрутизации каждому подынтерфейсу маршрутизатора необходимо назначить IP-адрес в своей подсети. Наконец, включите виртуальный интерфейс с помощью команды конфигурации интерфейса **no shutdown**. Если отключить физический интерфейс, то все подчиненные интерфейсы также отключаются.

5. Принципы STP

Назначение протокола STP. Избыточность в коммутируемых сетях уровня 2

Трехуровневая иерархическая модель сети, которая использует уровни ядра, распределения и доступа с избыточностью, призвана устранить единую точку отказа в сети. Использование нескольких физически подключенных каналов между коммутаторами обеспечивает физическую избыточность в коммутируемой сети. Это повышает надёжность и доступность сети. Наличие альтернативных физических каналов для передачи данных по сети позволяет пользователям получить доступ к сетевым ресурсам даже в случае сбоя одного из каналов.

Для многих организаций доступность сети является важнейшим фактором обеспечения соответствия требованиям бизнеса. Таким образом, модель инфраструктуры сети является критически важным для бизнеса компонентом. Избыточность маршрута предоставляет решение, обеспечивающее необходимую доступность нескольких сетевых служб за счёт устранения потенциальной единой точки отказа.

Примечание. Избыточность на 1 уровне модели OSI демонстрируется с использованием нескольких каналов и устройств, однако для настройки сети требуется нечто большее, чем просто физическое планирование. Для систематической работы избыточности также необходимо использовать протоколы 2 уровня OSI (например STP).

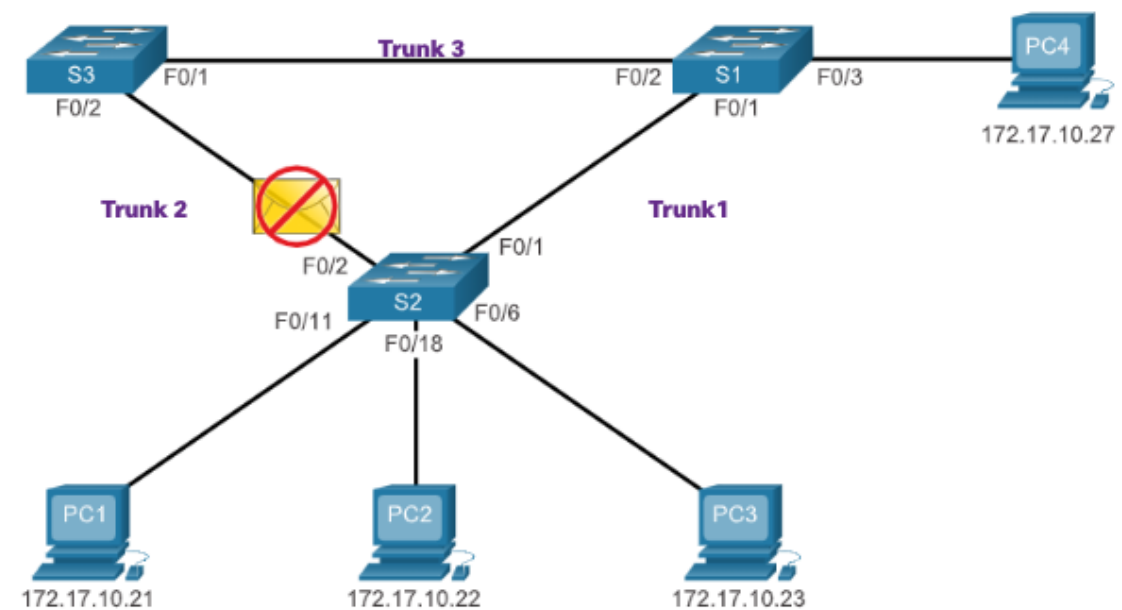
Важной частью иерархической архитектуры является избыточность, использование которой позволяет предотвратить перебои в обслуживании конечных пользователей. Для работы избыточных сетей требуются физические маршруты, однако и логическая избыточность также должна быть частью архитектуры. Тем не менее, избыточные маршруты в коммутируемой сети Ethernet могут привести к возникновению физических и логических петель 2 уровня.

Вследствие работы коммутаторов, особенно в процессе получения данных и пересылки, могут возникать логические петли 2 уровня. При наличии нескольких путей между двумя устройствами и отсутствии реализации протокола spanning-tree возникает петля 2 уровня. Как показано на рис. 2, петля 2 уровня, как правило, приводит к трем проблемам.

Spanning Tree Protocol

Протокол связующего дерева (STP) - это сетевой протокол предотвращения петель, который обеспечивает избыточность при создании топологии уровня 2 без петель.

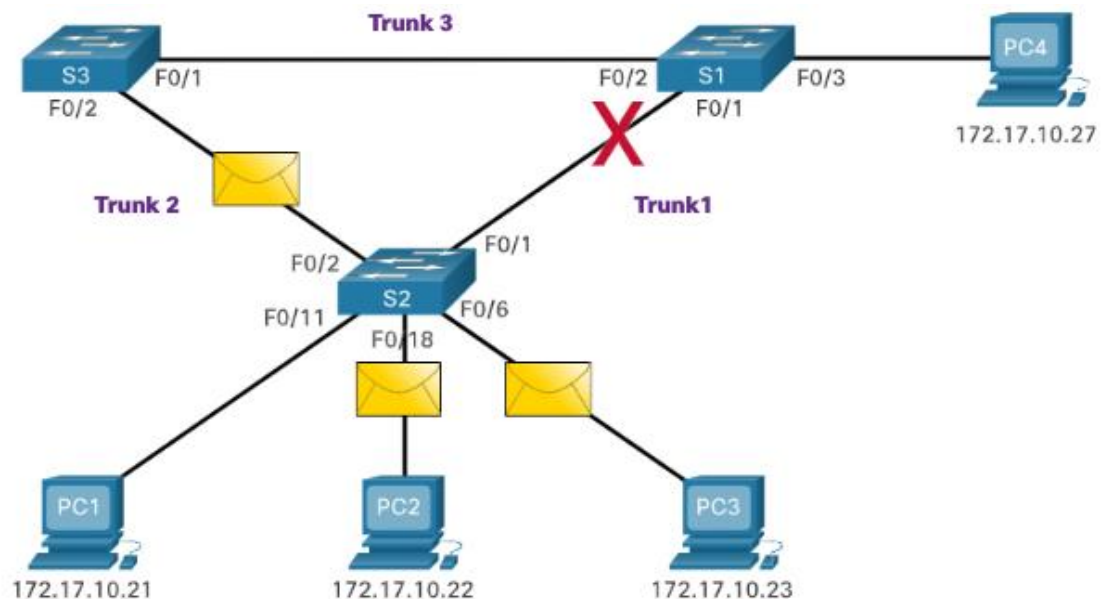
STP логически блокирует физические петли в сети уровня 2, предотвращая бесконечное хождение кадров в сети.



S2 drops the frame because it received it on a blocked port.

Пересчет STP

STP компенсирует сбой в сети путем перерасчета и открытия ранее заблокированных портов.



Пересчет STP

Резервирование путей обеспечивает необходимую доступность множества сетевых сервисов, устраняя вероятность перебоев в работе всех сетевых служб в случае отказа в отдельной точке. При наличии нескольких путей между двумя устройствами и отсутствии реализации протокола spanning-tree возникает петля 2-го уровня. Петли уровня 2 могут привести к нестабильности таблицы MAC-адресов, перегрузке каналов и высокой

загрузке ЦП на коммутаторах и конечных устройствах, в результате чего сеть становится непригодной для использования.

Уровень 2 Ethernet не включает в себя механизм распознавания и устранения бесконечно зацикливающихся кадров. Некоторые протоколы 3-го уровня используют механизмы времени жизни (TTL), которые ограничивают количество попыток повторной передачи пакетов сетевыми устройствами 3-го уровня. Маршрутизатор уменьшит TTL (Time to Live) в каждом пакете IPv4 и поле Hop Limit в каждом пакете IPv6. Когда эти поля уменьшатся до 0, маршрутизатор отбрасывает пакет. Коммутаторы Ethernet и протокол Ethernet не имеют сопоставимого механизма, когда коммутатор передает кадр уровня 2. STP был разработан специально в качестве механизма предотвращения петли для Ethernet уровня 2.

Петли уровня 2

Без включения STP петли уровня 2 могут сформироваться, что приводит к бесконечному циклу широковещательных, многоадресных и неизвестных одноадресных кадров. Это может быстро разрушить сеть.

При появлении петли возникает возможность постоянного изменения таблицы MAC-адресов на коммутаторе обновлениями из кадров широковещательной рассылки, что приводит к нестабильности базы данных MAC-адресов. Это может привести к высокой загрузке ЦП, что приводит коммутатор в нерабочее состояние.

Неизвестный одноадресный кадр с коммутатора формируется, когда у коммутатора нет MAC-адреса назначения в таблице MAC-адресов, и он должен переслать этот кадр со всех своих портов, за исключением входного порта.

Широковещательный шторм

Широковещательный шторм - это ненормально большое количество широковещательных передач, подавляющих сеть в течение определенного периода времени. Широковещательные штормы могут отключить сеть за считанные секунды, перегружая коммутаторы и конечные устройства. Широковещательные штормы могут быть вызваны аппаратными проблемами, такими как неисправный сетевой адаптер или петля 2-го уровня в сети.

Широковещательные рассылки уровня 2 в сети, такие как ARP-запросы, очень распространены. Многоадресные рассылки второго уровня обычно пересылаются так же, как и широковещательные рассылки коммутатором. Пакеты IPv6 никогда не пересылаются как широковещательная рассылка

уровня 2, ICMPv6 Neighbor Discovery использует многоадресную рассылку уровня 2.

Узел, участвующий в сетевой петле, недоступен для других узлов в сети. Кроме того, вследствие постоянных изменений в таблице MAC-адресов коммутатор не знает, из какого порта следует пересылать кадры одноадресной рассылки.

Во избежание подобных проблем в сети с избыточностью, на коммутаторах должны быть включены определённые типы протокола spanning-tree. Протокол spanning-tree по умолчанию включен на коммутаторах Cisco, предотвращая, таким образом, возникновение петель 2-го уровня.

Алгоритм STP

Протокол STP основан на алгоритме, изобретенном Радией Перлман (Radia Perlman) во время ее работы в Digital Equipment Corporation и опубликованном в статье 1985 г. «Алгоритм распределенного вычисления протокола связующего дерева в расширенной сети LAN» (An Algorithm for Distributed Computation of a Spanning Tree in an Extended LAN). Ее алгоритм связующего дерева (STA) создает топологию без петли, выбрав один корневой мост, где все остальные коммутаторы определяют один путь с наименьшей стоимостью.

Протокол STP предотвращает возникновение петель за счет настройки беспетлевого пути в сети с использованием портов, стратегически настроенных на заблокированное состояние. Коммутаторы, использующие протокол STP, могут компенсировать сбой за счет динамической разблокировки ранее заблокированных портов и разрешения передачи трафика по альтернативным путям.

Как STA создает топологию без петли?

Выбор корневого моста: этот мост (коммутатор) является опорной точкой для всей сети для построения STP.

Блокирование резервных путей: протокол STP обеспечивает наличие только одного логического пути между всеми узлами назначения в сети путем намеренного блокирования резервных путей, которые могли бы вызвать петлю. Порт считается заблокированным, когда заблокирована отправка и прием данных на этот порт.

Создание топологии без петли: заблокированный порт приводит к тому, что этот канал не пересылает кадры между двумя коммутаторами. Это создает топологию, в которой каждый коммутатор имеет только один путь к

корневому мосту, аналогично ветвям дерева, которые подключаются к корню дерева.

Пересчет в случае сбоя соединения: физические пути по-прежнему используются для обеспечения избыточности, однако эти пути отключены в целях предотвращения петель. Если путь потребуется для компенсации неисправности сетевого кабеля или коммутатора, протокол STP повторно рассчитывает пути и снимает блокировку с требуемых портов, чтобы разрешить активацию избыточного пути. Перерасчет STP также может происходить в любой момент, когда новый коммутатор или новый межкоммутационный канал добавляется в сеть.

| | | |
|-------------------------------|--------|-----|
| Принципы | работы | STP |
| Шаги к без петлевой топологии | | |

Используя STA, STP строит топологию без петель в четырехэтапном процессе:

1. Выбор корневого моста.
2. Выбор корневых портов.
3. Выбор назначенных портов.
4. Выбор альтернативных (заблокированных) портов.

При работе STA и STP коммутаторы используют блоки данных протокола моста (**BPDU**) для обмена информацией о себе и своих каналах. BPDU используются для выбора корневого моста, корневых портов, назначенных портов и альтернативных портов.

Каждый BPDU содержит идентификатор **VID**, который определяет коммутатор, отправивший BPDU. VID участвует в принятии многих решений STA, включая роли корневого моста и портов.

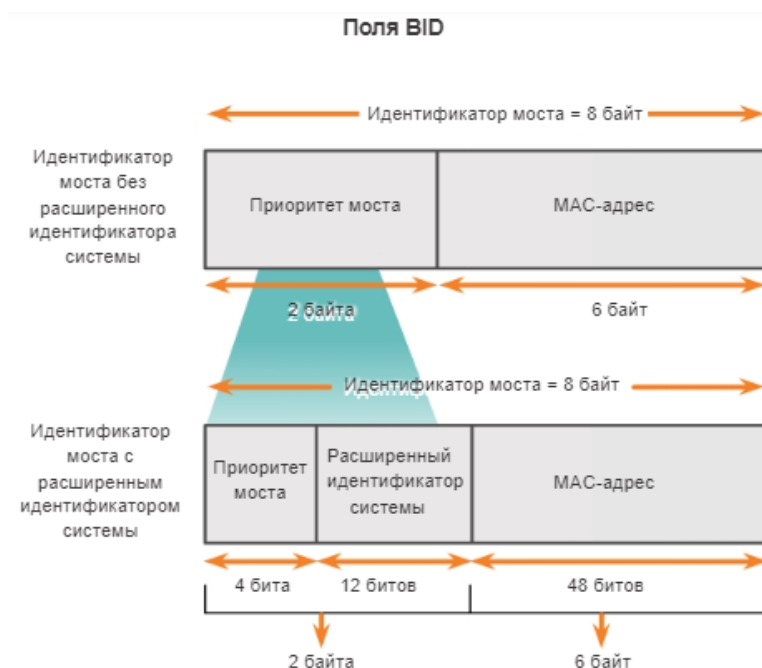
Идентификатор VID содержит значение приоритета, MAC-адрес отправляющего коммутатора и дополнительный расширенный идентификатор системы. Самое низкое значение VID определяется комбинацией значений в этих трех полях.

Приоритет моста: значение приоритета по умолчанию для всех коммутаторов Cisco равно десятичному значению 32768. Значения варьируются в диапазоне от 0 до 61440 с шагом в 4096. Предпочтительнее более низкий приоритет моста. Приоритет моста 0 имеет преимущество по сравнению со всеми остальными значениями приоритета моста.

Значение **расширенного идентификатора системы** — это десятичное значение, добавляемое к значению приоритета моста в BID для определения приоритета и сети VLAN кадра BPDU.

MAC-адрес: Если два коммутатора настроены с одинаковым приоритетом, и у них одинаковый расширенный идентификатор системы, то коммутатор с наименьшим значением MAC-адреса, выраженным в шестнадцатеричном формате, получит меньший идентификатор BID.

5.2.1 Шаги к без петельной топологии

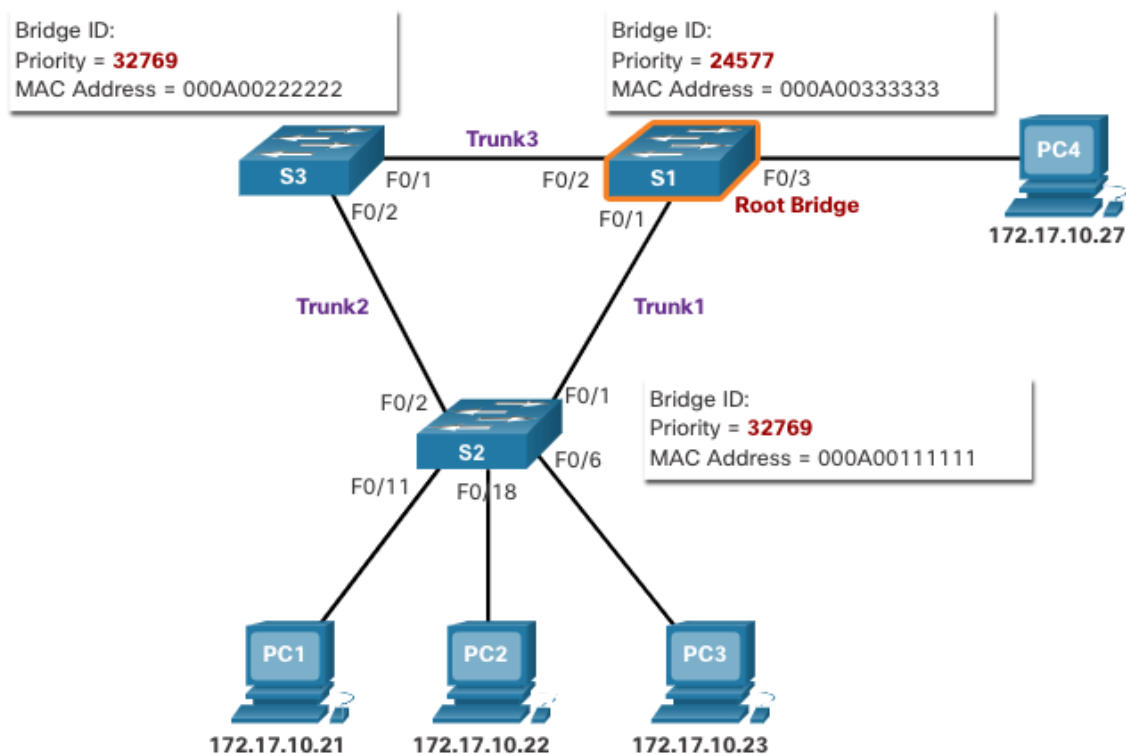


Выбор корневого моста

STA назначает один из коммутаторов в качестве корневого моста и использует его как точку привязки для расчёта всех путей. Коммутаторы обмениваются BPDU для создания безпетельной топологии, начиная с выбора корневого моста.

Все коммутаторы в домене широковещательной рассылки участвуют в процессе выбора. После загрузки коммутатора они начинают рассылать кадры BPDU с интервалом в две секунды. Эти кадры BPDU содержат BID передающего коммутатора и BID корневого моста, известный как Root ID.

Коммутатор с самым низким значением идентификатора моста (BID) становится корневым мостом. Сначала все коммутаторы объявляют себя корневым мостом с собственным BID, установленным в качестве корневого идентификатора. В конце концов коммутаторы узнают через обмен BPDU, какой коммутатор имеет самый низкий BID, и далее будет выбран один корневой мост.



Влияние BID по умолчанию

Поскольку значение BID по умолчанию равно 32768, два или более коммутаторов могут иметь одинаковый приоритет. В этом сценарии, где приоритеты одинаковы, коммутатор с самым низким MAC-адресом станет корневым мостом. Администратор должен настроить требуемый коммутатор в качестве корневого моста с более низким приоритетом.

MAC-адрес становится решающим фактором в отношении того, какой коммутатор становится корневым мостом. MAC-адрес с самым низким шестнадцатеричным значением считается предпочтительным корневым мостом. В этом примере S2 имеет наименьшее значение MAC-адреса и, следовательно, назначается корневым мостом для этого экземпляра протокола spanning-tree.

Примечание: для всех коммутаторов используется значение 32769. Это значение основано на значении приоритета по умолчанию 32768 и назначении сети VLAN 1, связанном с каждым из коммутаторов (32768+1).

Определение стоимости корневого пути

Если корневой мост выбран для экземпляра протокола spanning-tree, STA начинает процесс определения оптимальных путей к корневому мосту от всех некорневых коммутаторов в домене широковещательной рассылки. Информация о пути, известная как стоимость внутреннего корневого пути,

равна сумме стоимости отдельных портов на пути от коммутатора к корневому мосту.

Когда коммутатор получает блок BPDU, он добавляет стоимость входного порта сегмента для определения своей стоимости для внутреннего корневого пути.

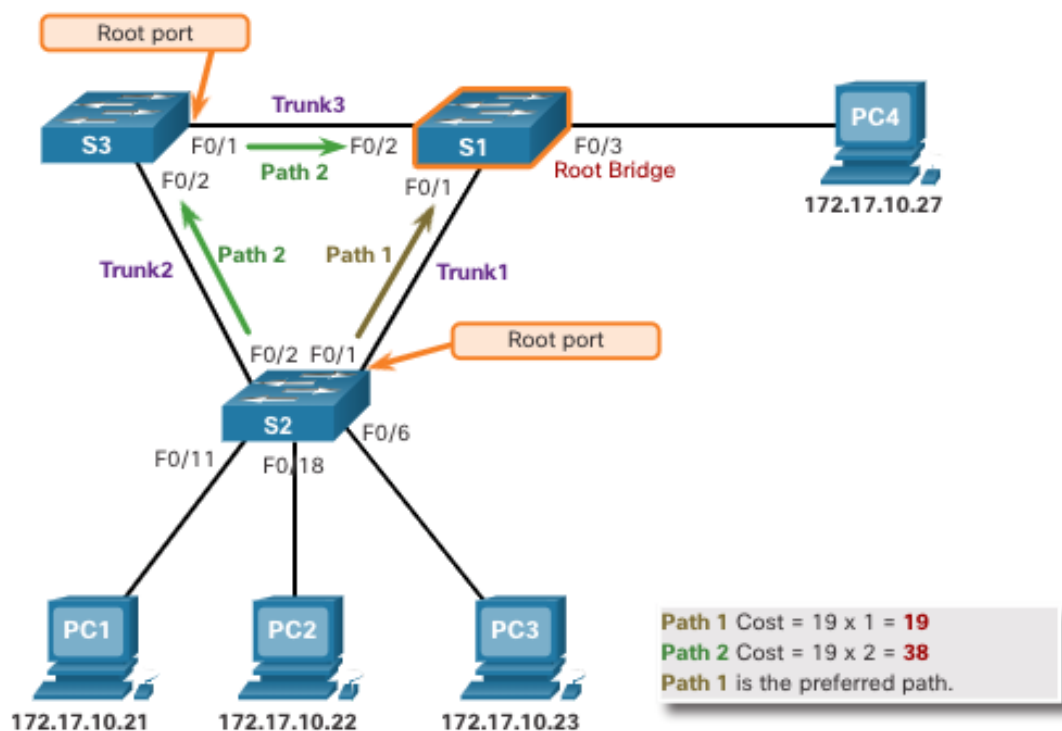
Стоимость портов по умолчанию определяется скоростью работы порта. В таблице показаны стоимости портов по умолчанию, предложенные IEEE. Коммутаторы Cisco по умолчанию используют значения, определенные стандартом IEEE 802.1D, также известные как стоимость наименьшего пути, как для STP, так и для RSTP.

Хотя с портами коммутатора связано значение стоимости пути по умолчанию, значение стоимости порта можно настроить. Возможность настройки отдельных портов предоставляет администратору необходимую гибкость при контроле путей протокола spanning-tree к корневому мосту.

Выбор корневых портов

После определения корневого моста для выбора корневого порта используется алгоритм STA. Каждый некорневой коммутатор выбирает один корневой порт. **Корневые порты** — порты коммутатора, ближайшие к корневому мосту с точки зрения общей стоимости маршрута к нему. Эта общая стоимость известна как стоимость пути до корневого моста.

Стоимость внутреннего корневого пути равна сумме стоимостей путей от всех портов к корневому мосту, как показано на рисунке. Пути с наименьшей стоимостью становятся предпочтительными, а все остальные избыточные пути блокируются. В этом примере стоимость внутреннего корневого пути от S2 до корневого моста S1 по пути 1 равна 19, а стоимость внутреннего корневого пути для пути 2 равна 38. Поскольку общая стоимость пути 1 к корневому мосту ниже, именно этот путь является предпочтительным.



Принципы работы RSTP

Протокол RSTP (802.1w) заменяет собой исходный стандарт 802.1D, поддерживая при этом функции обратной совместимости. Терминология, относящаяся к STP 802.1w, остается в основном той же, что и для исходного стандарта STP IEEE 802.1D. Большинство параметров остались без изменений. Пользователи, знакомые с исходным стандартом STP, могут легко настроить RSTP. Один и тот же алгоритм связующего дерева используется для STP и RSTP для определения ролей портов и топологии.

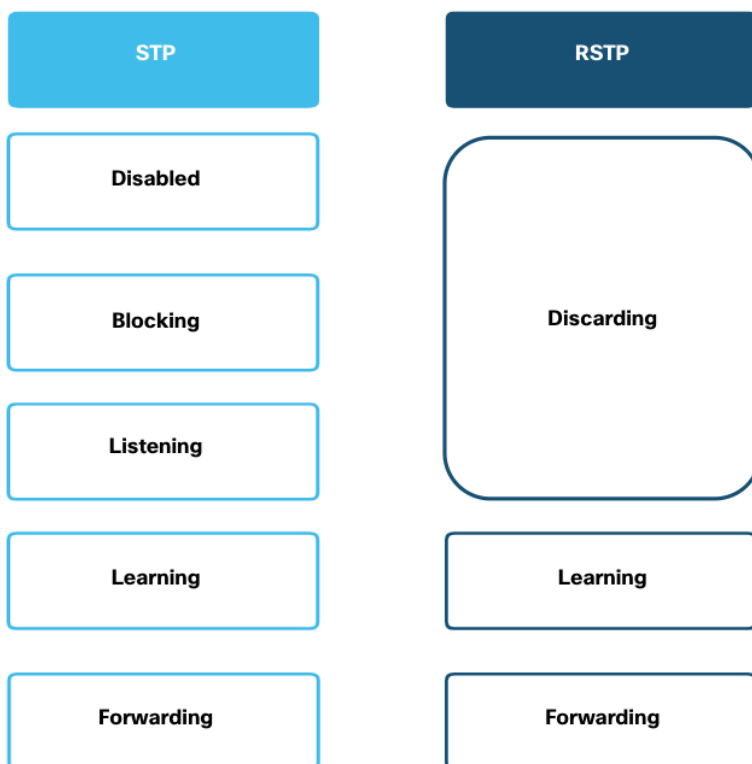
Протокол RSTP ускоряет повторный расчёт протокола spanning-tree в случае изменения топологии сети 2-го уровня. В правильно настроенной сети RSTP может достичь состояния сходимости гораздо быстрее, иногда всего за несколько сот миллисекунд. Если порт настроен альтернативным или резервным, он может немедленно перейти в состояние пересылки без ожидания сходимости сети.

Примечание: Rapid PVST+ представляет собой реализацию RSTP Cisco на основе отдельных VLAN. Для каждой VLAN запускается независимый экземпляр RSTP.

RSTP состояния и роли портов

Существует только три состояния порта, которые соответствуют трем возможным рабочим состояниям STP.

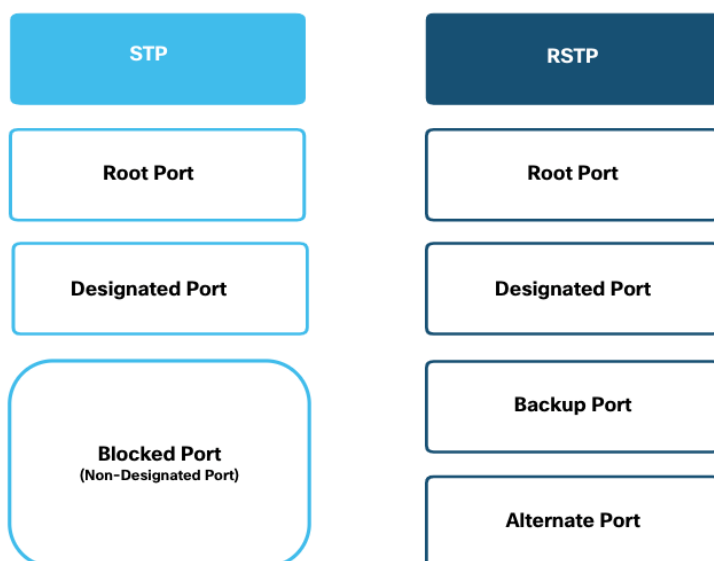
Состояние отключения, блокировки и прослушивания 802.1D объединяются в уникальное состояние отказа 802.1w.



RSTP состояния и роли портов

Корневые порты и назначенные порты одинаковы для STP и RSTP. Тем не менее существует две роли порта RSTP, которые соответствуют состоянию блокировки STP.

В STP заблокированный порт определяется как не являющийся назначенным или корневым портом. Для этой цели RSTP имеет две роли портов.



Rapid rvst+

На рисунке показаны примеры портов, отличных от граничных.

Примечание. Не рекомендуется настраивать граничные порты, которые будут соединены с другим коммутатором. Это может иметь негативные последствия для RSTP, поскольку появляется вероятность возникновения временной петли, приводящей к задержке схождения RSTP.



PortFast и BPDU Guard

Когда устройство подключено к порту коммутатора или когда коммутатор включается, порт коммутатора проходит как прослушивание, так и обучение, каждый раз ожидая истечения срока действия таймера задержки. Эта задержка составляет 15 секунд для каждого состояния и в общей сложности – 30 секунд. Это может вызвать проблему для DHCP-клиентов, пытающихся обнаружить DHCP-сервер, поскольку процесс DHCP займет больше этого времени ожидания. В результате клиент IPv4 не получит действительный адрес IPv4.

Когда порт коммутатора настроен с помощью **PortFast**, этот порт переходит из состояния блокировки в состояние пересылки немедленно, избегая 30-секундной задержки. Можно использовать PortFast для портов доступа, чтобы устройства, подключенные к этим портам, могли немедленно получить доступ к сети. PortFast следует использовать только для портов доступа. Если функция PortFast включена на порте, подключенном к другому коммутатору, появится риск возникновения петли протокола spanning-tree.

Порт коммутатора с включенной функцией PortFast никогда не должен получать BPDU, поскольку это указывает на то, что коммутатор подключен к порту, что может вызвать петлю. Коммутаторы Cisco поддерживают функцию **BPDU guard**. Когда функция BPDU guard включена, при получении блока BPDU она переводит порт в состояние errdisabled (error-disabled — отключение из-за ошибки). Это защищает от потенциальных петель, эффективно отключая порт. Администратор должен вручную вернуть интерфейс в эксплуатацию.

Альтернативы STP

С годами организациям требовалась повышенная отказоустойчивость и доступность локальной сети. Сети Ethernet перешли от нескольких взаимосвязанных коммутаторов, подключенных к одному маршрутизатору, к сложной иерархической структуре сети, включающей коммутаторы доступа, распределения и уровня ядра.

В зависимости от реализации уровень 2 может включать не только уровень доступа, но и распределение или даже уровни ядра. Эти топологии могут включать сотни коммутаторов с сотнями или даже тысячами VLAN. STP адаптировалась к дополнительной избыточности и сложности благодаря усовершенствованиям, как часть RSTP и MSTP.

Важным аспектом проектирования сети является быстрая и предсказуемая сходимость при сбое или изменении топологии. Связующее дерево не обеспечивает такую же эффективность и предсказуемость, которая обеспечивается протоколами маршрутизации на уровне 3.

Маршрутизация уровня 3 позволяет создавать избыточные пути и петли в топологии без блокировки портов. По этой причине некоторые среды переходят на уровень 3 везде, за исключением тех случаев, когда устройства подключаются к коммутатору уровня доступа. Другими словами, соединения между коммутаторами уровня доступа и коммутаторами распределения будут иметь уровень 3, а не уровень 2.

Проблемы настройки STP

Для анализа топологии STP выполните следующие действия:

Шаг 1. Обнаружение топологии 2 уровня. Используйте сетевую документацию (если есть) или команду **show cdp neighbors** для обнаружения топологии 2 уровня.

Шаг 2. После обнаружения топологии 2 уровня используйте сведения об STP для определения ожидаемого пути 2 уровня. Необходимо знать, какой коммутатор является корневым мостом.

Шаг 3. Чтобы определить, какой коммутатор является корневым мостом, используйте команду **show spanning-tree vlan**.

Шаг 4. Используйте команду **show spanning-tree vlan** для всех коммутаторов, чтобы выяснить, какие порты находятся в состоянии блокировки или пересылки и подтвердить ожидаемый путь 2 уровня.

6. ETHERCHANNEL

EtherChannel (EC) представляет собой метод агрегирования портов, при котором до восьми Ethernet-адаптеров определяются как один EtherChannel. Удаленные системы видят EtherChannel как один IP- и MAC-адрес, в результате при использовании одной сети пропускная способность потенциально может быть увеличена в восемь раз.

Трафик распределяется между адаптерами стандартным способом (адресный алгоритм – address algorithm) или на основе циклического (round robin) обслуживания. При отказе адаптера трафик автоматически пересылается на следующий доступный адаптер в EtherChannel, не нарушая пользовательские подключения. Если активно только одно подключение в основном EtherChannel, тест на отказ начинает немедленное обнаружение/перемещение (в течение 2-4 с) на требуемый резервный адаптер без нарушения пользовательских подключений. Возможно проведение двух тестов: на отказ физической связи адаптера с сетью и на отказ TCP/IP-пути к узлу, заданному пользователем. При обнаружении отказа на резервном адаптере активизируются MAC- и IP-адреса. При восстановлении хотя бы одного адаптера в основном канале происходит повторная активизация адресов в основном канале.

Режим конфигурации Network Interface Backup (NIB), реализованный в AIX V5.1, был заменен и усовершенствован в AIX V5.2. Новый метод состоит в использовании одного адаптера EtherChannel с резервным адаптером, обеспечивая приоритет (возврат после восстановления связи) между основными и резервными каналами, что в предыдущей версии не было реализовано. Усовершенствование функции динамического членства адаптеров (dynamic adapter membership, DAM) в AIX V 5.2 позволяют осуществлять динамическое реконфигурирование адаптеров в EtherChannel без нарушения работающего подключения.

Примечание. В HACMP не заявлена поддержка DAM, так как эта функция работает ниже уровня, на котором HACMP осуществляет мониторинг. Поэтому заявление о поддержке не требуется.

Все адаптеры, состоящие из нескольких каналов, требуют использования специальной конфигурации порта EtherChannel или IEEE 802.3ad в сетевом коммутаторе. В большинстве случаев коммутатор настраивается для применения в режиме EtherChannel. Однако если коммутатор не поддерживает ЕС или если корпорация в качестве стандарта использует IEEE 802.3ad, то следует сконфигурировать 802.3ad и в коммутаторе и в AIX. С другой стороны, подключения с одним адаптером не требуют специального конфигурирования на уровне сетевого коммутатора. Это включает EtherChannel с одним адаптером и подключение резервного адаптера.

EtherChannel имеет следующие преимущества:

Более высокая пропускная способность и возможности балансировки нагрузки:

Каналы с несколькими адаптерами агрегируют пропускную способность.

Возможность использования нескольких вариантов направления трафика через адаптеры канала, настраиваемых пользователем.

Встроенные функции обеспечения доступности:

Автоматическая обработка отказов адаптера, связей и сети.

Использование резервного адаптера для устранения единой точки отказа (single point of failure, SPOF) на уровне коммутатора сети. (Необязательно).

Методы проектирования для устранения единых точек отказа.

Простое, гибкое решение и возможности масштабирования:

Один MAC- и IP-адрес Ethernet для всей агрегированной конфигурации (включая резервный адаптер).

Легко приспособливается к будущим требованиям к пропускной способности.

Пользователь может добавлять, удалять и реконфигурировать адаптеры динамически (не прерывая обслуживания).

Несколько вариантов взаимодействия с сетевым коммутатором;

Каналы с несколькими адаптерами для коммутаторов с поддержкой EtherChannel и 802.3ad.

Каналы с одним адаптером и резервные связи адаптеров прозрачны для сетевого коммутатора.

Опция подключения резервного адаптера канала (к другому сетевому коммутатору, чтобы избежать единой точки отказа).

При прямой связи двух систем канал работает без коммутатора (напрямую; однако в среде HACMP это неприменимо).

Эта технология является бесплатной (при условии, что у вас уже установлены коммутаторы с поддержкой EC). Включена в AIX и регулярно улучшается, начиная с версии AIX v4.3.3.

Реализация EtherChannel в среде HACMP

HACMP официально поддерживает использование EtherChannel. Заявление о поддержке можно найти по адресу <http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/FLASH10284>

Интеграция технологии EtherChannel в кластер осуществляется сравнительно просто и может значительно упростить адресацию в сети и требования к подсетям. Очень часто все адреса конфигурируются на одном логическом интерфейсе.

В нашем примере мы рассмотрим только то, что относится к совместному использованию HACMP и EtherChannel. Чтобы избежать повторения материала в этой книге, описание базового конфигурирования кластера HACMP опущено; предполагается, что эти знания у вас уже есть. Мы не будем приводить пошаговые инструкции по работе с меню HACMP. Рекомендуется также настроить сети пульса, отличные от IP, а также использовать коммутатор с поддержкой EC вместо кроссоверных кабелей.

Конфигурация тестовой среды

Наша тестовая среда была построена с использованием следующих компонентов:

две системы pSeries p630 (с именами neo и trinity);

AIX V5.2 ML3;

HACMP V5.1;

сетевые подключения Ethernet ent0 – ent6:

ent0 и ent5 (не используется) представляют интегрированные адаптеры 10/100;

ent1, ent2, ent3, ent4 (не используется) представляют единый 4-портовый адаптер 10/100;

ent6 – EtherChannel (состоит из ent2, ent3 и ent0);

три кроссоверных кабеля UTP Ethernet.

В этом тесте мы успешно реализовали "сеть с одним адаптером", использующую перехват IP-адреса (IP Address Takeover, IPAT) с функцией EtherChannel, включенной в AIX V 5.2. EtherChannel отвечает за переключение локального адаптера, расположенного за пределами HASCMP. HASCMP не знает о существовании EtherChannel и полностью независим. Хотя сеть с одним адаптером не является идеальным вариантом, в EtherChannel ее использование считается нормальным, так как в действительности одно псевдоустройство EtherChannel содержит несколько физических адаптеров.

Таким образом, можно игнорировать предупреждения о недостаточном количестве адаптеров, выводимые в процессе синхронизации кластера.

Наша конфигурация содержала ротационную группу ресурсов и сеть с одним адаптером, использующую IP-синонимы. Наше тестирование подтвердило эффективность технологии в упрощении настройки HASCMP. Мы реализовали подключение EtherChannel без сетевого коммутатора, подключив две тестовые системы напрямую с примечанием кроссоверных кабелей. Это было сделано только в целях тестирования. Как правило, в среде HASCMP для полноценного использования этих адаптеров они подключаются к коммутатору с поддержкой Etherchannel.

Существуют сценарии, в которых требуется большая пропускная способность или избыточность между устройствами, что может быть обеспечено одним каналом. Для увеличения пропускной способности между устройствами может быть подключено несколько каналов связи. Однако протокол STP, который по умолчанию включен на устройствах уровня 2, таких как коммутаторы Cisco, блокирует избыточные каналы, чтобы предотвратить петли коммутации.

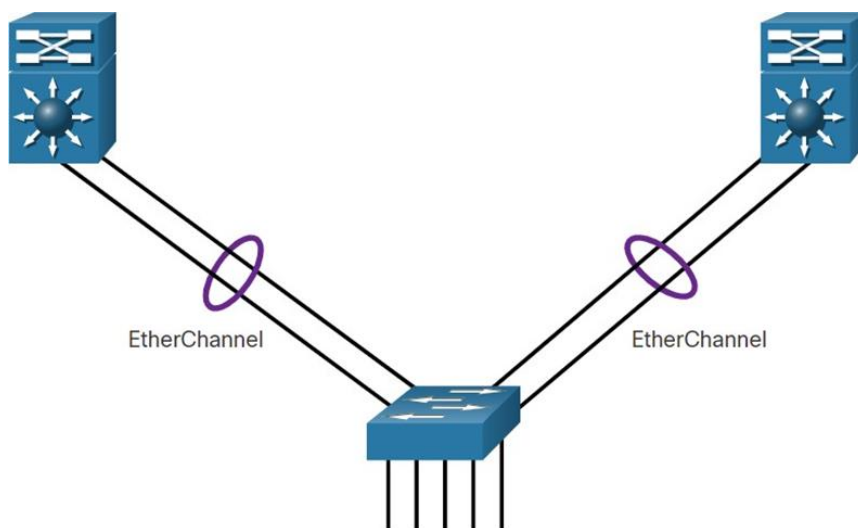
Необходима технология агрегации каналов, позволяющая создавать избыточные связи между устройствами, которые не будут блокироваться STP. Эта технология известна как EtherChannel.

EtherChannel — это технология агрегации каналов, которая группирует несколько физических каналов Ethernet вместе в один логический канал. Он используется для обеспечения отказоустойчивости, распределения нагрузки, увеличения пропускной способности и избыточности между коммутаторами, маршрутизаторами и серверами.

Технология EtherChannel может объединить несколько физических каналов между коммутаторами, что позволит увеличить общую скорость обмена данными между коммутаторами.

ETHERCHANNEL

Технология EtherChannel изначально была разработана компанией Cisco как технология LAN типа «коммутатор-коммутатор» для объединения нескольких портов Fast Ethernet или Gigabit Ethernet в один логический канал.



При настройке EtherChannel создаётся виртуальный интерфейс, который называется агрегированный канал (port channel). Физические интерфейсы объединяются в интерфейс агрегированного канала, как показано на рисунке.

Технология EtherChannel имеет много достоинств:

Большинство задач конфигурации выполняется на интерфейсе EtherChannel, а не на отдельных портах. Это обеспечивает согласованную конфигурацию на всех каналах.

EtherChannel использует существующие порты коммутатора. Для обеспечения более высокой пропускной способности не требуется дорогостоящая замена канала на более быстрый.

Между каналами, которые являются частью одного и того же EtherChannel, происходит распределение нагрузки.

EtherChannel создает объединение, которое рассматривается, как один логический канал. Если между двумя коммутаторами существует несколько объединений EtherChannel, протокол STP может заблокировать одно из объединений во избежание петель коммутации. Если протокол STP

блокирует один из избыточных каналов, он блокирует весь EtherChannel. При этом блокируются все порты, относящиеся к этому каналу EtherChannel.

Если существует только один канал EtherChannel, все физические каналы в EtherChannel активны, поскольку STP видит только один (логический) канал.

EtherChannel предоставляет функции избыточности, поскольку общий канал считается одним логическим соединением. Кроме того, потеря одного физического соединения в пределах канала не приводит к изменению в топологии.

EtherChannel имеет определенные ограничения реализации, в том числе следующие:

Нельзя одновременно использовать разные типы интерфейсов. Например, нельзя смешивать Fast Ethernet и Gigabit Ethernet в пределах одного канала EtherChannel.

В настоящее время все каналы EtherChannel могут содержать до восьми совместно настроенных Ethernet-портов. EtherChannel предоставляет полнодуплексную полосу пропускания до 800 Мбит/с (Fast EtherChannel) или 8 Гбит/с (Gigabit EtherChannel) между двумя коммутаторами или между коммутатором и узлом.

Коммутатор Cisco Catalyst 2960 уровня 2 в настоящее время поддерживает до шести каналов EtherChannel.

Конфигурация порта отдельного участника группы EtherChannel должна выполняться согласованно на обоих устройствах. Если физические порты на одной стороне настроены в качестве транковых, то физические порты на другой стороне также должны быть настроены в качестве транковых с тем же самым native VLAN. Кроме того, все порты в каждом канале EtherChannel должны быть настроены как порты 2-го уровня.

Каждый канал EtherChannel имеет логический интерфейс агрегированного канала. Настройка интерфейса агрегированного канала применяется на все физические интерфейсы, связанные с этим каналом.

ТИПЫ СЕТЕЙ VLAN

Etherchannel можно образовать путем согласования с использованием одного из двух протоколов, Port Aggregation Protocol (PAgP) или Link Aggregation Control Protocol (LACP). Данные протоколы позволяют портам со сходными характеристиками образовывать каналы путем динамического согласования со смежными коммутаторами.

Примечание. Также возможна настройка статического или безусловного канала EtherChannel без использования PAgP или LACP.

PAgP — это проприетарный протокол Cisco, который предназначен для автоматизации создания каналов EtherChannel. Когда канал EtherChannel настраивается с помощью PAgP, пакеты PAgP пересылаются между портами с поддержкой EtherChannel в целях согласования создания канала. Когда PAgP определяет совпадающие соединения Ethernet, он группирует их в канал EtherChannel. Далее EtherChannel добавляется в дерево кратчайших путей как один порт.

Если включён протокол PAgP, он также участвует в управлении EtherChannel. Отправка пакетов PAgP выполняется с интервалом в 30 секунд. PAgP проверяет согласованность конфигурации и обрабатывает добавление и выход из строя каналов между двумя коммутаторами. Таким образом обеспечивается использование согласованной конфигурации для всех портов при создании EtherChannel.

Примечание. В EtherChannel все порты обязательно должны иметь одинаковую скорость, одинаковые настройки дуплекса и одинаковые настройки VLAN. При любом изменении порта после создания канала также изменяются все остальные порты канала.

Протокол PAgP позволяет создать канал EtherChannel путем обнаружения конфигурации на каждой из сторон и обеспечения совместимости каналов, чтобы канал EtherChannel мог быть включён в случае необходимости. Режимы PAgP:

On (Вкл) - этот режим принудительно назначает интерфейс в канал без использования PAgP. Интерфейсы, настроенные в режиме On (Вкл), не обмениваются пакетами PAgP.

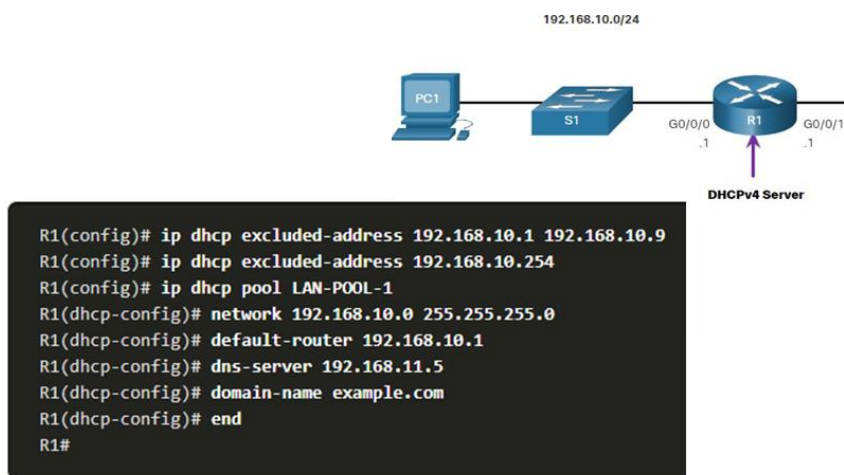
PAgP desirable (рекомендуемый) — этот режим PAgP помещает интерфейс в активное состояние согласования, в котором интерфейс инициирует согласование с другими интерфейсами путем отправки пакетов PAgP.

PAgP auto (автоматический) — этот режим PAgP помещает интерфейс в пассивное состояние согласования, в котором интерфейс отвечает на полученные пакеты PAgP, но не инициирует согласование PAgP.

Режимы должны быть совместимыми на каждой из сторон. Если одна из сторон настроена в автоматическом режиме, она помещается в пассивное состояние, ожидая инициации согласования EtherChannel другой стороной. Если для другой стороны также задан автоматический режим, то согласование не начнётся и EtherChannel не образуется. Если все режимы отключены с помощью команды no или ни один из режимов не настроен, EtherChannel отключается. Режим on помещает интерфейс в канал EtherChannel без

выполнения согласования. Этот режим работает только в том случае, если для другой стороны также задан режим on. Если для другой стороны параметры согласования заданы с помощью PAgP, образование EtherChannel не выполняется, поскольку та сторона, для которой задан режим on, не выполняет согласование. Отсутствие согласования между двумя коммутаторами означает отсутствие проверки, что все каналы в EtherChannel завершаются на другой стороне или что на другом коммутаторе используются совместимые параметры PAgP.

ПРИМЕР КОНФИГУРАЦИИ



Используйте команды, приведенные в таблице, чтобы проверить работоспособность сервера Cisco IOS DHCPv4.

Проверка конфигурации DHCPv4. Как показано в примере, выходные данные команды `show running-config | section dhcp` отображают текущую конфигурацию DHCPv4, выполненную на маршрутизаторе R1. Параметр `| section` отображает только те команды, которые связаны с настройкой DHCPv4.

```
R1# show running-config | section dhcp
ip dhcp excluded-address 192.168.10.1 192.168.10.9
ip dhcp excluded-address 192.168.10.254
ip dhcp pool LAN-POOL-1
network 192.168.10.0 255.255.255.0
default-router 192.168.10.1
dns-server 192.168.11.5
domain-name example.com
```

Проверка привязки DHCPv4. Как показано в примере, работу DHCPv4 можно проверить, используя команду `show ip dhcp binding`. Команда выводит список всех привязок адресов IPv4 к MAC-адресам, предоставленных службой DHCPv4.

```
R1# show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address      Client-ID/      Lease expiration    Type    State    Interface
                Hardware address/
                User name
192.168.10.10   0100.5056.b3ed.d8  Sep 15 2019 8:42 AM  Automatic Active
GigabitEthernet0/0/0
```

Проверка статистики DHCPv4. Выходные данные команды `show ip dhcp server statistics` используются для проверки того, что сообщения принимаются или отправляются маршрутизатором. Данная команда отображает информацию о количестве принятых и отправленных сообщений DHCPv4.

```
R1# show ip dhcp server statistics
Memory usage      19465
Address pools      1
Database agents    0
Automatic bindings 2
Manual bindings    0
Expired bindings   0
Malformed messages 0
Secure arp entries 0
Renew messages     0
Workspace timeouts 0
Static routes      0
Relay bindings     0
Relay bindings active 0
Relay bindings terminated 0
Relay bindings selecting 0
Message           Received
BOOTREQUEST       0
DHCPDISCOVER      4
DHCPREQUEST       2
DHCPDECLINE       0
DHCPRELEASE       0
DHCPINFORM        0
```

Проверка получения IPv4-адреса клиента DHCPv4. Команда `ipconfig /all` на PC1 отображает параметры TCP/IP, как показано в примере. Поскольку PC1 подключен к сегменту сети 192.168.10.0/24, он автоматически получает суффикс DNS, IPv4-адрес, маску подсети, шлюз по умолчанию и адрес сервера DNS из этого пула. Специальная настройка интерфейса маршрутизатора для DHCP не требуется. В случае если компьютер подключен к сегменту сети с доступным пулом DHCPv4, он может получить IPv4-адрес из пула автоматически.

```

C:\Users\Student> ipconfig /all
Windows IP Configuration

Host Name . . . . . : ciscolab
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : example.com
Description . . . . . : Realtek PCIe GBE Family Controller
Physical Address. . . . . : 00-05-9A-3C-7A-00
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . : 192.168.10.10
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained . . . . . : Saturday, September 14, 2019 8:42:22AM
Lease Expires . . . . . : Sunday, September 15, 2019 8:42:22AM
Default Gateway . . . . . : 192.168.10.1
DHCP Server . . . . . : 192.168.10.1
DNS Servers . . . . . : 192.168.11.5

```

Служба DHCPv4 включена по умолчанию. Для того чтобы отключить службу, введите команду в режиме глобальной конфигурации по `service dhcp`. Для возобновления работы DHCPv4- сервера используйте команду в режиме глобальной конфигурации `service dhcp`, как показано в примере. В случае, если параметры не настроены, активация службы не имеет эффекта.

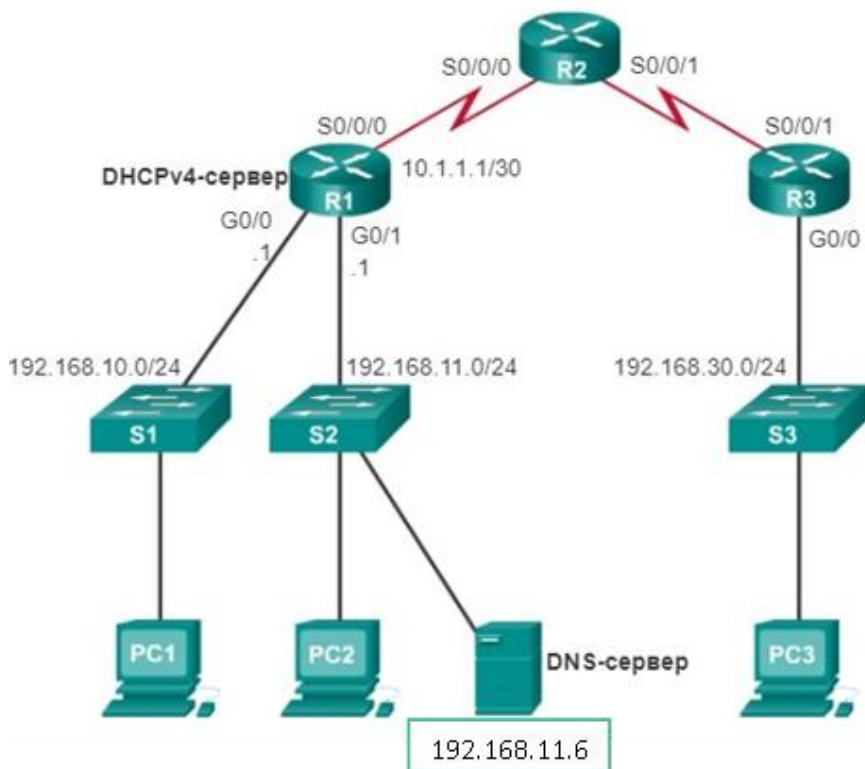
```

R1(config)# no service dhcp
R1(config)# service dhcp
R1(config)#

```

Примечание. Очистка привязок DHCP или остановка и перезапуск службы DHCP может привести к временному дублированию IP- адресов в сети.

Маршрутизатор R1 в качестве DHCPv4-сервера



В сложной иерархической сети корпоративные серверы обычно располагаются в серверной ферме. Данные серверы могут предоставлять службы DHCP, DNS, TFTP и FTP.

Клиенты сети и серверы, как правило, находятся в разных подсетях. Для определения местоположения серверов и получения услуг клиенты часто используют сообщения широковещательной рассылки.

Настройте R1 с помощью команды конфигурации интерфейса `ip helper-address`. Это приведет к тому, что R1 будет ретранслировать широковещательные рассылки DHCPv4 на сервер DHCPv4. Как показано в примере, интерфейс R1, принимающий широковещательную рассылку от PC1, настроен на ретрансляцию DHCPv4 на сервер DHCPv4 по адресу 192.168.11.6.

Когда маршрутизатор R1 сконфигурирован как агент DHCPv4-ретрансляции, он принимает широковещательные запросы, а затем отправляет эти запросы как одноадресную рассылку на IPv4-адрес 192.168.11.6. Администратор сети может использовать эту команду `show ip interface` для проверки конфигурации.

DHCPv4 — не единственная служба, на ретрансляцию которой может быть сконфигурирован маршрутизатор. По умолчанию команда `ip helper-address` переадресовывает следующие восемь служб UDP:

Порт 37: Time

7. DHCPv4

Когда клиент подключается к серверу DHCPv4, сервер присваивает или сдаёт ему в аренду IPv4-адрес. Клиент с арендованным IP-адресом подключается к сети до истечения срока аренды. Периодически клиент должен связываться с DHCP-сервером для продления срока аренды. Благодаря подобному механизму «переехавшие» или отключившиеся клиенты не занимают адреса, в которых они больше не нуждаются. По истечении срока аренды сервер DHCP возвращает адрес в пул, из которого адрес может быть повторно получен при необходимости.

Первоначальная аренда

При начальной загрузке клиента (или ином способе подключения к сети) начинается 4-шаговый процесс получения адреса в аренду. Как показано на рис. 2, клиент начинает процесс с сообщения DHCPDISCOVER широковещательной рассылки со своего MAC-адреса с целью обнаружения доступных DHCPv4-серверов.

Обнаружение DHCP (DHCPDISCOVER)

Сообщение DHCPDISCOVER находит в сети DHCPv4-серверы. Поскольку во время загрузки у клиента нет верной IPv4-информации, для связи с сервером используются широковещательные адреса уровня 2 и уровня 3.

Предложение DHCP (DHCPOFFER)

Когда сервер DHCPv4 получает сообщение DHCPDISCOVER, он резервирует доступные IPv4-адреса для выдачи в аренду клиенту. Сервер также создаёт запись ARP, состоящую из MAC-адреса запрашивающего клиента и выданного клиенту IPv4-адреса. Как показано на рис. 3, DHCPv4-сервер посылает сообщение привязки DHCPOFFER запрашивающему клиенту. Адресом источника одноадресной рассылки сообщения DHCPOFFER является MAC-адрес уровня 2 сервера, адресом назначения - MAC-адрес уровня 2 клиента.

Запрос DHCP (DHCPREQUEST)

Когда клиент получает от сервера сообщение DHCPOFFER, он отправляет в ответ сообщение DHCPREQUEST, как показано на рис. 4. Это сообщение используется как для первоначальной аренды адреса, так и для её продления. Когда сообщение используется при первоначальной аренде, DHCPREQUEST служит уведомлением о принятии предложения привязки к

предложенным сервером параметрам и косвенным отклонением для всех других серверов, которые могли предоставить клиенту предложение привязки.

В корпоративных сетях часто используется несколько DHCPv4-серверов. Сообщение DHCPREQUEST отправляется в форме широковещательной рассылки с целью информирования данного DHCPv4-сервера и других DHCPv4-серверов о том, что предложение было принято.

Подтверждение DHCP (DHCPACK)

При получении сообщения DHCPREQUEST, сервер проверяет, не используется ли выдаваемый в аренду IP-адрес с помощью отправки эхо-запроса по протоколу ICMP на этот адрес. После этого сервер создаёт новую запись ARP для клиентской аренды и отвечает сообщением одноадресной рассылки DHCPACK, как показано на рис. 5. Сообщение DHCPACK является копией сообщения DHCPOFFER, за исключением изменения в поле типа сообщения. При получении сообщения DHCPACK клиент загружает информацию о конфигурации и выполняет ARP-проверку присвоенного адреса. Если ARP-ответа нет, значит, IPv4-адрес доступен, и клиент начинает использовать его в качестве собственного адреса.

Продление аренды

Запрос DHCP (DHCPREQUEST)

Как показано на рис. 6, когда аренда заканчивается, клиент посылает сообщение DHCPREQUEST непосредственно DHCPv4-серверу, который первоначально предложил IPv4-адрес. Если сообщение DHCPACK не получено за определенный период времени, клиент отправляет другое сообщение DHCPREQUEST широковещательной рассылкой, чтобы другой DHCPv4-сервер мог продлить срок аренды.

Подтверждение DHCP (DHCPACK)

При получении сообщения DHCPREQUEST сервер подтверждает информацию об аренде ответным сообщением DHCPACK.

8. SLAAC И DHCPV6

Для каждого устройства, подключённого к сети, требуется уникальный IP-адрес. Сетевые администраторы присваивают статические IP-адреса маршрутизаторам, серверам, принтерам и другим сетевым устройствам, чье физическое и логическое расположение, скорее всего, не изменится. В

большинстве случаев речь идёт об устройствах, предоставляющих службы пользователям и устройствам в сети; таким образом, присваиваемые им адреса должны быть постоянными. Кроме того, статические адреса позволяют администраторам управлять этими устройствами удаленно. Сетевым администраторам проще получить доступ к устройству, если его IP-адрес легко определить.

Однако в организации часто меняется физическое и логическое местоположение пользователей и компьютеров. Присвоение новых IP-адресов при каждом перемещении сотрудника может представлять собой сложный и трудоёмкий процесс. При ручной настройке параметров сети для сотрудников, работающих из удаленных мест, администратор также может столкнуться с рядом трудностей. Кроме того, присвоение IP-адресов вручную и настройка другой информации об адресации для настольных ПК также требует усилий и временных затрат системного администратора, особенно в случае расширения сети.

Внедрение сервера с протоколом динамической конфигурации узла (DHCP) в локальную сеть упрощает процесс присвоения IP-адресов как стационарным, так и мобильным устройствам. Использование централизованного сервера DHCP позволяет организации управлять присвоением всех динамических IP-адресов с одного сервера. Подобная практика делает управление IP-адресацией более эффективной и обеспечивает последовательность процессов и согласованность данных по всей организации, включая филиалы.

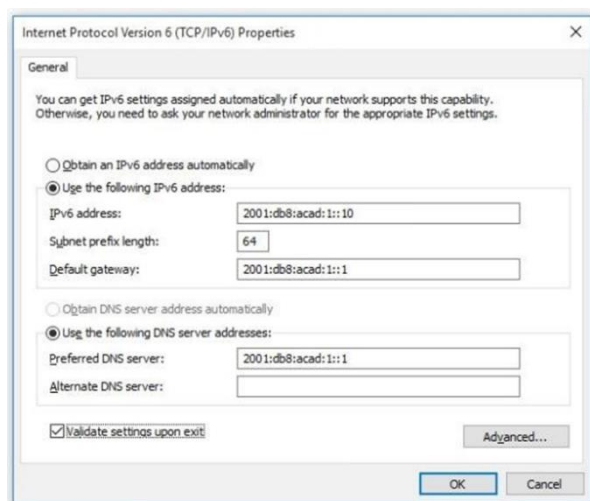
Протокол DHCP доступен как для IPv4 (DHCPv4), так и IPv6 (DHCPv6). В настоящей главе описываются функции, настройка, а также поиск и устранение неполадок протоколов DHCPv4 и DHCPv6.

На маршрутизаторе глобальный одноадресный адрес IPv6 настраивается вручную с помощью команды конфигурации интерфейса `ipv6-address/prefix-length ipv6-length`.

Узел Windows также может быть настроен вручную с помощью конфигурации адреса GUA IPv6, как показано на рисунке.

Однако ввод GUA IPv6 вручную может занять много времени и несколько подвержен ошибкам.

Таким образом большинство хостов Windows имеют возможность динамически приобретать конфигурацию GUA IPv6.



Если выбрана автоматическая адресация IPv6, узел будет использовать сообщение Router Advertisement (RA) протокола управления сообщениями Internet Control Message Protocol версии 6 (ICMPv6), чтобы помочь ему автоматически настроить конфигурацию IPv6.

Локальный адрес канала IPv6 автоматически создается хостом при загрузке и активном интерфейсе Ethernet.

Интерфейс не создал GUA IPv6 в выходных данных, так как сетевой сегмент не имел маршрутизатора для предоставления инструкций по настройке сети для узла.

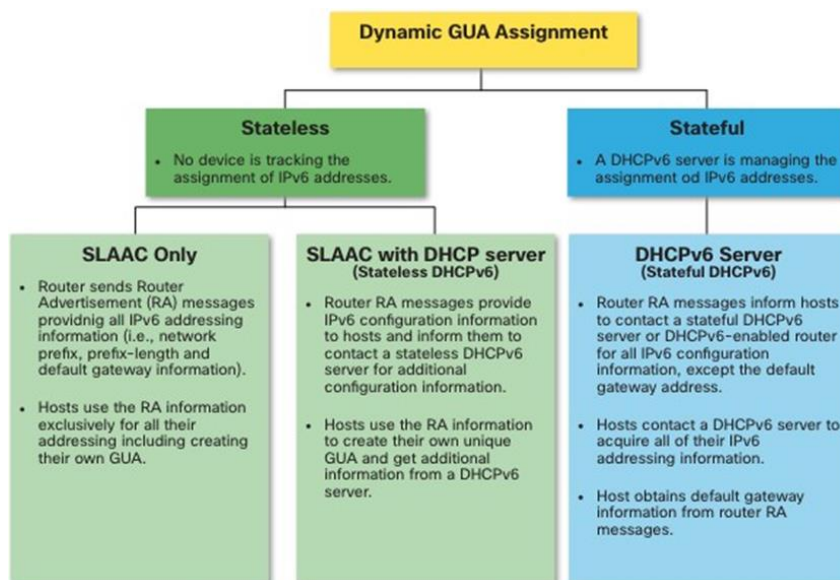
```
C:\PC1> ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 
    Link-local IPv6 Address . . . . . : fe80::fb:1d54:839f:f595%21
    IPv4 Address. . . . . : 169.254.202.140
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 

C:\PC1>
```

Примечание. «%» и число в конце локального адреса канала известны как идентификатор зоны или идентификатор области и используются ОС для связывания LLA с определенным интерфейсом.

По умолчанию маршрутизатор с поддержкой IPv6 периодически отправляет RA ICMPv6, что упрощает динамическое создание или получение хостом конфигурации IPv6.

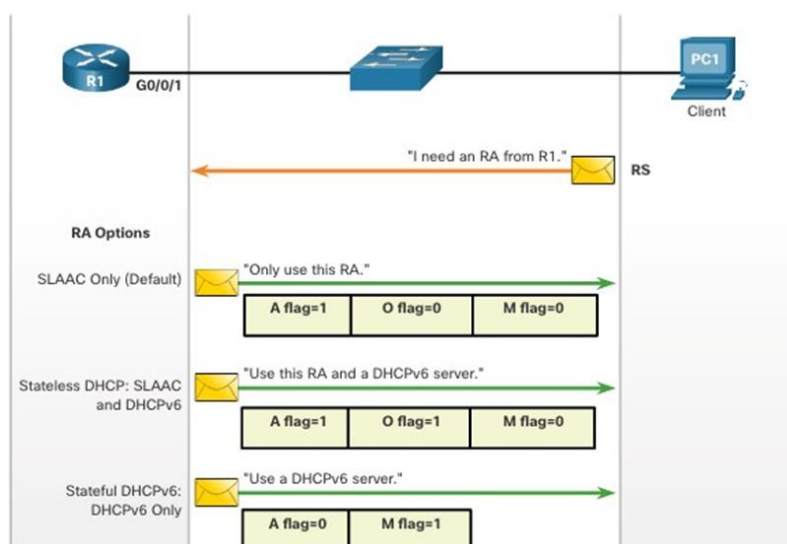


Хост может динамически назначать GUA с помощью служб без отслеживания состояния и с отслеживанием состояния.

Все методы без отслеживания состояния и с отслеживанием состояния в этом модуле используют ICMPv6 RA сообщения, чтобы предложить хосту создать или получить его конфигурацию IPv6.

Хотя хост-операционные системы следуют предложению RA, фактическое решение в конечном итоге зависит от хоста.

ТРИ ФЛАГА СООБЩЕНИЙ RA



Способ, благодаря которому клиент получает GUA IPv6, зависит от настроек в сообщении RA. Сообщение ICMPv6 RA содержит следующие три флага:

Флаг А. Флаг автонастройки адреса означает использование автоматической настройки адресов без состояния (SLAAC) для создания GUA IPv6

Значение флага О, равное 1, используется для информирования клиента о том, что на DHCPv6-сервере без отслеживания состояния доступна дополнительная информация о конфигурации.

Флаг М. Флаг конфигурации управляемого адреса означает использование сервера DHCPv6 с сохранением состояния для получения GUA IPv6.

Используя различные комбинации флагов А, О и М, сообщения RA информируют хост о доступных динамических параметрах.

SLAAC

Не каждая сеть имеет доступ к серверу DHCPv6, но каждое устройство в сети IPv6 нуждается в GUA. Метод SLAAC позволяет хостам создавать свой собственный уникальный глобальный одноадресный адрес IPv6 без использования служб DHCPv6 сервера.

SLAAC - это служба без определения состояния, которая означает, что нет сервера, который поддерживает информацию о сетевых адресах, чтобы знать, какие IPv6-адреса используются и какие из них доступны.

SLAAC отправляет периодические ICMPv6 RA-сообщения (то есть каждые 200 секунд), предоставляя адресацию и другую информацию о конфигурации для узлов для автонастройки их IPv6 адреса на основе информации в RA.

Хост также может отправить сообщение Router Solicitation (RS) с запросом RA. SLAAC может быть развернут только как SLAAC, или SLAAC с DHCPv6.

R1 G0/0/1 настроен с указанными IPv6 GUA и локальными адресами канала.

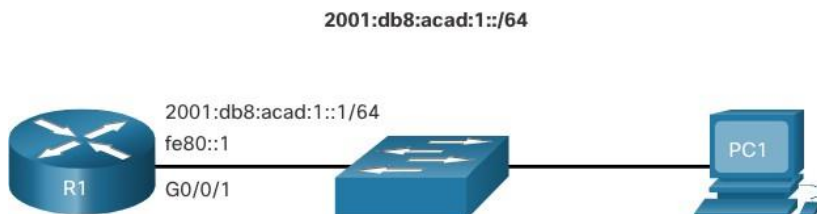
Адреса IPv6 R1 G0/0/01 включают:

Локальный адрес канала IPv6 - fe80::1

GUA/подсеть - 2001:db8:acad:1::1, 2001:db8:acad:1::/64

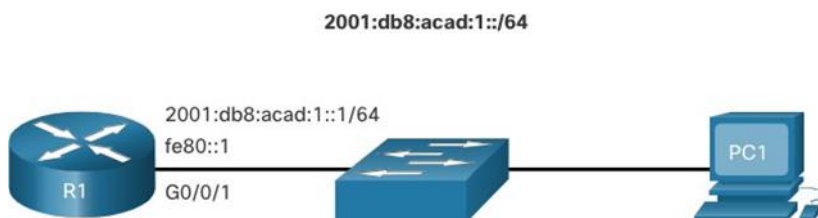
Многоадресная группа всех узлов IPv6 - ff02::1

R1 настроен на присоединение ко всей группе многоадресной рассылки IPv6 и начало отправки сообщений RA, содержащих сведения о конфигурации адресов, хостам с помощью SLAAC.



Сообщение RS отправляется на IPv6-адрес многоадресной рассылки FF02::2, который поддерживают все маршрутизаторы.

Команда `show ipv6 interface` проверяет, присоединился ли R1 к группе всех маршрутизаторов IPv6 (например, ff02::2).



Теперь R1 начнет отправлять сообщения RA каждые 200 секунд на адрес многоадресной рассылки IPv6 для всех узлов ff02::1.

Сообщения RA от R1 имеют следующие флаги:

A = 1 — сообщает клиенту использовать префикс GUA IPv6 в RA и динамически создает свой собственный идентификатор интерфейса.

O = 0 и M = 0 — Сообщает клиенту также использовать дополнительную информацию в сообщении RA (например, DNS-сервер, MTU и шлюз по умолчанию).

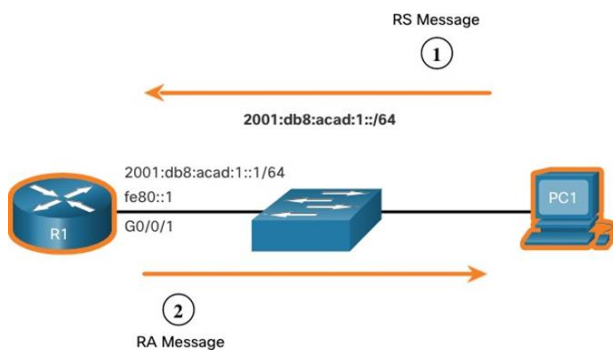
Команда `ipconfig Windows` подтверждает, что PC1 создал GUA IPv6 с помощью R1 RA.

Адрес шлюза по умолчанию — LLA интерфейса R1 G0/0/1.

Маршрутизатор отправляет сообщения RA каждые 200 секунд или при получении сообщения RS от хоста.

Узлы с поддержкой IPv6, желающие получить информацию об адресации IPv6, отправляют сообщение RS на адрес многоадресной рассылки всех маршрутизаторов IPv6 ff02::2.

На рисунке показано, как хост иницирует метод SLAAC.



1. PC1 только что загрузился и отправляет сообщение RS на адрес многоадресной рассылки IPv6 для всех маршрутизаторов ff02::2 с запросом RA.

2. R1 генерирует RA, а затем отправляет сообщение RA на адрес многоадресной рассылки IPv6 для всех узлов ff02::1. PC1 использует эту информацию для создания уникального GUA IPv6.

Используя SLAAC, хост получает информацию о 64-битной подсети IPv6 от маршрутизатора RA и должен генерировать оставшийся идентификатор 64-битного интерфейса (ID), используя методы:

Генерация случайным образом — 64-битный ID может быть случайным числом, сгенерированным операционной системой клиента. Этот метод теперь используется хостами Windows 10.

EUI-64 — хост создает идентификатор интерфейса, используя свой 48-битный MAC-адрес и вставляет шестнадцатеричное значение fffe в середине адреса. Некоторые операционные системы по умолчанию используют случайно сгенерированный идентификатор интерфейса вместо метода EUI-64, из-за проблем конфиденциальности. Это связано с тем, что MAC-адрес узла Ethernet используется EUI-64 для создания идентификатора интерфейса.

Примечание. Windows, Linux и Mac OS позволяют пользователю изменять генерирование идентификатора интерфейса либо случайным образом, либо использовать EUI-64.

```
R3# show ipv6 dhcp binding
Client: FE80::5C43:EE7C:2959:DA68
DUID: 0001000124F5CEA2005056B3636D
Username : unassigned
VRF : default
IA NA: IA ID 0x03000C29, T1 43200, T2 69120
Address: 2001:DB8:ACAD:2:9C3C:64DE:AADA:7857
        preferred lifetime 86400, valid lifetime 172800
        expires at Sep 29 2019 08:26 PM (172710 seconds)
R3#
```

9. Основные понятия FHRP

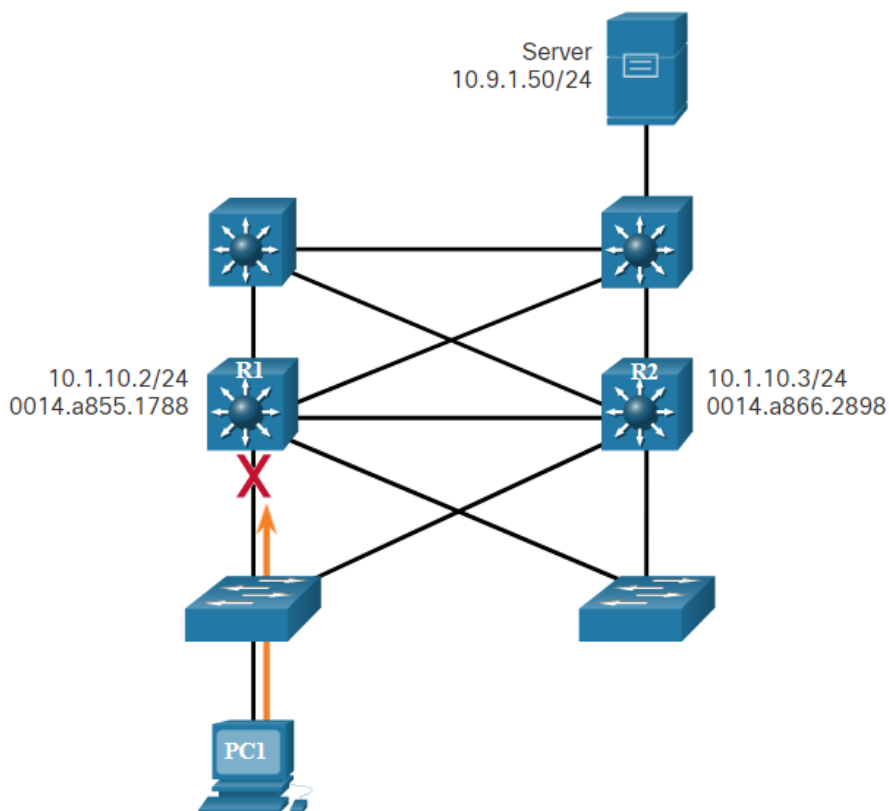
Протоколы резервирования первого перехода
Ограничения шлюза по умолчанию

Конечные устройства, как правило, настраиваются с одним IPv4-адресом для шлюза по умолчанию.

Если интерфейс маршрутизатора шлюза по умолчанию выходит из строя, хосты локальной сети теряют подключение за пределами локальной сети.

Это происходит, даже если существует избыточный маршрутизатор или коммутатор уровня 3, который может служить шлюзом по умолчанию.

First hop redundancy protocols (**FHRPs**) - механизм для предоставления альтернативных шлюзов по умолчанию в коммутируемых сетях, где два или более маршрутизаторов подключены к одним и тем же сетям VLAN.



Избыточность маршрутизатора

Один из способов устранения единой точки отказа на шлюзе по умолчанию — реализация виртуального маршрутизатора. Для реализации этого типа избыточности маршрутизатора несколько маршрутизаторов настраиваются для совместной работы, что создает иллюзию одного маршрутизатора на узлах сети LAN. При совместном использовании IP-адреса

и MAC-адреса два или более маршрутизаторов могут работать как один виртуальный маршрутизатор.

Адрес IPv4 виртуального маршрутизатора настраивается в качестве шлюза по умолчанию для рабочих станций в отдельном сегменте IPv4.

При отправке кадров с хост-устройств на шлюз по умолчанию хосты используют ARP для разрешения MAC-адреса, связанного с адресом IPv4 шлюза по умолчанию. С помощью протокола ARP определяется MAC-адрес виртуального маршрутизатора. После этого кадры, которые отправлены на MAC-адрес виртуального маршрутизатора, можно обработать физически с помощью текущего активного маршрутизатора в пределах группы виртуального маршрутизатора.

Протокол используется для определения двух или более маршрутизаторов в качестве устройств, отвечающих за обработку кадров, отправляемых на MAC- или IP-адрес одного виртуального маршрутизатора. Конечные устройства отправляют трафик на адреса виртуального маршрутизатора. Физический маршрутизатор, который пересылает этот трафик, является прозрачным для конечных устройств.

Протокол резервирования предоставляет механизм для определения маршрутизатора, который должен выполнять активную роль в пересылке трафика. Он также определяет, когда роль пересылки должна перейти к избыточному маршрутизатору. Переход от одного пересылающего маршрутизатора к другому является прозрачным для конечных устройств.

Способность сети динамически восстанавливаться после сбоя устройства, выполняющего функцию шлюза по умолчанию, называется избыточностью на первом хопе.

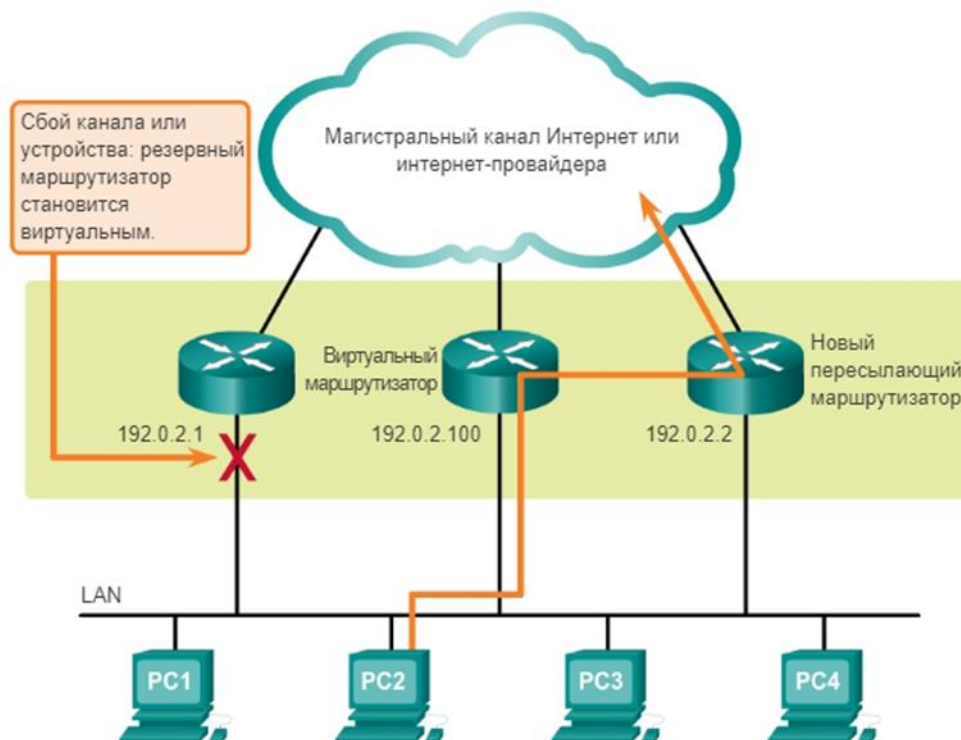
Действия при переключении при отказе маршрутизатора

В случае сбоя активного маршрутизатора протокол резервирования переводит резервный маршрутизатор на новые функции активного маршрутизатора. В случае сбоя активного маршрутизатора происходит следующее.

1. Резервный маршрутизатор перестает видеть сообщения приветствия от пересылающего маршрутизатора.
2. Резервный маршрутизатор принимает роль передающего маршрутизатора.

3. Поскольку новый пересылающий маршрутизатор использует как адрес IPv4, так и MAC-адрес виртуального маршрутизатора, хост-устройства не замечают перебоев в обслуживании.

Действия при переключении в случае отказа маршрутизатора



HSRP

Общие сведения о протоколе HSRP

Cisco предоставляет HSRP и HSRP для IPv6 как способ избежать потери доступа к внешней сети в случае сбоя маршрутизатора по умолчанию. Проприетарный протокол Cisco FHRP, предназначенный для обеспечения сквозного переключения IPv4-устройства первого перехода.

Протокол HSRP обеспечивает высокую доступность сети благодаря предоставлению функций обеспечения избыточности для маршрутизации на первом хопе для IPv4-узлов в сетях, настроенных с использованием IPv4-адреса шлюза по умолчанию. HSRP используется группой маршрутизаторов для выбора активного и резервного устройств. В рамках группы интерфейсов устройства активным называется устройство, используемое для маршрутизации пакетов; резервным — устройство, которое задействуется в случае сбоя активного устройства или при выполнении предварительно заданных условий. Задача резервного маршрутизатора HSRP заключается в мониторинге рабочего состояния группы HSRP и быстром переходе к

выполнению функций пересылки пакетов в случае сбоя активного маршрутизатора.

Приоритет и приоритетное вытеснение HSRP

Роль активных и резервных маршрутизаторов определяется во время процесса выбора HSRP. По умолчанию в качестве активного выбирается маршрутизатор с максимальным в численном отношении адресом IPv4. Однако всегда лучше контролировать, как сеть будет работать в нормальных условиях, чем оставлять это на волю случая.

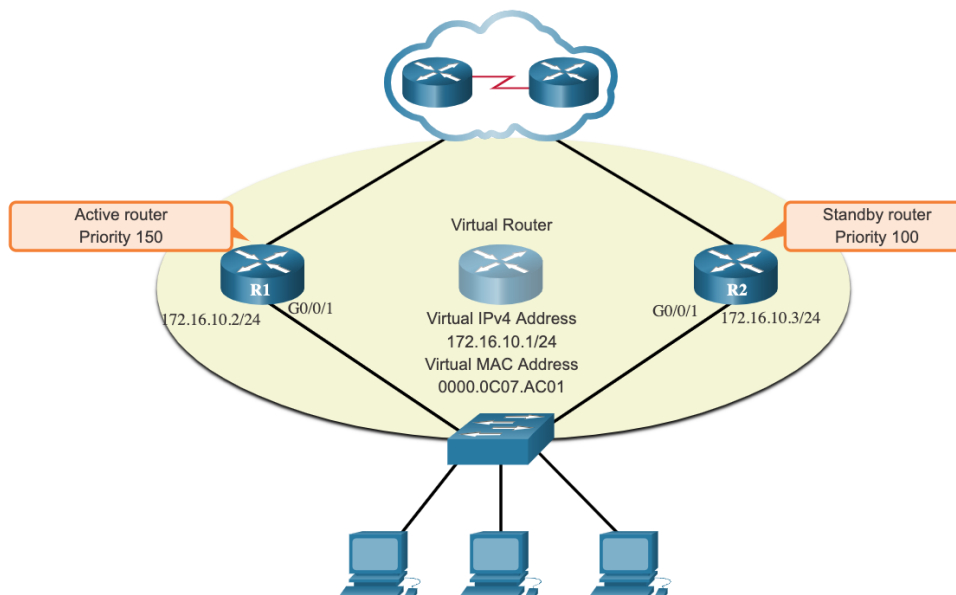
Для определения активного маршрутизатора можно использовать приоритет HSRP.

Маршрутизатор с наивысшим приоритетом HSRP станет активным маршрутизатором.

По умолчанию приоритет HSRP равен 100.

Если приоритеты равны, то в качестве активного выбирается маршрутизатор с максимальным в численном отношении адресом IPv4.

Чтобы настроить маршрутизатор в качестве активного, используйте команду интерфейса **standby priority**. Приоритеты HSRP имеют диапазон от 0 до 255.



По умолчанию, после того как маршрутизатор становится активным, он остается таковым, даже если в сети появляется другой маршрутизатор с более высоким приоритетом HSRP.

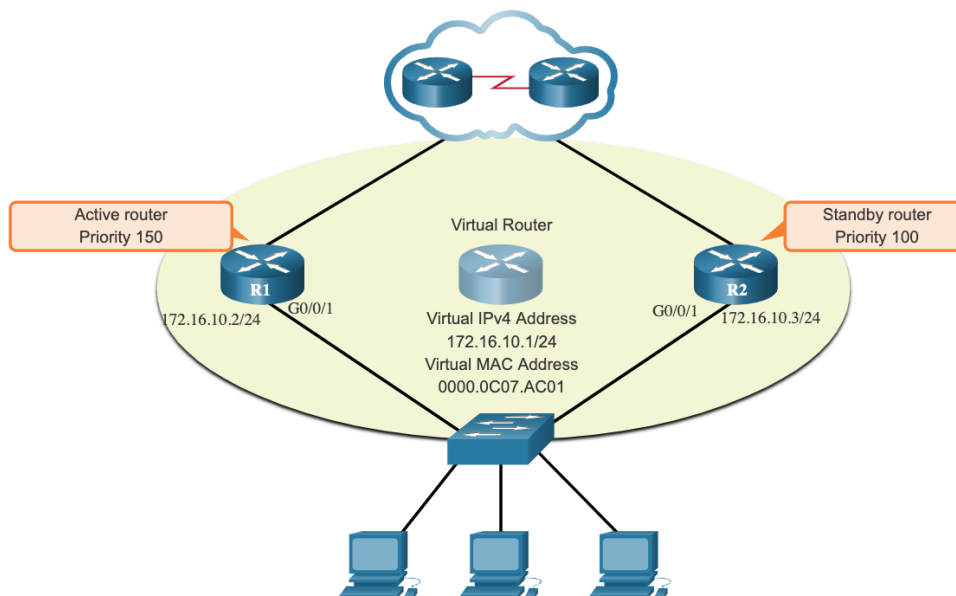
Чтобы принудительно провести новый процесс выборов HSRP, когда маршрутизатор с более высоким приоритетом подключается в оперативный

режим, необходимо включить механизм приоритетного вытеснения с помощью команды интерфейса **standby preempt**.

Приоритетное вытеснение — это способность маршрутизатора HSRP запускать процесс повторного выбора. Если приоритетное вытеснение включено, то при появлении в сети маршрутизатора с более высоким приоритетом HSRP он становится активным маршрутизатором.

Приоритетное вытеснение позволяет маршрутизатору стать активным, только если у него более высокий приоритет. Если у маршрутизатора такой же приоритет, но больший адрес IPv4, он не будет вытеснять действующий активный маршрутизатор. См. топологию на рисунке.

Примечание. Если приоритетное вытеснение отключено, то активным маршрутизатором становится первый загруженный маршрутизатор, если во время процесса выбора в сети нет других маршрутизаторов.



10. Принципы обеспечения безопасности сети

Безопасность оконечных устройств

В новостях часто рассказывают о внешних сетевых атаках на корпоративные сети. Просто найдите в Интернете «последние сетевые атаки», чтобы найти актуальную информацию о текущих атаках. Скорее всего, эти атаки будут включать одно или несколько из следующих действий:

Распределенный отказ в обслуживании (DDoS) — это скоординированная атака со многих устройств, называемых зомби, с целью ослабления или прекращения публичного доступа к веб-сайту и ресурсам организации.

Кража данных – это атака, при которой серверы или хосты организации подвергаются риску кражи конфиденциальной информации.

Вредоносное ПО – это атака, при которой узлы организации заражаются вредоносным программным обеспечением, вызывающим множество проблем. Например, вымогатель, такой как WannaCry, шифрует данные на хосте и блокирует доступ к нему, пока выкуп не будет выплачен.

Независимо от объема компьютерной сети проблема защиты информации и общей сетевой безопасности никогда не потеряет своей актуальности по той причине, что термин сетевая безопасность включает в себя не только процедуры защиты информации от хищения или изменения, но и, главным образом, комплекс мероприятий по предотвращению в сети всевозможных сбоев. Таким образом, специалист по сетевой безопасности должен владеть не только инструментами по безопасному хранению и передаче информации, но и адекватно реагировать на системные сбои.

Как и в любом проекте, при разработке системы безопасности сетевой инфраструктуры необходимо руководствоваться известным принципом "цель оправдывает средства". При чем этот принцип необходимо учитывать со всех сторон. То есть при разработке системы сетевой безопасности необходимо четко определить цель – защитить автоматические бизнес-процессы, протекающие на предприятии и, во-вторых, выбрать для решения этой задачи адекватные средства. Для этого необходимо определить требования руководства предприятия к защите сети в форме единого документа. В дальнейшем единый документ, согласованный сторонами, должен быть дополнен планом выполнения поставленных задач. Анализ поставленных руководством требований к безопасности сети необходимо проводить, учитывая следующие факторы:

сметная стоимость проекта (успешная реализация любого проекта, в т.ч. связанного с обеспечением сетевой инфраструктуры зависит от реальных финансовых возможностей предприятия);

соответствие системы безопасности требованиям закона (зачастую данные определенного типа и методы работы с ними подчинены законодательному регулированию, например, личные данные работников; необходимо, чтобы проектируемая система безопасности отвечала государственным стандартам по работе с данными);

принцип совместимости (проект должен реализовываться "малой кровью" с максимальным использованием возможностей уже имеющихся на предприятии систем);

принцип масштабируемости (при разработке системы безопасности всегда необходимо учитывать возможный в будущем рост корпоративной сети);

принцип удобства сопровождения (система документирования является одной из основных частей безопасности, поэтому возможность эффективной поддержки системы должна быть "поставлена во главу угла");

удобство работы конечных пользователей (в случае если система безопасности сети внедряется на предприятии управленческим решением, то, как правило, это вызывает негативную реакцию со стороны конечных пользователей в силу того, что им приходится отказываться от выработанных привычек при работе с сетью; негативное отношение персонала может свести на нет всю проделанную работу, поэтому при разработке и внедрении систем защиты корпоративной сети с пользователями необходимо вести разъяснительную работу).

Таким образом, очевидна необходимость проведения аудита уже имеющихся на предприятии систем, опрос конечных пользователей системы и интервьюирование руководства предприятия для того, чтобы анализ адекватности системы безопасности корпоративной сети можно было успешно завершить. Результатом проведенного анализа должен стать комплект документов, содержащий описание аппаратных и программных средств, используемых в корпоративной сети, описание автоматизированных бизнес-процессов, которые необходимо защитить, классификацию информации, используемой организацией, характеристику рисков используемой системы и описание влияния сотрудников на автоматизированную систему. Необходимо выяснить для чего используются те или иные данные, каков будет ущерб от ошибок или нехватки данных, а также определить степень конфиденциальности той или иной информации, поскольку данные разных типов требуют разной степени защиты. В данном случае цена ошибки или угрозы определяет количество затрат на защиту данных от этих ошибок и угроз.

Не нужно забывать, что одним из самых уязвимых мест в автоматизированной системе является человек. При разработке системы безопасности для последующего разграничения прав доступа к ресурсам и полномочий на действия в корпоративной сети необходимо иметь структурную схему предприятия и связанную с ней схему прав и полномочий сотрудников с выделением границ безопасности.

План защиты сети должен состоять из следующих структурных элементов:

описание способов профилактики и устранения последствий атак на корпоративную сеть ;

применяемые базовые принципы защиты информации;

методы моделирования угроз;

описание ответных действий при атаке;

описание процедуры аварийного восстановления;

описание сетевых сегментов.

В этой связи под базовыми принципами защиты информации необходимо понимать следующее:

принцип открытости системы (использование общепринятых стандартизированных алгоритмов зачастую гораздо лучше и эффективнее, чем использование малоизвестных или самостоятельно разработанных защитных алгоритмов);

принцип простоты (при взаимодействии с конечным пользователем система защиты должна быть простой, чтобы не создать путаницу; сложные механизмы должны быть отделены от пользователя);

принцип минимальной уязвимости (в случае если нужно защитить информацию от копирования, нужно просто снять с системных блоков пишущие устройства, а не применять сложных прав доступа к ним);

принцип наименьших привилегий (по умолчанию все порты и доступ к файлам для пользователей закрыты, сами пользователи разделены на группы и получают минимальный набор прав, необходимый для выполнения их производственных функций);

принцип контроля (всегда необходимо контролировать состояние системы, поддерживая ее техническое состояние на актуальном уровне, при этом также необходимо контролировать поведение администратора системы с помощью аудита, не забывая, что человек является слабым звеном в системе).

При разработке плана защиты около 30 процентов времени необходимо выделять моделированию угроз. В конечном итоге это снизит риск уязвимости системы. Процесс моделирования угроз необходимо проводить следующим образом:

сформировать команду по моделированию (в нее должны входить специалисты, имеющие опыт работы с внедряемым оборудованием и программным обеспечением);

использовать данные анализа, проведенного на предыдущих этапах построения концептуального плана защиты (на этой стадии выявляются недостатки собранной и разработанной к данному моменту документации);

поиск угроз (обсуждаются и прорабатываются все высказанные варианты атак с указанием степени их опасности и разработкой плана реакции на каждую из угроз);

выбор механизмов и методов предотвращения смоделированных угроз (при выборе технических средств необходимо учитывать их совместимость с уже имеющимися в корпоративной сети устройствами и программами. После проведения аудита имеющихся систем необходимо иметь список их технических ограничений для того, чтобы можно было в полной мере использовать возможности нового оборудования и программ и во избежание конфликтов новых систем с уже имеющимися).

После выбора технических средств реализации системы безопасности необходимо позаботиться о трех важных аспектах, два из которых являются техническими (спланировать процедуры восстановления и обсудить возможность сегментирования сети), а третий – психологический (это публичная реакция на атаку корпоративной сети).

Разделение сети на обособленные сегменты должно обеспечивать соответствие ее физической и логической инфраструктур. Компьютеры, выполняющие сходные задачи должны объединяться в группы. Разным группам компьютеров в зависимости от их задач требуется разная степень защиты, реализуемая разными механизмами. Сегментированная сеть понятнее в администрировании, т.к. разные администраторы четко знают пределы своей ответственности.

Процедуры экстренного восстановления нельзя сбрасывать со счетов, поскольку часто от скорости восстановления системы после сбоя зависит количество убытков организации. Поэтому при разработке плана защиты сети необходимо утвердить стратегию архивации, создать специальную группу администраторов, занимающихся восстановлением.

Что касается психологического аспекта, необходимо учесть, что активное внедрение в сознание пользователей информации о защите системы почти столь же эффективно, как и непосредственное наличие этой системы защиты. В случае обнаружения атаки на корпоративную сеть и ее успешного отражения, необходимо доводить информацию об этом до сведения сотрудников. Подобная информация остановит большинство внутренних атак на сеть, которые могли быть предприняты сотрудниками предприятия. **Запрашивающее устройство** – это устройство, на котором

выполняется совместимое с 802.1X клиентское программное обеспечение, доступное для проводных или беспроводных устройств.

Коммутатор (Аутентификатор) – коммутатор выступает в роли посредника (прокси) между клиентом и сервером аутентификации. Он запрашивает идентификационные данные у клиента, проверяет эту информацию на сервере аутентификации и передает ответ клиенту. Другим устройством, которое может действовать как аутентификатор, является беспроводная точка доступа.

Сервер аутентификации – сервер проверяет подлинность клиента и уведомляет коммутатор или беспроводную точку доступа о том, что клиент имеет или не авторизован для доступа к локальной сети и услугам коммутатора.

СПИСОК ЛИТЕРАТУРЫ

1. Гельбух С. С. Сети ЭВМ и телекоммуникации. Архитектура и организация [Электронный ресурс]: учебное пособие. - Санкт-Петербург: Лань, 2019. - 208 с.
2. Самуйлов К. Е., Василевский В. В., Васин Н. Н., Королькова А. В., Шалимов И. А., Кулябов Д. С. Сети и телекоммуникации [Электронный ресурс]: Учебник и практикум для вузов. - Москва: Юрайт, 2020. - 363 с.
3. Сергеев А. Н. Основы локальных компьютерных сетей [Электронный ресурс]: учебное пособие для вузов. - Санкт-Петербург: Лань, 2021. - 184 с.
4. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учеб. пособие для вузов. - СПб.: Питер, 2008. - 958 с.
5. Интернет-лаборатория Термилаб сетевой академии Cisco при РТУ МИРЭА <https://lms.termilab.ru>.