ICND2

Interconnecting Cisco Networking Devices Part 2

Том 1

Версия 1.0

Руководство для студента

Номер текста по каталогу: 97-2509-01

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Содержание

Том 1

Введение в курс

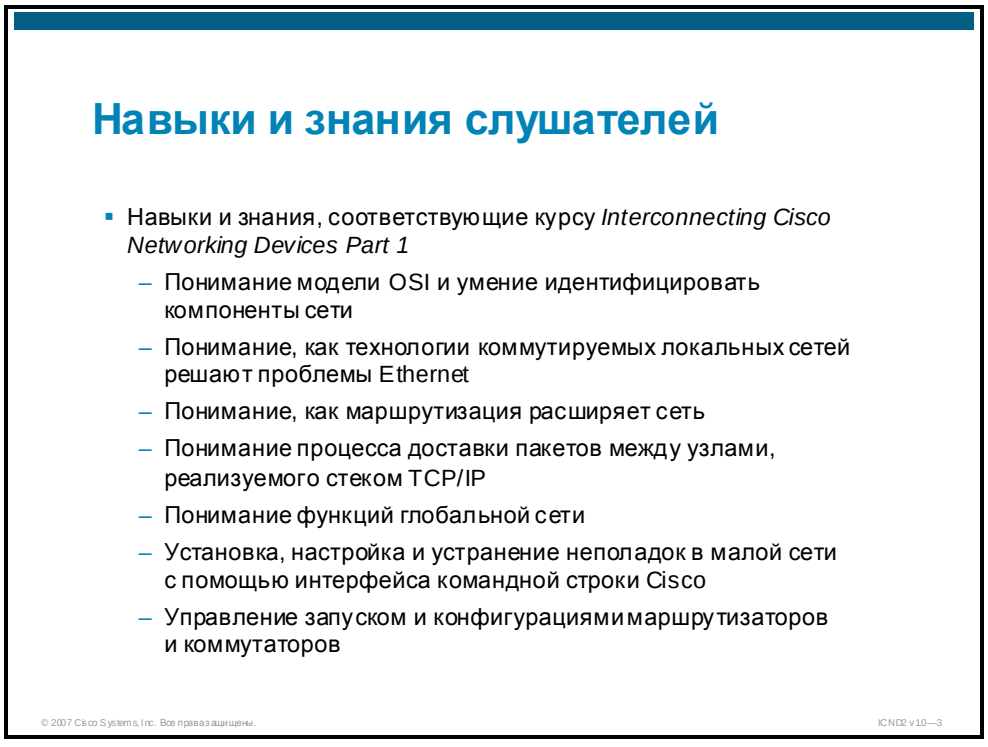
Обзор

Interconnecting Cisco Networking Devices Part 2 (ICND2) v1.0 — это курс под руководством инструктора, который партнеры Cisco по обучению предлагают конечным заказчикам. Этот пятидневный курс ориентирован на использование коммутаторов Cisco Catalyst и маршрутизаторов Cisco, включенных в локальные и глобальные сети, которые часто встречаются на сетевых площадках среднего размера.

По окончании этого курса вы сможете выполнять настройку и проверку, а также устранение неполадок для различных сетевых устройств Cisco.

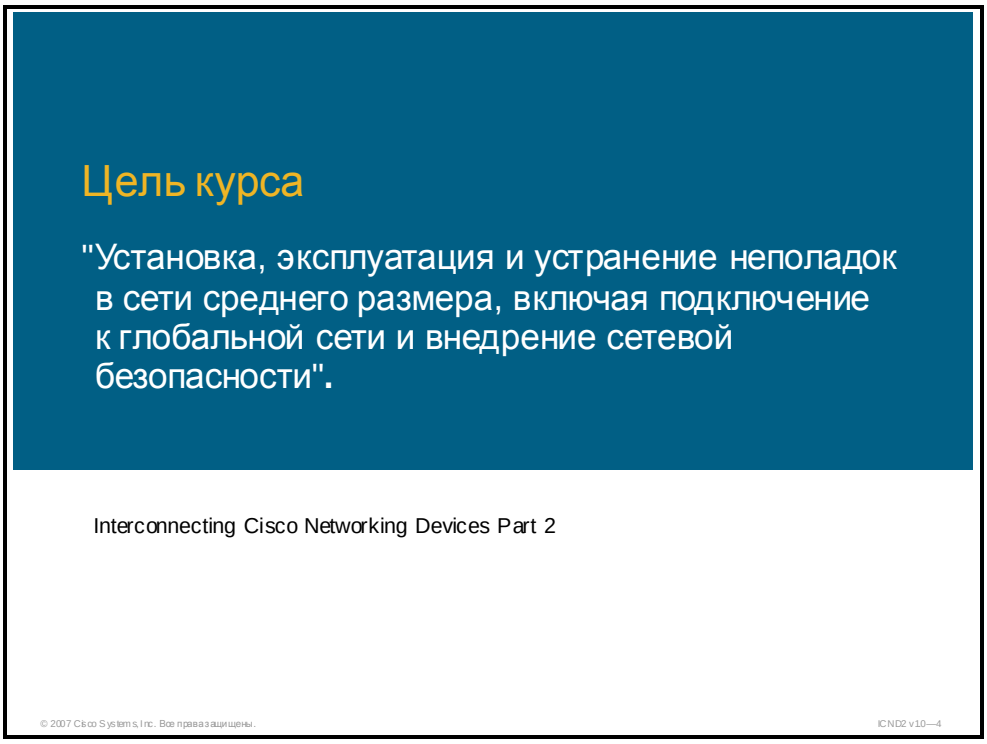
Навыки и знания слушателей

В этом подразделе перечисляются навыки и знания, которыми слушатели должны обладать, чтобы извлечь максимальную пользу из этого курса. Кроме того, здесь приводятся рекомендуемые решения Cisco по обучению, с которыми слушатели должны ознакомится, чтобы получить максимум от этого курса.



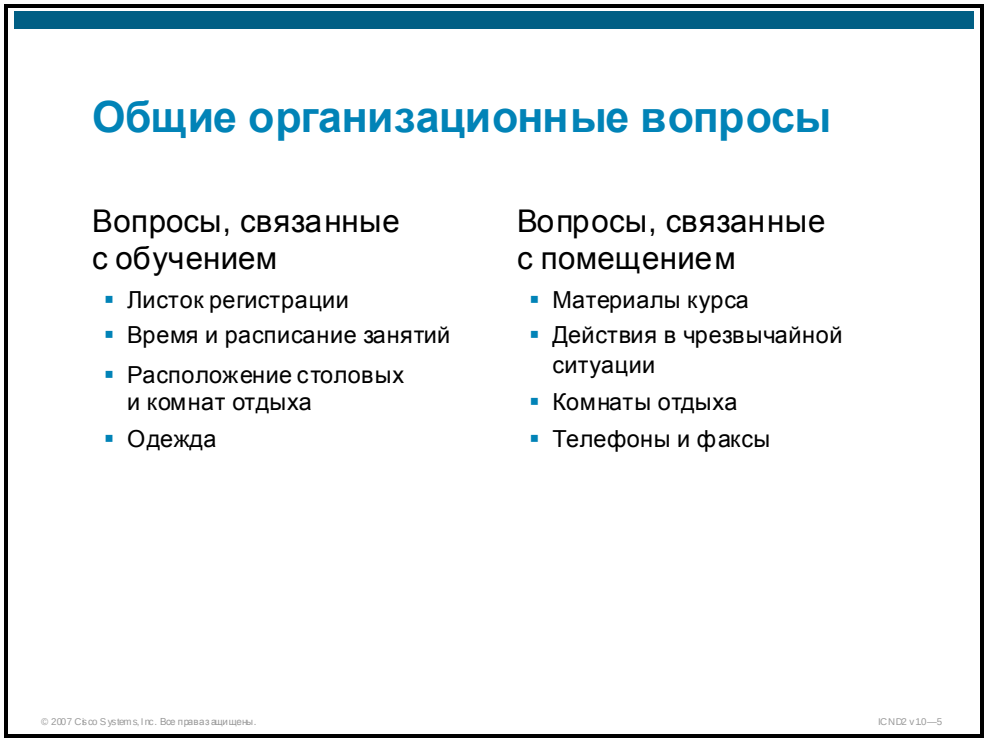
Цели и задачи курса

В этом разделе описываются цели и задачи курса.



В ходе этого курса вы должны выполнить следующие задачи:

- повторить изученный материал по настройке и устранению неполадок малой сети;
- расширить малую коммутируемую локальную сеть до локальной сети среднего размера с несколькими коммутаторами, поддержкой VLAN, транкинга и связующего дерева;
- описывать концепции маршрутизации в применении к сети среднего размера и анализировать ключевые факторы при внедрении маршрутизации в сети;
- выполнить настройку, проверку и устранение неполадок OSPF;
- выполнить настройку, проверку и устранение неполадок EIGRP;
- определять способы внедрения списков контроля доступа в зависимости от требований сети, а также выполнять настройку, проверку и устранение неполадок списков контроля доступа;
- описывать условия, в которых следует внедрять NAT или PAT в сети среднего размера, настраивать NAT и PAT на маршрутизаторах, объяснять принципы адресации IPv6 и настраивать протокол IPv6 на маршрутизаторе Cisco;
- определять и внедрять технологии глобальной сети в соответствии с требованиями сети.



Инструктор обсудит эти организационные вопросы, чтобы дать слушателям представление о том, чего им следует ждать от курса:

- процесс регистрации;
- время начала и примерное время окончания каждого учебного дня;
- перерывы между занятиями и перерыв на обед;
- одежда, пригодная для курса;
- материалы, которые слушатели получат во время обучения;
- действия в чрезвычайной ситуации;
- расположение комнат отдыха;
- отправление и получение телефонных и факсимильных сообщений.

Программа курса

В этом разделе представлена рекомендуемая последовательность освоения материалов курса.

Этот график отражает рекомендуемую структуру курса. Эта структура дает достаточно времени, чтобы инструктор мог донести информацию курса до слушателей, и чтобы слушатели могли выполнить лабораторные упражнения. Точное время тематических занятий и лабораторных работ зависит от ритма, в котором работает ваш класс.

Дополнительные справочные материалы

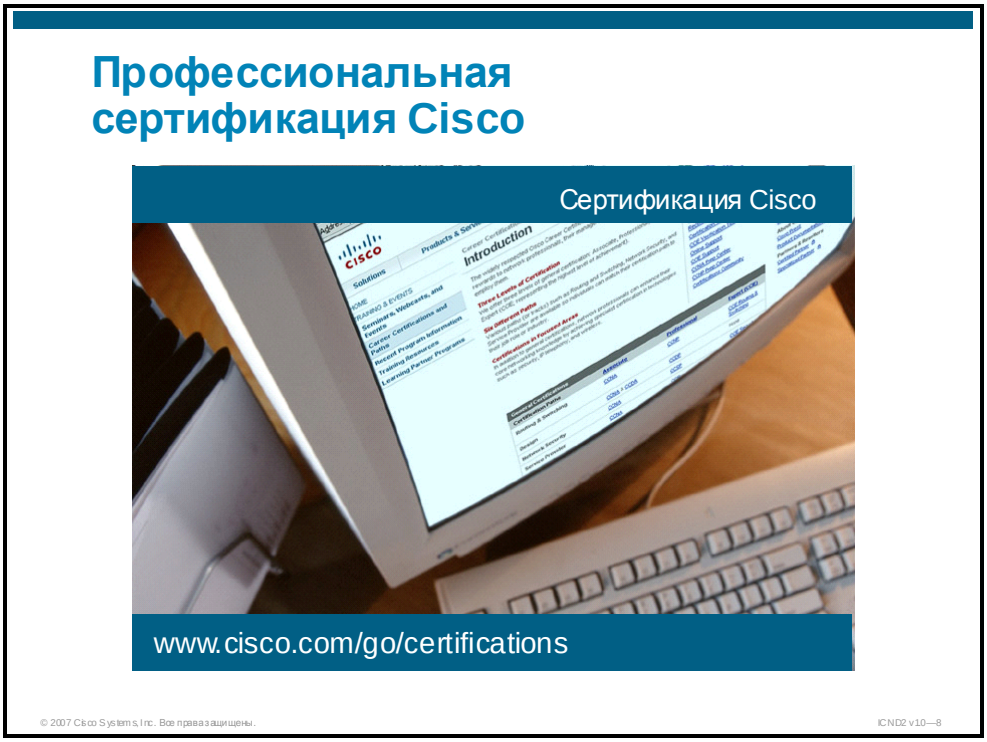
В этом разделе представлены значки и символы Cisco, используемые в этом курсе, а также сведения о том, где найти дополнительные технические материалы.

Глоссарий терминов Cisco

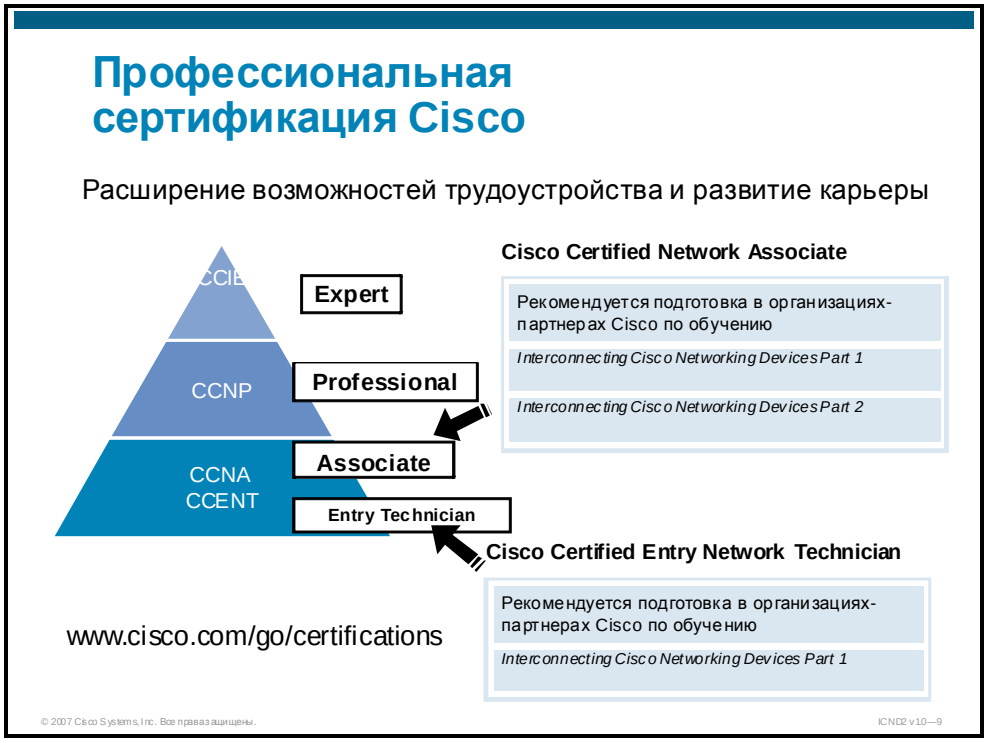
Дополнительные сведения о терминологии Cisco см. в *глоссарии сетевых терминов и аббревиатур Cisco* по адресу http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/index.htm.

Учебный план курса

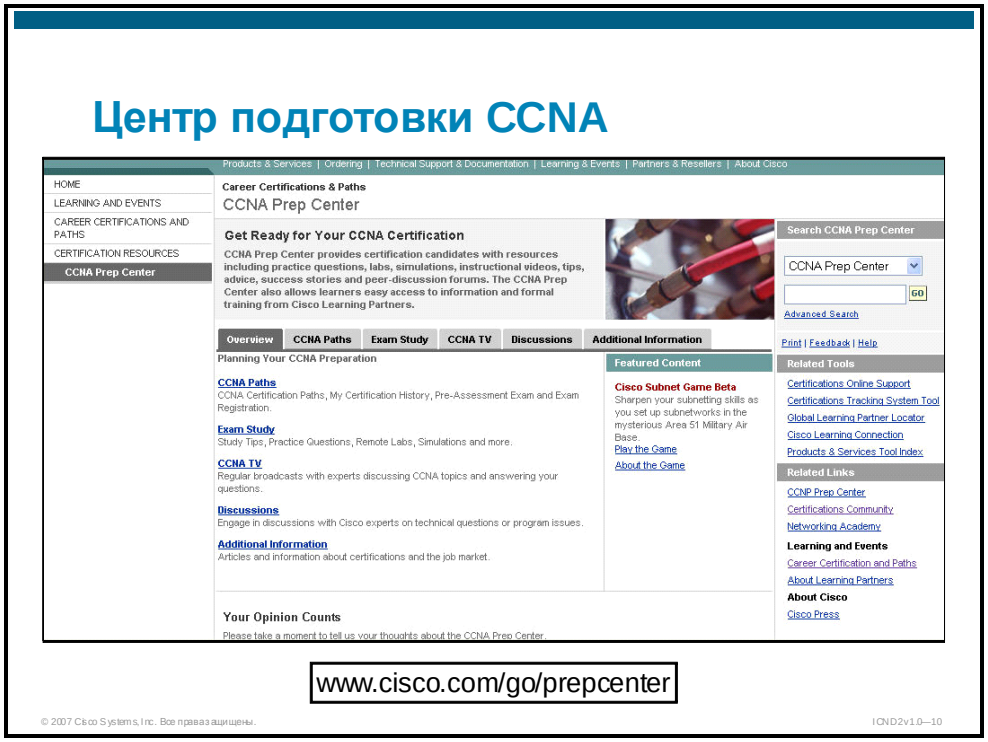
В этом разделе представлен учебный план курса.



Мы предлагаем вам присоединиться к сообществу сертификации Cisco, форум открыт для всех владельцев профессиональных сертификатов Cisco (таких как Cisco CCIE®, CCNA®, CCDA®, CCNP®, CCDP®, CCIP®, CCVP™ или CCSP®). Форум представляет собой место встречи для сертифицированных профессионалов Cisco, где они могут обмениваться вопросами, предложениями и сведениями по программам профессиональной сертификации Cisco и другим темам, связанным с сертификацией. Дополнительные сведения см. по адресу www.cisco.com/go/certifications.



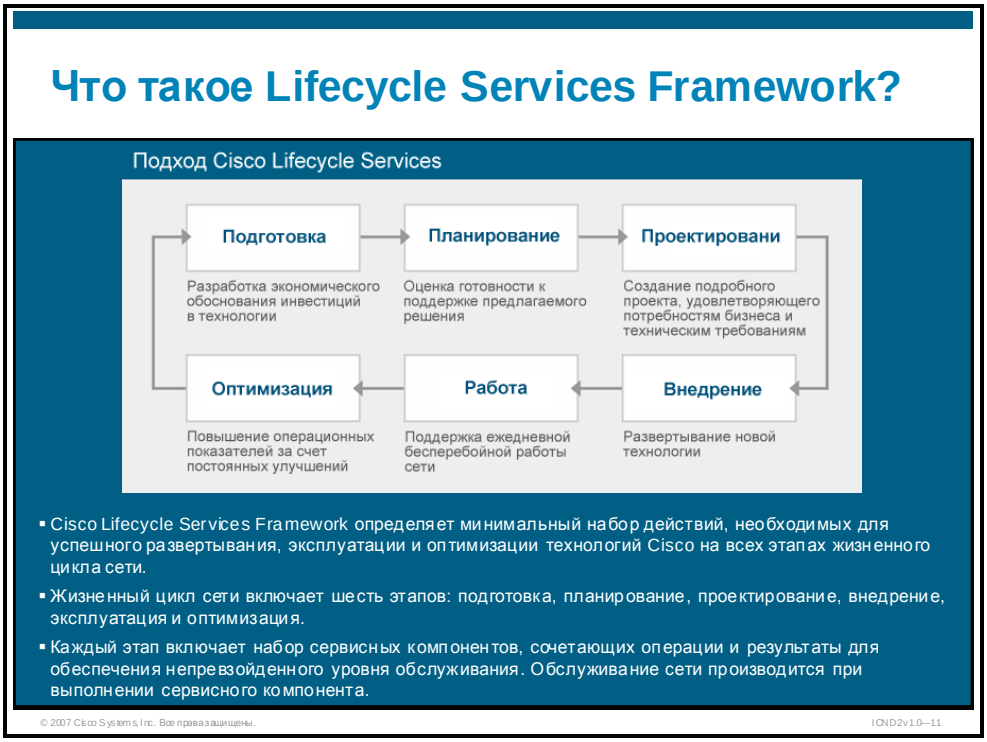
Дополнительные сведения о сертификации см. по адресу www.cisco.com/go/certifications.



Кроме того, информацию можно найти на странице www.cisco.com/go/prepcenter.

Структура услуг Lifecycle Services

На этом рисунке представлен общий обзор концепции жизненного цикла сети и подхода Cisco Lifecycle Services. Для успешного развертывание технологий требуется координация всей последовательности мероприятий. Эти мероприятия взаимосвязаны, взаимозависимы и следуют друг за другом в заданном порядке.



Этапы Cisco Lifecycle Services

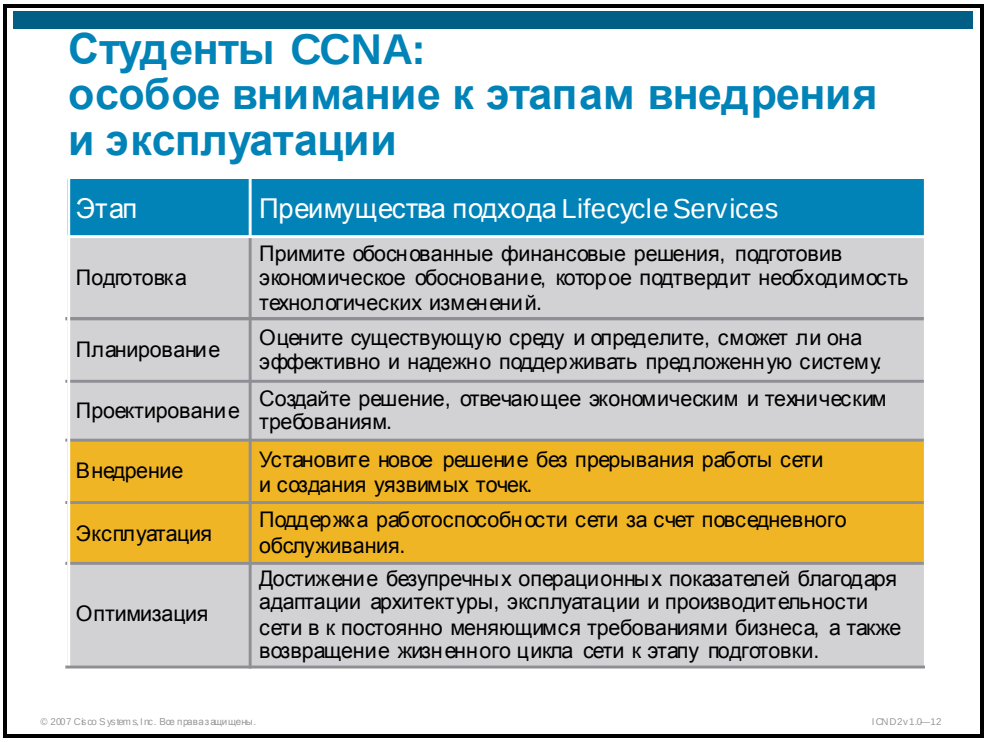
- **Подготовка:** принятие обоснованных решений по финансированию.
  - Создание экономического обоснования.
  - Уменьшение потребности в будущих модификациях за счет создания общей, концептуальной архитектуры.
- **Планирование:** создание основы для своевременного и беспрепятственного внедрения.
  - Оценка сети и площадок.
  - Разработка плана управления проектом.
- **Проектирование:** снижения риска модификаций, быстрое и успешное внедрение.
  - Разработка всестороннего детального проекта, отвечающего как экономическим, так и техническим требованиям.
- **Внедрение:** быстрый возврат инвестиций.
  - Интеграция устройств без прерывания работы существующей сети и создания уязвимых точек.
- **Эксплуатация:** поддержка высокой доступности и сокращение затрат.
  - Поддержка работоспособности сети за счет повседневного обслуживания.

- **Оптимизация:** улучшение производительности, доступности, емкости и безопасности.
  - Достижение безупречных операционных результатов за счет непрерывного улучшения производительности и функциональности системы.

Традиционный подход к сетевой безопасности подразумевает использование наборов продуктов для защиты сетевого периметра или соединений между площадками. В современных условиях методы поиска и устранения отдельных уязвимостей и "точечных" проблем сети перестают быть достаточными, поскольку затраты, связанные с нарушениями и прерываниями работы систем безопасности высоки и могут принимать множество форм — простой сети, кража конфиденциальной безопасности, упущенная прибыль, уменьшение престижа фирмы и так далее.

В настоящее время используется другой подход к решениям по безопасности:

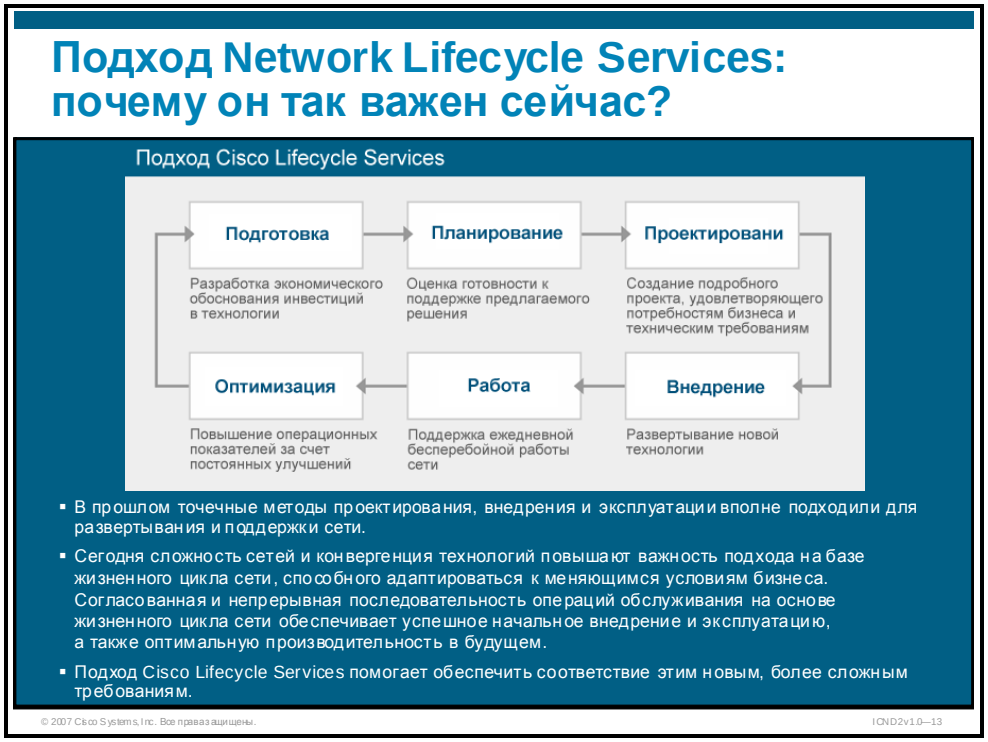
- теперь безопасность требует системного подхода, подразумевающего защиту всей сети — периметра, ЦОД, локальных сетей кампусов, беспроводных локальных сетей (WLAN) рабочих станций и терминальных узлов;
- обеспечение безопасности сети — это непрерывный процесс, который позволяет компании добиться эффективного выполнения корпоративных целей и задач.
- любая организация нуждается во всестороннем процессе обеспечения безопасности, который согласует задачи бизнеса, возможности сети и технические требования.



Подход Cisco Lifecycle Services

Подход Cisco Lifecycle Services позволяет определить минимальный набор необходимых операций (в зависимости от сложности технологии и сети) для успешного развертывания и эксплуатации технологий Cisco и оптимизации их производительности на всех этапах жизненного цикла сети. Жизненный цикл сети — это комплексное представление последовательности событий, которые имеют место на разных этапах существования сети.

Подход Cisco Lifecycle Services формирует методики, основанные на передовом опыте, который находит понимание и поддержку в сетевой отрасли, и согласует процессы обслуживания и поддержки с экономическими и техническими требованиями на всех этапах жизненного цикла сети.



В прошлом точечные методы проектирования, внедрения и эксплуатации вполне подходили для развертывания и поддержки сети.

Сегодня сложность сетей и конвергенция технологий повышают важность подхода на базе жизненного цикла сети, способного адаптироваться к меняющимся условиям бизнеса. Согласованная и непрерывная последовательность операций обслуживания на основе жизненного цикла сети обеспечивает успешное начальное внедрение и эксплуатацию, а также оптимальную производительность в будущем.

Подход Cisco Lifecycle Services помогает обеспечить соответствие этим новым, более сложным требованиям.

Представление слушателей

- Ваше имя
- Ваша компания
- Служебные обязанности
- Навыки и знания
- Краткая история
- Задача

Подготовьте следующие сведения

- Ваше имя.
- Ваша компания.
- Ваши служебные обязанности.
- Навыки, которыми вы владеете.
- Краткий обзор вашего профессионального опыта.
- Что бы вы хотели узнать из этого курса.

Модуль 1

Внедрение малой сети

Обзор

По мере роста и усложнения малых сетей, расширение их функциональности и повышение степени контроля над компонентами сети с помощью интеллектуальных сетевых устройств, таких как коммутаторы и маршрутизаторы, становится критически важным. Большинство аппаратных платформ Cisco, в том числе коммутаторы и маршрутизаторы используют ПО Cisco IOS. Это программное обеспечение позволяет использовать сетевые службы в продуктах Cisco, включая перенос сетевых протоколов и функций, контроль доступа, запрет несанкционированного использования сети, а также добавление интерфейсов и возможностей по мере роста сети. Для ввода параметров конфигурации в маршрутизаторы и коммутаторы в соответствии с требованиями организации к сети используется интерфейс командной строки (CLI) программного обеспечения Cisco IOS.

Задачи модуля

В ходе выполнения этого модуля вы повторили пройденный материал по настройке и устранению неполадок малой сети. Это значит, что вы способны выполнить следующую задачу:

- внедрение базовой конфигурации маршрутизатора и коммутатора и обеспечение правильной работы устройств.

Занятие 1

Введение в лабораторную работу для повторения пройденного

Обзор

ПО Cisco IOS используется на большинстве аппаратных платформ Cisco, включая маршрутизаторы и коммутаторы. Оно позволяет использовать сетевые службы в продуктах Cisco, в том числе перенос выбранных сетевых протоколов и функций, а также добавление интерфейсов и возможностей по мере роста сети.

Это занятие предназначено для повторения базовых знаний, необходимых для прохождения данного курса. Оно подразумевает повторение пройденного материала по структуре интерфейса командной строки (CLI) Cisco IOS и командам Cisco IOS, используемым для создания базовых конфигурации маршрутизатора и коммутатора. Вы воспользуетесь этими командами во время вводной лабораторной работы для создания начальной конфигурации, которая будет использоваться во всех последующих упражнениях.

Задачи

Во время выполнения этого задания вы повторили пройденный материал по настройке малой сети. Это значит, что вы способны выполнить следующие задачи:

- описывать функции интерфейса командной строки;
- описывать режимы конфигурации ПО Cisco IOS;
- описывать справочные модули ПО Cisco IOS;
- внедрять базовую конфигурацию маршрутизатора и коммутатора и обеспечивать их правильную работу.

Функции интерфейса командной строки Cisco IOS

ПО Cisco IOS использует интерфейс командной строки в качестве традиционной консольной среды для ввода команд. В этом разделе рассматриваются функции интерфейса командной строки Cisco IOS.

ПО Cisco IOS является базовой технологией, которая используется во многих продуктах, однако особенности его эксплуатации могут меняться в зависимости от конкретного устройства. Чтобы ввести команду в интерфейсе командной строки, введите или вставьте текст в одном из нескольких режимах конфигурации консоли. В режиме конфигурации терминала вызывается шаговый компилятор. Команды конфигурации вводятся, когда пользователь нажимает клавишу **ВВОД**.

Если в команде нет синтаксических ошибок, она выполняется и сохраняется в работающей конфигурации. Команда вступает в действие немедленно, но автоматическое сохранение в энергонезависимой памяти (NVRAM) не выполняется.

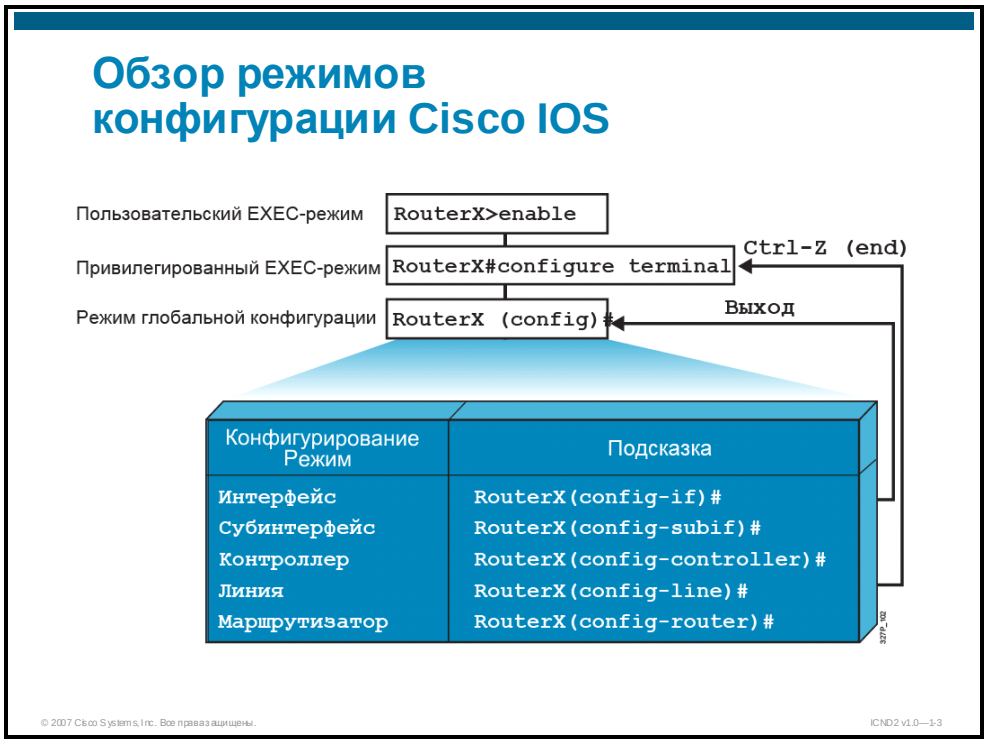
В структуре режимов конфигурации ПО Cisco IOS применяется иерархия команд. Все режимы конфигурации обозначаются отдельным приглашением. В каждом режиме конфигурации поддерживаются определенные команды Cisco IOS, связанные с режимом эксплуатации устройства.

По соображениям безопасности ПО Cisco IOS использует сеансы EXEC с двумя уровнями доступа.

- **User EXEC (пользовательский режим EXEC).** Обеспечивает доступ к ограниченному количеству базовых команд мониторинга.
- **Privileged EXEC (привилегированный режим EXEC).** Обеспечивает доступ ко всем командам устройства, в том числе командам для конфигурации и управления. Вход в этот режим может быть защищен паролем, чтобы разрешить доступ к устройству только авторизованным пользователям.

Режимы конфигурации ПО Cisco IOS

В привилегированном режиме EXEC вы можете войти в режим глобальной конфигурации, который обеспечивает доступ к другим режимам конфигурации Cisco. В этом разделе описываются режимы конфигурации Cisco IOS.



Первый метод конфигурации устройства Cisco — утилита установки, которая позволяет создать базовую начальную конфигурацию. Для создания более сложных и специализированных конфигураций используйте интерфейс командной строки, чтобы войти в режим конфигурации терминала.

В привилегированном режиме EXEC для входа в режим глобальной конфигурации используется команда **configure terminal**. В режиме глобальной конфигурации вы можете получить доступ к специальным режимам, включая (но не ограничиваясь) следующее:

- **Interface (интерфейс).** Поддерживает команды, которые используются для настройки отдельных интерфейсов.
- **Subinterface (субинтерфейс).** Поддерживает команды, которые используются для настройки нескольких виртуальных интерфейсов на одном физическом интерфейсе.
- **Controller (контроллер).** Поддерживает команды, которые используются для настройки контроллеров (например, контроллеров E1 и T1).
- **Line (канал).** Поддерживает команды, которые используются для настройки терминального канала, например консоли или портов VTY.
- **Router (маршрутизатор).** Поддерживает команды, которые используются для настройки протокола маршрутизации IP.

Если вы введете команду **exit**, маршрутизатор вернется на один уровень назад и, в конечном итоге, вы выйдете из системы. Как правило, команда **exit** вводится в специальных режимах конфигурации для возвращение в режим глобальной конфигурации. Нажмите **Ctrl-Z** или введите команду **end**, чтобы выйти из режима конфигурации и вернуться в привилегированный режим EXEC.

Команды, влияющие на устройство в целом, называются глобальными командами. Примеры глобальных команд: **hostname** и **enable password**.

Команды, указывающие или обозначающие процесс или интерфейс, который необходимо настроить, называются основными командами. Основные команды переводят интерфейс командной строки в специальный режим конфигурации. Основные команды не оказывают влияния на конфигурацию, если после них не вводится субкоманда с параметром конфигурации. Например, основная команда **interface serial 0** не оказывает влияния на конфигурацию, если после нее не введена субкоманда, которая указывает, что необходимо сделать с интерфейсом.

Ниже приведены примеры основных команд и соответствующих субкоманд.

```
Основная команда:   RouterX(config)#interface serial 0
Субкоманда:         RouterX(config-if)#shutdown

Основная команда:   RouterX(config-if)#line console 0
Субкоманд:          RouterX(config-line)#password cisco

Основная команда:   RouterX(config-line)#router rip
Субкоманда:         RouterX(config-router)#network 10.0.0.0
```

Обратите внимание, что при вводе основной команды выполняется переход из одного режима конфигурации в другой.

Примечание. Для изменения режима конфигурации не нужно возвращаться в режим глобальной конфигурации.

Справочные модули интерфейса командной строки Cisco IOS

ПО Cisco IOS включает несколько справочных модулей для интерфеса командной строки, включая контекстную справку. В этом разделе описывается использование клавиатурной справки в интерфейсе командной строки.

Чтобы получить справку, вы можете ввести знак вопроса (**?**) в любой момент во время сеанса EXEC. Доступно два типа контекстной справки.

- **Справка по словам.** Введите команду **?**, чтобы получить справку по словами для списка команд, которые начинаются с указанной последовательности символов. Введите последовательность символов после знака вопроса. Не ставьте пробел между знаком вопроса и последовательностью символов. Маршрутизатор выведет список команд, которые начинаются с указанных символов.
- **Справка по синтаксису команды.** Введите команду **?**, чтобы получить справку по синтаксису команды, которую вы хотите ввести. Введите знак вопроса вместо ключевого слова или аргумента. Перед знаком вопроса необходимо ввести пробел. Сетевое устройство выведет список доступных параметров команды. "<cr>" обозначает возврат каретки.

Обзор команд

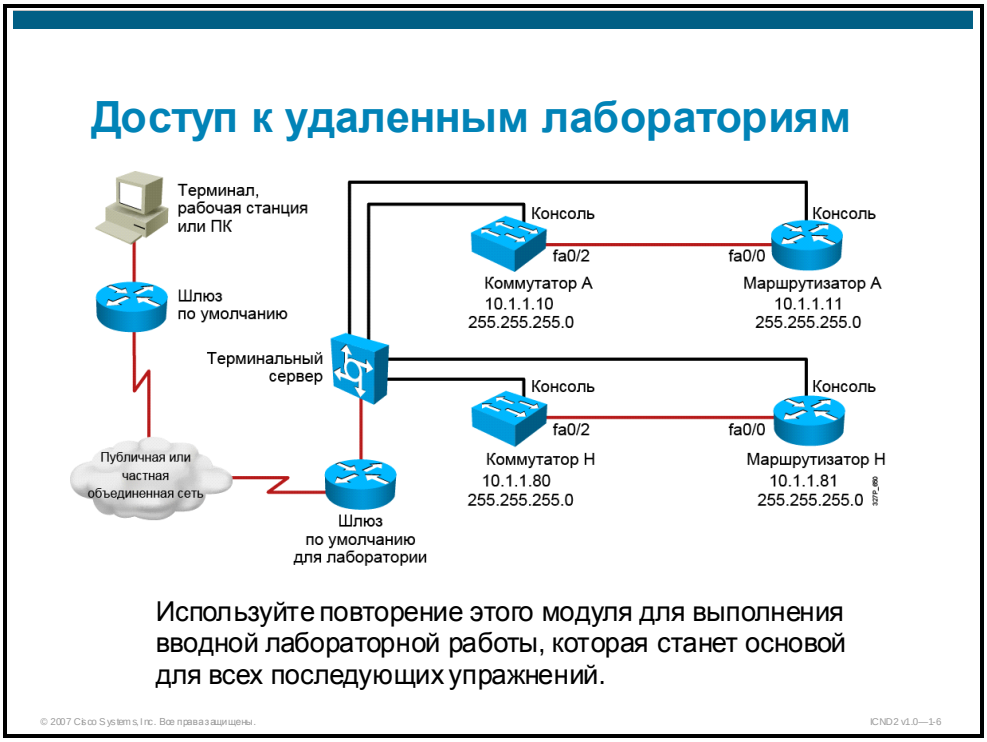
В этом разделе приводится обзор базовых команд интерфейса командной строки ПО Cisco IOS.

В таблице ниже приводятся команды интерфейса командной строки Cisco IOS, которые используются в маршрутизаторах и коммутаторах Cisco для создания базовой конфигурации в среде малой сети.

Обзор команд

Команда	Описание
banner motd	Настраивает баннер "Сообщение дня".
configure terminal	Переводит устройство в режим глобальной конфигурации из привилегированного режима EXEC.
copy running-config startup-config	Сохраняет работающую конфигурацию в энергонезависимую память (NVRAM) в качестве загрузочной конфигурации.
enable	Открывает интерпретатор команд в привилегированном режиме EXEC.
enable secret *пароль*	Устанавливает и активирует пароль для входа в привилегированный режим EXEC.
erase startup-configuration	Удаляет загрузочную конфигурацию из памяти.
hostname *имя*	Присваивает устройству имя узла.
interface *интерфейс*	Указывает интерфейс и активирует режим конфигурации интерфейса.

Команда	Описание
ip address *маска адреса*	Устанавливает IP-адрес и маску устройства.
ip default-gateway *адрес*	Устанавливает шлюз по умолчанию для коммутатора.
line console 0	Указывает канал консоли и активирует режим конфигурации канала.
line vty 0 4	Указывает канал VTY и активирует режим конфигурации канала.
login	Устанавливает запрос пароля при входе.
password *пароль*	Устанавливает пароль в канале.
ping *ip-адрес*	Использует эхо-запросы и эхо-ответы ICMP, чтобы определить, активен ли удаленный узел.
reload	Reboots the device to make your changes take effect.
show cdp neighbors	Отображает обновления протокола CDP (протокола обнаружения Cisco), полученные на всех локальных интерфейсах устройства.
show interfaces	Отображает сведения обо всех интерфейсах устройства.
show port-security [interface *идентификатор интерфейса*] **[address]**	Отображает административные и операционные состояния всех защищенных портов коммутатора. Также может отображать параметры безопасности определенного интерфейса или все защищенные MAC-адреса.
show running-configuration	Отображает активную конфигурацию.
show startup-configuration	Отображает параметры конфигурации в NVRAM маршрутизатора.
shutdown/no shutdown	Отключает или включает интерфейс.
switchport mode access	Устанавливает режим доступа для порта. Используйте версию "**no**" этой команды, чтобы вернуться к значением по умолчанию.
switchport port-security	Включает защиту порта на интерфейсе; вводится без ключевых слов.
switchport port-security mac-address *mac-адрес*	Назначает порту безопасный MAC-адрес. Используйте версию "**no**" этой команды, чтобы удалить MAC-адрес.
switchport port-security maximum *значение*	Устанавливает максимальное количество безопасных MAC-адресов для интерфейса.

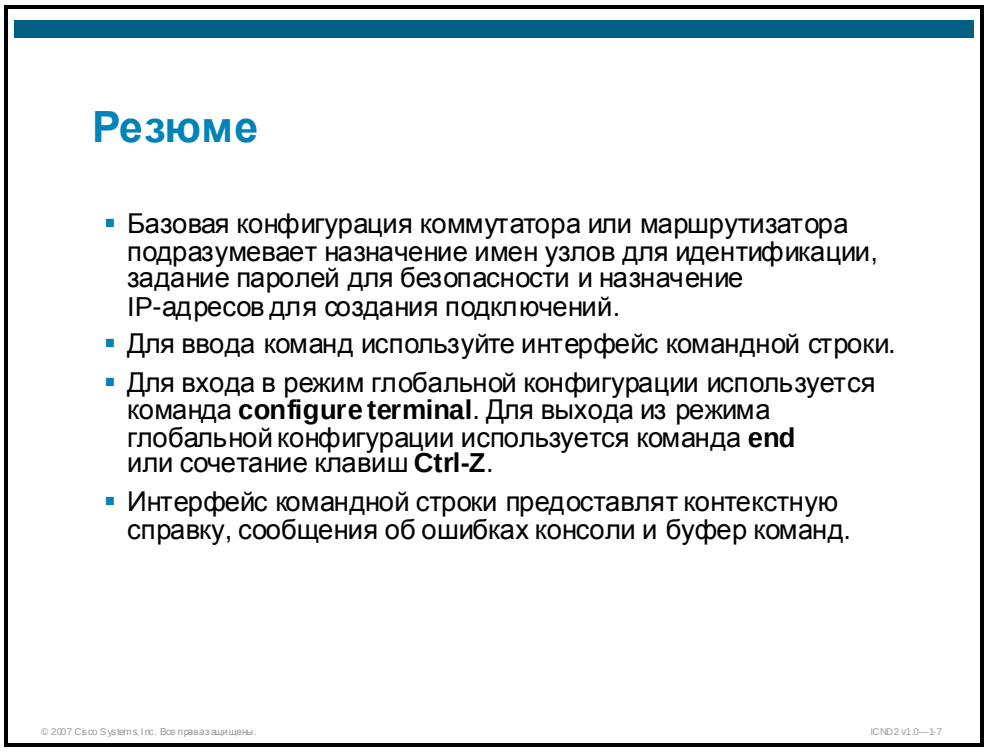


Для выполнения вводной лабораторной работы необходимо использовать удаленное лабораторное оборудование. Инструктор предоставит все сведения, необходимые для доступа к оборудованию.

Используйте навыки и знания, которые вы повторили во время этого занятия, чтобы выполнить вводную лабораторную работу, которая станет основой для всех остальных лабораторных упражнений.

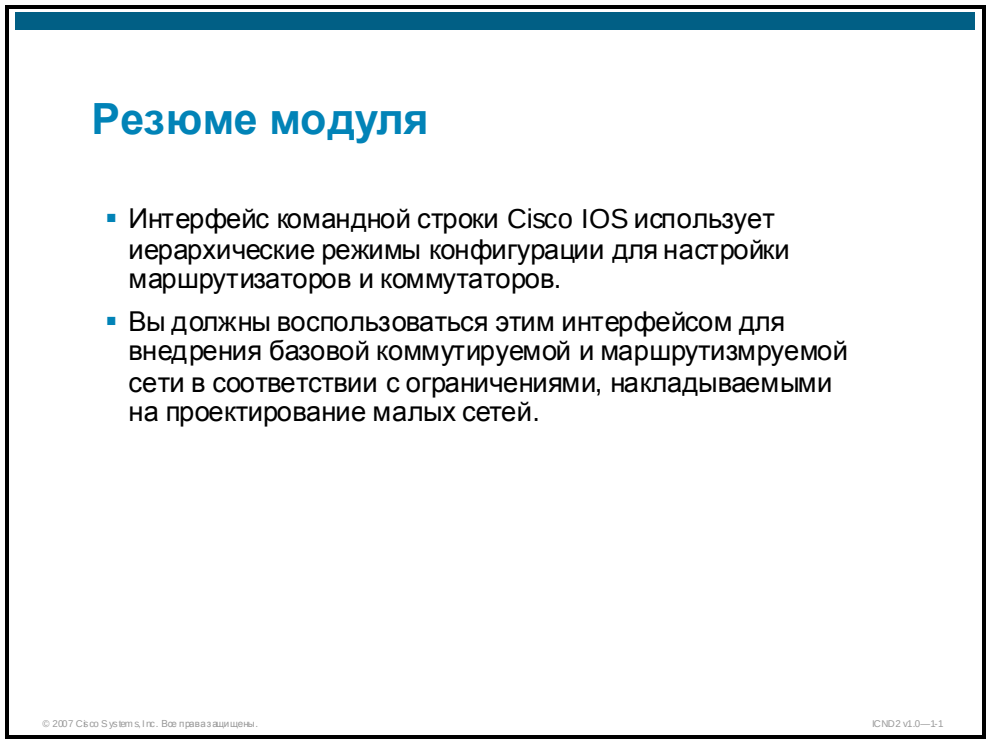
Резюме

В этом разделе приводятся основные вопросы, рассмотренные в этом занятии.



Резюме модуля

В этом разделе приводится резюме вопросов, рассмотренных в модуле.



Базовая конфигурация маршрутизатора или коммутаора включает назначение имен узлов для идентификации, назначение паролей для безопасности и выделение IP-адресов для создания подключений.

Вопросы для самопроверки по модулю

Используйте эти вопросы, чтобы повторить материал, изученный в данном модуле. Верные ответы и решения можно найти в разделе "Ответы на вопросы для самопроверки".

В1) Какой уровень доступа позволяет использовать все команды маршрутизатора и может быть защищен паролем для предотвращения несанкционированного доступа к маршрутизатору? (Источник: введение в лабораторную работу для повторения пройденного)

А) уровень "user EXEC"
Б) уровень "setup EXEC"
В) уровень "enable EXEC"
Г) уровень "privileged EXEC"

В2) Что надо сделать, чтобы устройство Cisco обработало и выполнило введенную команду? (Источник: введение в лабораторную работу для повторения пройденного)

А) Нажать клавишу **Send**.
Б) Нажать клавишу **ВВОД**.
В) Добавить пробел в конце команды.
Г) Подождать 5 секунд после ввода команды.

В3) Какое приглашение интерфейса командной строки CLI обозначает привилегированный режим EXEC? (Источник: введение в лабораторную работу для повторения пройденного)

А) hostname#
Б) hostname>
В) hostname-exec>
Г) hostname-config

В4) Какую команду необходимо ввести в режиме EXEC, чтобы вывести список всех доступных параметров команды? (Источник: введение в лабораторную работу для повторения пройденного)

А) **?**
Б) init
В) **help**
Г) **login**

В5) Какую команду интерфейса командной строки необходимо выполнить, чтобы вывести список команд, начинающихся с буквы "c" на коммутаторе Cisco Catalyst? (Источник: введение в лабораторную работу для повторения пройденного)

А) **c?**
Б) **c ?**
В) **help c**
Г) **help c***

В6) Какую команду интерфейса командной строки необходимо ввести, чтобы получить справку по синтаксису команды и узнать, как закончить команду, которая начинается с "config"? (Источник: введение в лабораторную работу для повторения пройденного)

А) **config?**
Б) **config ?**
В) **help config**
Г) **help config***

В7) Какая команда Cisco IOS настраивает IP-адрес и маску подсети на коммутаторе? (Источник: введение в лабораторную работу для повторения пройденного)

А) **ip address**
Б) **ip address 196.125.243.10**
В) **196.125.243.10 ip address**
Г) **ip address 196.125.243.10 255.255.255.0**

В8) Какой режим конфигурации используется для настройки отдельного порта коммутатора? (Источник: введение в лабораторную работу для повторения пройденного)

А) пользовательский режим
Б) режим глобальной конфигурации
В) режим конфигурации интерфейса
Г) режим конфигурации контроллера

В9) При использовании команды **show interface** для отображения состояния и статистики интерфейсов, настроенных на коммутаторе Catalyst, какое поле выходных данных обозначает MAC-адрес, идентифицирующий аппаратное обеспечение интерфейса? введение в лабораторную работу для повторения пройденного)

А) MTU 1500 bytes
Б) Hardware is … 10BaseT
В) Address is 0050.BD73.E2C1
Г) 802.1d STP State: Forwarding

В10) Какая команда **show** требует доступа к привилегированному режиму EXEC? (Источник: введение в лабораторную работу для повторения пройденного)

А) **show ip**
Б) **show version**
В) **show running**
Г) **show interfaces**

В11) Какое утверждение наилучшим образом отвечает на вопрос, какие команды пользовательского режима EXEC позволяют настраивать маршрутизатор Cisco? (Источник: введение в лабораторную работу для повторения пройденного)

А) Вы не можете настраивать что-либо, команды пользовательского режима используются для вывода информации.
Б) Пользовательский режим EXEC позволяет выполнять глобальные задачи конфигурации, влияющие на маршрутизатор в целом.
В) Команды пользовательского режима EXEC позволяют ввести пароль, который обеспечивает доступ к настройке маршрутизатора.
Г) Команды пользовательского режима EXEC позволяют настраивать интерфейсы, субинтерфейсы, каналы и маршрутизаторы.

В12) Какая команда Cisco IOS используется для возвращения в пользовательский режим EXEC из привилегированного режима EXEC? (Источник: введение в лабораторную работу для повторения пройденного)

А) **exit**
Б) **quit**
В) **disable**
Г) **userexec**

B13) Сопоставьте типы справки, доступные в интерфейсе командной строки Cisco IOS, их описаниям. (Источник: введение в лабораторную работу для повторения пройденного)

_____ 1. контекстная справка

_____ 2. сообщения об ошибках консоли

_____ 3. буфер команд

А) отображает список команд и аргументов, связанных с определенной командой

Б) позволяет восстанавливать длинные или сложные команды или записи для повторного ввода, проверки или исправления

В) указывает на проблемы, связанные с неверным вводом команд маршрутизатора, что позволяет пользователю изменить или исправить эти команды

B14) Какая команда возвращает список недавно введенных команд из буфера команд после их восстановления? (Источник: введение в лабораторную работу для повторения пройденного)

А) **Ctrl-N**
Б) **Ctrl-P**
В) **show history**
Г) **show terminal**

B15) Какие сведения команда **show running-config** выводит на маршрутизаторе Cisco? (Источник: введение в лабораторную работу для повторения пройденного)

А) текущая (работающая) конфигурация в оперативной памяти
Б) аппаратное обеспечение системы и имена файлов конфигурации
В) объем энергонезависимой памяти (NVRAM), используемый для хранения конфигурации
Г) версия ПО Cisco IOS, работающего на маршрутизаторе

B16) Сопоставьте приглашения маршрутизатора соответствующим режимам конфигурации. (Источник: введение в лабораторную работу для повторения пройденного)

_____ 1. канал

_____ 2. маршрутизатор

_____ 3. интерфейс

_____ 4. контроллер

_____ 5. субинтерфейс

А) Router(config-if)#
Б) Router(config-line)#
В) Router(config-subif)#
Г) Router(config-router)#
Д) Router(config-controller)#

B17) Что происходит при вводе основной команды на маршрутизаторе Cisco? (Источник: введение в лабораторную работу для повторения пройденного)

А) Маршрутизатор возвращается в пользовательский режим EXEC.
Б) Маршрутизатор возвращает список доступных команд.
В) Маршрутизатор вызывает команду глобальной конфигурации.
Г) Маршрутизатор переходит из одного режима конфигурации в другой.

В18) Какая команда Cisco IOS создает сообщение, которое отображается при входе? (Источник: введение в лабораторную работу для повторения пройденного)

А) **hostname** *имя узла*
Б) **banner motd** *сообщение*
В) **hostname interface description**
Г) **description interface description**

В19) Если на маршрутизаторе настроены команды **enable secret** и **enable password**, что надо сделать, чтобы вывести приглашение #? (Источник: введение в лабораторную работу для повторения пройденного)

А) Ввести команду **enable secret**.
Б) Ввести команду **enable password**.
В) Ввести команду **enable secret** или **enable password**.
Г) Ввести команды **enable secret** и **enable password**.

В20) Какая команда Cisco IOS настраивает последовательный порт на порте 1 слота 0 модульного маршрутизатора? (Источник: введение в лабораторную работу для повторения пройденного)

А) **serial 0/1 interface**
Б) **interface serial 0 1**
В) **interface serial 0/1**
Г) **serial 0 1 interface**

В21) Какая команда Cisco IOS используется для установки тактовой частоты 64 кбит/с на последовательном интерфейсе маршрутизатора Cisco? (Источник: введение в лабораторную работу для повторения пройденного)

А) **clock rate 64**
Б) **clock speed 64**
В) **clock rate 64000**
Г) **clock speed 64000**

В22) Какие команды Cisco IOS настраивают IP-адрес и маску подсети на Ethernet-интерфейсе 1 слота 1? (Источник: введение в лабораторную работу для повторения пройденного)

А) **interface Ethernet 1 1**
ip address 192.168.1.1 mask 255.255.255.0
Б) **interface Ethernet 1/1**
ip address 192.168.1.1/24
В) **interface Ethernet 1 1**
ip address 192.168.1.1 255.255.255.0
Г) **interface Ethernet 1/1**
ip address 192.168.1.1 255.255.255.0

Ответы на вопросы для самопроверки по модулю

В1) Г
В2) Б
В3) А
В4) А
В5) А
В6) Б
В7) Г
В8) В
В9) В
В10) В
В11) А
В12) В
В13) 1=А, 2=В, 3=Б
В14) А
В15) А
В16) 1=Б, 2=Г, 3=А, 4=Д, 5=В
В17) Г
В18) Б
В19) А
В20) В
В21) В
В22) Г

Модуль 2

Создание коммутируемой сети среднего размера

Обзор

При расширении коммутируемой сети администраторы должны учитывать множество факторов. В своем портфеле сетевых коммутаторов Cisco предлагает решения, которые не только устраняют неотложные проблемы, связанные с административными изменениями, но и обеспечивают масштабируемость, совместимость, повышенную выделенную полосу пропускания и безопасность.

Задачи модуля

По окончании этого модуля вы сможете расширить малую коммутируемую локальную сеть до локальной сети среднего размера с несколькими коммутаторами, поддержкой VLAN, транкинга и связующего дерева. Это значит, что вы сможете выполнить следующие задачи:

- описывать, как и когда следует внедрять и проверять VLAN и транкинг, а затем развертывать их в сети;
- описывать ситуации, в которых следует использовать связующее дерево, и внедрять его в сети;
- описывать применение и конфигурацию маршрутизации между VLAN в сетях среднего размера;
- описывать решения, требующие средств безопасности второго уровня, и внедрять их в сети;
- определять методы поиска, устранения и изоляции распространенных проблем коммутируемой сети и предлагать решения этих проблем.

Занятие 1

Внедрение сетей VLAN и транковых подключений

Обзор

VLAN — это группа конечных станций с общим набором требований, не зависящая от физического расположения этих станций. VLAN (виртуальная локальная сеть) имеет те же свойства, что физическая локальная сеть, но позволяет группировать конечные станции, которые находятся в разных сегментах локальной сети. Кроме того, VLAN позволяет группировать порты коммутатора, чтобы ограничить лавинную рассылку одноадресного, многоадресного и широковещательного трафика. Трафик, созданный в определенной VLAN, рассылается только по портам, которые принадлежат к этой VLAN.

Понимание принципов работы VLAN и знание протоколов, которые в них используются, очень важно для настройки, проверки и устранения неполадок VLAN на коммутаторах Cisco. В этом занятии описывается принцип работы VLAN и протоколы, которые в них используется.

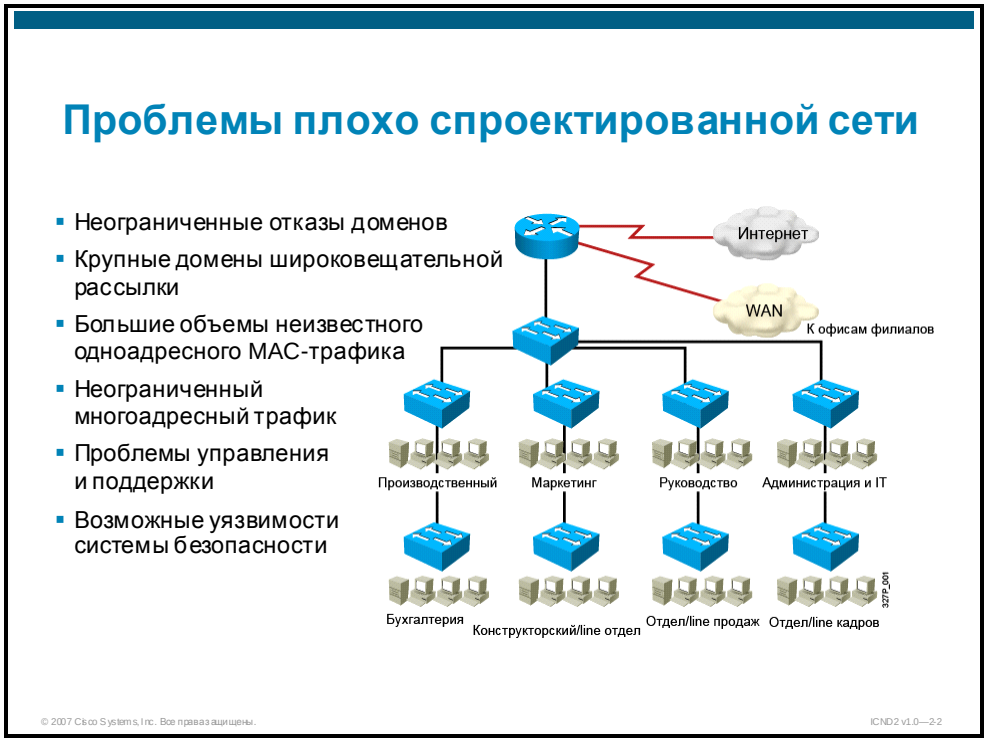
Задачи

По окончании этого занятия вы сможете рассказывать, как и когда следует внедрять и проверять функции VLAN и транков, а затем внедрять их в сети. Это значит, что вы сможете выполнить следующие задачи:

1. определять назначение и функцию сетей VLAN на коммутаторах Cisco Catalyst;
2. определять назначение и функцию транков IEEE 802.1Q на коммутаторах Cisco Catalyst;
3. определять назначение и функцию протокола VTP на коммутаторах Cisco Catalyst;
4. перечислять действия, необходимые для настройки VLAN обычного диапазона, использующей домен VTP и транкинг 802.1Q.

Общие сведения о VLAN

В этом разделе описываются базовые функции и режимы, а также принципы работы VLAN.



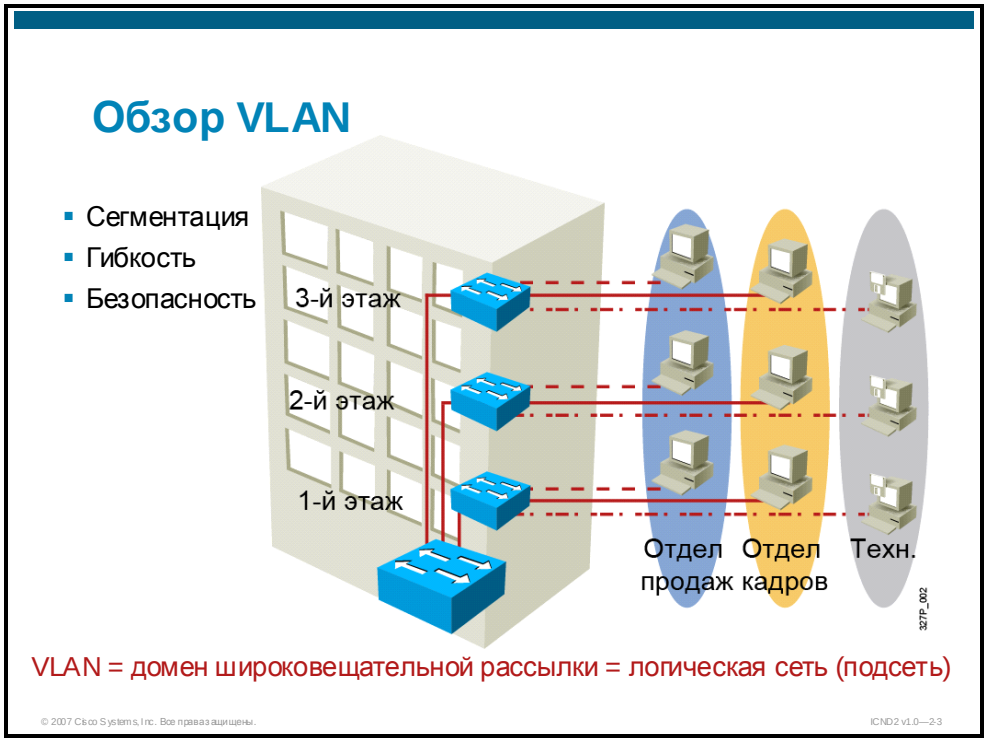
Проблемы, которые могут возникнуть в плохо спроектированной сети

Плохо спроектированная сеть означает повышенные затраты на поддержку, сниженную доступность служб и ограниченную совместимость с новыми приложениями и решениями. Неоптимальная производительность оказывает самое непосредственное влияние на работу конечных пользователей и доступ к центральным ресурсам. Ниже перечислены некоторые из проблем, которые могут быть вызваны некачественным проектированием сети.

- **Неисправные домены.** Одна из главных целей эффективного проекта сети — минимизация распространения возникающих проблем по сети. Если границы второго и третьего уровней заданы нечетко, отказ в одной из областей сети будет иметь серьезные последствия в других областях.
- **Широковещательные домены.** Широковещательная рассылка существует во всех сетях. Многие приложения и сетевые операции требуют корректной работы широковещательных рассылок, поэтому их полное исключение невозможно. Предотвращение неисправностей доменов подразумевает задание четких границ, решение проблемы широковещательных доменов аналогично. Для минимизации негативного эффекта широковещательных рассылок необходимо задать четкие границы и использовать оптимальное число устройств.

- **Большие объемы неизвестного одноадресного MAC-трафика.** Коммутаторы Cisco Catalyst ограничивают пересылку одноадресных кадров в порты, связанные с определенным адресом для одноадресной рассылки. Однако, когда кадры прибывают по MAC-адресу назначения, который не указан в таблице MAC-адресов, выполняется их лавинная рассылка из портов коммутатора. Это называется «одноадресная лавинная рассылка неизвестного MAC-трафика». Поскольку такой тип лавинной рассылки генерирует большие объемы трафика на всех портах коммутатора, сетевые адаптеры вынуждены обрабатывать большое количество кадров, поступающих из проводной сети. И, поскольку в проводной сети распространяются данные, которые не предназначены для этого, безопасность сети может быть нарушена.
- **Непредвиденный многоадресный трафик на портах.** Многоадресная рассылка IP — это технология, которая обеспечивает распространение IP-трафика из одного источника по многоадресной группе, которая идентифицируется одной парой IP- и MAC-адресов группы назначения. Как и при одноадресной лавинной рассылке и широковещательной рассылке, многоадресные кадры рассылаются из всех портов коммутатора. Качественный проект обеспечивает ограничение числа многоадресных кадров, но при этом сохраняет их функциональность.
- **Трудности при управлении и поддержке.** Некачественно спроектированная сеть будет неорганизованной и плохо документируемой. Кроме того, в ней не будет потоков трафика, которые можно легко идентифицировать. Все это сделает поддержку, обслуживание и устранение проблем крайне сложными и трудоемкими задачами.
- **Возможные уязвимости системы безопасности.** Коммутируемая сеть, спроектированная без учета требований безопасности на уровне доступа, может скомпрометировать целостность всей сети.

Некачественное проектирование сети всегда будет иметь негативные последствия и станет тяжким бременем для службы поддержки и финансового отдела любой организации.

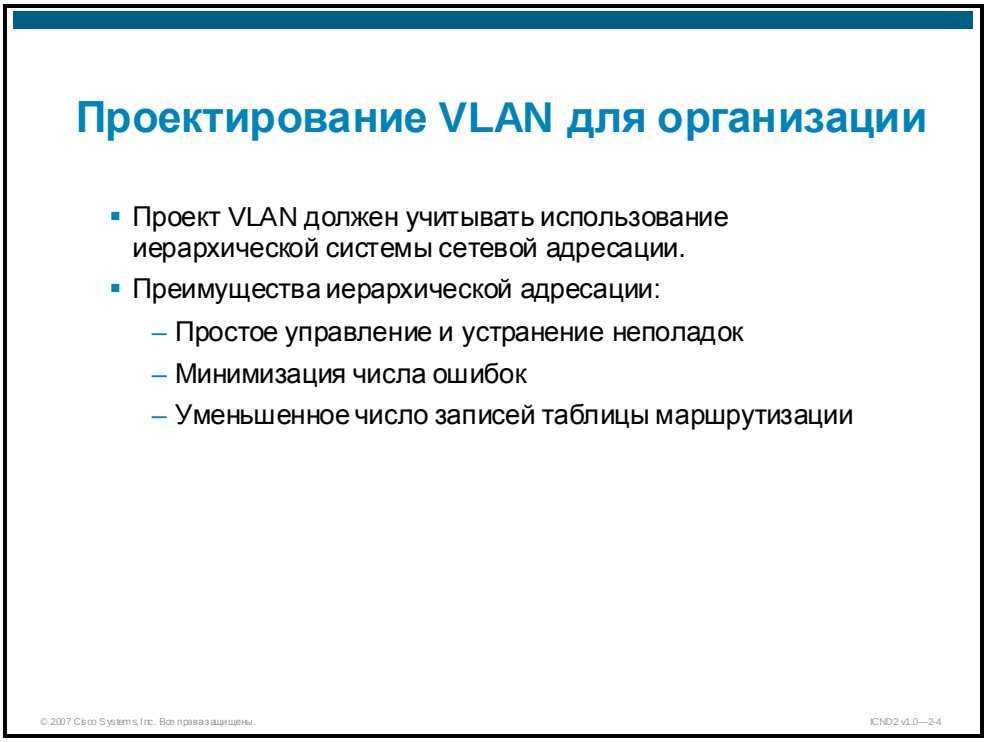


Обзор VLAN

VLAN — это логический широковещательный домен, который может охватывать несколько физических сегментов локальной сети. В коммутируемых интерсетях VLAN обеспечивает сегментацию и организационную гибкость. Можно спроектировать структуру VLAN, объединяющую станции с логической сегментацией по функциям, проектным группам и приложениям, независимо от физического расположения пользователей. Каждый порт коммутатора можно назначить только одной сети VLAN, что добавляет дополнительный уровень безопасности. Порты VLAN принимают широковещательные кадры, отправленные с одного из портов этой VLAN, порты в других VLAN не участвуют в широковещательной рассылке. Ограничение широковещательной рассылки одной VLAN улучшает общую производительность сети.

В коммутируемых интерсетях VLAN обеспечивает гибкость сегментации и организации. Технология VLAN позволяет группировать порты коммутатора и пользователей, которые к ним подключены, в логически заданные сообщества, например сотрудники одного отдела, многофункциональная группа разработки товара или группы различных пользователей, использующих одно сетевое приложение.

VLAN может быть существовать на одном коммутаторе или охватывать несколько коммутаторов. VLAN могут включать станции внутри одного здания или инфраструктуры, развернутые в нескольких зданиях. Кроме того, VLAN могут соединяться через глобальные сети.

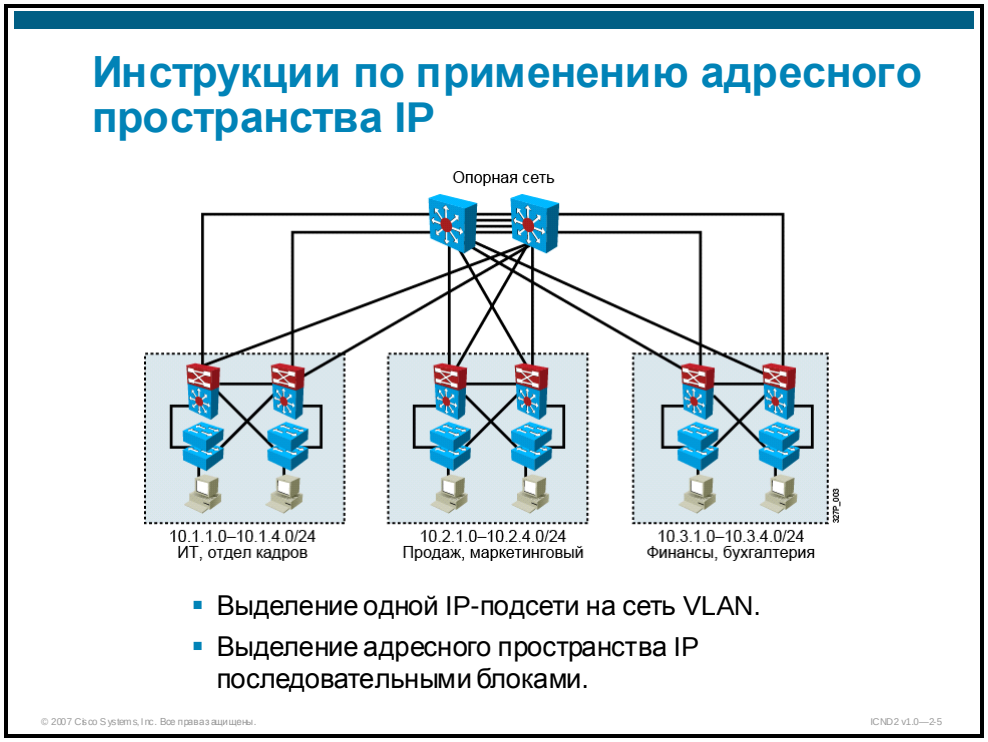


Группирование бизнес-функций в сети

Каждой VLAN в коммутируемой сети соответствует IP-сеть. Таким образом, проект VLAN должен учитывать использование иерархической системы сетевой адресации. Иерархическая адресация подразумевает упорядоченное назначение номеров IP-сети сегментам или VLAN с учетом сети в целом. Блоки смежных сетевых адресов резервируются и настраиваются на устройствах в отдельной области сети.

Ниже перечислены некоторые из преимуществ иерархической адресации.

- **Простое управление и устранение неполадок.** Иерархическая система адресации группирует сетевые адреса последовательно. Поскольку иерархическая система IP-адресации упрощает поиск проблемных компонентов, управление и устранение неполадок в сети становятся более эффективными.
- **Меньше ошибок.** Упорядоченное назначение сетевых адресов сводит к минимум количество ошибок и дублированных адресов.
- **Уменьшенные записи таблицы маршрутизации.** Протоколы маршрутизации поддерживают суммирование маршрутов для иерархических систем адресации, что позволяет одной записи таблицы маршрутизации представлять группу номеров IP-сетей. Суммирование маршрутов делает записи таблицы маршрутизации более управляемыми и обеспечивает следующие преимущества:
  - при повторном расчете таблицы маршрутизации и ее сортировке для поиска нужного маршрута используется меньше циклов ЦП;
  - сниженные требования к памяти маршрутизатора;
  - более быстрая конвергенция при модификациях сети;
  - ускоренное устранение неполадок.



Внедрение адресного пространства IP в корпоративной сети

Модель Cisco Enterprise Architecture предоставляет модульную архитектуру для проектирования и развертывания сетей. Кроме того, она обеспечивает идеальную структуру для внедрения иерархической системы IP-адресации. Ниже приведены некоторые инструкции.

- Проектируйте систему IP-адресации так, чтобы блоки последовательных сетевых номеров, соответствующих степеням двойки (такие как 4, 8, 16, 32, 64 и т. п.) могли быть назначены подсетям в на распределительном уровне здания и имели доступ к блоку коммутатора. Этот подход позволит суммировать все блоки коммутаторов в одном большом адресном блоке.
- На распределительном уровне здания следует продолжить последовательное назначение сетевых номеров устройствам уровня доступа.
- Одна IP-подсеть должна соответствовать одной VLAN. Каждая сеть VLAN должна представлять отдельный широковещательный домен.
- По возможности назначайте подсети с одним двоичным значением для всех сетевых номеров, чтобы избежать использования масок подсети переменной длины. Этот подход помогает минимизировать ошибки и путаницу при устранении неполадок и настройке новых устройств и сегментов.

Пример: проект сети

Организация с примерно 250 сотрудниками хочет перейти на модель Cisco Enterprise Architecture.

В таблице ниже приводится число сотрудников в каждом отделе.

Количество пользователей в отделах

Отдел	Количество пользователей	Расположение
ИТ-отдел	45	Здание A
Отдел кадров	10	Здание A
Отдел продаж	102	Здание B
Отдел маркетинга	29	Здание B
Финансовый отдел	18	Здание C
Бухгалтерия	26	Здание C

Необходимо создать 6 VLAN, по одной на группу пользователей. Таким образом, в соответствии с требованиями модели Cisco Enterprise Architecture необходимо настроить 6 IP-подсетей.

Организация решила использовать сеть 10.0.0.0 в качестве базового адреса.

Для пользователей самого большого отдела — отдела продаж — требуется минимум 102 адреса. Выбрана маска подсети 255.255.255.0 (/24), поддерживающая до 254 хостов на подсеть. Для поддержки будущего роста каждому зданию назначается один блок IP-адресов:

- зданию A назначается блок 10.1.0.0/16;
- зданию B назначается блок 10.2.0.0/16;
- зданию C назначается блок 10.2.0.0/16.

На таблицах ниже приводятся назначения сетей VLAN и IP-подсетей по зданиям.

Здание A: сети VLAN и IP-подсети

Отдел	VLAN	Адрес IP-подсети
ИТ-отдел	VLAN 11	10.1.1.0/24
Отдел кадров	VLAN 12	10.1.2.0/24
Для будущего роста		10.1.3.0–10.1.255.0

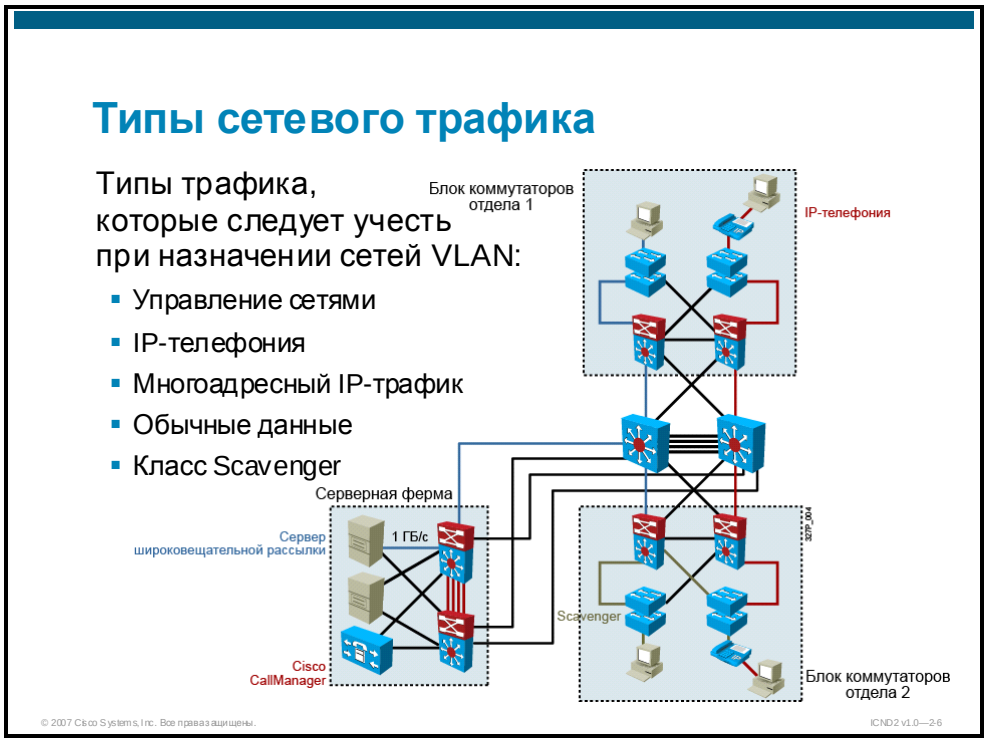
Здание B: сети VLAN и IP-подсети

Отдел	VLAN	Адрес IP-подсети
Отдел продаж	VLAN 21	10.2.1.0/24
Отдел маркетинга	VLAN 22	10.2.2.0/24
Для будущего роста		10.2.3.0–10.2.255.0

Здание C: сети VLAN и IP-подсети

Отдел	VLAN	Адрес IP-подсети
Финансовый отдел	VLAN 31	10.3.1.0/24
Бухгалтерия	VLAN 32	10.3.2.0/24
Для будущего роста		10.3.3.0–10.3.255.0

Некоторые из неиспользуемых VLAN и IP-подсетей будут применяться для управления сетевыми устройствами. Если компания решит внедрить IP-телефонию, некоторые из неиспользуемых VLAN и IP-подсетей могут быть назначены голосовым VLAN.



Учет источника трафика при создании маршрутов к адресатам

В этой таблице приводятся различные типы сетевого трафика, которые следует учесть перед размещением устройств и настройкой сети VLAN.

Типы трафика

Тип трафика	Описание
Управление сетями	В сети может присутствовать множество типов трафика сетевого управления, такие как блоки данных протокола STP (BPDU), обновления протокола обнаружения Cisco (CDP), а также трафик протоколов SNMP и RMON. Чтобы упростить устранение неполадок сети, некоторые разработчики назначают отдельную VLAN для переноса некоторых типов трафика управления сетью.

Тип трафика	Описание
IP-телефония	Существует два типа трафика IP-телефонии: данные сигнализации между конечными устройствами (IP-телефонами и программными коммутаторами, такими как Cisco Unified CallManager) и пакеты голосовых данных разговора. Разработчики часто выделяют отдельную голосовую VLAN для передачи данных в IP-телефоны и из них, что позволяет применить политики качества обслуживания (QoS) для присвоения максимального приоритета голосовому трафику.
Многоадресный IP-трафик	Многоадресный IP-трафик отправляется с одного адреса источника по заданному адресу многоадресной группы, который идентифицируется одной парой IP- и MAC-адресов назначения. В качестве примеров приложений, которые генерируют такой трафик, можно упомянуть вещание Cisco IP/TV и ПО для работы с образами, которое используется для быстрой настройки рабочих станций и серверов. Многоадресный трафик может создавать значительные потоки данных в сети. Например, видеотрафик от интерактивного обучения, приложений безопасности, Cisco Meeting Place и Cisco TelePresence может перегрузить некоторые сети. Необходимо настроить коммутаторы на предотвращение лавинной рассылки трафика устройствам, которые его не запрашивают. Кроме того, следует настроить маршрутизаторы на пересылку многоадресного трафика в области сети, которые нуждаются в этом трафике.
Обычные данные	Трафик обычных данных — это как правило трафик приложений, связанный с файловыми службами и службами печати, электронной почтой, использованием Интернета, доступом к БД и другим стандартным сетевым приложениям. В разных частях сети эти данные должны обрабатываться по-разному или одинаково, в зависимости от объема данных каждого из типов. Примеры этого типа трафика: блоки SMB, трафик протоколов NCP, SMTP и HTTP, а также запросы SQL.
Класс Scavenger	Класс Scavenger включает весь трафик от протоколов или шаблонов, превысивших свои стандартные потоки. Этот тип трафика используется для защиты сети от особых потоков трафика, которые могут быть результатом запуска вредоносных программ на конечных ПК. Кроме того, класс Scavenger используется для низкоприоритетного трафика, например для трафика P2P.

Основы голосовых VLAN

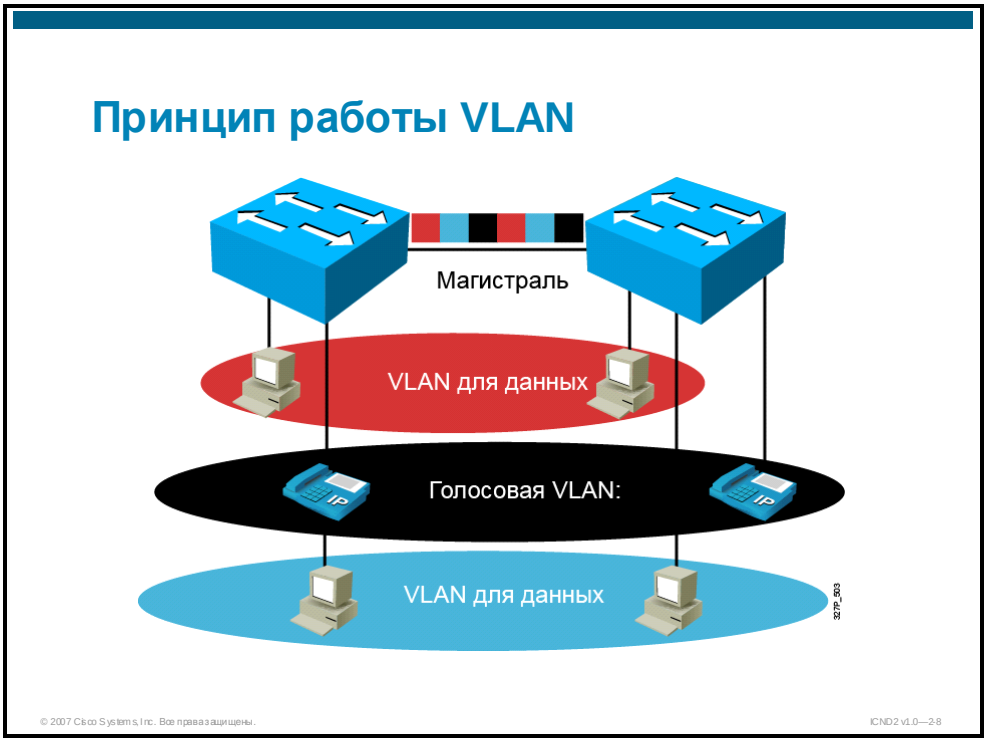
Некоторые коммутаторы Cisco Catalyst предлагают уникальную функцию, которая называется голосовой VLAN и позволяет наложить голосовую топологию на сеть передачи данных. Вы можете сегментировать телефоны в отдельные логические сети даже если для передачи голоса и данных используется одна инфраструктура.

Функция голосовых VLAN помещает телефоны в отдельные VLAN без вмешательства конечного пользователя. Пользователь просто включает телефон в коммутатор, который предоставляет телефону все необходимые сведения о VLAN.

Голосовые VLAN обеспечивают несколько преимуществ. Сетевые администраторы могут легко поддерживать такие назначения VLAN, даже если телефоны перемещаются в другое место. Помещая телефоны в отдельную VLAN, сетевые администраторы получают преимущества сегментации сети и контроля. Кроме того, эта функция позволяет администраторам сохранить существующую топологию IP для конечных станций передачи данных и легко назначать IP-телефоны в другие IP-подсети с помощью стандартной операции DHCP.

Когда телефоны находятся в своих IP-подсетях и VLAN, сетевые администраторы могут легко выявлять и устранять проблемы сети, а также создавать и приводить в действие политики QoS и безопасности.

С функцией голосовых VLAN сетевые администраторы получают все преимущества конвергенции физической инфраструктуры, и в то же время могут поддерживать отдельные логические топологии для голосовых терминалов и терминалов передачи данных. Эта конфигурация предлагает самый эффективный способ управления мультисервисной сетью.

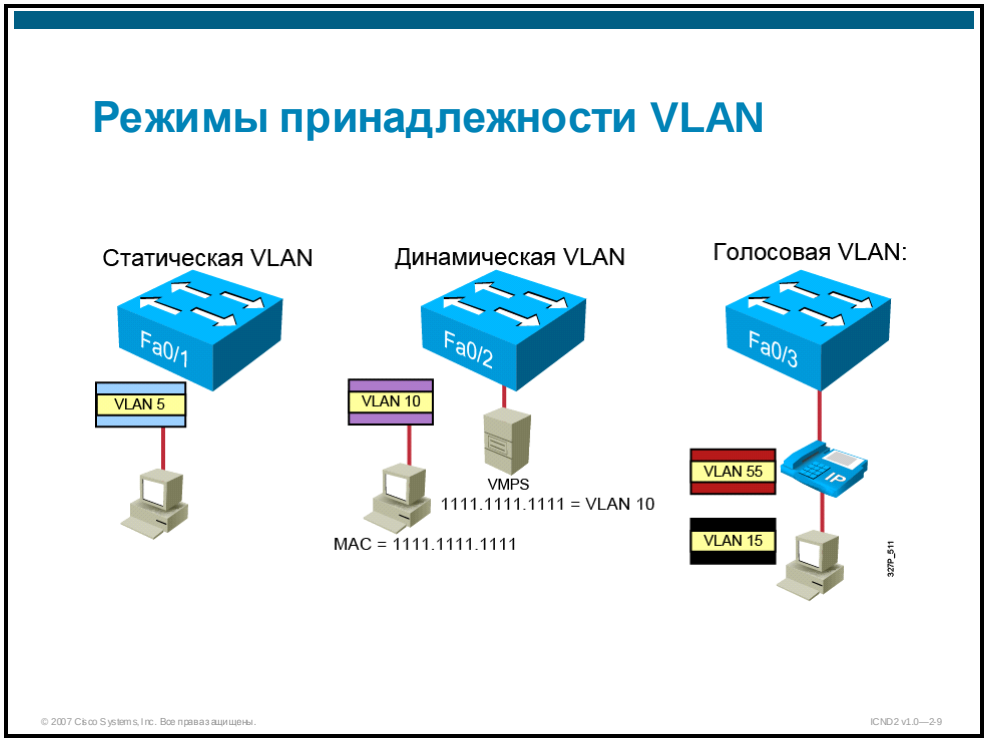


Принцип работы VLAN

В сети коммутатор Cisco Catalyst работает как традиционный мост. Каждая VLAN, настроенная на коммутаторе, принимает решения о получении адресов, пересылке и фильтрации, а также реализует механизмы, предотвращающие образование петель, так, как если бы VLAN была отдельным физическим мостом.

Коммутатор Cisco Catalyst реализует VLAN путем ограничения пересылки трафика в порты назначения, которые не находятся в одной VLAN с портами-источниками. Таким образом, когда кадр прибывает на порт коммутатора, коммутатор должен передавать его только в порты, которые находятся в одной сети VLAN с этим портом. В сущности, сеть VLAN, работающая на коммутаторе, ограничивает передачу одноадресного, многоадресного и широковещательного трафика. Трафик, созданный в той или иной VLAN, рассылается только в порты этой VLAN.

Порт, как правило, передает трафик только во VLAN, которой он принадлежит. Чтобы VLAN охватывала несколько коммутаторов, необходимо создать транковое подключение между двумя коммутаторами. Транковое подключение может использоваться для передачи данных нескольких сетей VLAN.



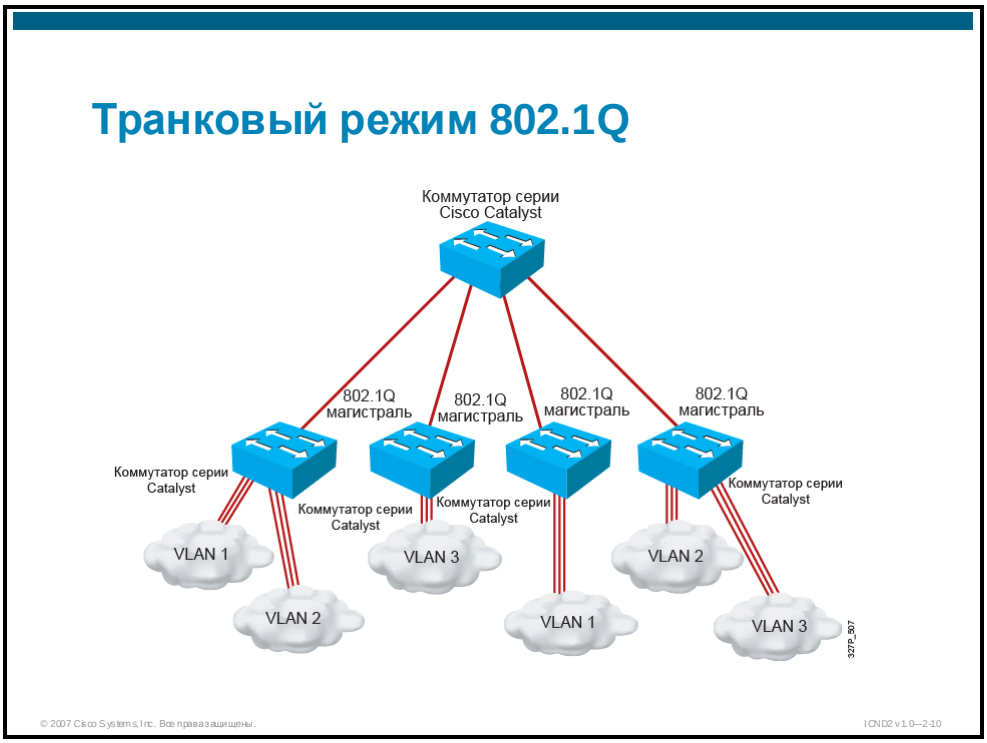
Режимы принадлежности VLAN

Порты VLAN настраиваются с режимом принадлежности, который определяет, к какой VLAN они принадлежат. Для портов коммутатора Cisco Catalyst могут заданы следующие режимы принадлежности VLAN.

- **Статическая VLAN.** Администратор статически назначает VLAN портам.
- **Динамическая VLAN.** Коммутаторы Cisco Catalyst поддерживают динамические VLAN на базе серверов управления политиками VLAN (VMPS). Некоторые коммутаторы Cisco Catalyst могут быть назначены VMPS-серверами. Кроме того, в качестве VMPS-сервера может служить внешний сервер. VMPS-сервер содержит базу данных, которая сопоставляет MAC-адреса и назначения VLAN. Когда кадр прибывает на динамический порт коммутатора доступа Cisco Catalyst, коммутатор запрашивает назначение VLAN у VMPS-сервера в соответствии с MAC-адресом прибывающего кадра. Динамический порт может принадлежать только одной VLAN. Несколько хостов могут быть активны на динамическом порте, только если они принадлежат одной сети VLAN.
- **Голосовая VLAN.** Голосовой порт VLAN — это порт доступа, подключенный к IP-телефону Cisco, который настроен на использование одной VLAN для передачи голосового трафика и другой VLAN для передачи данных от устройства, подключенного к телефону.

Общие сведения о транковом режиме 802.1Q

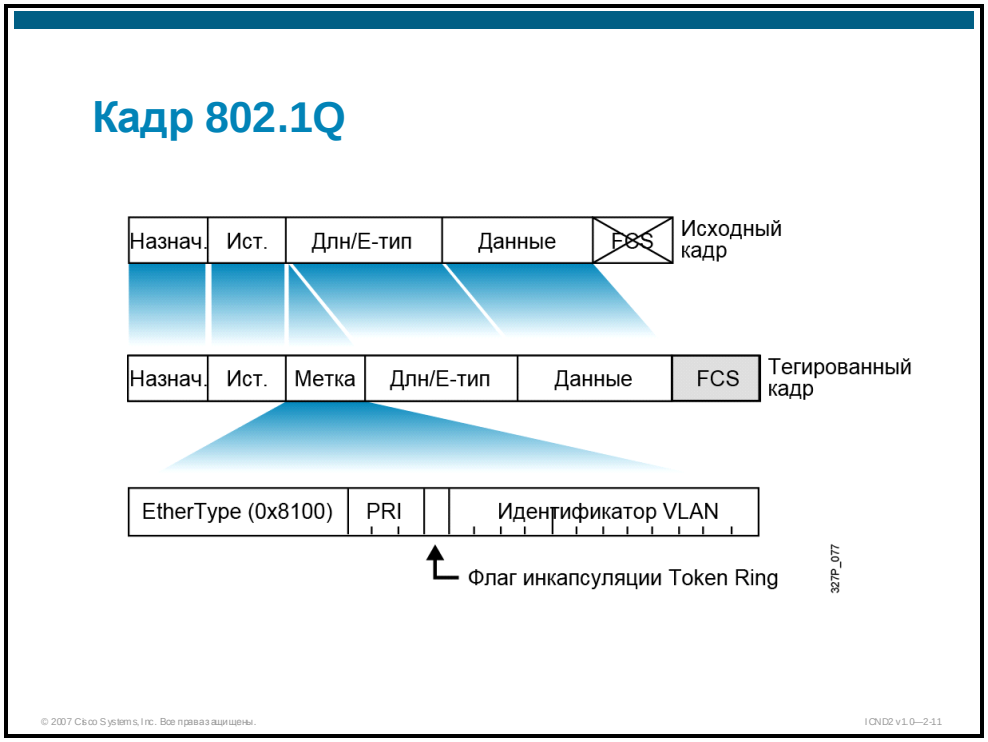
В этом разделе описываются базовые функции транкового режима 802.1Q.



Транковое подключение — это канал «точка-точка» между одним или несколькими Ethernet-интерфейсами коммутатора и другим сетевым устройством, например маршрутизатором или коммутатором. Транковое подключение Ethernet используются для передачи трафика из нескольких сетей VLAN через один канал и позволяет расширять VLAN на всю сеть. Cisco поддерживает протокол IEEE 802.1Q для интерфейсов Fast Ethernet и Gigabit Ethernet.

Транковое интерфейсы Ethernet поддерживают различные транковые режимы. Интерфейс можно настроить как транковый или как нетранковый. Кроме того, интерфейс может согласовывать транковый режим с соседним интерфейсом.

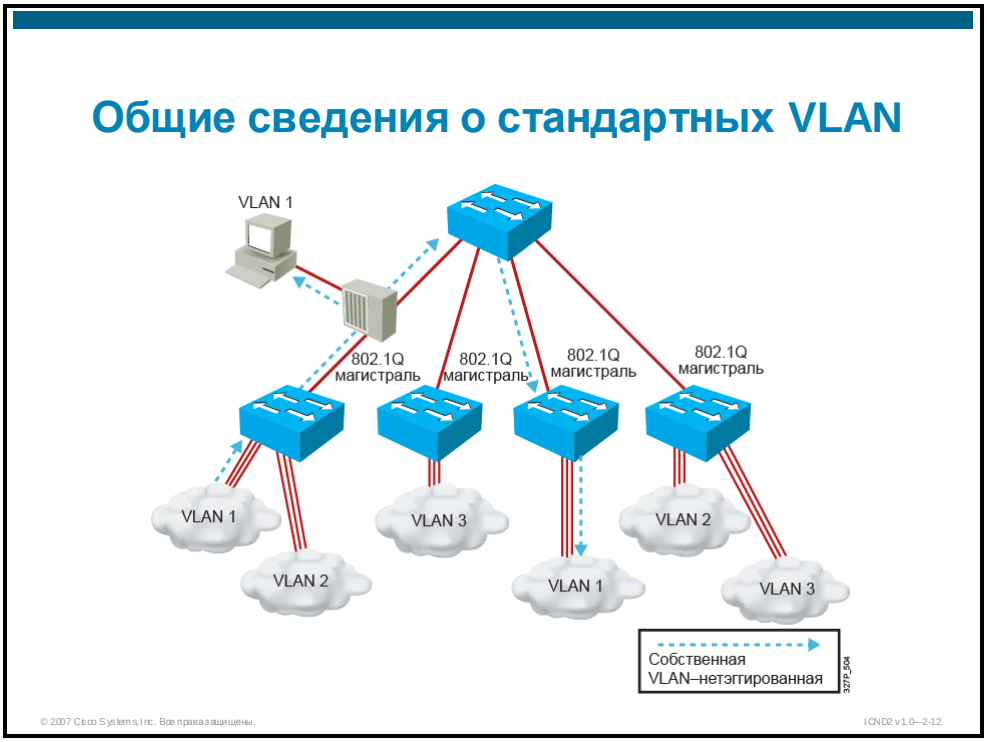
Каждый порт 802.1Q назначается транковому подключению. Все порты в транковом подключении находятся в стандартной VLAN. Всем портам 802.1Q назначается идентификатор, который соответствует идентификатору стандартной VLAN (VID) порта (значение по умолчанию — VLAN 1). Все немеченные кадры назначаются в сеть VLAN, указанную в этом параметре VID.



Кадр 802.1Q

Протокол IEEE 802.1Q использует внутренний механизм создания меток, который вставляет четырехбайтное поле метки в исходный кадр Ethernet между полем "Адрес источника" и полем "Тип" или "Длина". Поскольку протокол 802.1Q модифицирует кадр, транковое устройство пересчитывает контрольную последовательность кадра (FCS) для измененного кадра.

Коммутатор Ethernet должен проанализировать четырехбайтное поле метки, чтобы определить, куда доставить кадр. Небольшая часть четырехбайтного поля метки, а точнее три бита, используются для задания приоритета кадра. См. подробные сведения в описании стандарта IEEE 802.1pd. Заголовок 802.1Q содержит поле 802.1p, поэтому для использования протокола 802.1Q необходим протокол 802.1p.

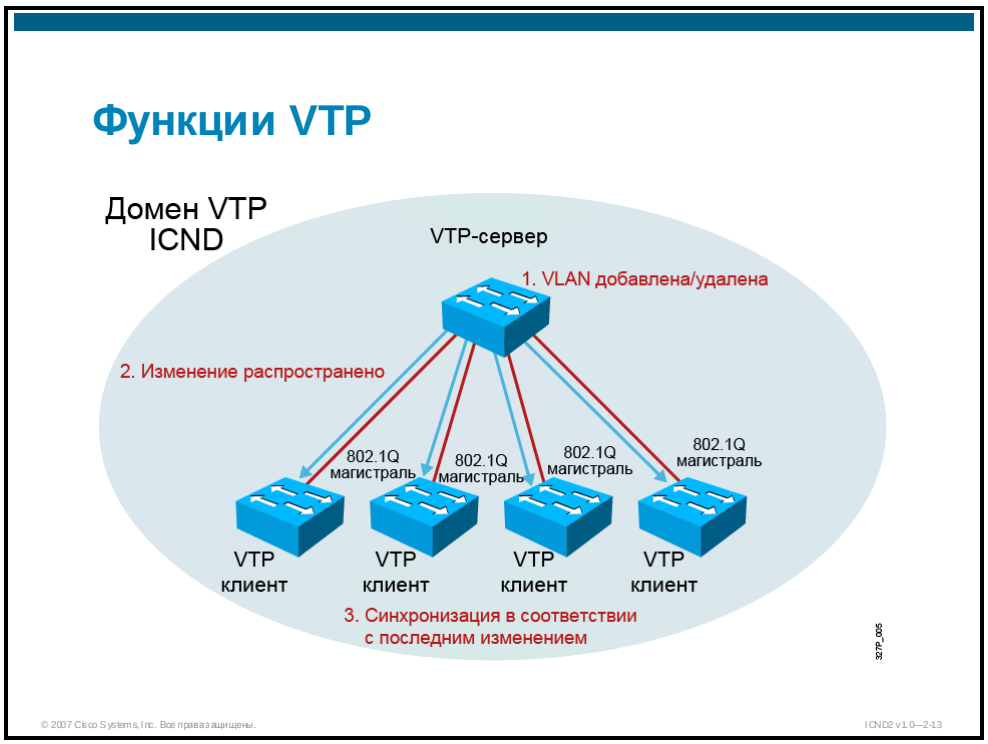


Стандартная VLAN протокола 802.1Q

Транковому подключению 802.1Q и связанным с ним транковым портам назначается стандартная сеть VLAN. 802.1Q не отмечает кадры для стандартной сети VLAN. Поэтому обычные станции могут читать стандартные немеченные кадры, но не могут читать меченные кадры.

Общие сведения о протоколе VTP (VLAN Trunking Protocol)

В этом разделе описываются функции протокола VTP, обеспечивающие поддержку VLAN, а также режимы работы протокола VTP.



VTP — это протокол обмена сообщениями второго уровня, который поддерживает согласованность конфигурации VLAN, управляя добавлением, удалением и переименованием VLAN по всей сети. VTP сводит к минимуму число неверно заданных и несогласованных параметров, которые могут стать причиной проблем, таких как дублированные имена VLAN и неверно заданный тип VLAN.

Домен VTP — это один коммутатор или несколько связанных коммутаторов, использующих одну среду VTP. Коммутатор можно настроить на участие только в одном домене VTP.

По умолчанию коммутатор Cisco Catalyst находится в состоянии "no-management-domain", пока не получает объявление домена через транковый канал или пока пользователь не настроит домен управления. Настройки, сделанные на одном VTP-сервере, распространяются через транковые каналы по всем подключенным коммутаторам в сети.

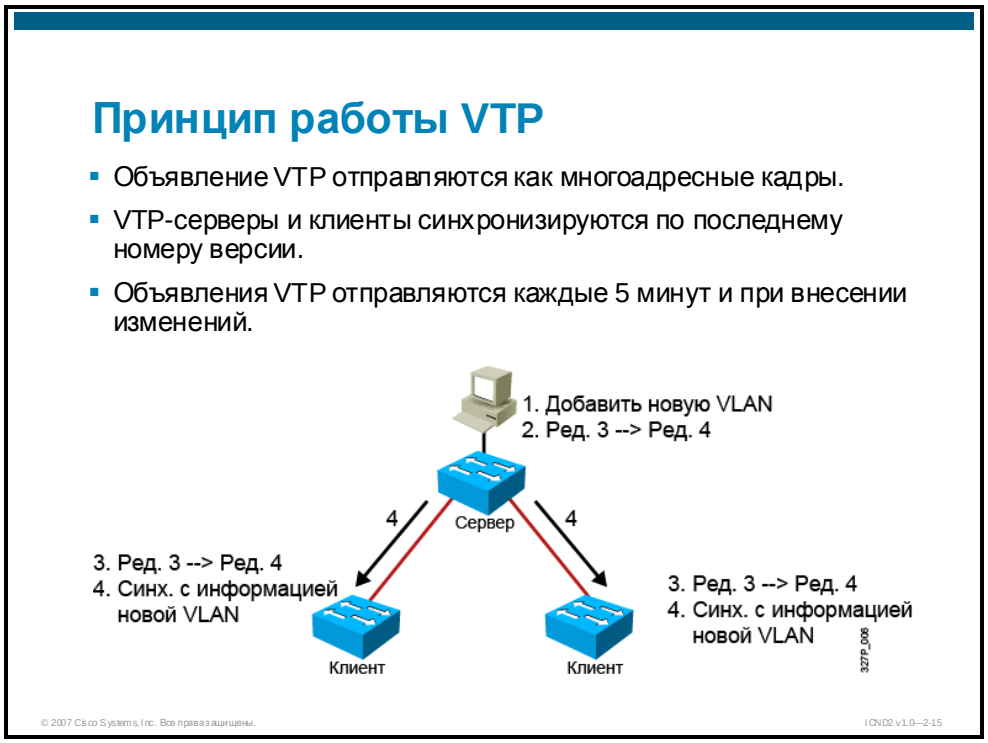
Режимы VTP

Протокол VTP может работать в одном из трех режимов: серверный, прозрачный и клиентский. В зависимости от режима работы VTP пользователи будут доступны разные задачи. Характеристики трех режимов VTP приводятся ниже.

- **Серверный.** Режим VTP по умолчанию — серверный, но данные о VLAN не распространяются через сеть, пока имя домена управления не будет получено или задано. Изменения в конфигурации VLAN, сделанные на VTP-сервере, распространяются по всем коммутаторам в домене VTP. Сообщения VTP рассылаются по всем транковым подключениям.
- **Прозрачный.** Изменения конфигурации VLAN, сделанные в прозрачном режиме VTP, влияют только на локальный коммутатор и не распространяются на другие коммутаторы в домене VTP. В прозрачном режиме полученные объявления VTP пересылаются другим коммутаторам домена.
- **Клиентский.** Вносить изменения в конфигурацию VLAN в клиентском режиме VTP невозможно, однако VTP-клиент может отправлять данные о любых VLAN, записанных в его базе данных, другим коммутаторам VTP. В клиентском режиме VTP также выполняется пересылка объявлений VTP.

VTP-клиенты, работающие под управлением операционных систем Cisco Catalyst, не сохраняют VLAN в NVRAM. Когда коммутатор перезагружается, VLAN не сохраняются и номеру версии конфигурации присваивается значение «0». Однако VTP-клиенты Cisco IOS сохраняют сети VLAN в файл vlan.dat во flash-памяти, что позволяет сохранить таблицу VLAN и номер версии.

Внимание В коммутаторах Cisco IOS команда **erase startup-config** не действует на файл vlan.dat. VTP-клиенты с более высоким номером версии конфигурации могут перезаписать сети VLAN на VTP-сервере, который находится в том же домене VTP. Удалите файл vlan.dat и перезагрузите коммутатор, чтобы сбросить данные VTP и VLAN. Сведения о том, как удалить файл vlan.dat см. в документации по вашей модели коммутатора.



Принцип работы VTP

Объявления VTP распространяются через домен управления. Объявления VTP отправляются каждые 5 минут, а также при изменениях в конфигурации VLAN. Объявления распространяются через VLAN по умолчанию (VLAN 1) посредством многоадресного кадра. В каждое объявление VTP включается номер версии конфигурации. Более высокий номер версии означает, что объявляемые данные VLAN являются более актуальными, чем сохраненные данные.

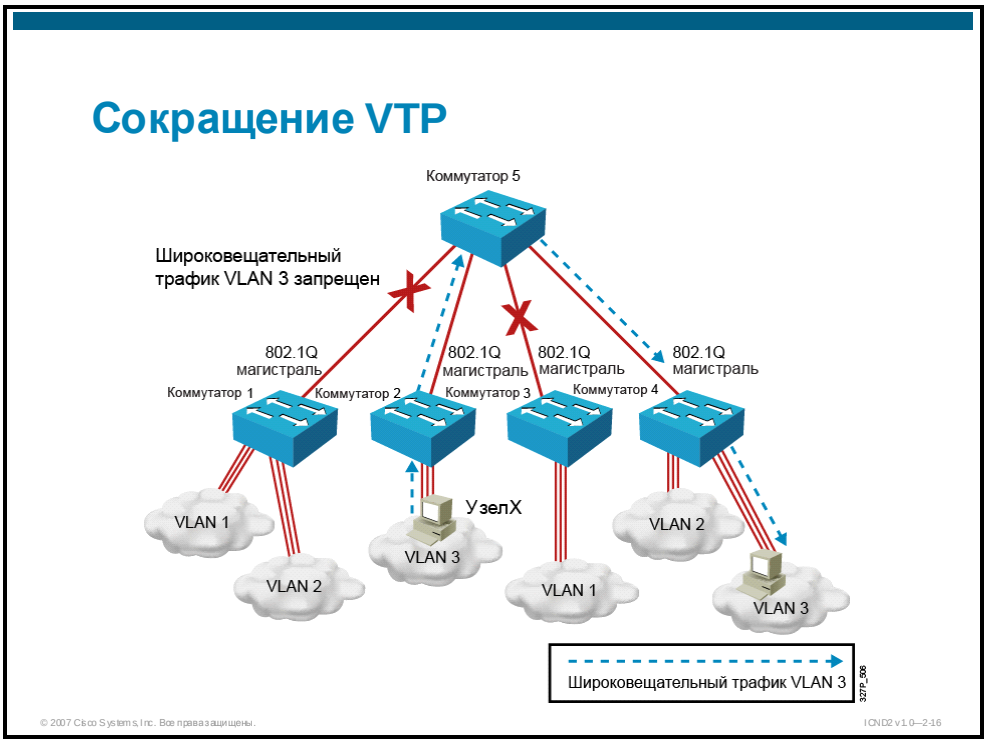
Номер версии конфигурации — один из самых важных компонентов протокола VTP. Каждый раз, когда VTP-сервер изменяет данные о VLAN, к номеру версии конфигурации добавляется единица. После этого сервер рассылает объявление VTP с новым номером версии конфигурации. Если объявляемый номер версии конфигурации выше, чем номер сохраненный в других коммутаторах домена VTP, они заменяют свои конфигурации VLAN на новые объявленные конфигурации.

Номер версии конфигурации коммутатора в прозрачном режиме VTP всегда равняется нулю.

Примечание Если во время процесса перезаписи VTP-сервер удаляет все сети VLAN и имеет более высокий номер версии конфигурации, другие устройства в домене VTP также удалят свои сети VLAN.

Устройство, получающее объявления VTP, должно проверить различные параметры перед применение полученных данных о VLAN. Во-первых, имя домена управления и пароль в объявлении должны совпадать с именем и паролем, заданными на локальном коммутаторе. Затем, если номер версии конфигурации указывает, что сообщение было создано позже, чем используемая конфигурация, коммутатор примет объявленные данные VLAN.

Чтобы сбросить номер версии конфигурации на отдельных коммутаторах Cisco Catalyst, используйте команду delete vtp привилегированного режима EXEC. На многих коммутаторах Cisco Catalyst можно изменить имя домена VTP, а затем вернуть старое имя, чтобы сбросить номер версии конфигурации.



VTP Pruning

Функция VTP Pruning использует объявления VLAN, чтобы определить транковые подключения, выполняющие ненужную рассылку трафика.

По умолчанию транковое подключение используется для передачи трафика для всех сетей VLAN в домене управления VTP. В корпоративной сети некоторые коммутаторы могут не иметь локальных портов во всех сетях VLAN. Такая ситуация встречается довольно часто.

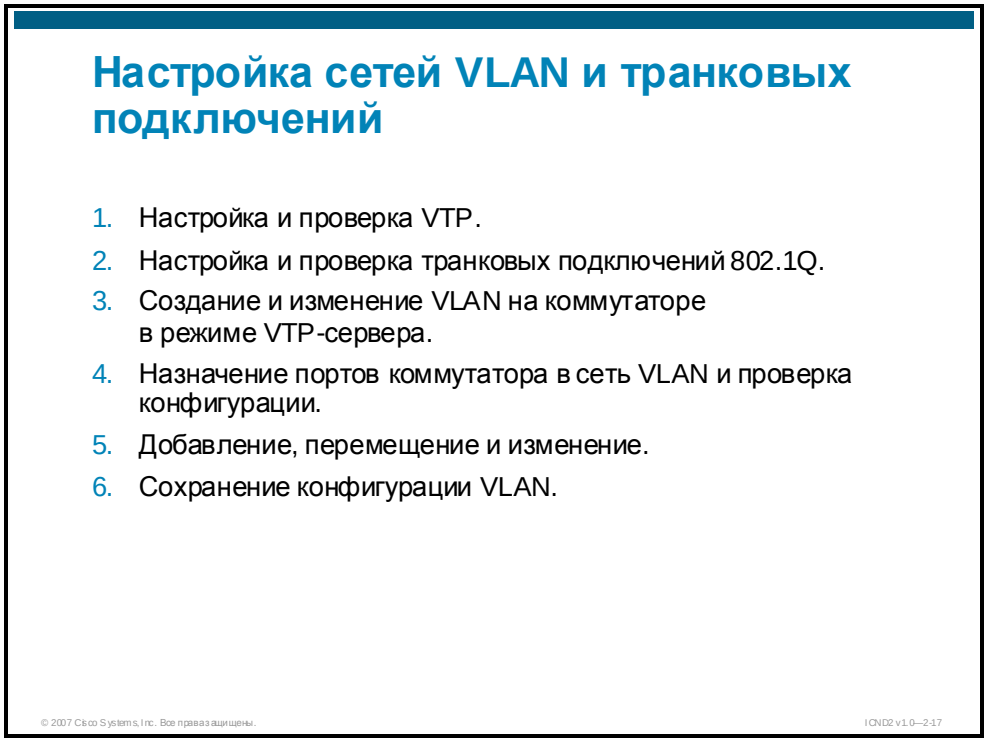
На рисунке изображена коммутируемая сеть с функцией VTP Pruning. Только коммутаторы 2, 4 и 5 имеют порты в сети VLAN 3. Коммутатор 5 не пересылает широковещательный трафик с хоста X на коммутаторы 1 и 3, поскольку трафик для VLAN 3 удален из каналов между коммутатором 5 и коммутаторами 1 и 3, как показано на рисунке.

VTP Pruning повышает доступную полосу пропускания сети путем ограничения трафика, распространяемого в транковых подключениях, которые используются для передачи трафика в соответствующие сетевые устройства.

VTP Pruning можно включить только на коммутаторах Cisco Catalyst, настроенных в качестве VTP-серверов, клиенты не поддерживают эту функцию.

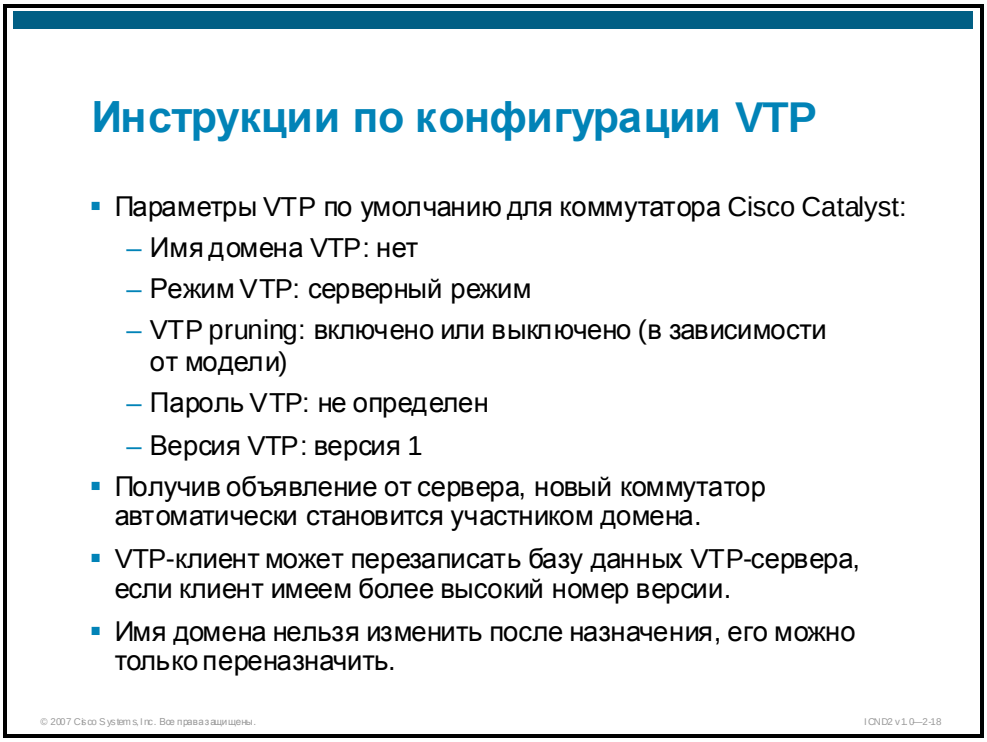
Настройка сетей VLAN и транковых подключений

В этом разделе описываются действия, которые необходимо выполнить для настройки и проверки сетей VLAN, транкового режима и протокола VTP в коммутируемой сети.



Действия по настройке сетей VLAN в коммутируемой сети перечислены ниже.

- Определите, нужно ли использовать VTP. Если да, включите протокол VTP в серверном, клиентском или прозрачной режиме.
- Включите транковый режим для соединений между коммутаторами.
- Создайте сети VLAN на VTP-сервере и распространите их на другие коммутаторы.
- Статически или динамически назначьте порты коммутатора в сеть VLAN.
- Добавьте, переместите или измените порты.
- Сохраните конфигурацию VLAN.



Конфигурация VTP

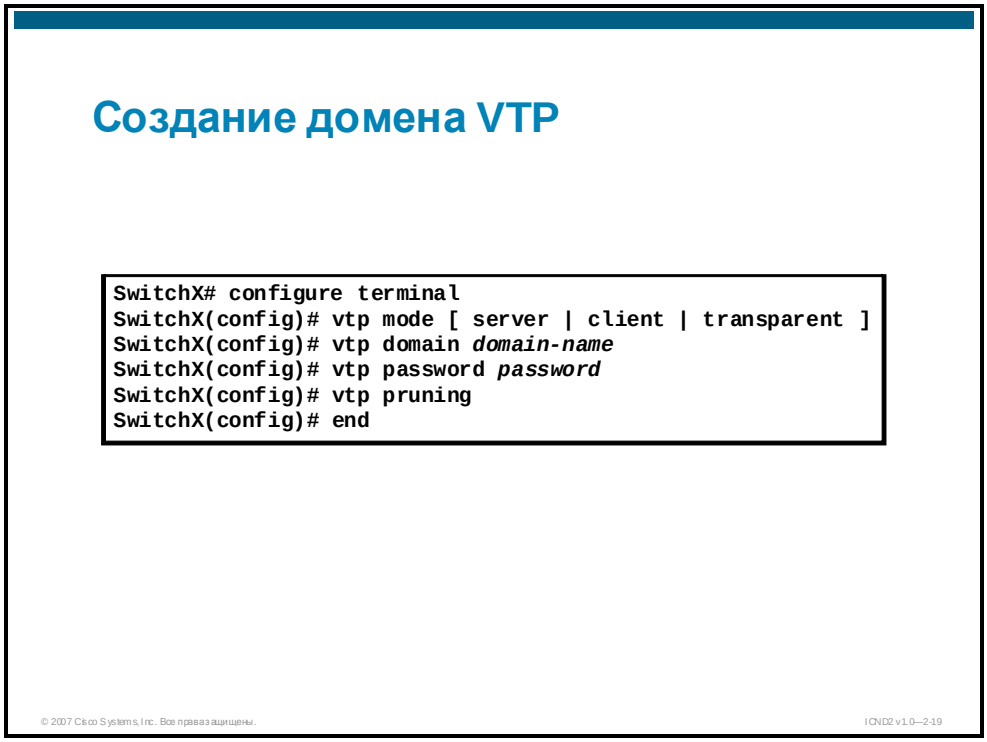
После создания сетей VLAN необходимо решить, следует ли использовать протокол VTP в вашей сети. VTP позволяет автоматически передавать изменения конфигурации, сделанные в одном или нескольких коммутаторах, всем остальным коммутаторам в домене VTP.

Параметры конфигурации VTP по умолчанию зависят от модели коммутатора и версии ПО. Параметры коммутаторов Cisco Catalyst:

- Имя домена VTP: нет
- Режим VTP: серверный
- Пароль VTP: не определен
- VTP pruning: включено или выключено (в зависимости от модели)
- Версия VTP: версия 1

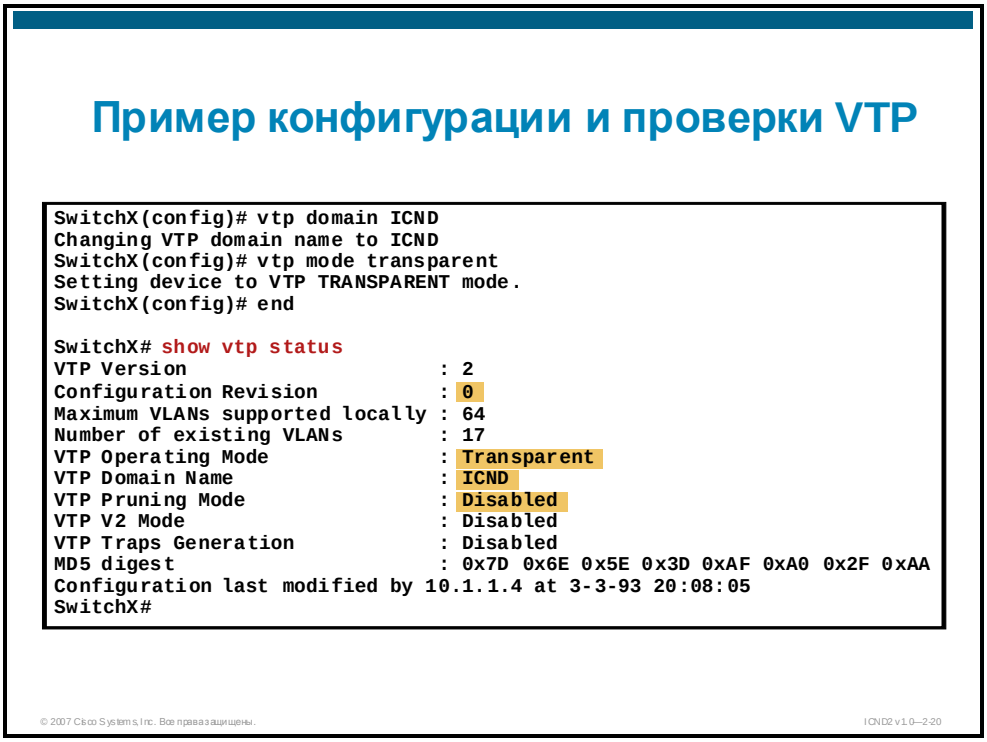
Имя домена VTP может быть указано или получено. По умолчанию имя домена не задается. Вы можете задать пароль для домена управления VTP. Однако, чтобы протокол VTP работал должным образом, необходимо назначить одинаковые пароли всем коммутаторам в домене.

Применимость VTP Pruning — один из параметров VLAN, распространяемый протоколом VTP. Операции включения или выключения функции VTP Pruning на VTP-сервере распространяются по всему домену управления.



Используйте команду глобальной конфигурации **vtp**, чтобы изменить конфигурацию VTP, в том числе имя файла хранилища, имя домена, интерфейс и режим. Используйте версию "**no**" этой команды, чтобы удалить имя файла или вернуться к параметрам по умолчанию. При использовании прозрачного режима VTP, вы можете сохранить конфигурацию VTP в файл конфигурации коммутатора с помощью команды **copy running-config startup-config** привилегированного режима EXEC .

Примечание	Имя домена и пароль вводятся с учетом регистра. После того, как имя домена задано, его нельзя изменить, только переназначить.



Пример: конфигурация VTP

На рисунке указаны команды, которые необходимо ввести для настройки VTP и вывода данных о состоянии VTP. В этом примере коммутатор имеет следующие характеристики:

- коммутатор в домене VTP находится в прозрачном режиме;
- имя домена VTP — ICND;
- функция Pruning включена;
- номер версии конфигурации — 0.

Примечание В выводе команды show vtp status строка "VTP Version" определяет версию VTP, с которой может работать коммутатор. Строка "VTP V2 Mode2" указывает, используется ли версия 2 протокола VTP. Если параметр "VTP V2 Mode" имеет значение "disabled", используется версия 1 протокола VTP.

Конфигурация транковjuj ht;bvf 802.1Q

Протокол 802.1Q выполняет передачу трафика нескольких сетей VLAN через один канал в сети с компонентами разных производителей.

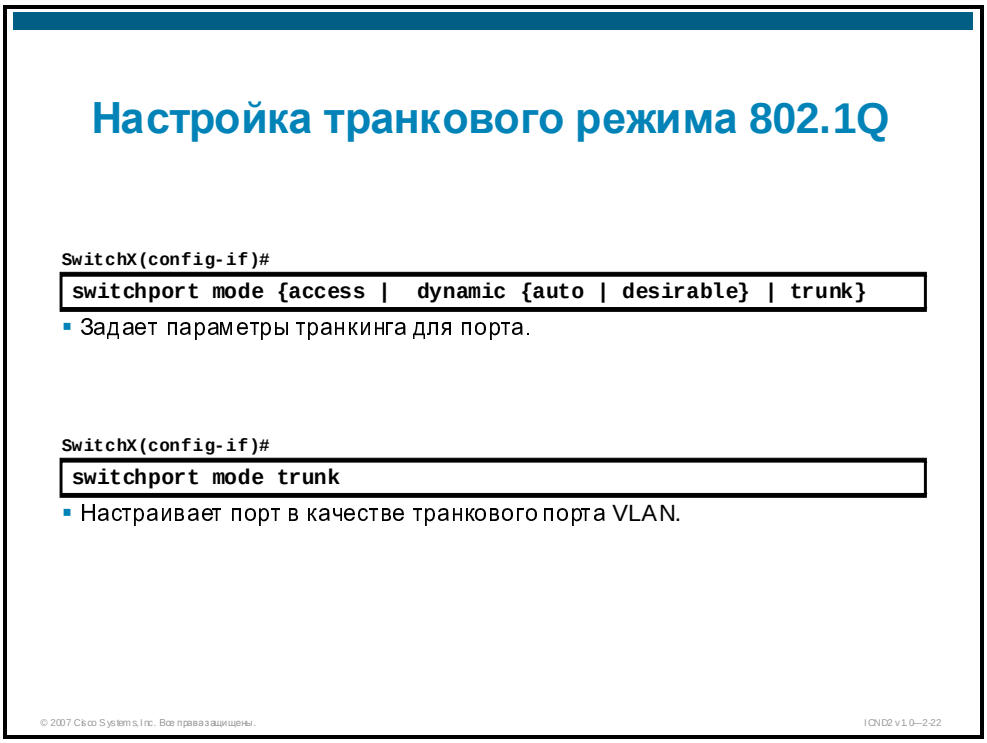
Транковые подключения 802.1Q накладывают ряд ограничений на стратегию транкового режима. Необходимо учесть следующее:

- убедитесь, что стандартная VLAN для транкового подключения 802.1Q одинакова на обеих сторонах канала, если это не так, могут возникнут петли протокола "spanning tree";
- кадры стандартной VLAN должны быть немеченными.

На таблице ниже описывается взаимодействие транкинга 802.1Q с другими функциями коммутатора.

Взаимодействие транкового режима с функциями коммутатора

Функция коммутатора	Взаимодействие с транковым портом
Защищенные порты	Транковый порт не может быть защищенным портом.
Группирование портов	Транковые подключения 802.1Q можно объединять в группы портов EtherChannel, но все транковые подключения в группе должны иметь одинаковую конфигурацию. При создании группы ко всем портам применяются параметры, заданные для первого порта, добавленного в группу. Если вы измените конфигурацию одного из этих параметров, коммутатор распространит это изменение на все порты в группе. Эти параметры включают следующее: ■ список допустимых VLAN; ■ стоимость маршрута протокола "spanning tree" (STP) для каждой VLAN; ■ приоритет порта STP для каждой VLAN; ■ параметр STP PortFast; ■ состояние транкового подключения, если один порт в группе портов перестает быть транковыми, то же происходит с остальными портами.



Используйте команду switchport mode режима конфигурации интерфейса для перевода порта Fast Ethernet или Gigabit Ethernet в транковый режим. Многие коммутаторы Cisco Catalyst поддерживают динамический транковый протокол (DTP), который управляет автоматическим согласованием транковых подключений.

Для команды switchport mode доступно 4 параметра.

Параметры режима порта коммутатора

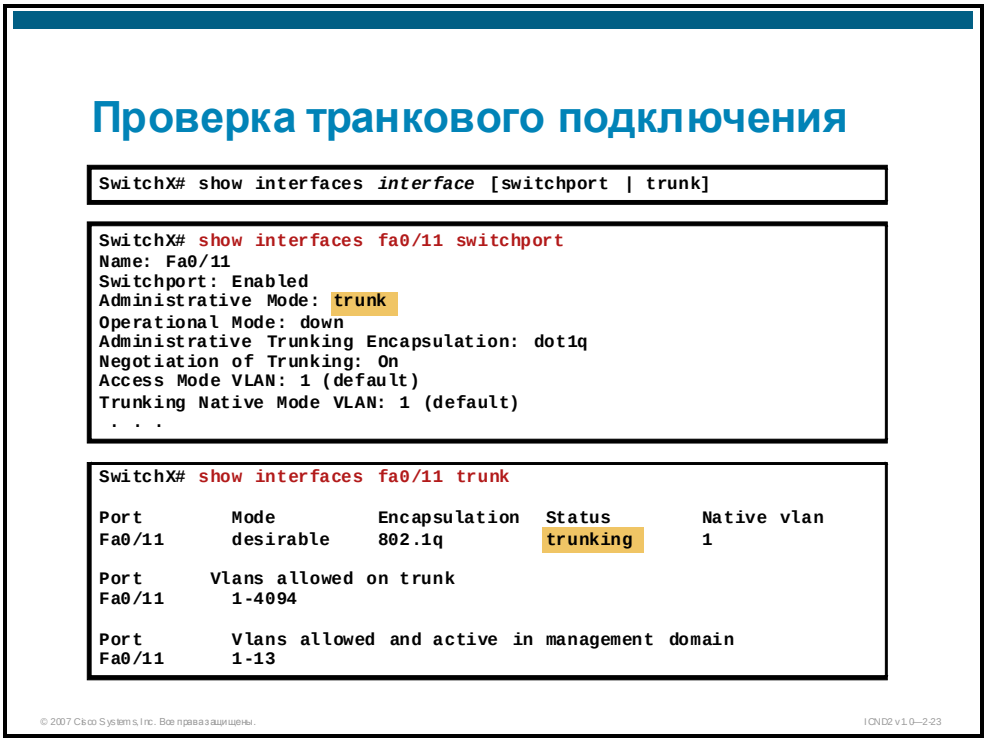
Параметр	Описание
`trunk`	Активирует постоянный транковый режим 802.1Q на порте и выполняет согласование с подключенным устройством для перевода канала в транковый режим.
`access`	Отключает транковый режим порта и выполняет согласование с подключенным устройством для перевода канала в нетранковый режим
`dynamic desirable`	Заставляет порт согласовать канал для перевода из нетранкового режима в транковый. Порт переводится в транковый режим, если подключенное устройство находится в режиме «trunk», «desirable» или «auto». В противном случае порт становится нетранковым.
`dynamic auto`	Переводит порт в транковый режим только если подключенное устройство находится в режиме «trunk» или «desirable». В противном случае порт становится нетранковым.

Команда **switchport nonegotiate** отменяет отправку пакетов согласования DTP в интерфейс уровня 2. Коммутатор не будет запускать согласование DTP на этом интерфейсе. Эта команда действует только если порт коммутатора интерфейса находится в режиме доступа или транковом режиме (для этого используются команды конфигурации интерфейса **switchport mode** access или **switchport mode trunk**). Эта команда возвращает ошибку при вводе в динамическом режиме ("auto" или "desirable"). Чтобы вернуться к параметрам по умолчанию, используйте версию "**no**" этой команды. При вводе команды **switchport nonegotiate** на интерфейсе порт переходит в транковый режим только если порт на другой стороне находится в транковом режиме. Команда **switchport nonegotiate** не формирует транковый канал с портами, которые находятся в динамическом режиме "desirable" или "auto".

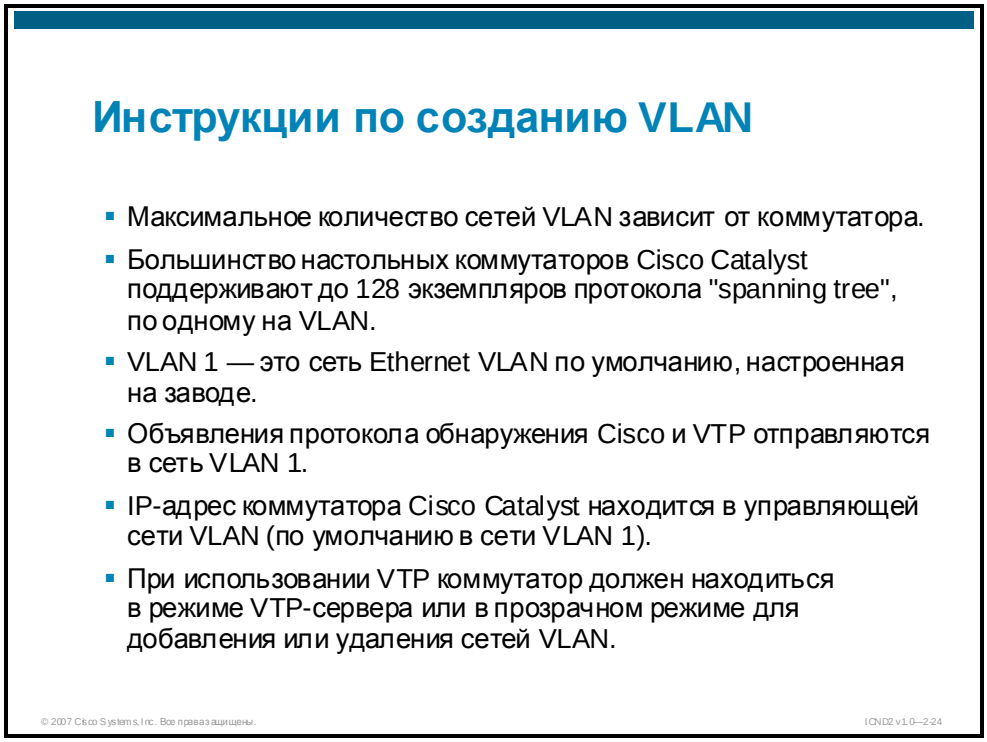
На таблице ниже описываются действия, необходимые для настройки порта в качестве транкового порта 802.1Q в привилегированном режиме EXEC.

№	Действие	Примечания
1.	Войдите в режим конфигурации интерфейса и выберите порт, для которого необходимо настроить транковый режим `SwitchX(config)# interface int_type int_number`	После ввода команды **interface** приглашение командной строки изменится с (config) # на (config-if) #.
2.	Настройте порт VLAN в качестве транкового. `SwitchX(config-if)# switchport mode trunk`	Включите транковый режим на выбранном интерфейсе.

Некоторые коммутаторы Cisco Catalyst поддерживают только инкапсуляцию 802.1Q, которая настраивается автоматически при включении транкового режима на интерфейсе с помощью команды switchport mode trunk.



Для проверки конфигурации транкового режима на многих коммутаторах Cisco Catalyst используются команды **show interfaces** *интерфейс* **switchport** и **show interfaces** *интерфейс* **trunk**, которые отображают параметры транкового режима и данные VLAN для порта.



Создание VLAN

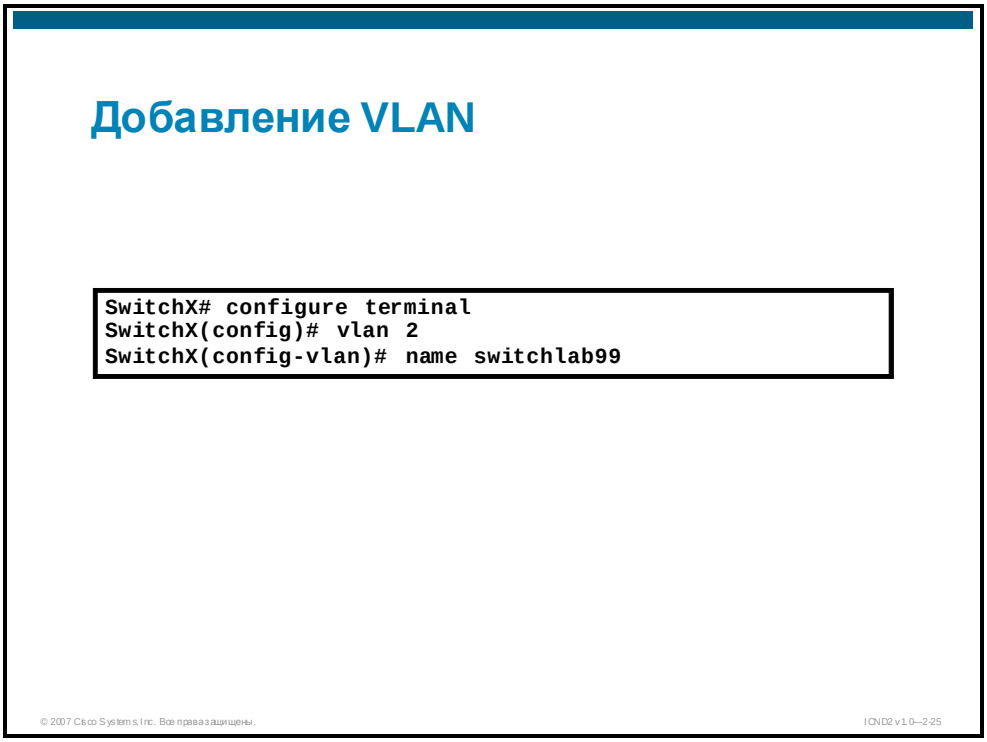
Перед созданием VLAN необходимо решить, нужно ли использовать протокол VTP для обслуживания данных глобальной конфигурации VLAN в сети.

Большинство настольных коммутаторов Cisco Catalyst поддерживают до 128 экземпляров протокола "spanning tree". Если количество сетей VLAN на коммутаторе превышает количество поддерживаемых экземпляров протокола "spanning tree", рекомендуется настроить протокол MSTP на коммутаторе для назначения нескольких сетей VLAN одному экземпляру протокола "spanning tree".

Максимальное количество сетей VLAN зависит от коммутатора. Многие коммутаторы Cisco Catalyst уровня доступа поддерживают до 250 пользовательских сетей VLAN.

Коммутаторы Cisco Catalyst имеют заводскую конфигурацию по умолчанию, в которой заданы различные сети VLAN для поддержки различных сред и типов протоколов. Сеть VLAN по умолчанию для Ethernet — VLAN 1. Объявления CDP и VTP рассылаются в сети VLAN 1.

Чтобы пользователи могли удаленно подключаться к коммутатору Cisco Catalyst для выполнения задач управления, коммутатор должен иметь IP-адрес. Этот IP-адрес должен находиться в управляющей сети VLAN (по умолчанию в сети VLAN 1). Если в сети настроен домен VTP, перед созданием VLAN необходимо перевести коммутатор в северный или прозрачный режим VTP.



На таблице ниже перечислены команды, используемые для добавления VLAN.

Команда/*переменная*	**Описание**
vlan *идентификатор vlan*	Идентификатор VLAN, которую необходимо добавить и настроить. Диапазон идентификаторов VLAN составляет от 1 до 4094, если установлен расширенный образ ПО или от 1 до 1005, если установлен стандартный образ ПО. Не вводите нули в начале чисел. Вы можете ввести один идентификатор VID, последовательность идентификаторов VID, разделенных запятыми, или диапазон идентификаторов VID, разделенный дефисом.
name *имя vlan*	(Необязательно) Указывает имя VLAN (строку ASCII от 1 до 32 символов). Должно быть уникально в административном домене.

По умолчанию коммутатор находится в режиме VTP-сервера, который позволяет добавлять, изменять и удалять VLAN. Если коммутатор находится в режиме VTP-клиента, добавление, изменение и удаление сетей VLAN невозможно.

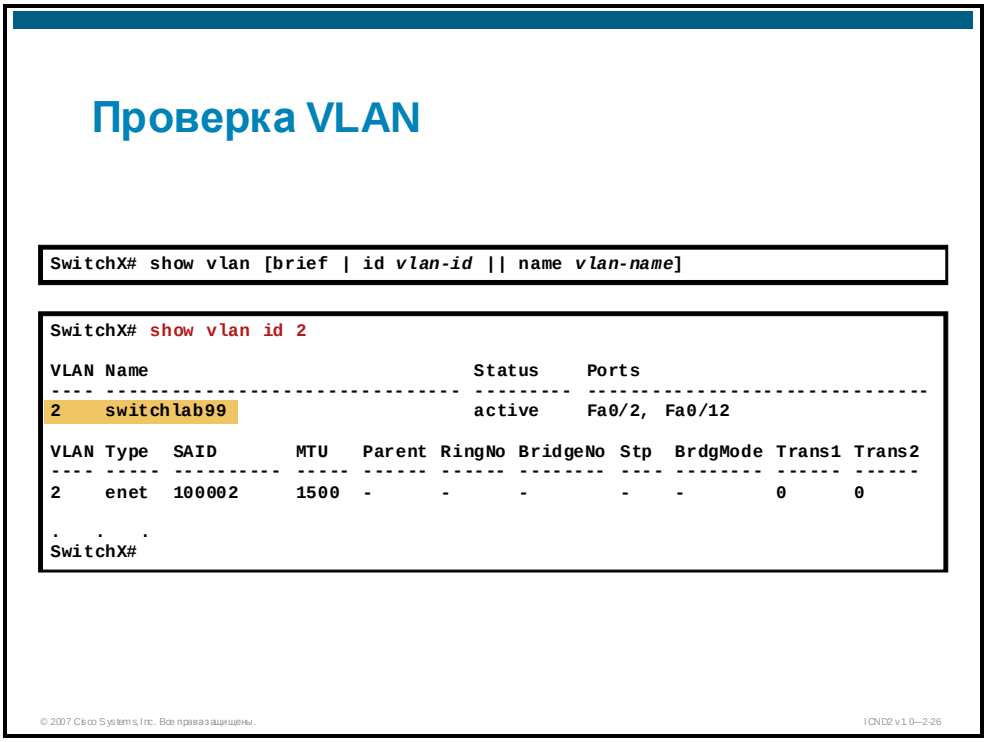
На многих коммутаторах Cisco Catalyst для создания VLAN и перехода в режим глобальной конфигурации VLAN используется команда глобальной конфигурации **vlan**. Используйте версию «**no**» этой команды, чтобы удалить VLAN.

Чтобы добавить сеть VLAN в базу данных VLAN, назначьте этой сети имя и номер. Сеть VLAN по умолчанию, заданная на заводе, — VLAN 1. Сети обычного диапазона VLAN идентифицируются числом от 1 до 1001. Номера VLAN от 1002 до 1005 зарезервированы для Token Ring VLAN и FDDI VLAN. Если коммутатор находится в режиме VTP-сервера или в прозрачном режиме VTP, вы можете добавлять, изменять и удалять конфигурации для сетей VLAN с номерами от 2 до 1001 в базе данных VLAN. (Идентификатор VID 1, а также идентификаторы от 1002 до 1005 создаются автоматически и не могут быть удалены.)

Примечание Если коммутатор находится в прозрачном режиме VTP и установлен расширенный образ ПО, вы можете создать сети VLAN расширенного диапазона (сети VLAN с идентификаторами от 1006 до 4094), но такие сети VLAN не будут сохраняться в базе данных VLAN.

Конфигурации для VID от 1 до 1005 записываются в файл vlan.dat (базу данных VLAN). Данные о сетях VLAN можно вывести с помощью команды **show vlan** привилегированного режима EXEC. Файл vlan.dat сохраняется во flash-память.

Чтобы добавить сеть Ethernet VLAN, необходимо указать как минимум номер VLAN. Если для сети VLAN не указано имя, будет использовано имя по умолчанию, состоящее из слова **vlan** и номера сети. Например, VLAN0004 будет именем по умолчанию для сети VLAN 4, если не указано иное имя.

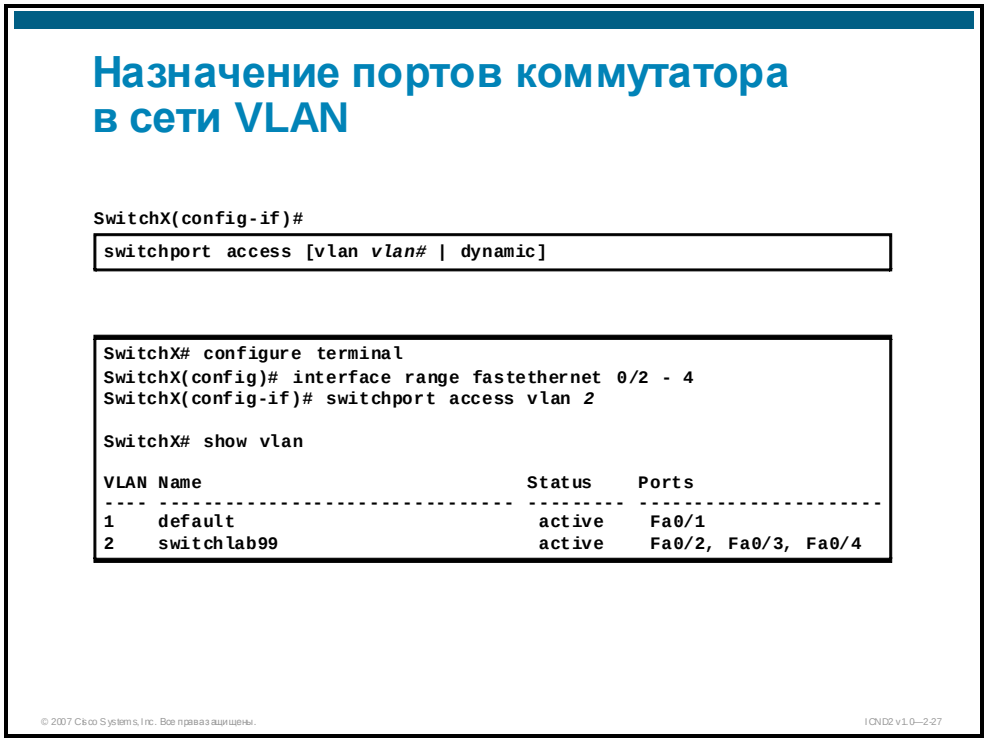


После настройки сети VLAN необходимо проверить ее параметры.

Сведения об указанной сети VLAN выводятся с помощью команд **show vlan id** *номер_vlan* и s**how vlan name** *имя_vlan*.

Команда **show vlan brief** выводит одну строку для каждой VLAN. Эта строка включает имя, сведения о состоянии и портах коммутатора.

Для вывода сведений обо всех настроенных VLAN используется команда **show vlan**. Команда **show vlan** отображает порты коммутатора, назначенные в каждую VLAN. Другие параметры VLAN, которые отображаются при вводе этой команды: тип (значение по умолчанию — Ethernet); идентификатор привязки безопасности (SAID), используется для транковых подключений FDDI; максимальный размер передаваемого блока (MTU) (значение по умолчанию для Ethernet VLAN — 1500); STP и другие параметры, используемые для Token Ring VLAN или FDDI VLAN.



Назначение портов VLAN

После создания сети VLAN вы можете вручную назначить в нее один или несколько портов. Порт может принадлежат только одной сети VLAN. Порт, назначенный в сеть VLAN, с помощью этого метода называется портом статического доступа.

На большинстве коммутаторов Cisco Catalyst назначение портов VLAN выполняется в режиме конфигурации интерфейса с помощью команды switchport access. Используйте параметр vlan номер_vlan, чтобы настроить принадлежность порта статического доступа. Используйте параметр dynamic, чтобы сеть VLAN управлялась и назначалась протоколом VMPS.

Примечание По умолчанию все порты принадлежат VLAN 1.

Проверка принадлежности VLAN

```
SwitchX# show vlan brief
```

```
SwitchX# show vlan brief
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1
2    switchlab99                      active    Fa0/2, Fa0/3, Fa0/4
3    vlan3                            active
4    vlan4                            active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

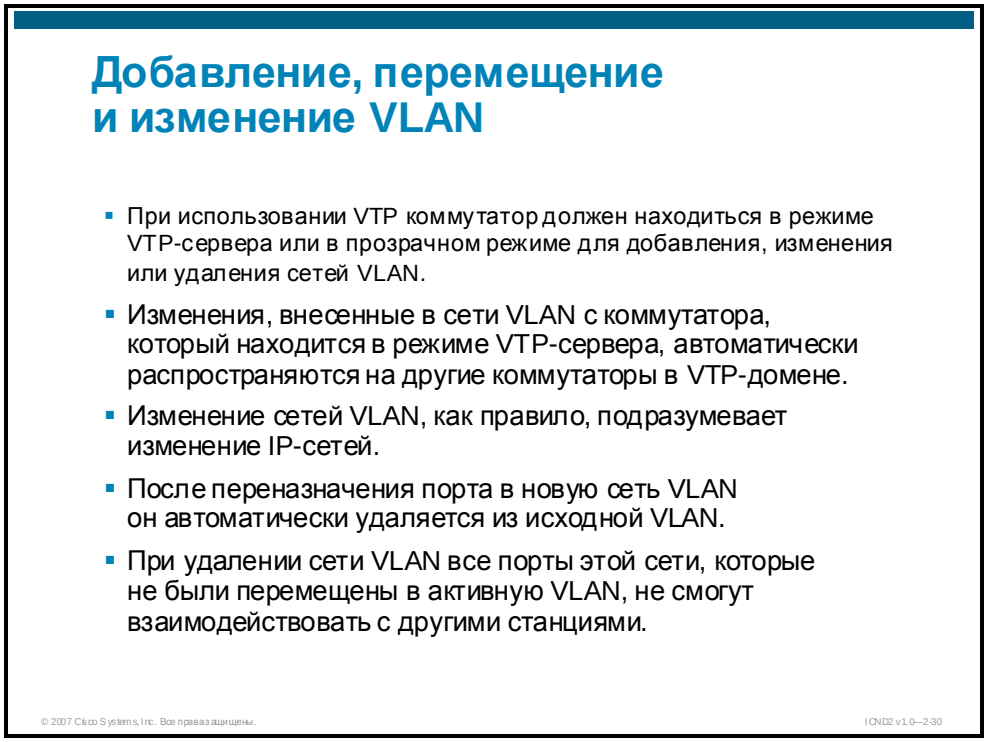

Используйте команду **show vlan brief** привилегированного режима EXEC, чтобы вывести данные о назначении и типе принадлежности VLAN для всех портов коммутаторов.

Проверка принадлежности VLAN (прод.)

```
SwitchX(config-if)#
show interfaces интерфейс switchport
```

```
SwitchX# show interfaces fa0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 2 (switchlab99)
Trunking Native Mode VLAN: 1 (default)
--- output omitted ----
```


Другой способ: используйте команду **show interfaces** интерфейс **switchport** привилегированного режима EXEC, чтобы вывести данные по VLAN для определенного интерфейса.



Добавление, перемещение и изменение VLAN

По мере изменения сетевых топологий, требований бизнеса и ролей пользователей, требования к VLAN также меняются.

Для добавления, изменения или удаления VLAN коммутатор должен находиться в режиме VTP-сервера или в прозрачном режиме. Изменения, внесенные в сети VLAN с коммутатора, который находится в режиме VTP-сервера, автоматически распространяются на другие коммутаторы в VTP-домене. Изменения, внесенные в сети VLAN с коммутатора, который находится в прозрачном режиме, влияют только на локальный коммутатор и не распространяются на домен.

Добавление сетей VLAN и принадлежность портов

После создания сети VLAN, обязательно внесите все необходимые изменения в назначения портов VLAN.

Отдельные VLAN, как правило, подразумевают отдельные IP-сети. Обязательно спланируйте новую систему IP-адресации и ее развертывание на станциях перед перемещением пользователей в новую VLAN. Кроме того, раздельные VLAN требуют настройки маршрутизации между VLAN, чтобы дать пользователям новых VLAN возможность взаимодействовать с другими VLAN. Маршрутизация между сетями VLAN требует настройки соответствующих параметров и служб IP, включая шлюз по умолчанию и DHCP.

Изменение сетей VLAN и принадлежности портов

Для изменения атрибутов VLAN, таких как имя VLAN, используется команда глобальной конфигурации **vlan** *идентификатор vlan*.

Примечание Изменить номер VLAN нельзя. Чтобы использовать другой номер VLAN, создайте новую сеть VLAN с новым номером, а затем переназначьте все порты в эту VLAN.

Чтобы переместить порт в другую VLAN, используйте те же команды, что для создания исходных назначений.

Для этого изменения не нужно удалять порт из исходной VLAN. После переназначения порта в новую VLAN он автоматически удаляется из исходной VLAN.

Удаление сетей VLAN и принадлежности портов

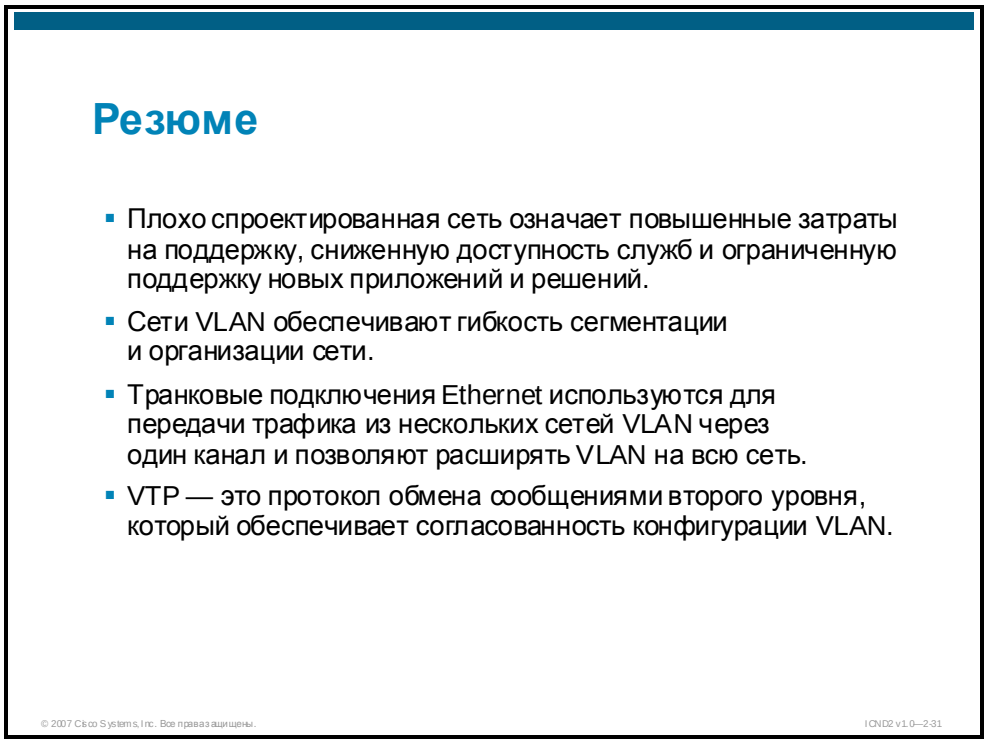
При удалении сети VLAN с коммутатора, который находится в режиме VTP-сервера, сеть удаляется со всех коммутаторов домена VTP. При удалении сети VLAN с коммутатора, который находится в прозрачном режиме VTP, сеть удаляется только с данного коммутатора. Для удаления VLAN используется команда глобальной конфигурации **no vlan** *идентификатор vlan*.

Примечание Перед удалением сети VLAN обязательно переназначьте все порты, которые ей принадлежат, в другие сети VLAN. Порты, которые не будут перемещены в активную VLAN, не смогут взаимодействовать с другими станциями после удаления VLAN.

Для переназначения портов в сеть VLAN по умолчанию (VLAN 1) используется команда **no switchport access vlan** режима конфигурации интерфейса.

Резюме

В этом разделе приводится резюме основных вопросов, рассмотренных в занятии.



Занятие 2

Улучшение производительности с помощью протокола "spanning tree"

Обзор

Большинство сложных сетей включают резервные устройства для исключения критических точек отказа. Хотя топология с резервированием решает ряд проблем, она может создавать новые проблемы. Протокол "spanning tree" (STP) — это протокол управления каналами второго уровня, который обеспечивает резервирование маршрутов и предотвращает образование нежелательных петель в коммутируемой сети.

В этом занятии описываются проблемы, которые возникают в резервируемой топологии коммутируемых сетей и функции STP, которые позволяют предотвратить эти проблемы.

Задачи

По окончании этого занятия вы сможете описывать ситуации, в которых используется протокол "spanning tree", и внедрять его в сети. Это значит, что вы сможете выполнить следующие задачи:

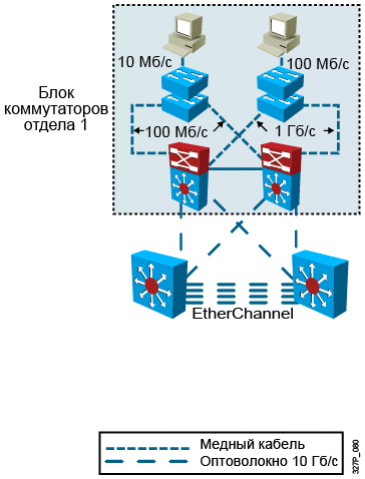
- описывать методы, которые используются для создания физических подключений между коммутаторами в резервируемой топологии;
- определять потенциальные проблемы резервируемой коммутируемой топологии;
- описывать, как протокол "spanning tree" решает проблемы резервируемых коммутируемых сетей;
- настраивать протокол RSTP, в том числе корневой коммутатор или резервный корневой коммутатор.

Создание резервируемой коммутируемой топологии

В этом разделе описываются способы добавления резервируемых каналов и устройств в коммутируемые и мостовые сети.

Технологии соединения

Технология	Использование
Fast Ethernet	Соединение устройств конечных пользователей с коммутаторами уровня доступа
Gigabit Ethernet	Соединение коммутатора доступа с коммутатором распределения, а также соединение требовательных серверов с коммутаторами
10-Gigabit Ethernet	Высокоскоростные каналы связи между коммутаторами, магистрали
EtherChannel	Высокоскоростные каналы связи между коммутаторами, магистрали с резервированием

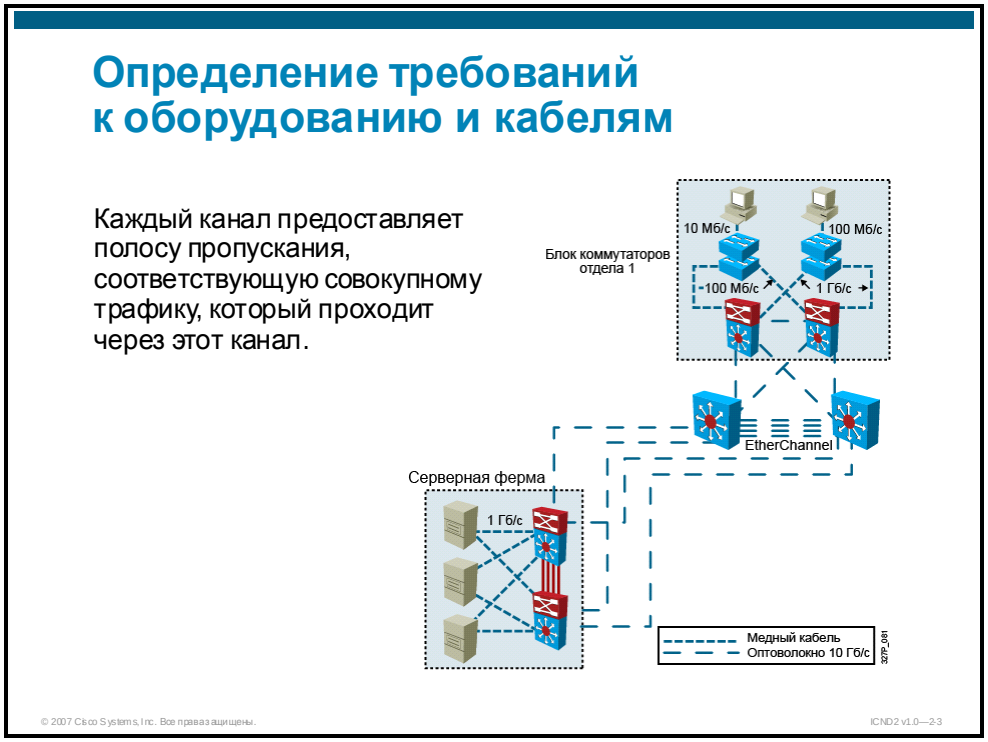


Выбор технологий соединения

Для соединения устройств в коммутируемой сети используется несколько технологий. Выбор подходящей технологии должен зависеть от объемов трафика, которые будет передавать канал. Скорее всего будет использоваться комбинация медных и волоконно-оптических кабелей, в зависимости от расстояния, требований к помехоустойчивости, безопасности и других требований бизнеса. Ниже перечислены некоторые из наиболее распространенных технологий.

- **Fast Ethernet (Ethernet 100 Мбит/с).** ЛВС, построенные по этой спецификации (IEEE 802.3u), работают со скоростью 100 Мбит/с и используют витую пару. Стандарт Fast Ethernet увеличивает скорость Ethernet с 10 Мбит/с до 100 Мбит/с и требует минимальных изменений существующей кабельной инфраструктуры. Коммутаторы с портами 10 Мбит/с и 100 Мбит/с могут передавать кадры между портами без преобразования протоколов второго уровня.
- **Gigabit Ethernet.** Расширение стандарта IEEE 802.3 Ethernet, Gigabit Ethernet увеличивает скорость Fast Ethernet в 10 раз, до 1000 Мбит/с или 1 Гбит/с. Спецификация IEEE 802.3z стандартизирует работу в волоконно-оптических средах, спецификация IEEE 802.3ab стандартизирует работу через витую пару.

- **10-Gigabit Ethernet.** Технология 10-Gigabit Ethernet была формально ратифицирована как стандарт 802.3 Ethernet в июне 2002 г. Она представляет собой следующий шаг в наращивании производительности и функциональных возможностей корпоративной среды. По мере распространения технологии Gigabit Ethernet, стандарт 10-Gigabit Ethernet все чаще используется для восходящих каналов.
- **EtherChannel.** Эта функция обеспечивает объединение полосы пропускания в каналах второго уровня между двумя коммутаторами. EtherChannel группирует отдельные порты Ethernet в один логический порт или канал. Все интерфейсы в группе EtherChannel должны иметь одинаковые параметры скорости, дуплексной передачи и принадлежности VLAN.



Определение требований к оборудованию и кабелям

При проектировании любой высокопроизводительной сети рассматриваются 4 показателя: безопасность, доступность, масштабируемость и управляемость. В этом списке описываются решения по выбору оборудования и кабелей, которые необходимо принять при изменении инфраструктуры.

- На уровне доступа здания замените концентраторы и устаревшие концентраторы на новые коммутаторы. Выберите оборудование с количеством портов уровня доступа, достаточным для обслуживания текущей пользовательской базы и поддержки будущего роста. Некоторые разработчики начинают с планирования 30-процентного роста. Если бюджет позволяет, используйте модульные коммутаторы доступа для поддержки расширения в будущем. Рассмотрите планы поддержки питания по сигнальным проводам и внедрению политик качества обслуживания (QoS), если вы думаете, что в будущем может понадобиться развертывание IP-телефонии.
- При создании кабельной системы для соединения устройств уровня доступа и устройств уровня распределения в здании помните, что эти каналы будут использоваться для передачи объединенного трафика от конечных узлов уровня доступа в распределительные коммутаторы задания. Убедитесь, что эти каналы имеют достаточную полосу пропускания. Для увеличения полосы пропускания можно использовать группы EtherChannel.
- На уровне распределения выберите коммутаторы с производительностью, достаточной для обработки нагрузки текущего уровня доступа. Кроме того, необходимо учесть дополнительные порты для добавления транковых подключений в будущем, чтобы обеспечить поддержку новых устройств доступа. Устройства на этом уровне должны быть многоуровневыми коммутаторами (уровней 2 и 3) с поддержкой маршрутизации между VLAN рабочей группы и сетевыми ресурсами. В зависимости от размера сети, устройства уровня распределения могут быть модульными или иметь

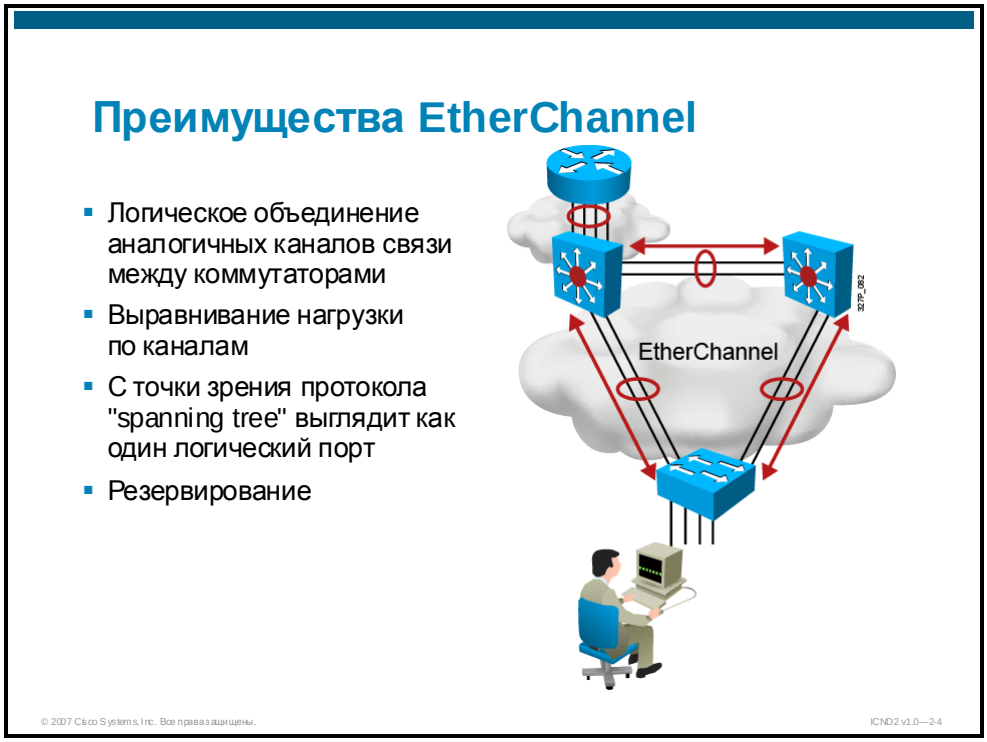
фиксированное шасси. Планируйте резервирование для шасси и подключений на уровне доступа и центральном уровне в соответствии с требованиями бизнеса.

- Магистральное оборудование уровня комплекса зданий должно поддерживать высокоскоростное соединение между другими подмодулями. При определении параметров магистрали учтите требования масштабируемости и планы резервирования.

Cisco предлагает интерактивные средства, которые помогают разработчиками принять верные решения по выбору устройств с учетом требований бизнеса и технологий. Ниже приводятся коэффициенты превышения физической полосы пропускания канала, которые можно использовать для планирования полосы пропускания каналов между основными устройствами сети с учетом средних потоков трафика.

- **Каналы между уровнями доступа и распределения.** Коэффициент превышения физической полосы пропускания канала не должен быть больше 20:1. Это значит, что канал может составлять 1/20 от совокупной полосы пропускания, доступной всем конечным устройствам, которые используют этот канал.
- **Каналы между уровнем распределения и центральным уровнем.** Коэффициент не должен превышать 4:1.
- **Каналы между центральными устройствами.** Для каналов между центральными устройствами не следует планировать превышение физической пропускной способности каналов или его необходимо свести к минимуму. Это значит, что каналы между центральными устройствами должны передавать трафик со скоростью, равной объединенной пропускной способности всех восходящих каналов к центральным устройствам.

Внимание Эти коэффициенты используются для определения среднего трафика с конечных пользовательских устройств уровня доступа. Они будут неточны при планировании превышения физической полосы пропускания для трафика от фермы серверов или периферийного распределительного модуля. Кроме того, они будут неточны при планировании полосы пропускания, необходимой для коммутаторов доступа, которые обслуживают пользовательские приложения, потребляющие значительную полосу пропускания (например, базы данных, не работающие в режиме "клиент-сервер" или одноадресные потоки мультимедиа). Использование QoS для всех компонентов тракта позволяет задать приоритеты трафика, который будет отбрасываться при перегрузке сети.



Обзор EtherChannel

Распространение Ethernet в настольных компьютерах может привести к неконтролируемому увеличению числа приложений с высокими требованиями к полосе пропускания. Новые приложения, такие как трансляция видео на настольные ПК, интерактивный обмен сообщениями и среды совместной работы, используют связь по принципу «все со всеми» и значительно увеличивают потребность в масштабируемой полосе пропускания. В то же время, для критически важных приложений необходима устойчивая архитектура сети. С широким распространением быстрых коммутируемых Ethernet-каналов на уровне комплекса зданий, организациям приходится объединять существующие ресурсы или модернизировать скорость восходящих каналов и центральных сетей для наращивания производительности сетевой магистрали.

EtherChannel — это технология, которую компания Cisco изначально разрабатывала для обратного межкоммуникаторного мультиплексирования нескольких портов Fast Ethernet или Gigabit Ethernet в один логический канал. Преимущества технологии EtherChannel — низкая стоимость по сравнению с высокоскоростными каналами и использование существующих портов коммутатора.

Преимущества технологии EtherChannel:

- позволяет создавать логические каналы с очень высокой полосой пропускания;
- поддерживает выравнивание нагрузки между физическими каналами группы;
- обеспечивает автоматическое аварийного переключение;
- упрощает последующую логическую настройку (конфигурация задается на уровне логического канала, а не на уровне физического канала)

Технология EtherChannel предлагает масштабируемую полосу пропускания на уровне комплекса зданий. Поддерживаются следующие значения объединенной полосы пропускания.

- **Fast Ethernet:** до 800 Мбит/с.
- **Gigabit Ethernet:** до 8 Гбит/с.
- **10-Gigabit Ethernet:** до 80 Гбит/с.

Эти скорости могут меняться на величину, равную скорости используемых каналов (100 Мбит/с, 1 Гбит/с или 10 Гбит/с). Даже в сценариях с самыми высокими требованиями к полосе пропускания технология EtherChannel помогает объединить трафик, сводит к минимуму потребность в превышении физической полосы пропускания и, в то же время, обеспечивает эффективные механизмы повышения устойчивости канала.

Резервируемые архитектуры исключают критические точки отказа, которые могут привести к отказу всей коммутируемой или мостовой сети, однако следует учитывать проблемы, которые могут возникнуть в таких сетях. Ниже перечислены некоторые из проблем, которые могут возникнуть в резервируемых каналах и устройствах коммутируемой или мостовой сети.

- **Широковещательные штормы.** Без процессов, предотвращающих образование петель, все коммутаторы и мосты будут непрерывно рассылать сообщения. Как правило, такая ситуация называется широковещательным штормом.
- **Множественная передача кадров.** В станции назначения могут быть доставлены несколько копий одноадресных кадров. Многие протоколы предполагают получение только одной копии каждого передаваемого блока. Прием нескольких копий одного кадра может привести к неустранимым ошибкам.
- **Нестабильность базы данных MAC-адресов.** Нестабильность таблицы MAC-адресов возникает из-за копий одного кадра, полученных на разных портах коммутатора. Если коммутатор использует все ресурсы для преодоления последствий нестабильности таблицы MAC-адресов, эффективность пересылки данных может быть снижена.

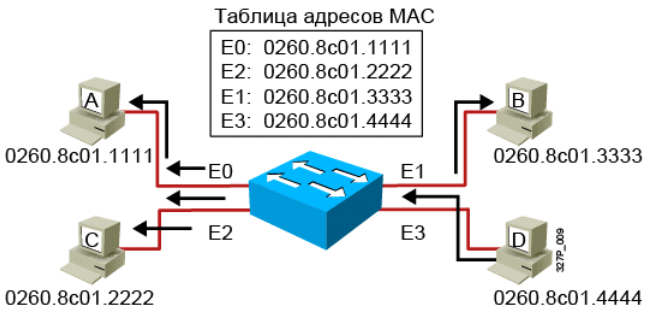
Протоколы ЛВС второго уровня, такие как Ethernet, не поддерживают механизмы распознавания и предотвращения бесконечных петель генерации кадров. Некоторые протоколы третьего уровня используют механизмы времени существования (TTL), которые ограничивают количество попыток повторной передачи пакетов сетевыми устройствами. В отсутствие такого механизма устройства второго уровня будут производить трафик в бесконечном цикле.

Для решения подобных проблем необходим механизм, предотвращающий образование петель.

Выявление проблем резервируемой избыточной топологии

В этом разделе описываются проблемы, которые могут возникнуть в резервируемой коммутируемой топологии.

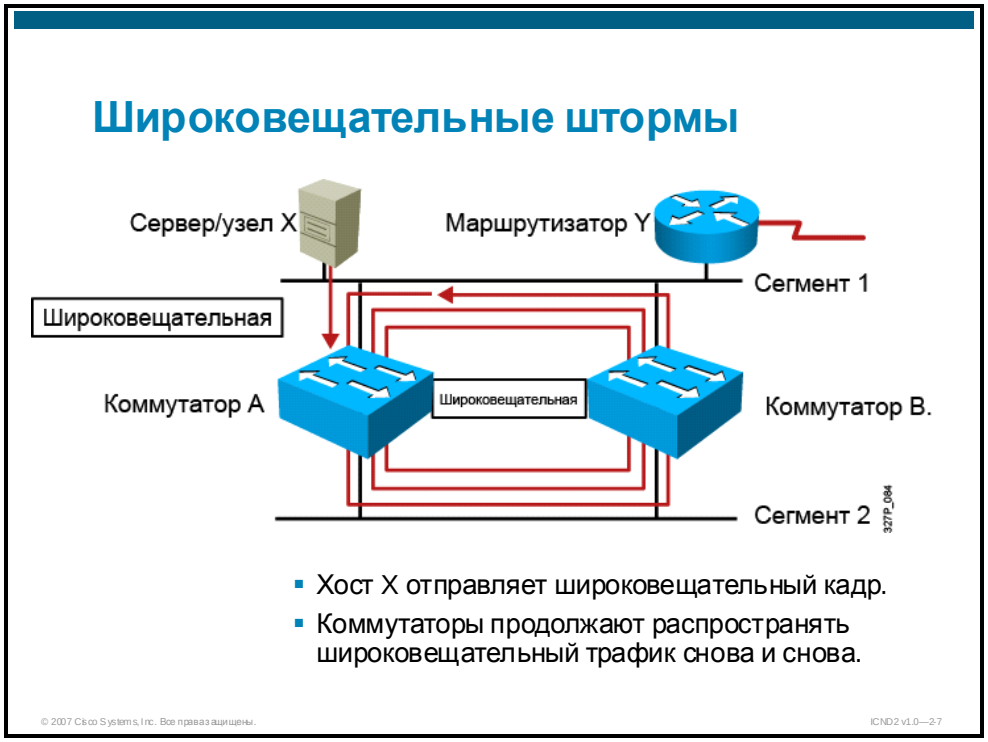
Широковещательные кадры



- Станция D отправляет широковещательный кадр.
- Широковещательные кадры рассылаются по всем портам, кроме порта источника.

Обработка широковещательных кадров коммутаторами

Коммутаторы обрабатывают широковещательные и многоадресные кадры не так, как одноадресные кадры. Поскольку широковещательные и многоадресные кадры могут представлять интерес для всех станций, коммутатор или маршрутизатор рассылают такие кадры по всем портам, кроме исходного. Коммутатор или мост никогда не знают адреса многоадресной рассылки, поскольку адреса многоадресной и широковещательной рассылки никогда на отображаются в качестве адреса источника кадра. Такая рассылка широковещательных и многоадресных кадров потенциально может привести к возникновению проблем в резервируемой избыточной топологии.



Широковещательные штормы

Широковещательный шторм происходит, когда все коммутаторы в резервируемой сети выполняют бесконечную рассылку кадров. Коммутаторы рассылают кадры по всем портам за исключением порта, с которого этот кадр был получен.

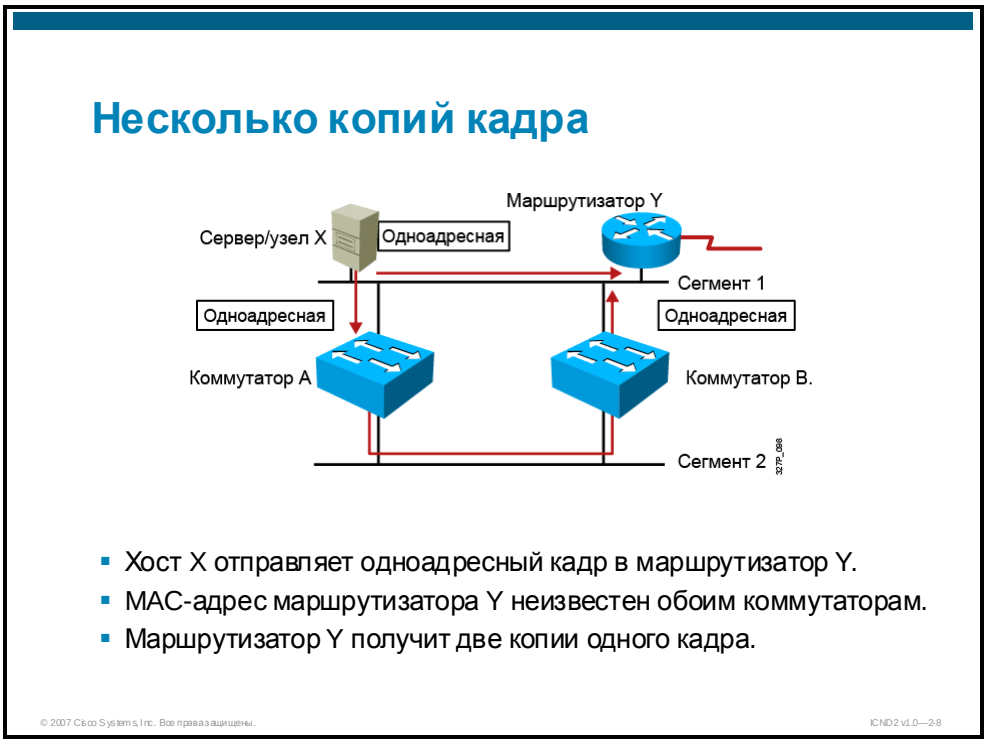
Пример широковещательного шторма

Проблема широковещательного шторма проиллюстрирована на рисунке. Ниже описывается последовательность событий, которая приводит к образованию широковещательного шторма.

1. Когда хост X отправляет широковещательный кадр, например кадр ARP, в свой шлюз по умолчанию (маршрутизатор Y), коммутатор A получает кадр.
2. Коммутатор A анализирует поле адреса назначения и определяет, что кадр должен быть распространен в нижнем канале Ethernet, сегмент 2.
3. Затем копия кадра прибывает в коммутатор B, процесс повторяется, и кадр пересылается в верхний сегмент Ethernet (сегмент 1) коммутатора B.
4. Поскольку исходная копия кадра также прибывает в коммутатор B с верхнего канала Ethernet, кадры двигаются в бесконечной петле в обоих направлениях даже после того, как станция назначения получает копию кадра.

Широковещательный шторм может нарушить нормальное течение трафика. Кроме того, он может прервать работу устройств коммутируемой или мостовой сети, поскольку ЦП каждого устройства в сегменте будет вынужден обрабатывать широковещательные кадры. Следовательно, широковещательный шторм может заблокировать работу ПК и серверов, которые пытаются обработать широковещательные кадры.

Механизмы предотвращения образования петель устраняют проблему, не позволяя одному из четырех интерфейсов передавать кадры во время нормальной эксплуатации и, таким образом, разбивая петлю.



Множественная передача кадров

В резервируемой топологии на хост-адресат могут прибыть несколько копий одного кадра, что может привести к возникновению проблем в протоколе-получателе. Большинство протоколов не предназначены для распознавания или устранения проблемы дублированной передачи. Как правило, протоколы, использующие последовательную нумерацию предполагают, что несколько операций передачи закончились неудачей и номер был сброшен. Другие протоколы пытаются перенаправить дублированную передачу соответствующему протоколу верхнего уровня (ULP), что приводит к непредсказуемым результатам.

Пример множественной передачи

Процесс возникновения множественной передачи иллюстрируется на рисунке. Ниже описывается последовательность событий, которая приводит к прибытию нескольких копий одного кадра в хост назначения.

1. Когда хост X отправляет одноадресный кадр в маршрутизатор Y, одна из копий принимается через прямое Ethernet-подключение (сегмент 1). Примерно в то же время коммутатор A получает копию кадра и помещает ее в свои буферы.

2. Если коммутатор A при анализе поля адреса назначения не находит в таблице MAC-адресов записи для маршрутизатора Y, коммутатор A рассылает кадр по всем портам, кроме исходного.

3. Когда коммутатор B получает копию кадра через коммутатор A в сегменте 2, коммутатор B также пересылает копию кадра в сегмент 1, если ему не удается найти в таблице MAC-адресов запись для маршрутизатора Y.

4. Маршрутизатор Y получает копию кадра второй раз.

Механизмы предотвращения образования петель устраняют проблему, не позволяя одному из четырех интерфейсов передавать кадры во время нормальной эксплуатации и, таким образом, разбивая петлю.

Нестабильность базы данных MAC-адресов

Нестабильность базы данных MAC возникает, когда несколько копий кадра прибывают на разные порты коммутатора. В этом подразделе описывается, как возникает нестабильность базы данных MAC и к каким проблемам она может привести.

Пример нестабильности базы данных MAC

На рисунке коммутатор B устанавливает запись базы данных, сопоставляя MAC-адрес хоста X и порт 1. Некоторое время спустя копия кадра, переданная через коммутатор A, прибывает на порт 2 коммутатора B, порт B удаляет первую запись и устанавливает вторую, которая неверно сопоставляет MAC-адрес хоста X и порт 2, подключенный к сегменту 2.

В зависимости от внутренней архитектуры проблемный коммутатор может не справиться с быстрым изменением базы данных MAC. И снова механизмы предотвращения образования петель устраняют эту проблему, не позволяя одному из четырех интерфейсов передавать кадры во время нормальной эксплуатации и, таким образом, разбивая петлю.

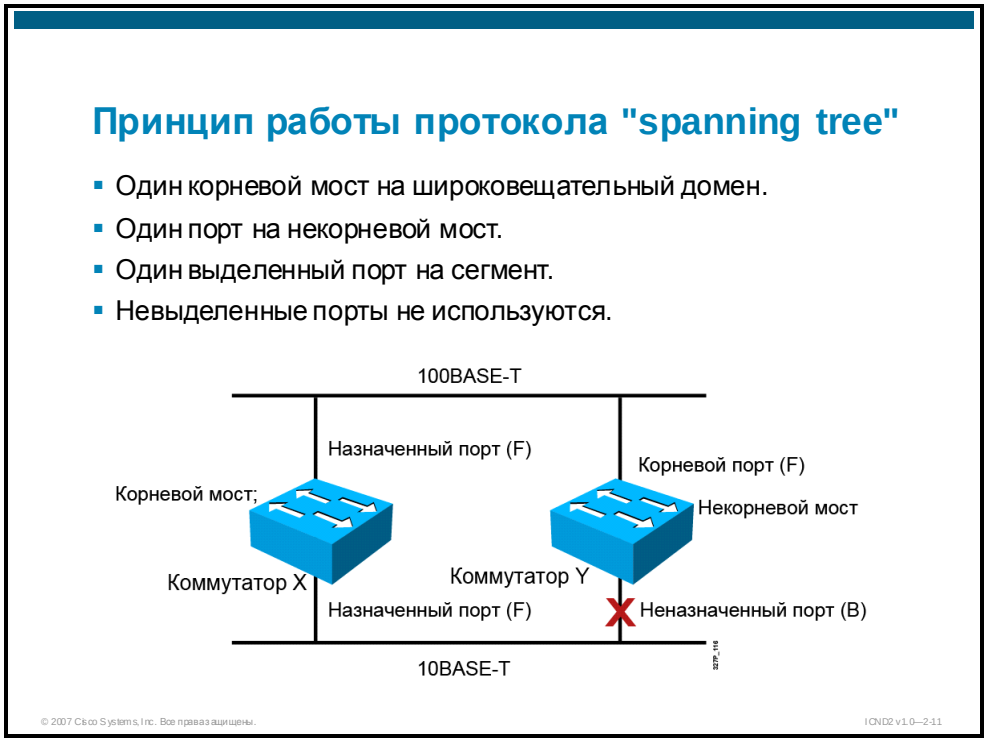
Решение проблем с помощью STP

В этом разделе описывается процесс, который протоколом STP для создания сетевой топологии с защитой от петель.

STP устраняет проблему петель за счет направления физических маршрутов в заданные сегменты сети. STP обеспечивает резервирование физических маршрутов и предотвращает нежелательные эффекты, связанные с образованием активных петель в сети. STP — это стандарт комитета IEEE, определяемый как 802.1D.

STP работает следующим образом.

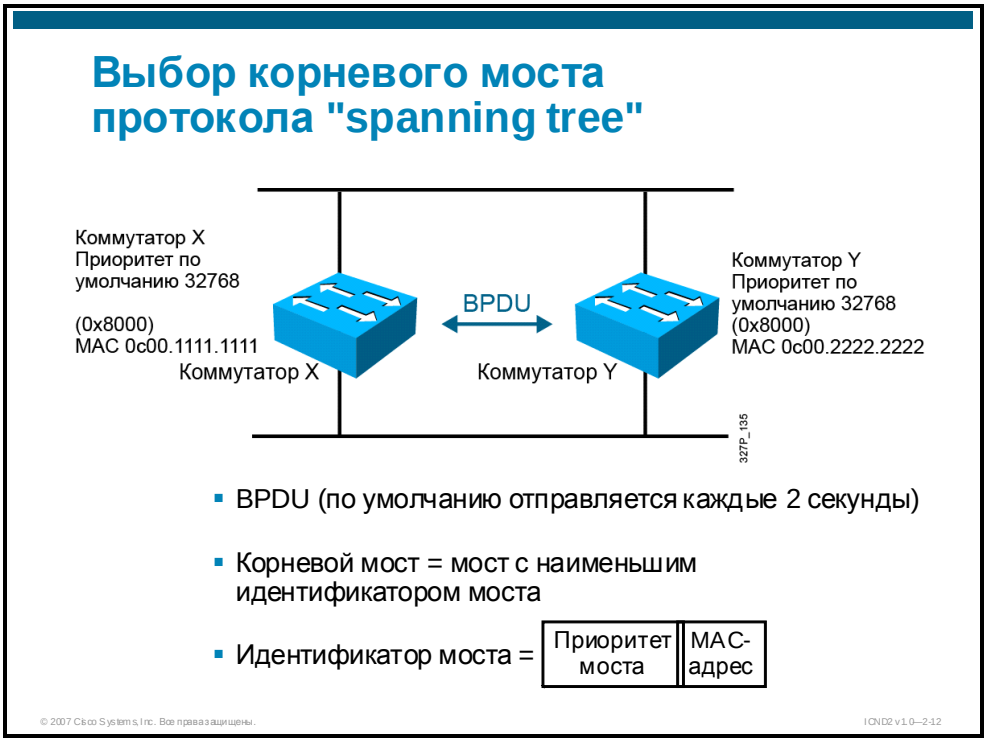
- STP переводит отдельные порты в состояние ненагруженного резерва, в котором они не могут прослушивать, пересылать или выполнять лавинную рассылку кадров. В результате к каждому сегменту ведет только один постоянно активный маршрут.
- Если в подключении к любому из сегментов в сети возникает проблема, STP восстанавливает подключение путем автоматической активации неактивного маршрута (если он существует).



Принцип работы протокола "spanning tree"

Для создание логической топологии сети с защитой от образования петель STP выполняет следующие действия.

1. **Выбор одного корневого моста.** STP включает процесс выбора корневого моста. Только один мост может служить корневым мостом в сети. Все порты корневого моста являются выделенными. Как правило, выделенные порты находятся в режиме пересылки. Порт в режиме пересылки может отправлять и принимать трафик. На рисунке ниже в качестве корневого моста выбран коммутатор X.
2. **Выбор корневого порта на некорневом мосту.** STP устанавливает один корневой порт на каждом некорневом мосту. Корневой порт представляет маршрут с наименьшей стоимостью от некорневого моста к корневому. Как правило, корневые порты находятся в режиме пересылки. Стоимость маршрута протокола "spanning tree" и совокупная стоимость рассчитываются на основе полосы пропускания. На рисунке минимальную стоимость будет иметь маршрут к корневому мосту с коммутатора Y через канал 100BASE-T Fast Ethernet.
3. **Выбор выделенного порта для каждого сегмента.** STP устанавливает выделенный порт в каждом сегменте. Выделенный порт выбирается на мосту, который предоставляет маршрут с наименьшей стоимостью к корневому мосту. Как правило, выделенные порты находятся в режиме пересылки и выполняют пересылку трафика для сегмента На рисунке выделенные порты для обоих сегментов находятся на корневом мосту, поскольку корневой мост имеет прямое подключение к обоим сегментам. Порт 10BASE-T Ethernet на коммутаторе Y не является выделенным, поскольку в сегменте может быть только один выделенный порт. Невыделенные порты, как правило, находятся в блокирующем режиме для логического прерывания петли. Когда порт находится в блокирующем режиме, он не пересылает трафик, однако может принимать его.



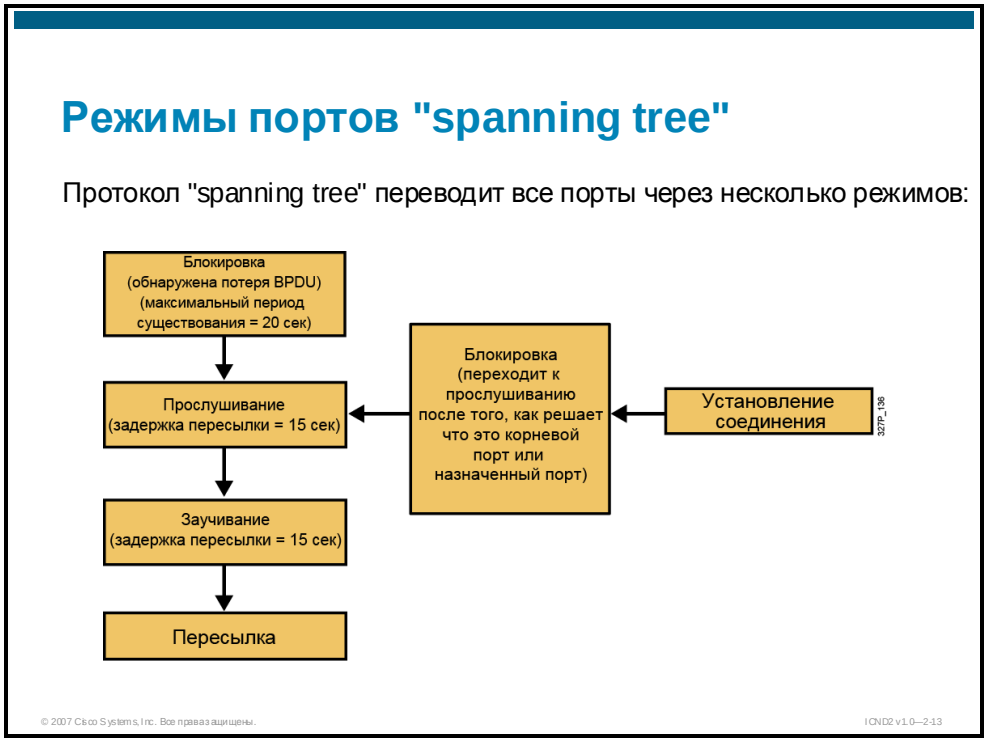
Коммутаторы и мосты под управлением алгоритма "spanning tree" обмениваются сообщениями конфигурации с другими коммутаторами и мостами через регулярные интервалы (по умолчанию через каждые 2 сек). Коммутаторы и мосты обмениваются этими сообщениями с помощью многоадресных кадров, которые называются блоками данных протокола (BPDU). Один из информационных элементов, входящих в BPDU, — идентификатор моста (BID).

Вызовам STP для каждого коммутатора и моста должен быть назначен уникальный BID. Как правило, BID состоит из значения приоритета (2 байта) и MAC-адреса моста (6 байт). В соответствии со стандартом IEEE 802.1D приоритет по умолчанию — 32 768 (1000 0000 0000 0000 в двоичном исчислении или 0x8000 в шестнадцатеричном). Это среднее значение. Корневой мост — это мост с наименьшим BID.

Примечание Коммутатор Cisco Catalyst использует один из MAC-адресов из пула MAC-адресов, которые назначаются коммутационной панели или контролирующему модулю в зависимости от модели коммутатора.

Пример выбора корневого моста

На этом рисунке оба коммутатора используют одинаковые значения по умолчанию. Коммутатор с минимальным MAC-адресом является корневым мостом. В этом примере коммутатор X является корневым мостом и имеет BID 0x8000 (0c00.1111.1111).



В STP задано 5 режимов работы порта:

- блокирующий режим;
- режим прослушивания;
- режим обучения;
- режим пересылки;
- отключен.

Примечание В строгом смысле режим «Отключен» не является частью протокола STP. Администратор сети может отключить порт вручную.

Когда протокол STP активирован, во время загрузки все мосты в сети проходят через блокирующий режим, а также переходные режимы прослушивания и обучения. Если сеть настроена верно, все порты стабилизируются в режиме пересылки или блокирующем режиме. Порты в режиме пересылки обеспечивают маршрут с наименьшей стоимостью к корневому мосту. При изменении топологии порт временно переходит в режимы прослушивания и обучения.

Все порты моста начинают работу в блокирующем режиме, в котором они ожидают получения блока BPDU. При первой загрузке мост функционирует как корневой и переходит в режим прослушивания. Отсутствие блока BPDU в течение определенного периода времени называется максимальным возрастом (max_age), значение по умолчанию — 20 секунд. Если порт в блокирующем режиме не получает нового блока BPDU в течение периода max_age, мост переходит из блокирующего режима в режим прослушивания. Когда порт находится в переходном режиме прослушивания, он может отправлять и принимать блоки BPDU для определения активной топологии.

В этот момент через мост не проходят пользовательские данные. В режиме прослушивания мост выполняет три действия:

- выбор корневого моста;
- выбор корневых портов на некорневых мостах;
- выбор выделенных портов для всех сегментов.

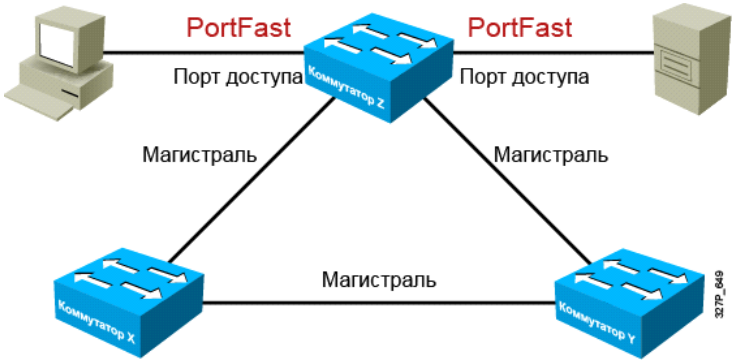
Время, которое уходит на переход порта из режима прослушивания в режим обучения и из режима обучения в режим пересылки называется задержкой пересылки. Значение задержки по умолчанию — 15 секунд.

Режим обучения уменьшает объем рассылки, необходимой при запуске пересылки. Если порт остается выделенным или корневым по окончании режима обучения, он переходит в режим пересылки. В режиме пересылки порт может отправлять и передавать пользовательские данные. Порты, которые не являются выделенными или корневыми возвращаются в блокирующий режим.

Как правило порт переходит из блокирующего режима в режим пересылки за 30 – 50 секунд. Вы можете настроить таймеры протокола "spanning tree", чтобы изменить эти периоды времени, однако эти таймеры предназначены для работы со значениями по умолчанию. Значение по умолчанию дают сети достаточно времени для сбора всех необходимых данных.

Примечание Для портов коммутаторов, подключенных только к конечным пользовательским станциям (а не к другому коммутатору или мосту), необходимо включить функцию коммутаторов Cisco Catalyst под названием PortFast. Порт коммутатора, на котором включена функция PortFast, автоматически переходит с блокирующего режима в режим пересылки при первой загрузке. Это приемлемо, так как порт, к которому не подключены другое коммутаторы и мосты, не может образовывать петли.

Описание PortFast

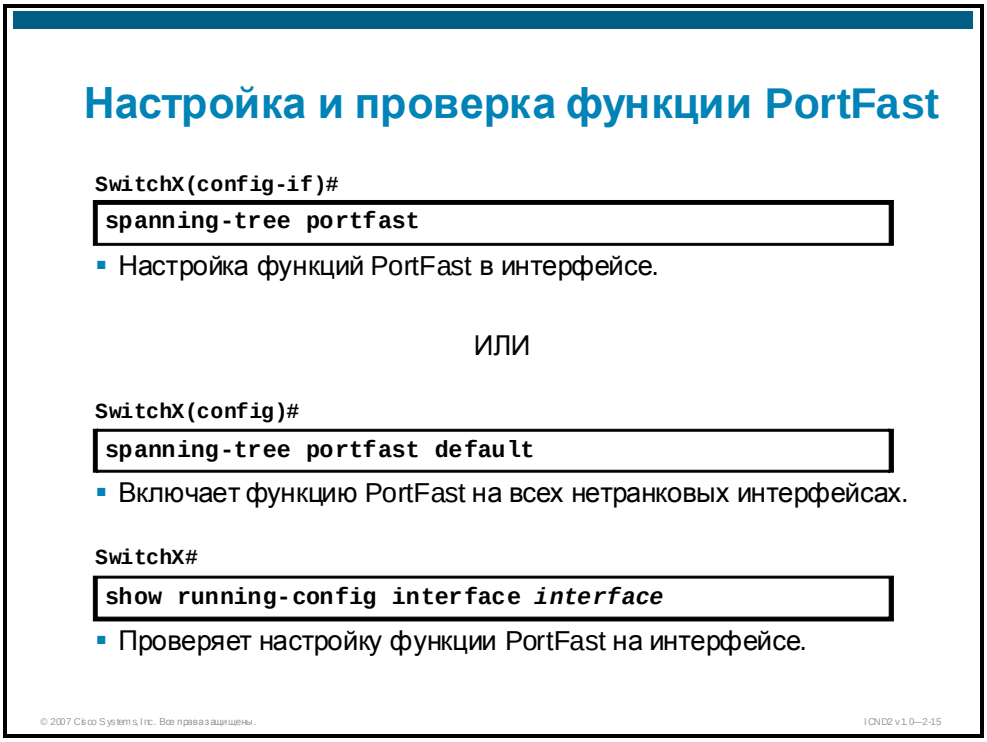


Функция PortFast настраивается на портах доступа, но не на транковых портах.

Функция PortFast немедленно переводит интерфейс, настроенный как порт доступа второго уровня, из блокирующего режима в режим пересылки, минуя режимы прослушивания и обучения. Функцию PortFast можно использовать на портах доступа второго уровня, подключенных к одной рабочей станции или серверу, чтобы разрешить им немедленно подключаться к сети, не ожидая конвергенции "spanning tree".

Если интерфейс, настроенный с функцией PortFast, получает блок BPDU, протокол "spanning tree" может перевести порт в блокирующее состояние с помощью функции под названием "сторож BPDU". .

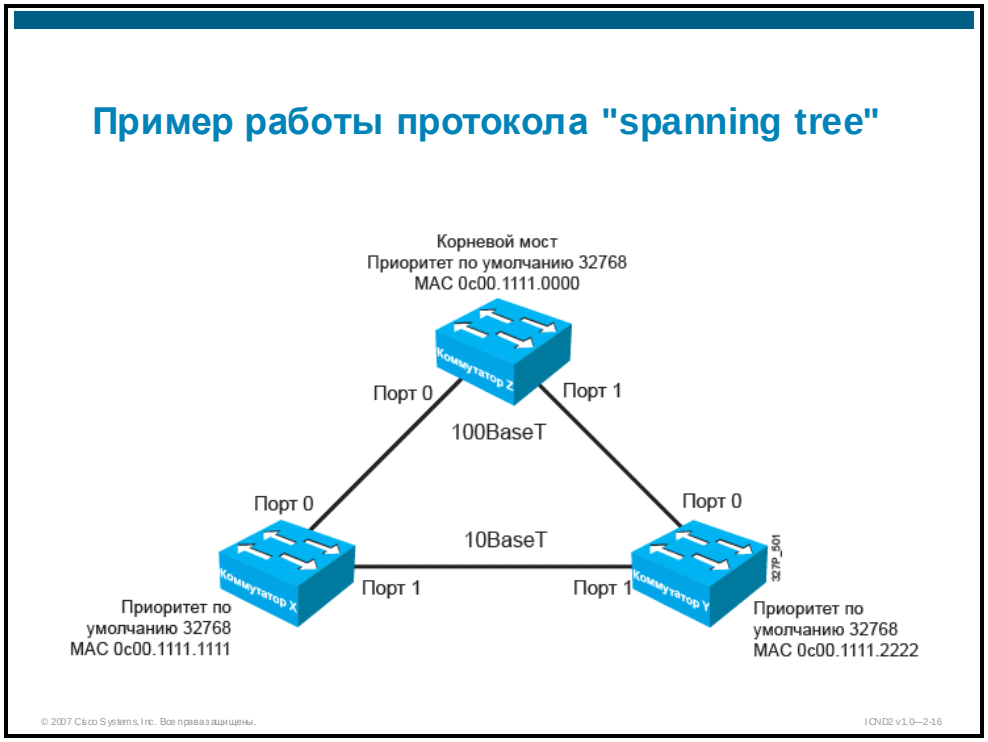
Внимание Поскольку цель функции PortFast — позволить портам доступа немедленно подключится к сети, не ожидая конвергенции протокола "spanning tree", она должна использоваться только на портах доступа. Если функция PortFast будет включена на порте, подключенном к другому коммутатору, возникнет риск образования петли протокола "spanning tree".



В таблицы ниже приведены команды, необходимые для включения и проверки функции PortFast на интерфейсе.

Команды PortFast

Аргумент	Описание
Switch(config-if)# **spanning-tree portfast**	Включает функцию PortFast на порте доступа второго уровня и немедленно переводит его в режим пересылки.
Switch(config-if)# **no spanning-tree portfast**	Отключает функцию PortFast на порте доступа второго уровня. Функция PortFast отключена по умолчанию.
Switch(config)#**spanning-tree portfast default**	Глобально активирует функцию PortFast на всех нетранковых портах. Когда функция PortFast включена, порт переходит из блокирующего режима в режим пересылки не выполняя промежуточных переходов, которые необходимы для протокола "spanning tree".
Switch# **show running-config interface** *type slot/port*	Сообщает, настроена ли функция PortFast на порте. Кроме того, команда позволяет узнать, была ли конфигурация выполнена в канале EtherChannel. Для этого необходимо указать параметры *port-channel channel_number* вместо *type slot/port.*



Пример работы протокола "spanning tree"

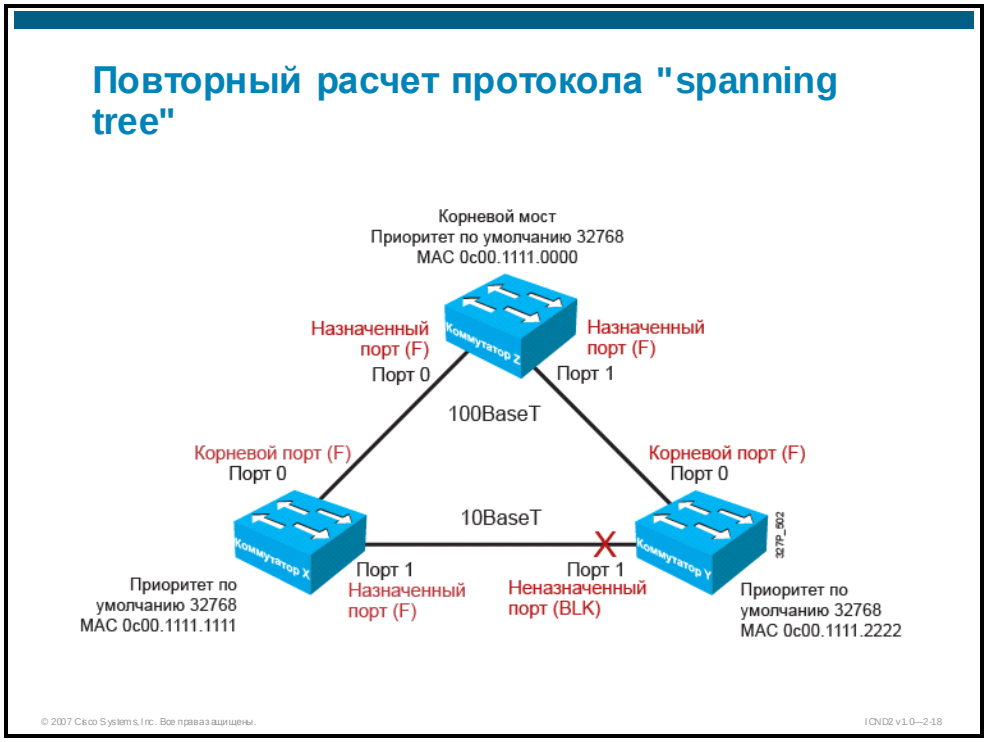
Ниже описываются режимы портов STP, указанных на рисунке.

- В качестве корневого моста используется коммутатор Z, имеющий наименьшее значение BID.
- В качестве корневых портов коммутаторов X и Y используется порт 1. Порт 1 на обоих коммутаторах обеспечивает маршрут с минимальной стоимостью к корневому мосту.
- В качестве выделенных портов используются порты 1 и 2 коммутатора Z. Все порты корневого моста являются выделенными. Порт 2 коммутатора X — выделенный порт сегмента между коммутаторами X и Y. Поскольку коммутаторы X и Y обеспечивают одинаковую стоимость маршрута к корневому мосту, выделенный порт выбирается на коммутаторе X, так как его значение BID ниже, чем у коммутатора Y.
- Порт 2 коммутатора Y является невыделенным портом сегмента и находится в блокирующем режиме.
- Все выделенные и корневые порты находятся в режиме пересылки.

Пример: стоимость маршрута протокола "spanning tree"

Стоимость маршрута протокола "spanning tree" — это совокупная стоимость маршрута, которая определяется полосой пропускания всех каналов, участвующих в этом маршруте. На рисунке приводится стоимость для некоторых каналов, прописанная в спецификации 802.1D. Спецификация 802.1D была изменена, в старой версии стоимость рассчитывалась по полосе пропускания 1 000 Мбит/с. В новой версии используется нелинейная шкала, позволяющая учитывать высокопроизводительные интерфейсы.

Примечание Большинство коммутаторов Cisco Catalyst используют новую версию спецификации для расчета стоимости. Основная особенность стоимости STP, которую следует иметь в виду, — чем ниже стоимость, тем лучше.



При изменении топологии из-за отказа моста или канала протокола "spanning tree" перенастраивает топологию сети для сохранения соединений, переводя заблокированные порты режим пересылки.

Пример: повторный расчет "spanning tree"

В сценарии рисунке коммутатор Z (корневой мост) отказывает и не посылает блок BPDU в коммутатор Y в течение периода max_age (значение по умолчанию — 20 секунд, что соответствует 10 пропущенным блокам BPDU), коммутатор Y обнаруживает отсутствие блока BPDU от корневого моста. Если таймер max_age коммутатора Y истекает до получения нового блока BPDU от коммутатора Z, выполняется повторный расчет протокола "spanning tree". Коммутатор Y переводит порт в блокирующем режиме (порт 2) в режим прослушивания, затем в режим обучения и наконец в режим пересылки.

По окончании этого процесса все порты коммутаторов и мостов переходят в режим пересылки или блокирующий режим, коммутатор X становится корневым мостом и начинает выполнять пересылку трафика между сегментами.

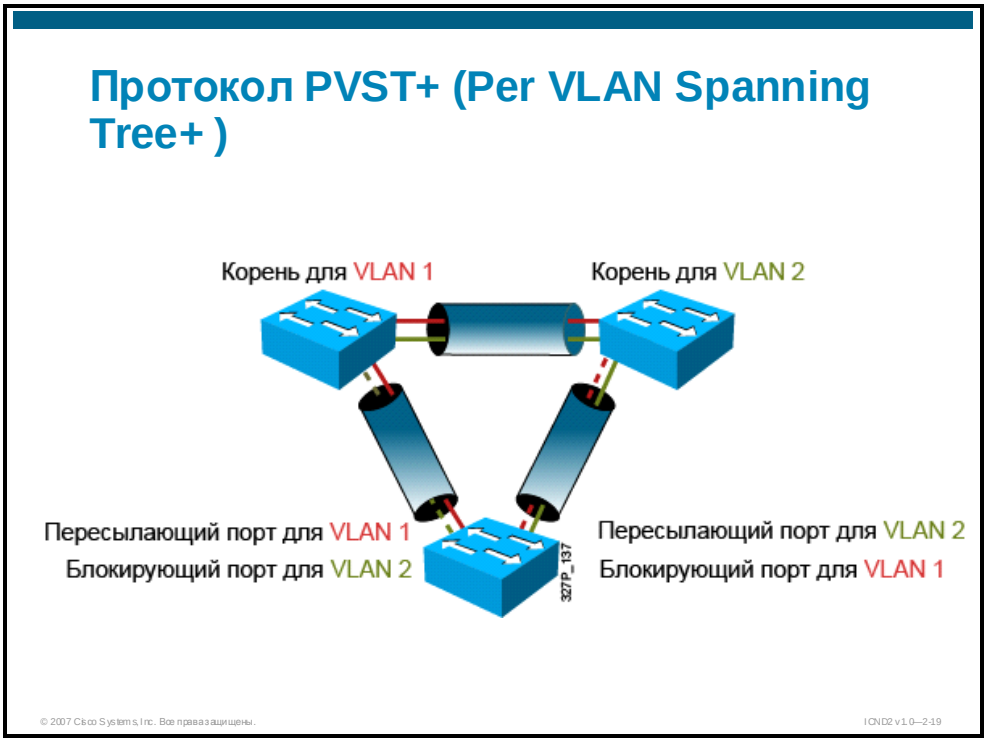
Конвергенция STP

Конвергенция STP — это состояние, в котором все порты коммутаторов и мостов находятся в режиме пересылки или блокирующем режиме. Конвергенция необходима для нормальной работы сети. Главная проблема коммутируемой и мостовой сети — время, необходимое для конвергенции при изменении топологии сети.

Быстрая конвергенция — желательная характеристика сети, так как она сокращает период времени, в течение которого порты коммутатора и моста находятся в переходных состояниях и не передают пользовательский трафик. Для протокола STP 802.1D стандартное время конвергенции составляет от 30 до 50.

Протокол PVST+ (Per VLAN Spanning Tree+)

В этом подразделе описывается принцип работы протокола PVST+ (Per VLAN Spanning Tree+).



Стандарт 802.1D определяет протокол Common Spanning Tree (CST), который разрешает только один экземпляр протокола "spanning tree" на коммутируемую сеть, независимо от количества VLAN. В сети под управлением CST справедливы следующие утверждения:

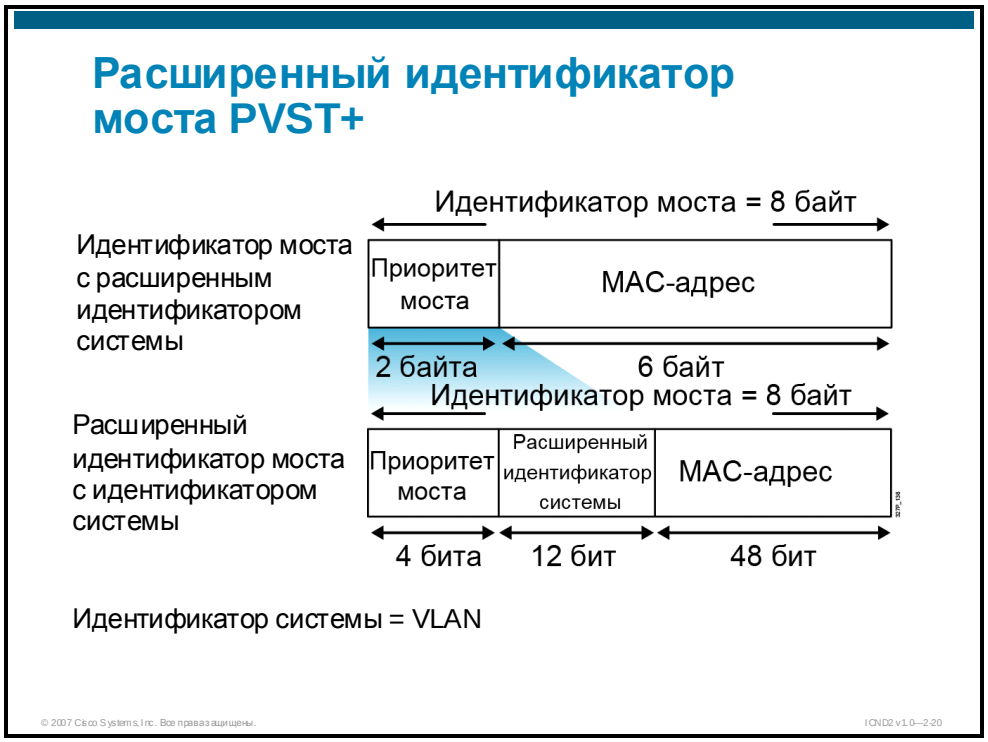
- выравнивание нагрузки невозможно, один восходящий канал должен блокировать все VLAN;
- потребление ресурсов ЦП невелико, рассчитывается только один экземпляр протокола "spanning tree".

Стандарт PVST+ определяет протокол "spanning tree", который поддерживает работу нескольких экземпляров протокола "spanning tree" в сети, по одному на каждую VLAN. В сети с несколькими экземплярами протокола "spanning tree" справедливы следующие утверждения:

- можно обеспечить оптимальное выравнивание нагрузки;
- поддержка одного экземпляра протокола "spanning tree" на каждую VLAN может привести к значительному потреблению ресурсов ЦП для всех коммутаторов в сети (в дополнение к потреблению полосы пропускания в связи с тем, что каждый экземпляр отправляет свои блоки BPDU).

Принцип работы PVST+

В среде Cisco PVST+ можно настроить параметры протокола "spanning tree" так, чтобы половина сетей VLAN выполняла пересылку на всех транковых каналах. Для того необходимо настроить один из коммутаторов так, чтобы он был выбран корневым в половине VLAN. Другой коммутатор должен быть выбран в качестве корневого коммутатора для другой половины VLAN. Разные корневые коммутаторы STP для разных VLAN позволяют добиться более эффективного резервирования.



Для функционирования протокола "spanning tree" каждый коммутатор должен иметь уникальное значение BID. В оригинальном стандарте 802.1D идентификатор BID состоял из приоритета моста и MAC-адреса коммутатора, и все VLAN были представлены общим протоколом "spanning tree". Поскольку протокол PVST+ требует отдельного экземпляра протокола "spanning tree" для каждой VLAN, поле BID должно включать данные об идентификаторе VLAN (VID). Для этого часть поля приоритета используется для передачи расширенного идентификатора системы, включающего VID.

Для поддержки расширенного идентификатора системы оригинальное 16-битное поле приоритета моста 802.1D разделяется на два. Измененный BID состоит из следующих компонентов.

- **Приоритет моста.** 4-битное поле все еще используется для данных о приоритете моста. Из-за ограниченного числа битов приоритет передается дискретными значениями с шагом 4096, а не с шагом 1, который использовался бы в полном 16-битном поле. Приоритет по умолчанию, согласно стандарту IEEE 802.1D — 32 768 (среднее значение).
- **Расширенный идентификатор системы.** 12-битное поле, используемое для передачи VID для PVST+ (в этом случае).

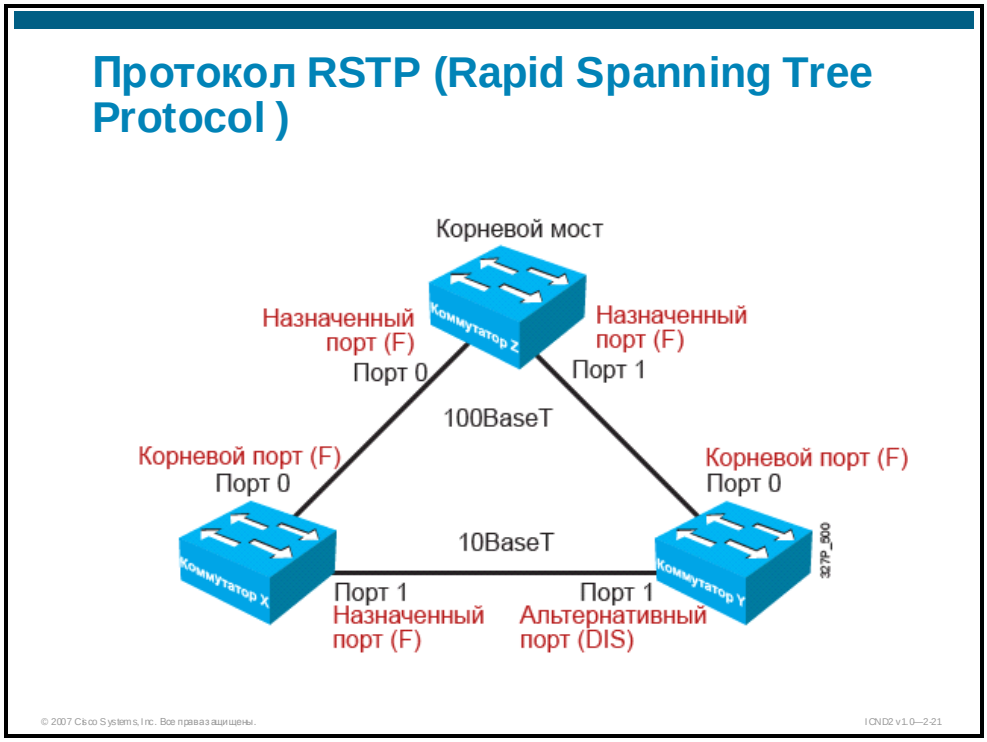
- **MAC Address.** 6-байтное поле с MAC-адресом одного коммутатора.

Благодаря MAC-адресу идентификатор BID всегда будет уникален. Если перед приоритетом и расширенным идентификатором системы записан MAC-адрес, каждая VLAN коммутатора представляется уникальным идентификатором BID.

Если приоритет не задан, коммутаторы будут использовать одинаковое значение приоритета по умолчанию и выбор корневого моста для каждой VLAN будет выполняться на основе MAC-адреса. Этот метод выбора корневого моста является случайным, поэтому рекомендуется назначить более низкий приоритет коммутатору, который должен служить корневым мостом.

Протокол RSTP (Rapid Spanning Tree Protocol)

В этом подразделе описывается функционирование протокола RSTP (Rapid Spanning Tree Protocol).



Протокол RSTP, определенный стандартом IEEE 802.1w, заменяет протокол STP, определенный в стандарте 802.1D, но остается совместимым с STP. RSTP следует рассматривать как эволюцию, а не революцию стандарта 802.1D. В целом терминология 802.1D не меняется. Большинство параметров остаются прежними, поэтому пользователи, знакомые с 802.1D, смогут без проблем настроить новый протокол.

RSTP значительно уменьшает время повторной конвергенции активной топологии при изменении физической топологии или параметров ее конфигурации. RSTP определяет дополнительные роли портов (альтернативный и резервный) и использует следующие режимы портов: режим отбрасывания, режим обучения и режим пересылки.

RSTP выбирает один коммутатор корневым мостом активной топологии протокола "spanning tree" и назначает роли отдельным портам коммутатора, в зависимости от того, входят ли они в активную топологию.

RSTP обеспечивает быстрое восстановление подключение после отказа коммутатора, порта коммутатора или ЛВС. Новые корневой порт и выделенный порт на другой стороне моста переходят в режим пересылки в результате развернутого процесса согласования подключения. RSTP разрешает настройку портов коммутатора, что позволяет переводить порты в режим пересылки сразу после повторной инициализации коммутатора.

Протокол PVRST+ (Per VLAN Rapid Spanning Tree Plus)

Стандарт RSTP (802.1w) использует общий протокол "spanning tree", что подразумевает использование одного экземпляра протокола "spanning tree" на сеть, независимо от количества VLAN. Стандарт PVRST+ определяет протокол "spanning tree", который позволяет использовать отдельный экземпляр RSTP для каждой VLAN.

Протокол MSTP (Multiple Spanning Tree Protocol)

Протокол MSTP изначально был определен в стандарте IEEE 802.1s, а затем добавлен в стандарт IEEE 802.1Q-2003. Он представляет собой протокол "spanning tree" с несколькими экземплярами "spanning tree" на сеть. Но в отличие от протокола PVRST+, который подразумевает использование одного RSTP на VLAN, MSTP уменьшает нагрузку на коммутаторы благодаря использованию одного экземпляра протокола "spanning tree" для нескольких VLAN.

Роли портов RSTP

RSTP определяет следующие роли портов.

- **Корневой.** Порт в режиме пересылки, выбранный для топологии "spanning tree".
- **Выделенный.** Порт в режиме пересылки, выбирается для каждого сегмента коммутируемой ЛВС.
- **Альтернативный.** Альтернативный маршрут к корневому мосту, отличный от маршрута корневого порта.
- **Резервный.** Резервный маршрут, который предлагает резервное (но менее предпочтительное) подключение к сегменту, к которому уже подключен другой порт коммутатора. Резервные порты могут существовать только если два порта объединены в возвратную петлю с помощью канала типа "точка-точка" или моста с двумя или более подключениями к общему сегменту ЛВС.
- **Отключен.** Порт, не имеющий роли в "spanning tree".

Роли "Корневой" и "Выделенный" включают порт в активную топологию. Роли "Альтернативный" и "Резервный" исключают порт из активной топологии.

Примечание Версия стандарта 802.1D от Cisco включает несколько функций 802.1w. Например, версия стандарта 802.1D от Cisco определяет альтернативный корневой порт, если он существует.

Режимы портов RSTP

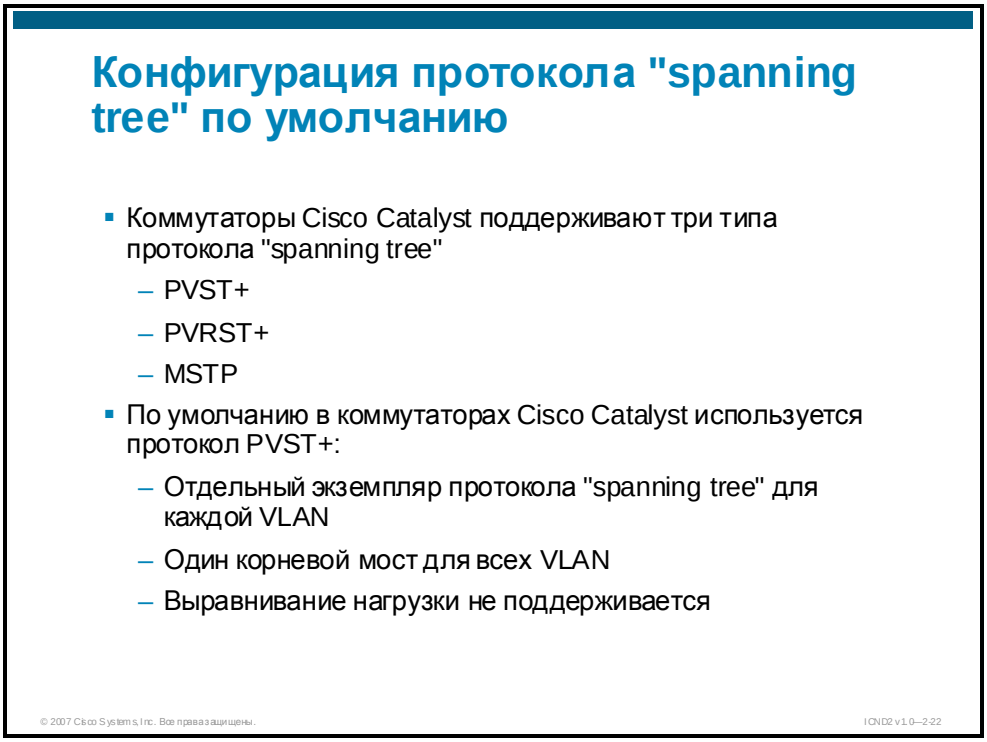
Режим порта контролирует процессы пересылки и обучения и предоставляет значения параметров для отбрасывания, обучения и пересылки. В таблице ниже приводится сравнение режимов портов для STP и RSTP.

Рабочее состояние	Режим порта STP	Режим порта RSTP	Порт входит в активную топологию
Включен	Блокирующий режим	Режим отбрасывания	Нет
Включен	Режим прослушивания	Режим отбрасывания	Нет
Включен	Режим обучения	Режим обучения	Да
Включен	Режим пересылки	Режим пересылки	Да
Отключен	Отключен	Режим отбрасывания	Нет

В стабильной топологии RSTP обеспечивает переход всех корневых и выделенных портов в режим пересылки, в то время как альтернативные и резервные порты находятся в режиме отбрасывания.

Настройка RSTP

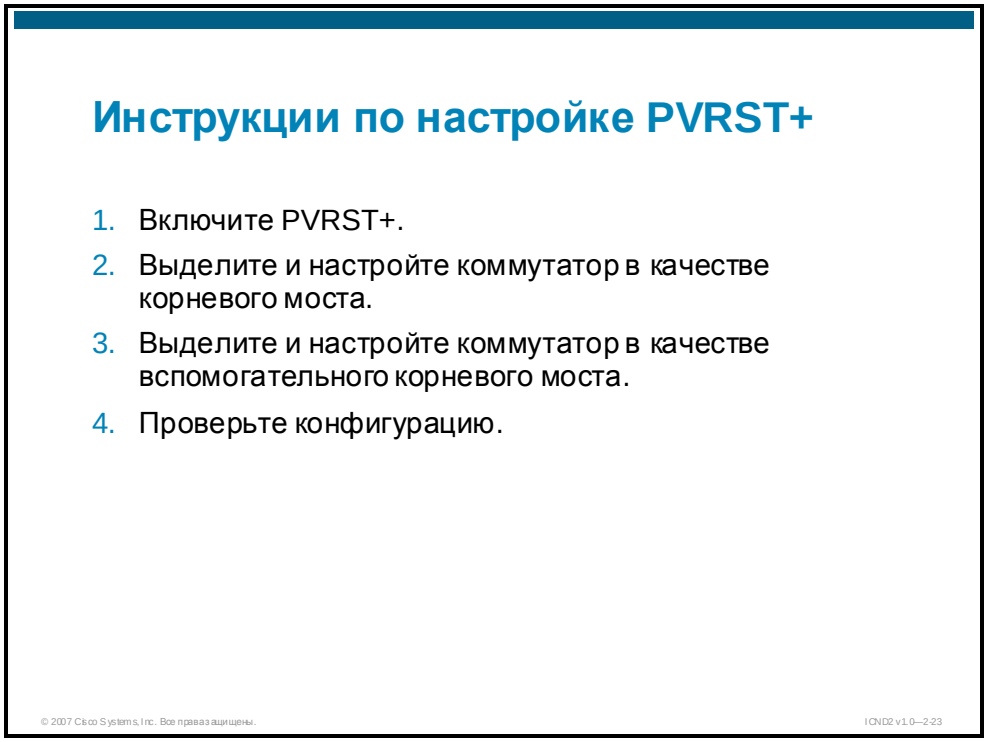
В этом разделе описывается настройка RSTP, в том числе настройка корневого коммутатора и резервного корневого коммутатора.



Настройка протокола "spanning tree"

Коммутаторы Cisco Catalyst поддерживают три типа протоколов "spanning tree": PVST+, PVRST+ и MSTP.

- **PVST+.** Основывается на стандарте 802.1D и включает проприетарные расширения Cisco, такие как BackboneFast, UplinkFast, and PortFast.
- **PVRST+.** Основывается на стандарте 802.1w и предлагает более быструю конвергенцию, чем 802.1D
- **MSTP (802.1s).** Объединяет лучшие характеристики PVST+ и стандартов IEEE.



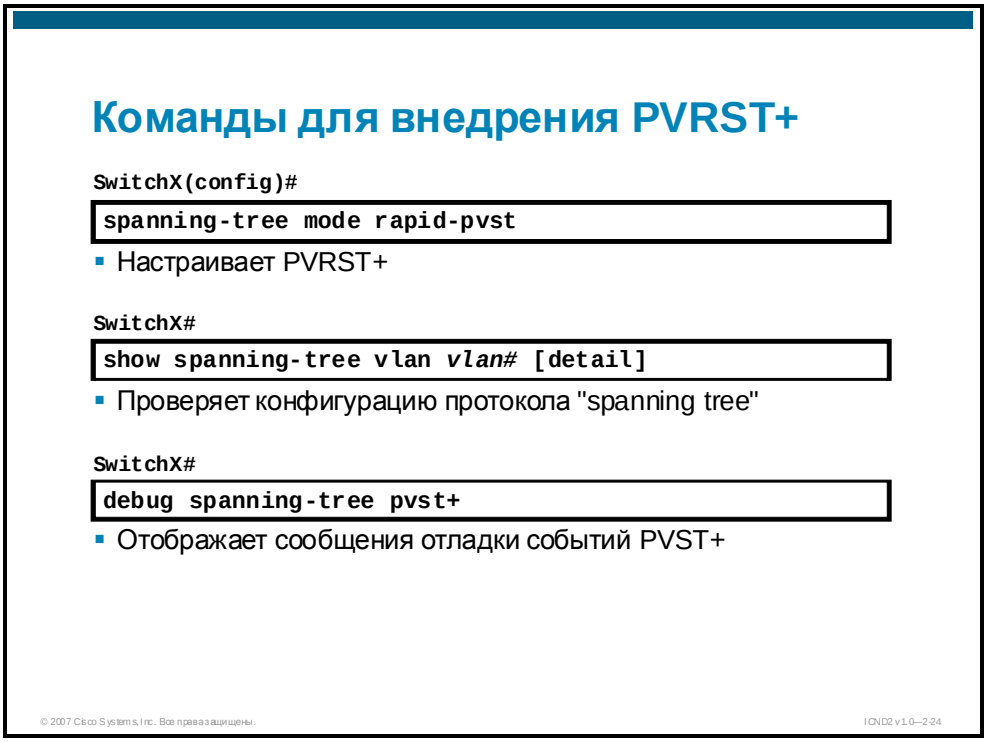
Для внедрения PVRST+ выполните следующие действия.

Действие 1 Включите PVRST+.

Действие 2 Выделите и настройте коммутатор в качестве корневого моста.

Действие 3 Выделите и настройте коммутатор в качестве вспомогательного (резервного) корневого моста.

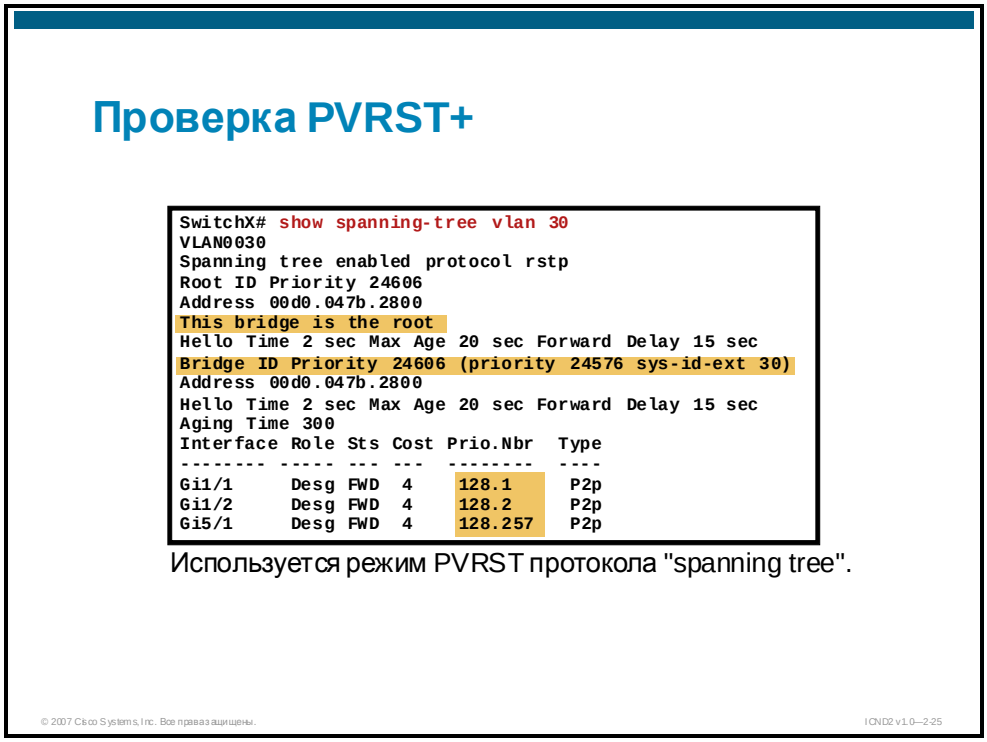
Действие 4 Проверьте конфигурацию.



В таблице ниже описываются команды, которые используются для включения и проверки протокола PVRST+.

Команды PVRST+

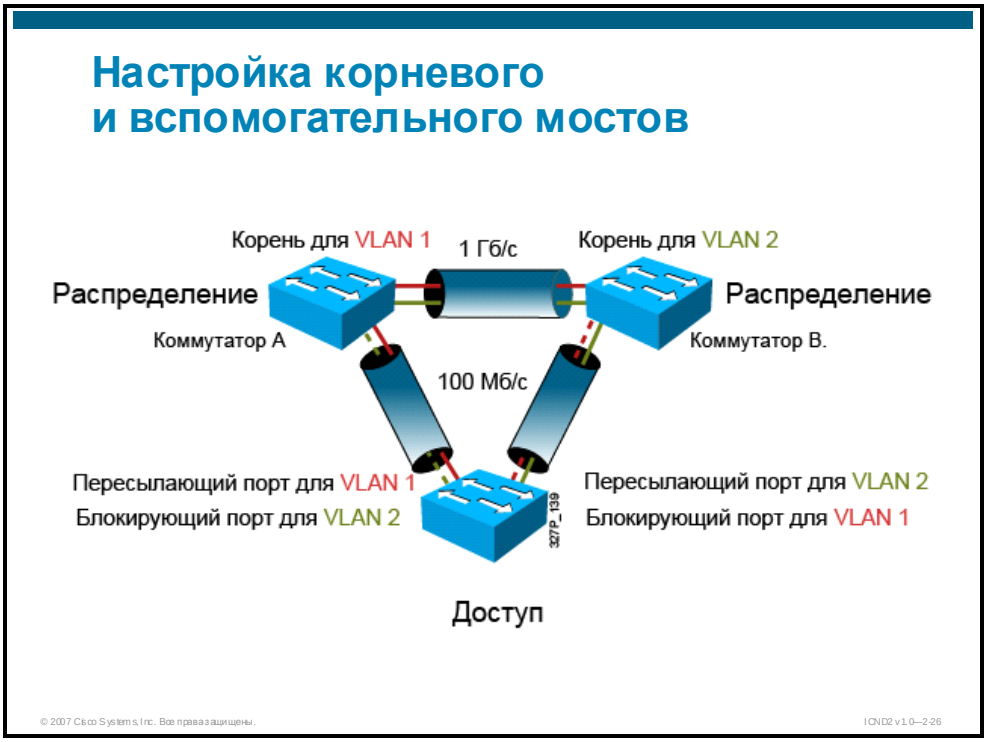
Команда	Описание
SwitchX(config)#**spanning-tree mode rapid-pvst**	Переводит протокол "spanning tree" в режим PVRST+.
SwitchX#**show spanning-tree vlan** *vlan-number* [**detail**]	Выводит сведения о протоколе "spanning tree" с точки зрения VLAN, а не по экземплярам.
SwitchX#**debug spanning-tree pvst+**	Выполняет отладку событий PVST+.
SwitchX#**debug spanning-tree switch state**	Выполняет отладку изменений портов. Примечание. Как и все команды отладки, эта команда может повлиять на производительность сети.



В этом примере строка "Spanning tree enabled protocol rstp" означает, что на коммутаторе X работает PVRST+, версия RSTP от Cisco.

Коммутатор X является корневым мостом для VLAN 30. Его приоритет (24606) является производной от суммы назначенного приоритета 24576 и идентификатора VLAN 30. MAC-адрес коммутатора X (00d0.047b.2800) добавляется к приоритету (24606), в результате чего формируется идентификатор моста (BID).

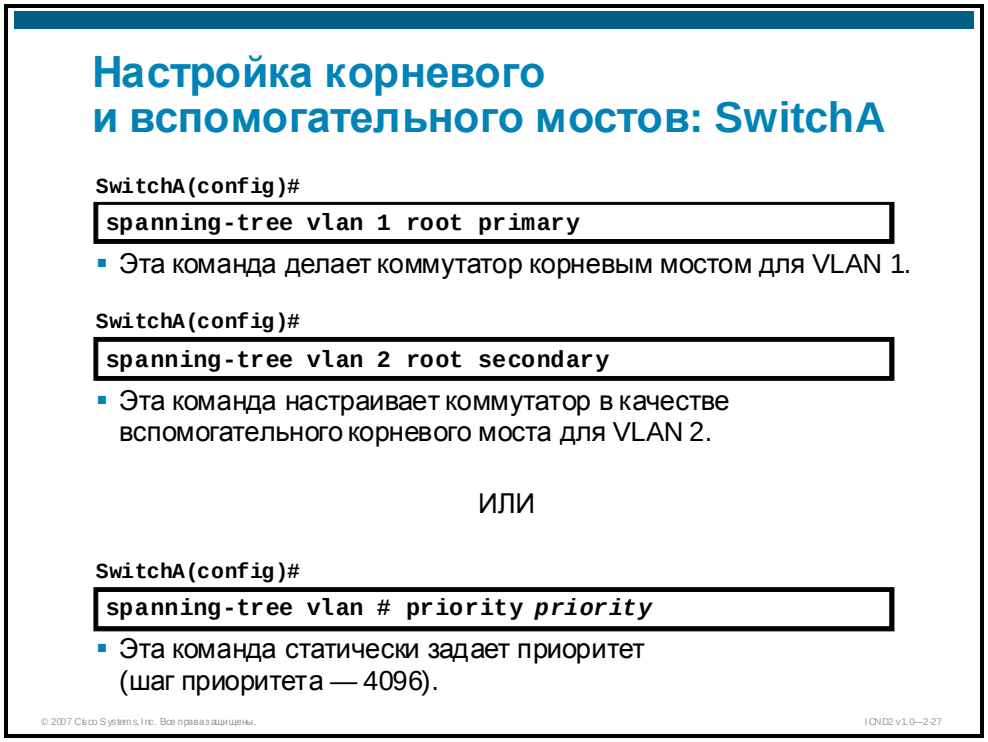
Так как коммутатор X является корневым мостом VLAN 30, всего его интерфейсы являются выделенными портами и находятся в режиме пересылки.



Если все коммутаторы в сети настроены с параметрами протокола "spanning tree" по умолчанию, коммутатор с наименьшим MAC-адресом становится корневым мостом. Однако корневой мост по умолчанию может не быть идеальным корневым мостом в связи с моделью трафика, количеством интерфейсов в режиме пересылки или типами каналов.

Перед настройкой STP выберите коммутатор, который будет корневым мостом протокола "spanning tree". Этот коммутатор не обязательно должен являться самым производительным коммутатором, но он должен быть самым централизованном коммутатором в сети. Все потоки данных в сети будут проходить через этот коммутатор. Коммутаторы уровня распределения часто служат корневыми мостами протокола "spanning tree", так как они, как правило, не имеют подключения к конечным станциям. Кроме того, перемещения и изменения в сети скорее всего не повлияют на эти коммутаторы.

Повышая приоритет (уменьшая численное значение) предпочтительного коммутатора, чтобы сделать его корневым мостом, вы заставляете протокол "spanning tree" выполнить повторный расчет в соответствии с новой топологией, в которой предпочтительный коммутатор является корневым мостом.

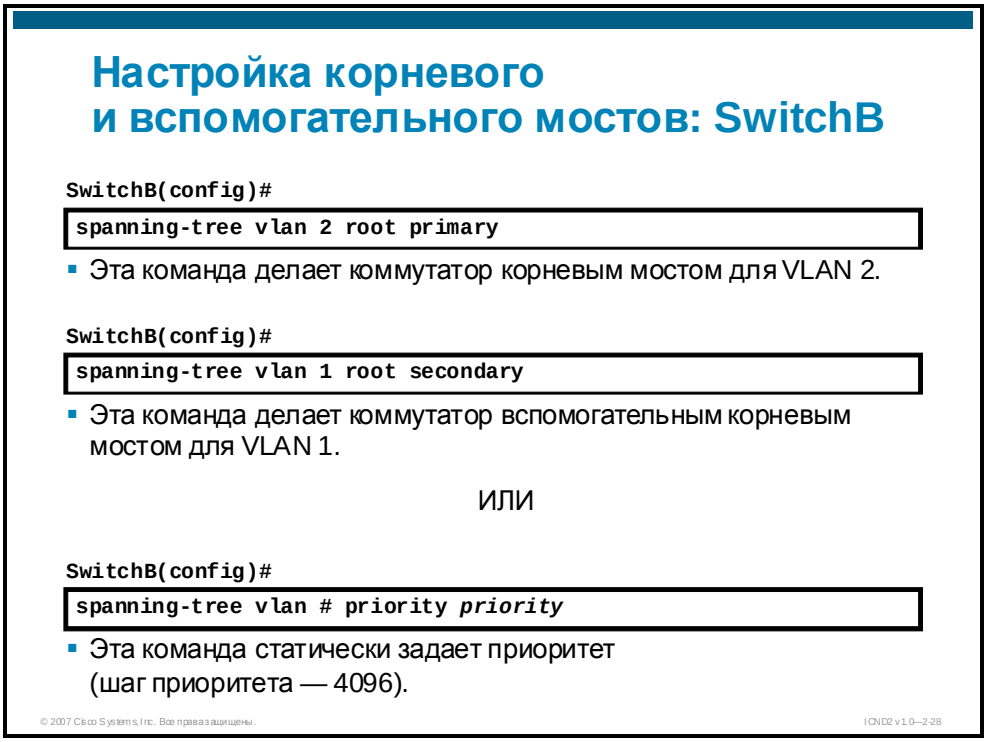


Коммутатор с наименьшим значением BID становится корневым мостом протокола "spanning tree" для сети VLAN. Чтобы определить, какой коммутатор станет корневым мостом, можно использовать команды конфигурации.

Коммутатор Cisco Catalyst под управлением PVST+ или PVRST+ поддерживает экземпляр протокола "spanning tree" для каждой активной VLAN, настроенной на коммутаторе. Каждому экземпляру присваивается уникальный идентификатор BID. В каждой сети VLAN коммутатор с наименьшим значением BID становится корневым мостом. Значение BID меняется при каждом изменении приоритета моста. Это изменение приводит к повторному расчету приоритета корневого моста для VLAN.

Чтобы настроить коммутатор в качестве корневого моста для указанной VLAN, используйте команду **spanning-tree vlan** *идентификатор vlan* **root primary**. При вводе этой команды коммутатор проверяет приоритет корневого моста для указанной VLAN. Из-за расширенного идентификатора системы на коммутаторе задается значение приоритета 24 576 для указанной VLAN, если это значение делает коммутатор корневым мостом этой VLAN. Если в указанной VLAN есть другой коммутатор с приоритетом ниже 24 576, коммутатор, на котором вы настраиваете команду **spanning-tree vlan** *идентификатор vlan-ID* **root primary** устанавливает свой приоритет для указанной VLAN на 4096 ниже самого низкого значения приоритета.

Внимание Команды протокола "spanning tree" вступают в силу немедленно, поэтому поток трафика прерывается при переконфигурации.

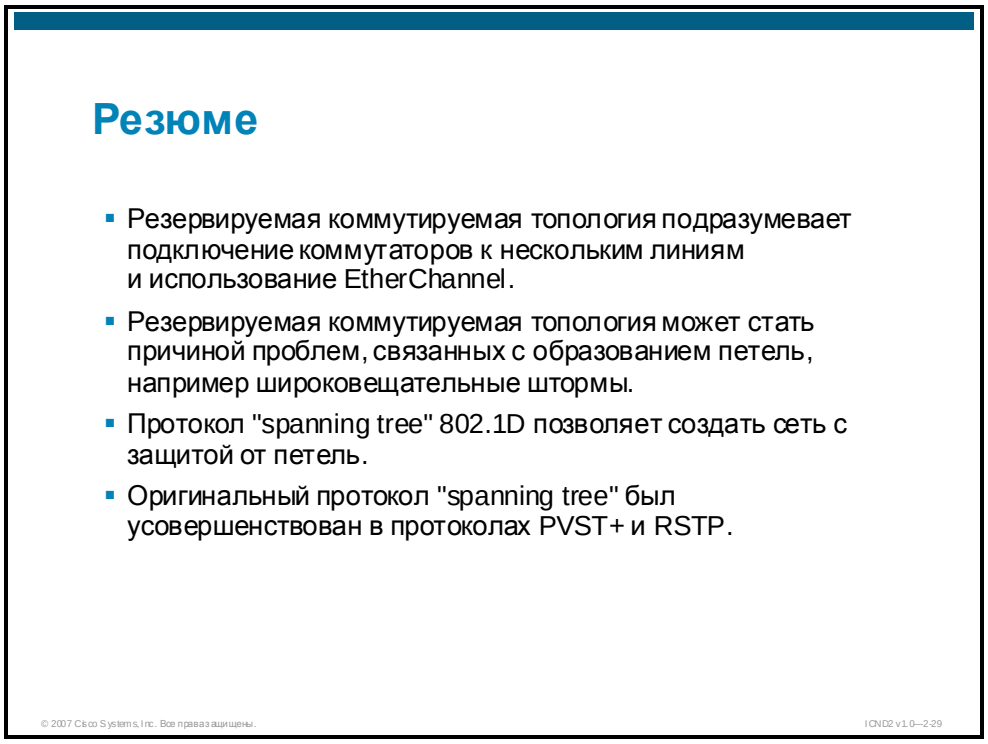


Вспомогательный корневой мост — это коммутатор, который становится корневым мостом VLAN при отказе основного корневого моста. Чтобы настроить коммутатор в качестве вспомогательного корневого моста VLAN, используйте команду **spanning-tree vlan** *идентификатор vlan* **root secondary**.

При вводе этой команды приоритет коммутатора меняется со значения по умолчанию 32 768 на 28 672. Если другие мосты VLAN сохранят приоритет STP по умолчанию, этот коммутатор становится корневым мостом при отказе основного корневого моста. Эту команду можно выполнить на нескольких коммутаторах, чтобы настроить несколько резервных корневых мостов.

Резюме

В этом разделе приводится резюме основных вопросов, рассмотренных в занятии.



Занятие 3

Маршрутизация между VLAN

Обзор

Маршрутизация — это процесс определения места назначения для отправки пакетов данных, направленных за пределы локальной сети. Маршрутизаторы собирают и хранят данные маршрутизации, чтобы обеспечивать прием и передачу пакетов данных. Чтобы трафик мог передаваться из одной VLAN в другую необходим процесс третьего уровня.

В этом занятии описывается принцип работы маршрутизации между VLAN с использованием конфигурации Router-on-a-stick.

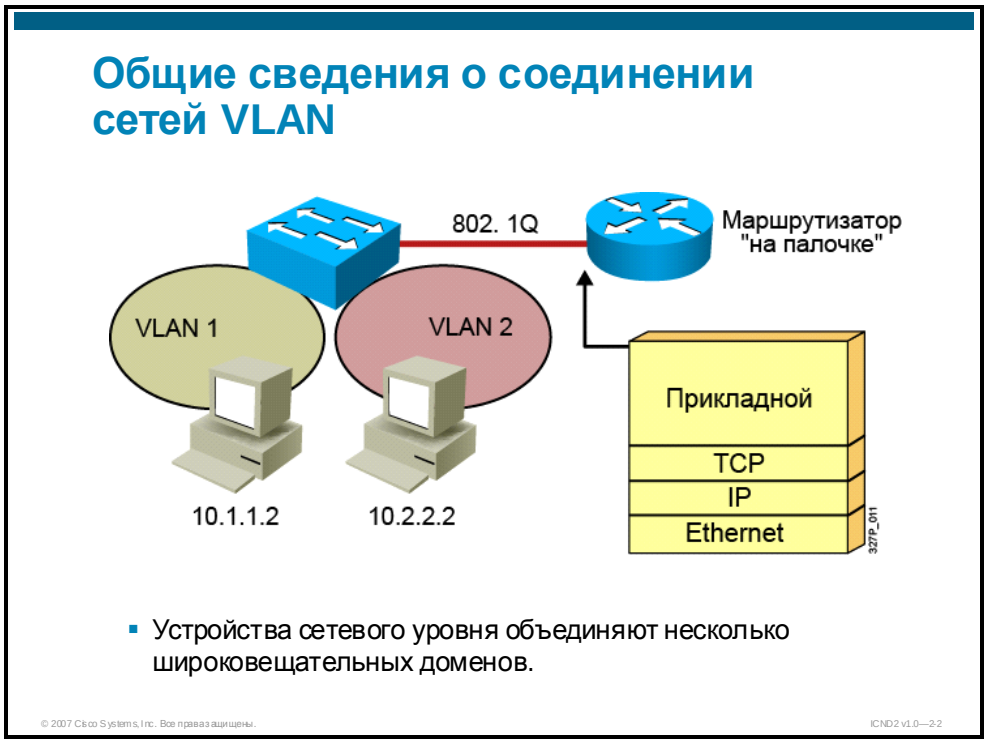
Задачи

По окончании этого занятия вы сможете описывать применение и настройку маршрутизации между VLAN в маршрутизируемой сети среднего размера. Это значит, что вы сможете выполнить следующие задачи:

- описывать назначение субинтерфейсов для маршрутизации между VLAN;
- настраивать маршрутизацию между VLAN на базе 802.1Q и внешнего маршрутизатора.

Общие сведения о маршрутизации между VLAN

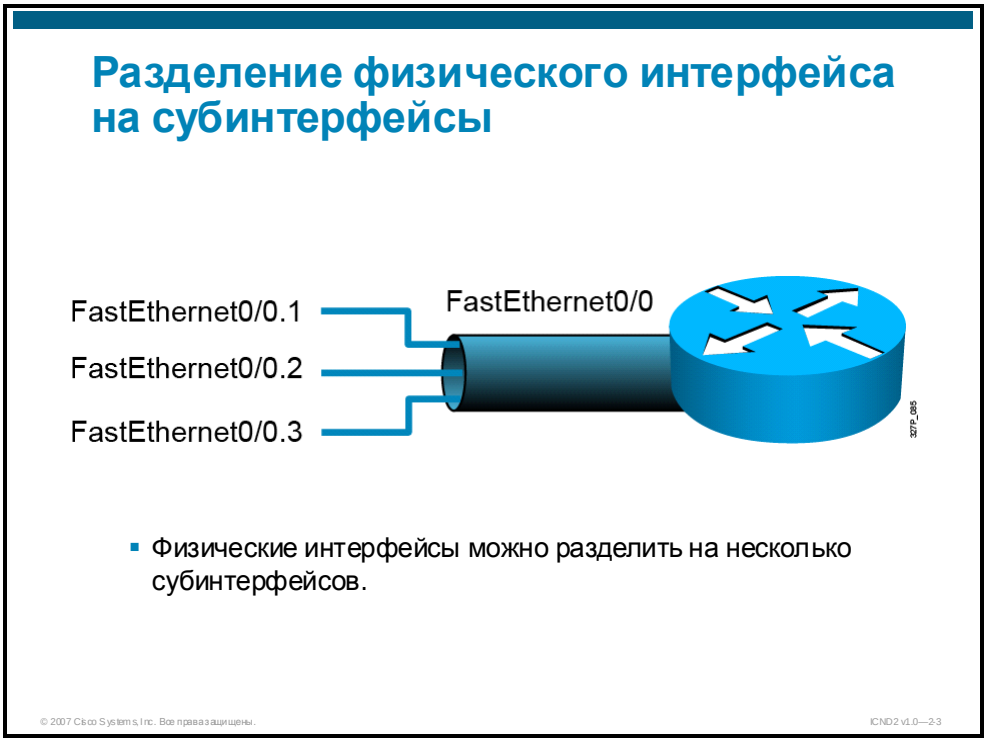
В этом разделе описываются основы маршрутизации между VLAN.



Связь между VLAN реализуется между широковещательными доменами через устройство третьего уровня. В среде VLAN кадры коммутируются только между портами в одном широковещательном домене. VLAN выполняет разбиение сети и разделение трафика на втором уровне. Связь между VLAN невозможна без устройства третьего уровня, например маршрутизатора. Для активации транкового режима на субинтерфейсе маршрутизатора используется протокол IEEE 802.1Q.

Пример: Router-on-a-stick

На рисунке изображен маршрутизатор, подключенный к центральному коммутатору. Конфигурация между маршрутизатором и центральным коммутатором иногда называется Router-on-a-stick. Маршрутизатор может получать пакеты одной VLAN и пересылать их в другую VLAN. Для маршрутизации между VLAN маршрутизатор должен знать пути ко всем соединяемым VLAN. Между маршрутизатором и каждой VLAN необходимо создать отдельные подключения и активировать транковый режим 802.1Q на этих подключениях. Маршрутизатору уже известны сети с прямым подключением. Он должен получить данные о маршрутах к сетям без прямого подключения.



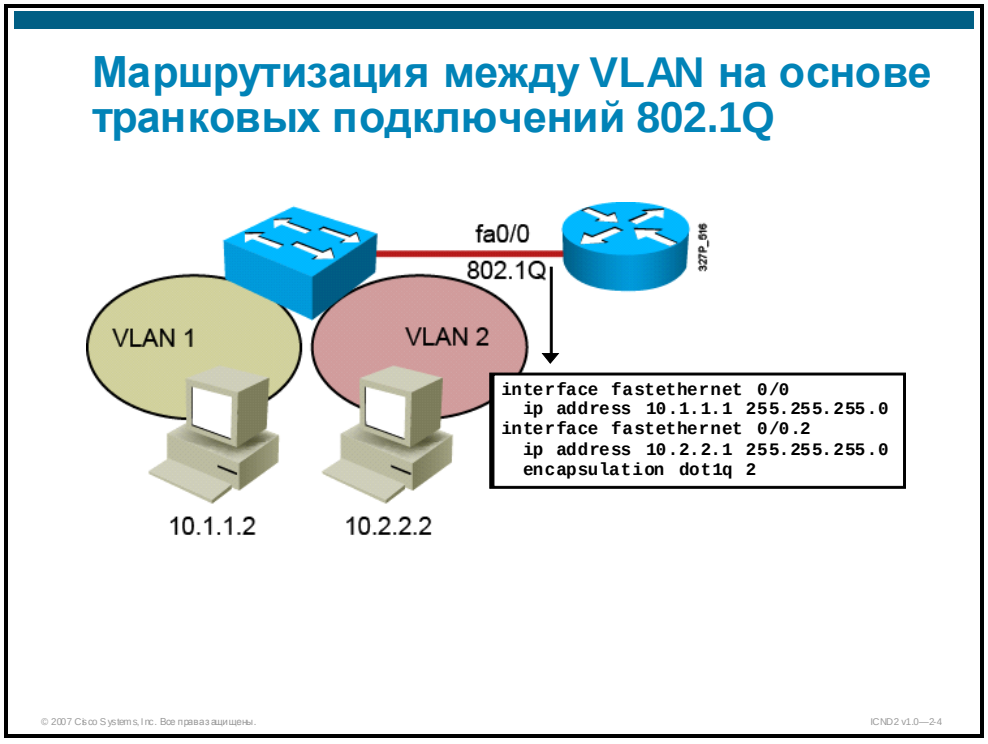
Для поддержки транкового режима 802.1Q необходимо разделить физический интерфейс Fast Ethernet на несколько логических адресуемых интерфейсов, по одному на каждую VLAN. Такие логические интерфейсы называются субинтерфейсами. Без этого разделения пришлось бы назначать отдельный физический интерфейс каждой VLAN.

Пример: субинтерфейсы

На этом рисунке интерфейс FastEthernet0/0 разделен на несколько субинтерфейсов: FastEthernet0/0.1, FastEthernet0/0.2 и FastEthernet0/0.3.

Настройка маршрутизации между VLAN

В этом разделе приводятся примеры конфигурации маршрутизации между VLAN на базе 802.1Q.



Пример: маршрутизация между VLAN на основе 802.1Q

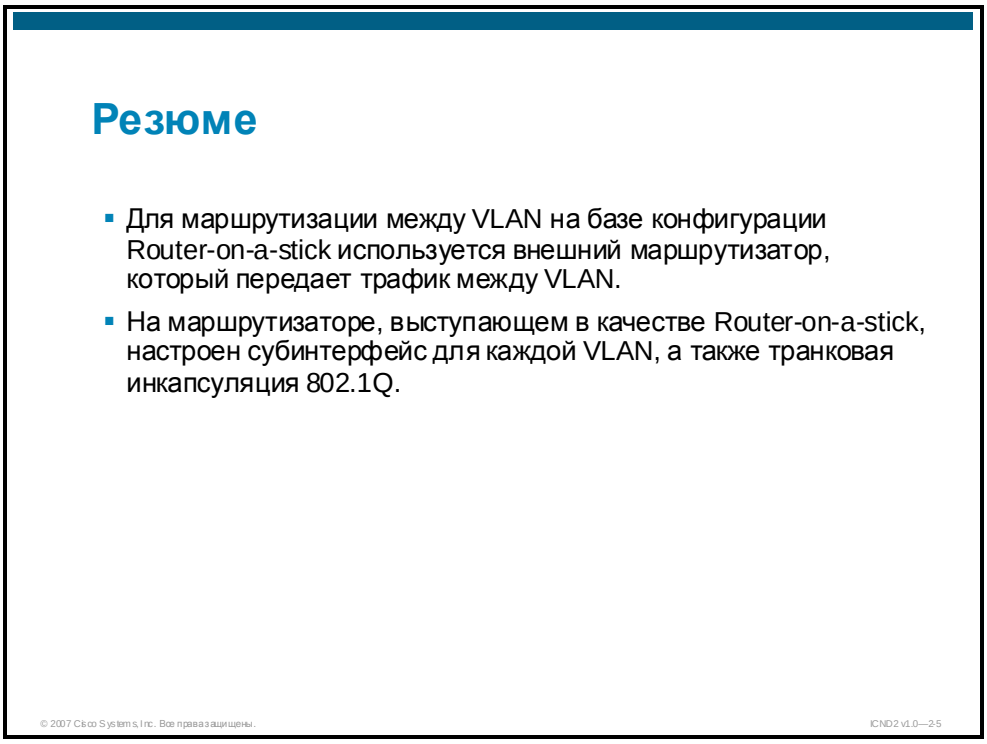
На этом рисунке интерфейс FastEthernet0/0 разделен на субинтерфейсы: FastEthernet0/0.1 и FastEthernet0/0.2. Каждый субинтерфейс представляет маршрутизатор в каждой VLAN, для которых выполняется маршрутизация.

Введите команду **encapsulation dot1q** *идентификатор vlan* (где *идентификатор vlan* — номер VLAN) на всех субинтерфейсах, чтобы включить транковый режим с инкапсуляцией 802.1Q. Совпадение номера субинтерфейса и номера dot1Q VLAN не обязательно. Однако управление значительно упростится, если эти два номера будут одинаковы.

Кадры стандартной VLAN в 802.1Q не имеют метки. Поэтому субинтерфейс стандартной VLAN настраивается с помощью команды **encapsulation dot1Q** *идентификатор vlan* **native**. Убедитесь, что номер VLAN, назначенный субинтерфейсу стандартной VLAN совпадает с номером стандартной VLAN коммутатора, к которому она подключена.

Резюме

В этом разделе приводится резюме основных вопросов, рассмотренных в занятии.



Занятие 4

Обеспечение безопасности расширенной сети

Обзор

Внутренние маршрутизаторы и коммутаторы организаций часто используют минимальные конфигурации безопасности, что делает их потенциальной целью для атак злоумышленников. Если атака инициирована на втором уровне с внутреннего устройства комплекса зданий, оставшаяся сеть может быть быстро взломана, причем злоумышленник часто остается необнаруженным.

В этом занятии рассматриваются функции безопасности, которые позволяют защитить коммутаторы и операции второго уровня.

Задачи

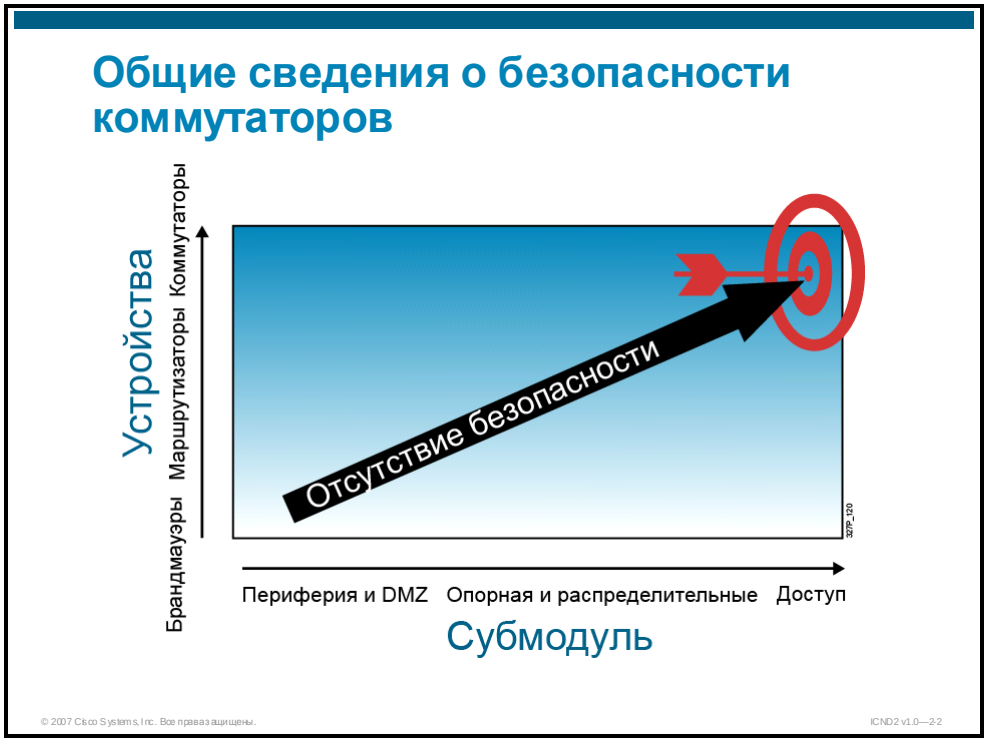
По окончании этого занятия вы сможете описывать ситуации, в которых используются функции безопасности второго уровня, и внедрять их в сети. Это значит, что вы сможете выполнить следующие задачи:

описывать требования расширенной сети к безопасности и характеристики политики безопасности организации;

описывать способы защиты коммутаторов, в том числе защиты доступа к коммутатору и протоколам коммутации, а также подавления атак, запущенных с коммутатора.

Общие сведения о проблемах безопасности коммутаторов

В этом разделе описываются требования к безопасности в расширенной сети.

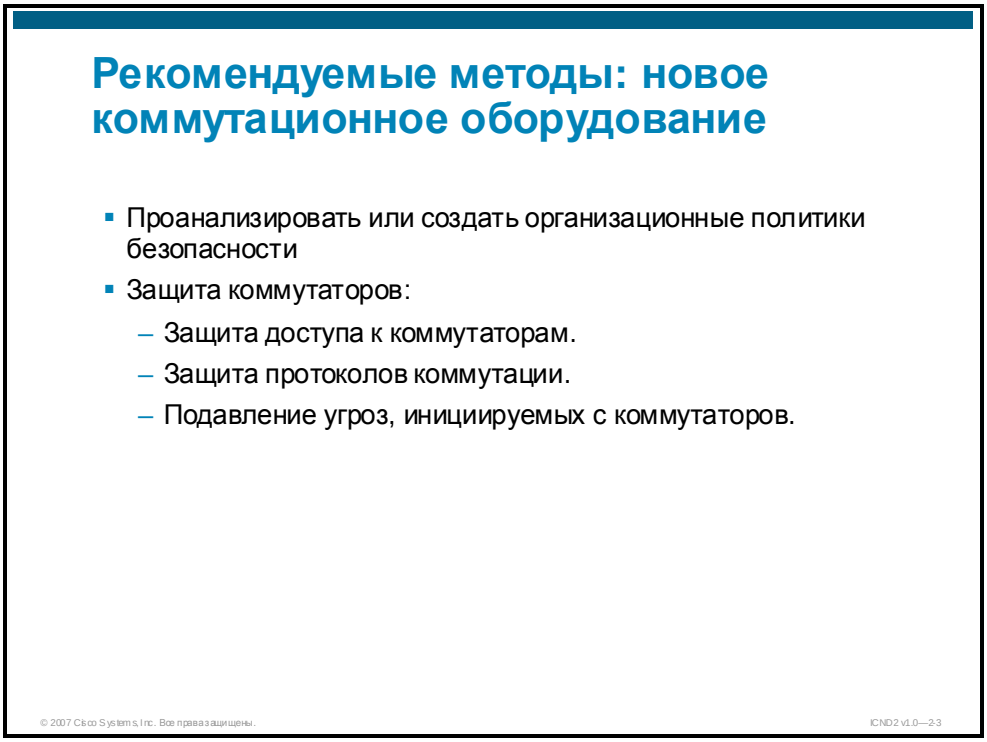


Отрасль уделяет значительное внимание защите от атак, направленных извне стен организации и использующие протоколы верхних уровней OSI. Сетевая безопасность часто сосредотачивается на периферийных маршрутизаторах и фильтрации пакетов на базе заголовков, портов, анализа пакетов с учетом состояния и других функций третьего и четвертого уровней. Этот подход охватывает уровни начиная с третьего, так как трафик попадает в сеть комплекса зданий из Интернета. Устройство доступа в комплексе зданий и каналы связи второго уровня не рассматриваются в большинстве дискуссий по безопасности.

Внутренние маршрутизаторы и коммутаторы организации предназначены для обеспечения связи за счет передачи трафика комплекса зданий. По умолчанию они пересылают весь трафик, если иное не задано в конфигурации. Цель таких устройств — обеспечение связи, поэтому их конфигурации безопасности зачастую минимальны и это делает устройства потенциальной целью для атак злоумышленников. Если атака инициирована на втором уровне с внутреннего устройства комплекса зданий, оставшаяся сеть может быть быстро взломана, причем злоумышленник часто остается необнаруженным.

Как и третий уровень, где меры безопасности традиционно применялись на устройствах внутри комплекса зданий, второй уровень требует мер безопасности для защиты от атак, основанных на обычных операциях коммутатора второго уровня. Для коммутаторов и маршрутизаторов доступно множество функций безопасности, однако, чтобы эти функции работали, их необходимо включить. Администратор должен создать политики и настроить функции для защиты от действий злоумышленников (процесс аналогичен

внедрению списков контроля доступа (ACL) для обеспечения безопасности на верхних уровнях), и в то же время поддерживать нормальную работу сети.



Риски сетевой безопасности включают нарушение конфиденциальности, кражу данных, персонацию и потерю целостности данных. Для уменьшения последствий небрежности пользователей и вредоносных действий необходимо принять базовые меры безопасности для всех сетей.

Рекомендуемые методы предполагают два базовых действия, которые необходимо выполнить при вводе нового оборудования в эксплуатацию:

Действие 1 проанализировать или создать организационные политики безопасности;

Действие 2 обеспечить безопасность коммутаторов, защитив доступ к коммутатору и протоколам коммутации и снизить риски, связанные с угрозами, инициированными с коммутатора.

Организационные политики безопасности

При определении уровня и типа безопасности для сети необходимо учесть политики организации. Вы должны найти компромисс между разумным уровнем сетевой безопасности и административными издержками, связанными со слишком строгими мерами безопасности.

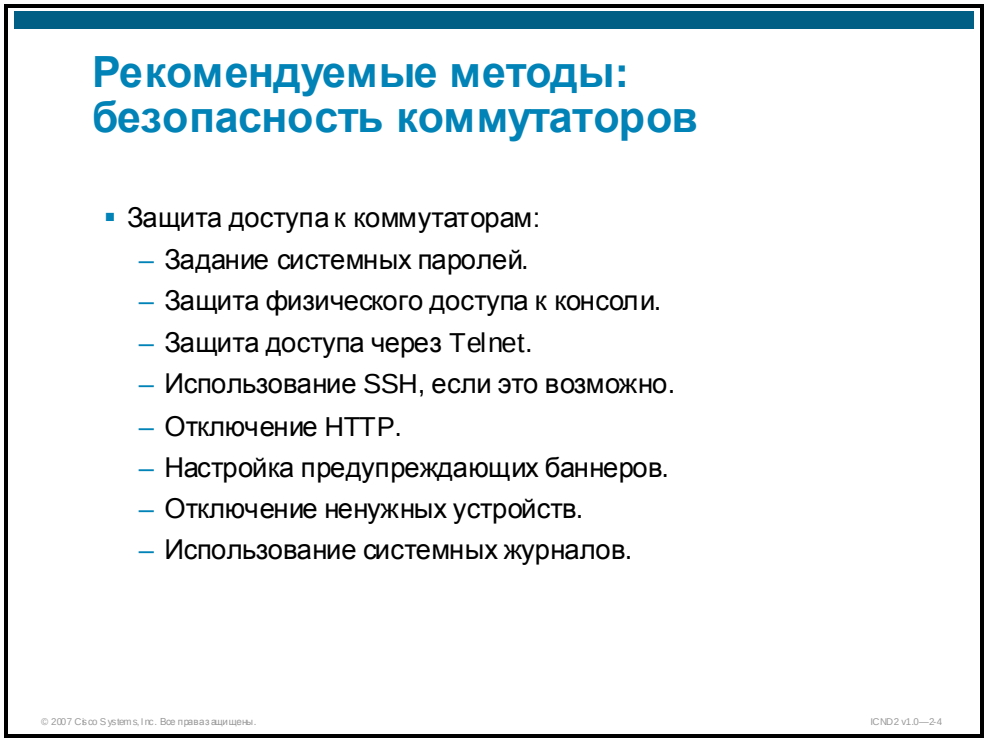
Качественная политика безопасности должна иметь следующие свойства.

- Поддержка процесса для ревизии существующей системы сетевой безопасности.
- Поддержка общей структуры безопасности, на базе которой будет внедряться сетевая безопасность.
- Определение запрещенных режимов работы с данными в электронном формате.

- Определение инструментов и процедур, необходимых для организации.
- Политика должна быть основана на консенсусе между лицами, принимающими решения, и должна включать обязанности пользователей и администраторов.
- Определение процесса обработки инцидентов сетевой безопасности.
- Создание плана внедрения безопасности, охватывающий все площадки предприятия, и приведение этого плана в действие.

Обеспечение безопасности коммутаторов

В этом разделе описываются действия, которые необходимо предпринять, чтобы обеспечить безопасность коммутаторов.



Для защиты доступа к коммутаторам рекомендуются следующие методы.

- **Задание системных паролей.** Используйте команду **enable secret**, чтобы задать пароль доступа к привилегированному режиму системы Cisco IOS. Поскольку команда **enable secret** просто внедряет хэш Message Digest 5 (MD5) для настроенного пароля, этот пароль может быть уязвим к атакам, основанным на словарях. Поэтому используйте стандартные методы выбора пароля.

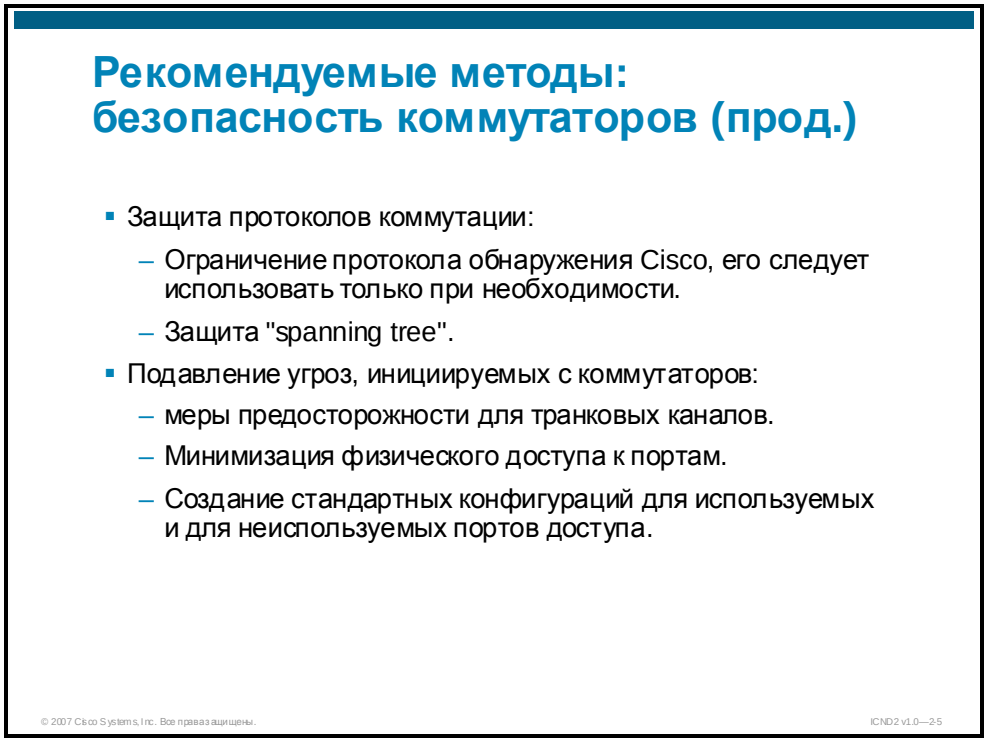
  Используйте пароли, включающие цифры и буквы, а также специальные символы. Например, используйте "$pecia1" вместо "specials", заменяя "s" на "$" и "l" на "1" (единицу).

- **Безопасный доступ к консоли.** Доступ к консоли требует хотя бы минимальной безопасности на логическом и физическом уровнях. Лицо, которое получает доступ системе через консоль, может восстановить или сбросить системный пароль, что позволит ему обойти другие меры безопасности, внедренные в системе. Поэтому защита физического доступа к консоли абсолютно необходима.

- **Безопасный доступ к линиям VTY.** Ниже приведен минимальный набор рекомендуемых действий по защите доступа через Telnet:
  - применение базового входящего списка контроля доступа ко всем линиям VTY;
  - задание пароля для всех настроенных линий VTY;
  - для удаленного доступа к устройству используйте протокол SSH вместо протокола Telnet, если установленная версия ПО Cisco IOS позволяет это сделать.
- **Использование SSH.** Протокол и приложение SSH обеспечивают безопасное удаленное подключение к маршрутизатору. Существует две версии SSH: SSH 1 (SSHv1) и SSH 2 (SSHv2). В ПО Cisco IOS используется протокол SSHv1. Он шифрует весь трафик, включая пароли, который передается между удаленной консолью и сетевым маршрутизатором во время сеанса Telnet. Поскольку SSH не отправляет данные в виде незашифрованного текста, администраторы сети могут работать в удаленных сеансах, недоступных взгляду случайного наблюдателя. SSH-сервер ПО Cisco IOS работает с общедоступными и коммерческими SSH-клиентами.
- **Отключение встроенного HTTP-демона, если он не используется.** ПО Cisco IOS включает интегрированный HTTP-сервер для управления, мы настоятельно рекомендуем отключить его для снижения общей уязвимости сети. Если вам необходим доступ к коммутатору через HTTP, используйте список контроля доступа, чтобы разрешить доступ только из доверенных подсетей.
- **Настройка предупреждающих баннеров.** С точки зрения юриспруденции и администрирования, настройка предупреждающего баннера, который будет отображаться перед входом в систему, является удобным и эффективным способом укрепления политик безопасности и общего пользования. Четко обозначив политики принадлежности, использования, доступа и защиты перед входом, вы создадите хорошую основу для последующего судебного преследования.
- **Отключение ненужных устройств.** По умолчанию устройства Cisco используют несколько TCP- и UDP-серверов для управления и интеграции в существующие среды. В большинстве сред эти службы не требуются и их отключение значительно уменьшит уязвимость системы безопасности. Команды, которые используются для отключения редко используемых служб:

```
no service tcp-small-servers
no service udp-small-servers
no service finger
no service config
```

- **Настройка базового ведения журналов.** Чтобы упростить поиск и устранение проблем, а также расследование нарушений системы безопасности, отслеживайте данные коммутирующей подсистемы, полученные от сервера ведения журнала. Вывод можно просмотреть в системном буфере ведения журналов. Чтобы повысить полезность системных журналов, увеличьте размер буфера по умолчанию.



Защита протоколов коммутации

Для защиты доступа к протоколам маршрутизации рекомендуются следующие методы.

- **Протокол обнаружения Cisco.** Протокол обнаружения Cisco не раскрывает данных безопасности, однако злоумышленник может воспользоваться информацией протокола для зондирования, что позволит ему получить доступ к информации об устройстве и IP-адресе устройства и использовать их для других атак. Для обеспечения безопасности протокола обнаружения Cisco следуйте следующим инструкциям.
  - Если протокол обнаружения Cisco не нужен или устройство находится в небезопасной среде, глобально отключите протокол обнаружения Cisco на устройстве.
  - Если протокол обнаружения Cisco необходим, отключите его на интерфейсах, подключенных к недоверенным сетям. Поскольку протокол обнаружения Cisco действует на уровне каналов, он не является транзитным для сети, если в ней не используется механизм обнаружения второго уровня. Разрешите работу протокола между доверенными устройствами и запретите на всех остальных. Однако, протокол обнаружения Cisco необходимо активировать на всех портах доступа, к которым подключаются IP-телефоны Cisco для установки отношений доверия.
- **Защита протокола "spanning tree".** Защита процесса протокола "spanning tree" (STP) на коммутаторах инфраструктуры очень важна. Непреднамеренное или вредоносное добавление блоков BPDU протокола "spanning tree" может нарушить работу устройства или сделать его уязвимым для DoS-атаки. Первый этап стабилизации топологии "spanning tree" — определение коммутатора, который будет служить корневым мостом в архитектуре и установка приоритета моста, которая позволит назначить мост корневым. Повторите операцию для резервного корневого моста. Это позволит предотвратить непреднамеренные изменения STP, вызванные неуправляемым добавлением нового коммутатора.

На некоторых платформах доступна функция сторожа BPDU. Если это так, включите эту функцию и функцию PortFast на портах доступа для защиты от ввода нежелательного трафика BPDU. При получении блока BPDU функция сторожа BPDU автоматически отключает порт.

Снижение рисков от угроз, инициированных на коммутаторе

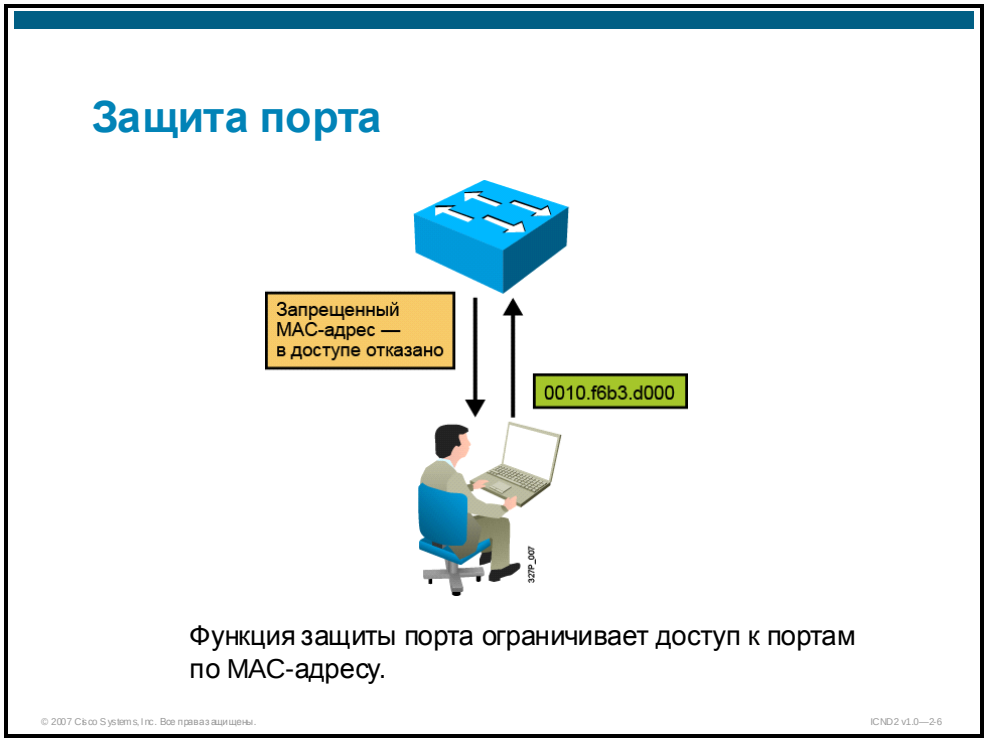
Для снижения рисков от угроз, инициированных на коммутаторе, рекомендуются следующие методы.

- **Предварительная настройка неиспользуемых портов маршрутизаторов и коммутаторов.**
  - Выполните команду **shut** на всех неиспользуемых портах и интерфейсах.
  - Поместите неиспользуемые порты в «парковочную» VLAN, предназначенную для группирования неиспользуемых портов, порты остаются в этой VLAN пока они не будут введены в эксплуатацию.
  - Настройте все неиспользуемые порты в качестве портов доступа и запретите автоматическое согласование трафика.
- **Соображения по транковым каналам.** По умолчанию коммутаторы Cisco Catalyst под управлением Cisco IOS настраиваются на автоматическое согласование функций транкового режима. Эта ситуация представляет серьезную угрозу для инфраструктуры, поскольку небезопасные устройства сторонних производителей могут быть введены в сеть как действительные компоненты инфраструктуры. В числе потенциальных атак перехват трафика, перенаправление трафика, DoS-атаки и др. Чтобы избежать этого риска, отключите автоматическое согласование транкового режима и вручную включите его на каналах, для которых такое согласование необходимо. Убедитесь, что транковые подключения используют стандартную VLAN, выделенную для транковых подключений.
- **Физический доступ к устройствам.** Вы должны тщательно контролировать физический доступ к коммутатору, чтобы предотвратить установку вредоносных устройств в монтажные шкафы с прямым доступом к портам коммутатора.
- **Безопасность портов доступа.** Особые меры следует предпринять на всех портах доступа всех коммутаторов, которые вводятся в эксплуатацию. Убедитесь, что задана политика, описывающая конфигурацию неиспользуемых портов коммутаторов дополнение к используемым портам.

  Для портов, которые будут подключаться к конечным устройствам, можно использовать макрос **switchport host**. При выполнении этой команды на порте коммутатора этот порт переводится в режим доступа, на нем включается функция PortFast протокола "spanning tree" и отключается группирование каналов.

Примечание	Макрос switchport host отключает EtherChannel и транковый режим и включает функцию PortFast протокола STP.

Команда **switchport host** — это макрос, который выполняет несколько команд конфигурации. Действие команды **switchport host** нельзя отменить с помощью версии "**no**", поскольку она не существует. Для возврата интерфейса к параметрам по умолчанию используйте команду глобальной конфигурации **default interface** *идентификатор интерфейса*. Эта команда возвращает конфигурации всех интерфейсов к параметрам по умолчанию.



Описание защиты портов

Защита портов — эта функция коммутаторов Cisco Catalyst, которая разрешает доступ к порту ограниченному набору MAC-адресов. Коммутатор может добавлять эти адреса динамически или вы можете задать их статически. Порт, на котором настроена функция защиты порта, принимает кадры только от добавленных или заданных портов.

Существует несколько вариантов защиты порта.

- **Динамический.** Вы можете указать, сколько MAC-адресов могут одновременно использовать порт. Динамический метод используется, если имеет значение только количество разрешенных MAC-адресов, а не их значения. В зависимости от конфигурации коммутатора, эти динамически добавленные адреса устаревают по прошествии определенного периода времени. Вместо устаревших адресов порт добавляет новые адреса, пока из количество не увеличивается до заданного максимального значения.
- **Статический.** Вы статически назначаете MAC-адреса, которые имеют право на использование порта. MAC-адреса источника, которым не будет присвоено это право, не смогут отправлять кадры в порт.
- **Комбинация статического и динамического добавления адресов.** Вы можете задать несколько разрешенных MAC-адресов и позволить коммутатору динамически добавить остальные MAC-адреса. Например, если задано максимальное число MAC-адресов, равное четырем, и вы статически настроили два MAC-адреса, коммутатор динамически добавит два следующих MAC-адреса, полученных на соответствующем порте. Доступ к порту будет предоставляться только этим четырем адресам, два из которых заданы статически и другие два добавлены динамически. Статически заданные адреса не устаревают, однако динамически добавленные адреса могут устареть, в зависимости от конфигурации коммутатора.

- **Динамическая запись с закреплением.** Если на интерфейсе настроена эта функция, он автоматически «закрепляет» динамически добавленные адреса. Это значит, что динамически добавленные адреса записываются в работающую конфигурацию так, как если бы они были статически заданы с помощь команды switchport port-security mac-address. Закрепленные адреса не устаревают.

Сценарий

Представим пять пользователей с лэптопами, которые имеют разрешение на подключение к определенному порту при посещении здания. Необходим разрешить доступ к порту коммутатора MAC-адресам этих лэптопов, и запретить динамическое добавление адресов на этом порте.

Процесс

В таблице ниже описывается процесс, который позволит решить задачи, поставленные в сценарии.

№	Действие	Примечания
1.	Защита порта настраивается на разрешение максимум пяти подключений, для каждого из пяти разрешенных MAC-адресов настраивается одна запись.	Это действие позволяет заполнить таблицу MAC-адресов пятью записями для данного порта и запретить динамическое добавление записей.
2.	Обрабатываются разрешенные кадры.	Когда кадры прибывают на порт коммутатора, их MAC-адрес источника сравнивается с записями таблицы маршрутизации. Если MAC-адрес источника совпадает с одной из записей таблицы для этого порта, кадры будут обработаны аналогично любым другим кадрам, полученным коммутатором.
3.	Новым MAC-адресам запрещено создавать записи в таблице MAC-адресов.	Когда на порт прибывают кадры с неавторизованным MAC-адресом, коммутатор определяет, что эти адреса отсутствуют в таблице MAC-адресов и не создает динамическую запись для этого MAC-адреса.
4.	Коммутатор реагирует на неавторизованные кадры.	Коммутатор запрещает доступ к порту и предпринимает одно из следующих действий (в зависимости от конфигурации): (а) полное отключение порта коммутатора; (б) отказ в доступе для данного MAC-адреса и генерация сообщения об ошибке для занесения в журнал; (в) отказ в доступе для данного MAC-адреса без генерации сообщения об ошибке для занесения в журнал.

Примечание Функцию защиты порта нельзя использовать для транковых портов, поскольку адреса транковых каналов могут часто меняться. Варианты защиты порта могут различаться в зависимости от используемой модели коммутатора Cisco Catalyst. Сведения о поддержке функции на том или ином устройстве можно найти в соответствующей документации.

Аутентификация портов 802.1X

Стандарт IEEE 802.1X определяет протокол контроля доступа и аутентификации на уровне портов, запрещающий неавторизованным рабочим станциям подключаться к ЛВС через общедоступные порты коммутатора. Сервер аутентификации аутентифицирует все рабочие станции, которые подключаются к порту коммутатора, перед тем, как предоставить им доступ к службам коммутатора или ЛВС.

Пока рабочая станция не аутентифицирована, контроль доступа 802.1X разрешает передачу только трафика EAPOL через порт, к которому подключена эта рабочая станция. После успешной аутентификации порт переходит в нормальный режим передачи трафика.

При использовании аутентификации 802.1X на уровне портов устройства в сети могут иметь следующие роли.

- **Клиент.** Устройство (рабочая станция), которая запрашивает доступ к службам ЛВС и коммутатора и отвечает на запросы этого коммутатора. На рабочей станции должно быть запущено клиентское ПО, совместимое с 802.1X, например клиент, входящий в состав ОС Microsoft Windows XP. Порт, к которому подключается клиент, в спецификации IEEE 802.1X называется просителем (supplicant).
- **Сервер аутентификации.** Выполняет аутентификацию клиентов. Сервер аутентификации проверяет удостоверение клиента и сообщает коммутатору, авторизован ли клиент для доступа к службам ЛВС и коммутатора. Поскольку коммутатор действует как прокси-сервер, служба аутентификации является прозрачной для клиента. В качестве сервера аутентификации поддерживается только система безопасности RADIUS с расширениями протокола EAP.

- **Коммутатор (также называется аутентификатором).** Контролирует физический доступ к сети в зависимости от состояния аутентификации клиента. Коммутатор действует как промежуточное звено (прокси) между клиентом (просителем) и сервером аутентификации. Он запрашивает идентификационные данные клиента, проверяет эти данные с помощью сервера аутентификации и передает клиенту ответ. Коммутатор использует программный агент RADIUS, который выполняет инкапсуляцию и декапсуляцию кадров EAP и обеспечивает взаимодействие с сервером аутентификации.

От состояния порта зависит, разрешен ли клиенту доступ к сети. Порт начинает работу в неавторизованном состоянии. В этом состоянии порт блокирует весь входящий и исходящий трафик за исключением пакетов протокола 802.1X. Если клиент аутентифицируется успешно, порт переходит в авторизованное состояние, которое обеспечивает нормальную передачу трафика клиента.

Если коммутатор запрашивает клиентское удостоверение (инициация коммутатора), но клиент не поддерживает 802.1X, порт остается в неавторизованном состоянии и клиент получает отказ в доступе к сети.

Когда клиент с поддержкой 802.1X подключается к порту и инициирует процесс аутентификации (инициация просителя), отправляя запускающий кадр EAPOL в коммутатор под управлением 802.1X, но не получает ответа, клиент начинает передавать кадры так, как если бы порт находился в авторизованном режиме.

Если клиент аутентифицируется успешно (получает кадр «Accept» от сервера аутентификации), порт переходит в авторизованное состояние и все кадры от аутентифицированного клиента передаются через порт.

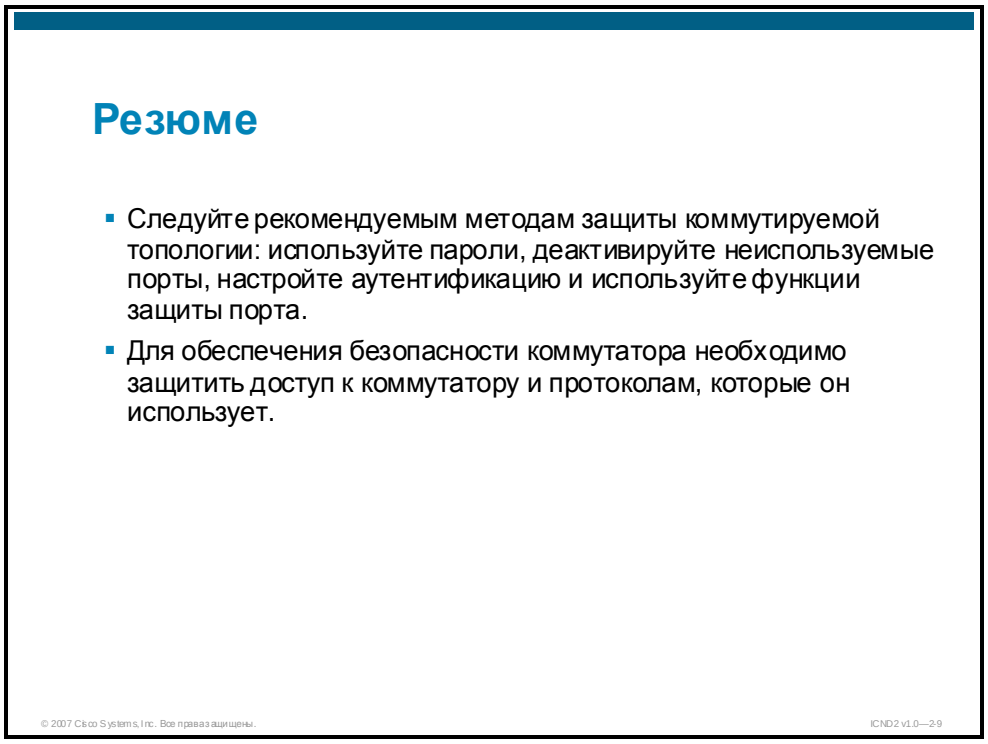
Если аутентификация заканчивается неудачей, порт остается в неавторизованном состоянии, однако попытку аутентификации можно повторить. Если сервер аутентификации недоступен, коммутатор может повторить запрос. Если сервер не возвращает ответ на заданное количество запросов, аутентификация заканчивается неудачей, и клиент получает отказ в доступе к сети.

Когда клиент выходит из системы, он отправляет кадр EAPOL о выходе, которое переводит порт в неавторизованное состояние.

Примечание Дополнительные сведения об аутентификации 802.1X на уровне портов можно найти в курсах Cisco CCNP.

Резюме

В этом разделе приводится резюме основных вопросов, рассмотренных в занятии.



Занятие 5

Устранение неполадок в коммутируемых сетях

Обзор

С ростом количества функций коммутатора растет вероятность возникновения неисправностей также растет. В этом занятии представлены рекомендации по обеспечению исправной работы сети. Кроме того, в нем описываются распространенные причины отказов конфигурации VLAN, а также протоколов VTP и STP, и приводятся сведения о том, какие данные следует собрать для определения источника проблемы.

Задачи

По окончании этого занятия вы сможете определять методы поиска и изоляции распространенных проблем коммутируемой сети, а также предлагать решения этих проблем. Это значит, что вы сможете выполнить следующие задачи:

- описывать базовый набор действий по поиску и устранению неполадок в коммутируемой сети;
- определять и решать проблемы подключения;
- выявлять и решать проблемы VLAN и транкового режима;
- выявлять и решать проблемы VTP;
- выявлять и решать проблемы STP.

Устранение неполадок коммутаторов

В этом разделе описывается базовый набор действий по устранению неполадок коммутируемой сети.

Существует множество методов устранения неполадок в коммутаторе. Разработка метода поиска и устранения неполадок или плана тестирования будет гораздо эффективнее неструктурированного подхода. Ниже представлены некоторые рекомендации по повышению эффективности поиска и устранения неполадок.

- **Потратьте время на ознакомление с принципами работы коммутатора.** На веб-сайте Cisco (cisco.com) доступны подробные технические сведения о принципе работы коммутатора. Руководства по конфигурации будут особенно полезны.
- **Для более сложных случаев подготовьте физическую и логическую схемы сети.** На физической схеме изображаются соединения устройств и кабелей. Логическая схема предоставляет сведения о сегментах (VLAN) сети и маршрутизаторах, которые обеспечивают маршрутизацию для этих сегментов. Схема протокола "spanning tree" также будет полезна для устранения неполадок в сложных случаях. Поскольку коммутатор может создавать различные сегменты на основе VLAN, схема физических подключений не дает всей необходимой информации. Вы также должны знать конфигурацию коммутаторов, сегменты (VLAN), заданные в сети, и схему их логических соединений.

- **Создайте план.** Некоторые проблемы имеют очевидные решения, другие — нет. Симптомы, наблюдаемые в сети, могут быть результатом проблем в другой области или на другом уровне. Перед тем, как делать выводы, попробуйте определить работающие и неработающие компоненты сети, используя упорядоченные методы. Поскольку сети могут быть довольно сложными, имеет смысл изолировать потенциальные проблемные домены. Один из способов достичь этого — воспользоваться семиуровневой моделью взаимодействия открытых систем OSI. Например: проверка физических подключений (уровень 1), проверка подключений внутри VLAN (уровень 2), проверка подключений между VLAN (уровень 3) и т. д. Если коммутатор настроен верно, многие из проблем, с которыми вы столкнетесь, будут иметь место на физическом уровне (физические порты и кабели).
- **Не предполагайте, что компонент работает, не убедившись в этом на 100%.** Если ПК не может выполнить вход на сервер через сеть, это может быть вызвано множеством причин. Не предполагайте, что базовые компоненты работают верно, не протестировав их. Кто-то мог изменить из конфигурацию, не проинформировав вас. Как правило, проверка базовых компонентов (например, проверка правильности подключения и активности портов), занимает не более минуты, но она поможет сэкономить много времени.

Устранение неполадок подключений портов

В этом разделе описывается базовый набор действий по устранению неполадок подключений портов.

Если вы столкнулись с проблемами подключения, начните с проверки портов. Порты являются основой коммутируемой сети. Если они не работают, не работает и сеть. Некоторые порты имеют особое значение из-за своего положения в сети и объема трафика, который они переносят. Это порты, подключенные к другим коммутаторам, маршрутизаторам и серверам. Устранение неполадок в таких портах может быть более сложным, поскольку они часто используют такие функции, как транковый режим и EtherChannel. Однако не стоит игнорировать другие порты, они тоже имеют значение, так как используются для подключения пользователей к сети.

Неисправности оборудования

Одной из причин проблем подключения может быть неисправность оборудования. Чтобы исключить такие проблемы, проверьте следующее.

- **Состояние обоих портов, участвующих в канале.** Убедитесь, что ни один из портов не отключен. Администратор мог вручную отключить один из портов. Кроме того, один из портов мог быть отключен программным обеспечением коммутатора из-за ошибки конфигурации. Если один порт включен, а другой выключен, активный порт будет иметь состояние "не подключен" (так как не обнаруживает соседний узел на другой стороне канала). Состояние отключенного порта будет "disable", "errDisable" или что-то подобное (в зависимости от причины отключения порта). Канал не будет активен, если хотя бы один порт отключен.
- **Тип кабеля, используемого для подключения.** Для подключений с полосой пропускания 100 Мбит/с следует использовать кабель как минимум 5-ой категории, для подключений 1 Гбит/с — как минимум категории 5e. Для подключения конечных

станций, маршрутизаторов и серверов к коммутаторам или концентраторам используйте прямой кабель RJ-45. Для подключений между коммутаторами и концентраторами используется перекрестный кабель Ethernet. Максимально расстояние для медных линий Ethernet и Fast Ethernet составляет 100 метров.

- **Отключение порта программным процессом.** Немигающий оранжевый индикатор рядом с портом означает, что он отключен программным обеспечением коммутатора, — либо через пользовательский интерфейс, либо из-за действий внутренних процессов, например сторожа BPDU, инструмента Root Guard или из-за нарушений безопасности порта.

Проблемы конфигурации

Конфигурация порта — другая возможная причина проблем подключения портов. Ниже перечислены некоторые из наиболее распространенных проблем конфигурации.

- **Сеть VLAN, которой принадлежит порт, исчезла.** Каждый коммутатора принадлежит VLAN. При удалении VLAN порт становится неактивным.

  Код ниже показывает, что команда **show interface** *интерфейс* не поможет определить проблему, если порт принадлежит несуществующей VLAN.

```
SwitchX# sh int fa0/2
FastEthernet0/2 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0017.596d.2a02 (bia
0017.596d.2a02)
  Description: Interface to RouterA F0/0
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
```

  Однако команда show interface интерфейс switchport покажет, что порт неактивен и не будет работать, пока отсутствующая VLAN не будет заменена.

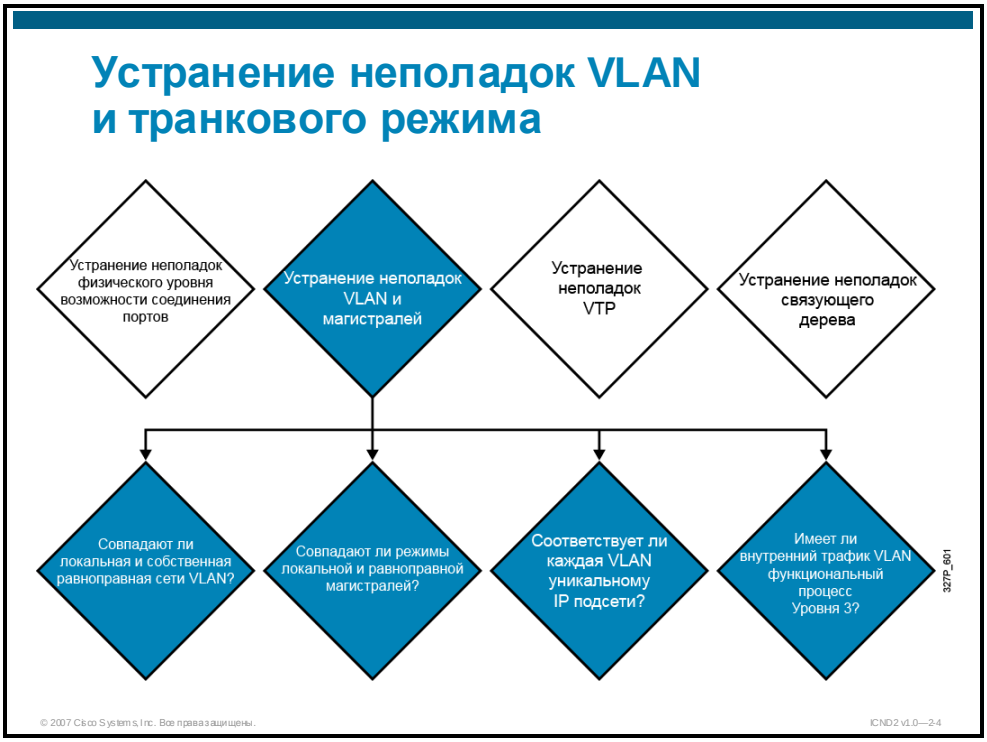
```
SwitchX# sh int fa0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 5 (Inactive)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
```

На некоторых коммутаторах рядом с портами, VLAN которых удалена, горит немигающий оранжевый индикатор. Если на коммутаторе горит много оранжевых индикаторов, не паникуйте. Это может быть вызвано тем, что эти порты принадлежат VLAN, которая была случайно удалена. При возвращении VLAN в таблицу VLAN порты снова станут активными. Порт запоминает VLAN, в которую он назначен.

- **Включено автосогласование.** Автосогласование — одна из оригинальных функций стандарта Fast Ethernet (IEEE 802.3u), которая позволяет устройствам автоматически обмениваться информацией о скорости и функциях дуплексной передачи через канал. Не следует использовать автосогласование для портов, которые поддерживают устройства сетевой инфраструктуры, такие как коммутаторы, маршрутизаторы и другие нетранзитные конечные системы, такие как серверы и принтеры. Автосогласование скорости и параметров дуплексной передачи — стандартный режим работы портов коммутатора с поддержкой этой функции. Однако для портов, которые подключаются к фиксированным устройствам, следует задавать верные значения скорости и параметры дуплексной передачи, не используя автосогласование этих параметров. Эта конфигурация исключает возможные проблемы согласования и предоставляет сведения о том, в каком режиме должны работать порты.

Устранение неполадок VLAN и транкового режима

В этом разделе описывается выявление и устранение проблем производительности VLAN. При этом предполагается, что вы нашли и устранили проблемы портов и автосогласования.



Несовпадения стандартной VLAN

Стандартная VLAN должна быть одинакова на обоих концах транкового подключения IEEE 802.1Q. Помните, что коммутатор, получающий немеченные кадры, назначает их в стандартную VLAN транкового подключения. Если на одном конце транкового подключения настроена стандартная сеть VLAN 1, а на другом — стандартная сеть VLAN 2, кадр, отправленный из сети VLAN 1 на одном конце, будет получен в сети VLAN 2 на другом конце. Трафик VLAN 1 «утекает» в сегмент VLAN 2. Нет причин, по которым такое поведение было бы необходимо. Несовпадение VLAN может вызвать проблемы подключение сети.

Несовпадение транкового режима

Транковые каналы следует настраивать статически везде, где это возможно. Однако по умолчанию коммутаторы Cisco Catalyst работают под управлением динамического транкового протокола, который пытается автоматически согласовать транковый канал. Этот проприетарный протокол Cisco определяет режим работы и протокол порта коммутатора при подключении к другому устройству с поддержкой динамического согласования транкинга.

Примеры режимов DTP

Параметр конфигурации	Описание
Dynamic Auto	Создает транковый канал по запросу от соседнего коммутатора. Режим Dynamic Auto не запускает процесс согласования, поэтому два коммутатора, работающие в этом режиме, не создадут транковый канал.
Dynamic Desirable	Сообщает соседнему коммутатору через протокол DTP, что интерфейс следует сделать транковым, если соседний интерфейс коммутатора также способен стать транковым.

VLAN и IP-подсети

Каждой VLAN должна соответствовать IP-подсеть. Два устройства в одной VLAN должны иметь адреса в одной подсети. Для внутреннего трафика VLAN устройство-отправитель распознает адресата как локальное устройство и отправляет широковещательный кадр ARP для обнаружения MAC-адреса назначения.

Два устройства в разных VLAN должны иметь адреса в разных подсетях. Для трафика между VLAN устройство-отправитель распознает адресата как удаленное устройство отправляет широковещательный кадр ARP для обнаружения MAC-адреса шлюза по умолчанию.

Подключение между VLAN

В большинстве случаев проблемы подключения между VLAN вызваны неверной настройкой. Например, если вы неверно настроите конфигурацию Router-on-a-stick или многоуровневую коммутацию (Cisco Express Forwarding), пакеты из одной VLAN могут не дойти до другой VLAN. Чтобы избежать ошибок конфигурации и обеспечить эффективное устранение неполадок, необходимо понять механизм, который используется пересылающими устройствами третьего уровня. Если вы уверены, что оборудование настроено должным образом, но коммутация не выполняется, причиной может быть неисправность оборудования и ошибка программного обеспечения.

Другой тип ошибок конфигурации, влияющих на маршрутизацию между VLAN, — неверная настройка устройств конечного пользователя, таких как ПК. Распространенная ситуация — неверная настройка шлюза по умолчанию на ПК. Слишком большое число ПК с одинаковыми шлюзами по умолчанию может перегрузить ЦП шлюза, что в свою очередь приведет к ухудшению скорости пересылки.

Устранение неполадок VTP

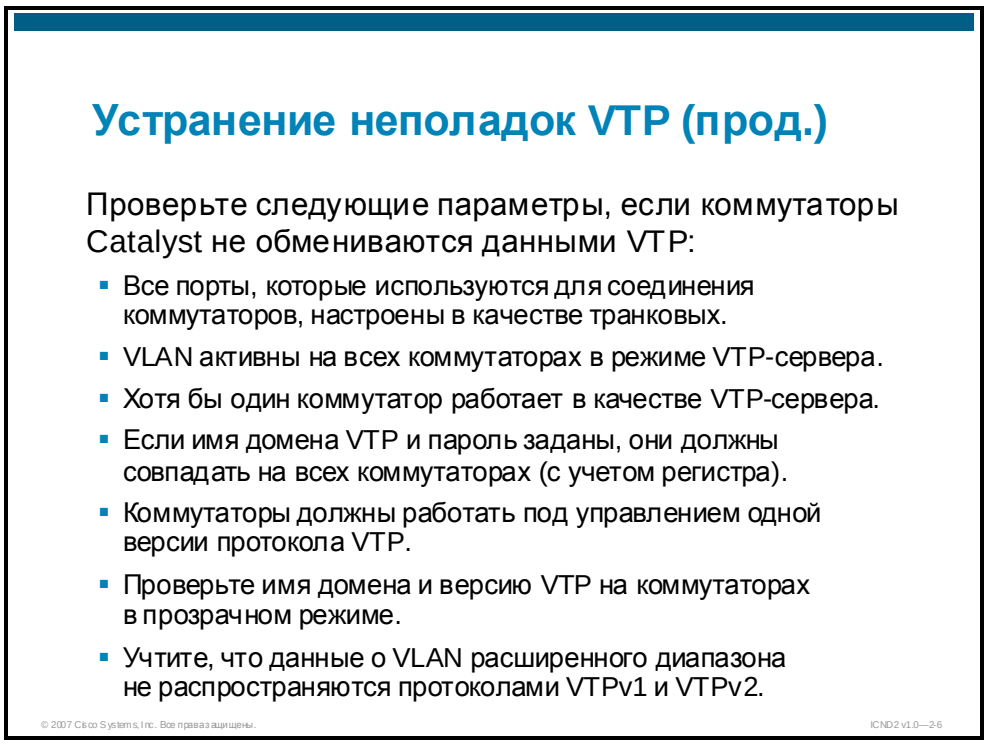
В этом разделе описывается выявление и решение проблем VTP. При этом предполагается, что вы нашли и устранили проблемы подключений портов и VLAN.

Сведения о VLAN не отображаются в выводе команды show run

VTP-клиенты и VTP-серверы требуют немедленного сохранения обновлений VTP без вмешательства пользователя. База данных VLAN была добавлена в ПО Cisco IOS в качестве метода немедленного сохранения обновлений VTP на VTP-клиентах и VTP-серверах. В некоторых версиях ПО база данных VLAN представлена в виде отдельного файла во Flash-памяти, который называется vlan.dat. Если команда **show vtp status** не работает должным образом, вы можете посмотреть сведения о VTP и VLAN, сохраненные в файле vlan.dat, для VTP-клиента или VTP-сервера, в котором возникли проблемы.

Коммутаторы в режиме VTP-сервера или VTP-клиента не сохраняют полные конфигурации VTP и VLAN в файл загрузочной конфигурации в энергонезависимой памяти (NVRAM) при вводе команды **copy running-config startup-config**. Они сохраняют конфигурацию в файл vlan.dat. Вышеизложенное неприменимо к системам в прозрачном режиме VTP. Коммутаторы в прозрачном режиме VTP сохраняют полные конфигурации VTP и VLAN в файл загрузочной конфигурации в NVRAM при вводе команды **copy running-config startup-config**. Например, если вы удалите файл vlan.dat на коммутаторе в режиме VTP-сервера или VTP-клиента после настройки VLAN, а затем перезагрузите коммутатор, протокол VTP вернется к параметрам по умолчанию (все пользовательские VLAN будут удалены). Но если вы удалите файл vlan.dat на коммутаторе в прозрачном режиме VTP, а затем перезагрузите коммутатор, конфигурация VTP сохранится. Это пример конфигурации VTP по умолчанию.

VLAN обычного диапазона (с номерами от 2 до 1000) можно настроить, когда коммутатор находится в прозрачном режиме или в режиме VTP-сервера. Но на коммутаторах Cisco Catalyst 2960 в прозрачном режиме VTP можно настраивать только VLAN расширенного диапазона (с номерами от 1025 до 4094).



Коммутаторы Cisco Catalyst не обмениваются данными VTP

Отсутствие обмена данными о VLAN в домене VTP может быть вызвано несколькими причинами. Если коммутаторы под управлением VTP не обмениваются данными о VLAN, проверьте следующее.

- Данные VTP передаются только через транковый порт. Убедитесь, что все порты, используемые для соединения коммутаторов, настроены как транковые и работают в транковом режиме.
- Убедитесь, что VLAN активны на всех коммутаторах в режиме VTP-сервера.
- Один из коммутаторов в домене VTP должен быть назначен VTP-сервером. Чтобы обеспечить распространение на VTP-клиенты, все изменения VLAN должны выполняться на этом коммутаторе.
- Имена домена VTP, заданные на устройствах в этом домене, должны совпадать. Имена вводятся с учетом регистра. Например CISCO и cisco — два разных имени домена.
- Убедитесь, что между сервером и клиентом не задан пароль. Если пароль задан, убедитесь, что он одинаков на обеих сторонах. При вводе пароля также учитывается регистр.
- Все коммутаторы в домене VTP должны работать с одной версией протокола VTP. VTP 1 (VTPv1) и VTP 2 (VTPv2) нельзя использовать на коммутаторах в одном VTP-домене. Включайте VTPv2 только если все коммутаторы в домене VTP поддерживают VTP 2.

Примечание По умолчанию протокол VTPv2 отключен на коммутаторах, которые его поддерживают. При включении VTPv2 на коммутаторе все коммутаторы в домене с поддержкой VTPv2 также активируют этот протокол. Версию протокола можно задать только на коммутаторах в режиме VTP-сервера или в прозрачном режиме.

- Коммутатор, который под управлением VTPv2, который находится в прозрачном режиме, распространяет все сообщения VTP, независимо от указанного домена VTP. Однако коммутатор под управлением VTPv1 распространяет только сообщения VTP, которые принадлежат тому же домену VTP, что локальный коммутатор. Коммутаторы в прозрачном режиме VTP, использующие VTPv1 отбрасывают объявления VTP, если они получены из другого домена VTP.
- VLAN расширенного диапазона не распространяются. Поэтому VLAN расширенного диапазона необходимо настраивать вручную на каждом устройстве.

Примечание Для коммутаторов Cisco Catalyst 6500 под управлением ПО Cisco IOS запланирована поддержка VTP 3 (VTPv3). Эта версия может передавать данные о VLAN расширенного диапазона. На данный момент VTPv3 поддерживается только в ОС Cisco Catalyst. Дополнительные сведения о VTPv3 см. по адресу http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a008019f048.html#wp1017196.

- Обновления, отправленные с VTP-сервера, не применяются на клиенте, если он имеет более высокий номер версии конфигурации VTP. Кроме того, клиент не распространяет обновления VTP среди соседних устройств VTP более низкого уровня, если его конфигурация имеет более высокую версию, чем обновления, рассылаемые VTP-сервером.

Недавно установленный коммутатор вызывает проблемы в сети

Недавно установленный коммутатор может вызвать проблемы, если все коммутаторы в сети находятся в одном домене VTP, и новый коммутатор не имеет конфигурации VTP и VLAN.

Если номер версии конфигурации коммутатора, добавленного в домен VTP, выше, чем номер версии конфигурации существующих коммутаторов домена VTP, новый коммутатор перезапишет базу данных VLAN домена своей базой данных VLAN. Это происходит независимо от того, в каком режиме работает коммутатор — в режиме VTP-клиента или VTP-сервера. VTP-клиент может удалить данные о VLAN с VTP-сервера. Обычный признак такой ситуации — многие порты переходят в неактивный режим, но при этом остаются назначенными в несуществующие VLAN.

Чтобы предотвратить эту проблему, следите, чтобы номер версии конфигурации коммутаторов, добавляемых в домен VTP, был ниже, чем номер версии конфигурации портов, которые уже находятся в домене VTP.

Все порты становятся неактивными после выключения и включения питания

Порты коммутатора переходят в неактивное состояние, если они принадлежат VLAN, которые отсутствуют в базе данных VLAN. Переход всех портов в неактивное состояние

после включения и выключения питания — обычная проблема. Как правило это происходит, если коммутатор настроен в качестве VTP-клиента и имеет транковый порт восходящего канала не во VLAN1. Поскольку коммутатор находится в режиме VTP-клиента, при сбросе он теряет свою базу данных VLAN, что приводит к переходу порта восходящего канала и других портов, не входящих в сеть VLAN1, в неактивное состояние.

Для решения этой проблемы выполните следующие действия.

Действие 1 Временно измените режим VTP на прозрачный.

Действие 2 Добавьте VLAN, в которую назначен порт восходящего канала, в базу данных VLAN.

Действие 3 Верните коммутатор в прозрачный режим VTP после того, как порт восходящего канала начнет пересылку.

Устранение неполадок протокола "spanning tree"

В этом разделе описывается выявление и решение проблем протокола "spanning tree". При этом предполагается, что вы нашли и устранили проблемы подключений портов, VLAN и VTP.

Использование схемы сети

Перед устранением неполадок петель моста необходимо узнать следующее.

- Топологию мостовой сети.
- Расположение корневого моста.
- Расположение заблокированных портов и резервных каналов.

Эта информация необходима по следующим причинам.

- Перед определение компонентов сети, которые необходимо исправить, необходимо узнать как выглядит нормально функционирующая сеть.
- Большинство действий по устранению неполадок подразумевают использование команд **show** для идентификации неисправных состояний. Знание сети поможет вам сосредоточиться на критически важных портах основных устройств.

Выявление мостовых петель

Раньше широковещательные штормы оказывали разрушительное действие на сети. Сегодня, с широким распространением высокоскоростных каналов и устройств, которые выполняют коммутацию на аппаратном уровне, вероятность, что широковещательная рассылка с отдельного узла (например сервера) вызовет отказ всей сети очень мала. Лучший способ выявления мостовых петель — отследить трафик в нагруженном канале и проверить его на наличие одинаковых пакетов. Однако, если все пользователи определенного домена моста испытывают проблемы с подключением, можно предположить, что это вызвано мостовой петлей. Проанализируйте нагрузку на устройстве и определите значения, выходящие за пределы нормы.

Быстрое восстановление подключений

Мостовые петли оказывают значительное воздействие на коммутируемую сеть. Как правило, у администраторов нет времени на поиск причин образования петли и они стремятся как можно скорее восстановить подключение. Самый простой способ достичь этого — вручную отключить все резервные порты в сети.

Отключение портов для разрыва петли

Если вы определили часть сети, пораженную сильнее всего, начните отключать порты в этой области. Или, по возможности, отключите порты, которые должны находиться в блокирующем режиме. При каждом отключении порта проверяйте, восстановлено ли подключение. Определив порт, отключение которого разрывает петлю, найдите резервируемый маршрут, которому принадлежит этот порт. Если этот порт должен находится в блокирующем режиме, значит вы нашли канал, в котором возникла неисправность.

Ведение журнала событий STP

Если вы не можете точно определите источник проблемы или если проблема является транзитной, включите ведение журнала событий STP на коммутаторе в неисправной сети. Если вы хотите ограничить число настраиваемых устройств, включите ведение журнала хотя бы на устройствах с заблокированными портами. Петля возникает, когда заблокированный порт становится незаблокированным.

Введите команду привилегированного режима EXEC **debug spanning-tree events**, чтобы вывести данные отладки STP. Введите команду глобальной конфигурации **logging buffered**, чтобы записать эти данные отладки в буферы устройства. Кроме того, попробуйте отправить эти данные отладки в сервер системного журнала. К сожалению при возникновении мостовой петли подключение к серверу системного журнала сохраняется редко.

Временное отключение ненужных функций

Отключите максимально возможное количество функций, чтобы упростить структуру сети и облегчить выявление проблемы. Например функция EtherChannel требует, чтобы протокол STP логически объединял несколько каналов в один, поэтому ее отключение во время устранения неполадок может быть целесообразно. Как правило, вам следует максимально упростить конфигурацию, чтобы облегчить поиск и устранение неполадок.

Назначение корневого моста

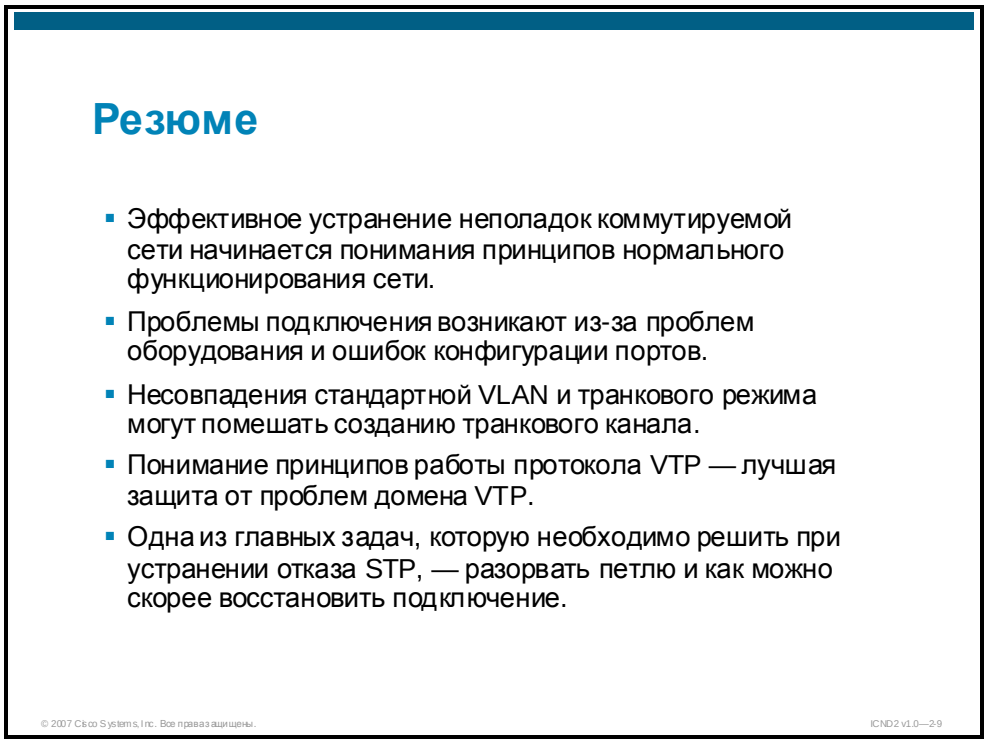
Часто информация о расположении корневого моста протокола "spanning tree" бывает недоступна во время устранения неполадок. Не позволяйте протоколу STP определить, какой коммутатор будет служить корневым мостом. Для каждой VLAN можно определить коммутатор, который будет лучше всего подходит для роли корневого моста. Выбор коммутатора, который будет наилучшим корневым мостом, зависит от архитектуры сети. Как правило, следует выбирать самых мощный коммутатор в центре сети. Если вы поместите корневой мост с прямым подключением к серверам и маршрутизаторам в центр сети, вы уменьшите среднее расстояние от клиентов до серверов и маршрутизаторов. Для всех VLAN задайте коммутаторы, которые будут служить основным и вспомогательным корневыми мостами.

Проверка настройки RSTP

Время конвергенции протоколов "spanning tree" 802.1d и PVST+ составляет 30–50 секунд. Конвергенция протоколов "spanning tree" RSTP и PVRST+ занимает 1–2 секунды. Длительная конвергенция может указывать на то, что протокол RSTP настроен не на всех коммутаторов, что замедляет время конвергенции всей сети. Для проверки режима "spanning tree" используется команда **show spanning-tree**.

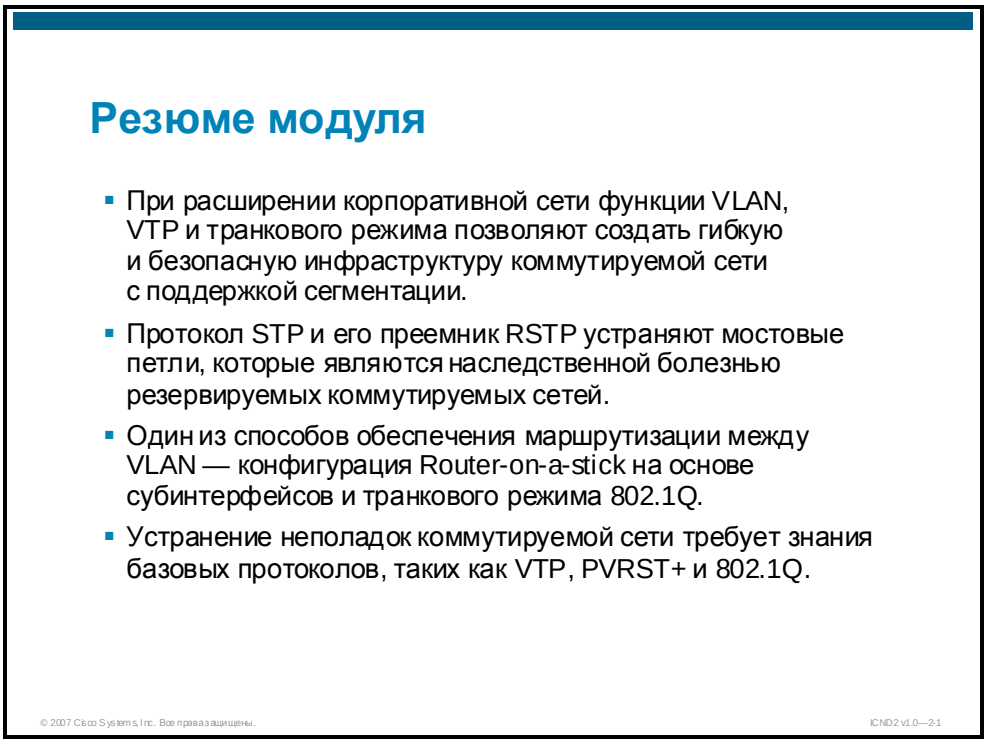
Резюме

В этом разделе приводится резюме основных вопросов, рассмотренных в занятии.



Резюме модуля

В этом разделе приводится резюме вопросов, рассмотренных в модуле.



Существует множество аспектов расширения коммутируемой сети, которые администраторы должны учитывать и применять на практике, когда их организация растет. В своем портфеле сетевых коммутаторов Cisco предлагает решения, которые не только устраняют неотложные проблемы, связанные с административными изменениями, но и обеспечивают масштабируемость, совместимость, повышенную выделенную полосу пропускания и безопасность.

Вопросы для самопроверки по модулю

Используйте эти вопросы, чтобы повторить материал, изученный в данном модуле. Верные ответы и решения можно найти в разделе "Ответы на вопросы для самопроверки".

В1) Какая функция обеспечивает охват нескольких коммутаторов несколькими VLAN? (Источник: внедрение сетей VLAN и транковых подключений

А) транковое подключение для соединения коммутаторов
Б) маршрутизатор для соединения коммутаторов
В) мост для соединения коммутаторов
Г) VLAN, настроенная между коммутаторами

В2) Что VMPS-сервер связывает с назначениями VLAN? (Источник: внедрение сетей VLAN и транковых подключений)

А) идентификаторы хостов
Б) имена пользователей
В) IP-адреса
Г) MAC-адреса

В3) Назовите две причины для использования 802.1Q? (Выберите два варианта.) (Источник: внедрение сетей VLAN и транковых подключений)

А) чтобы коммутаторы могли предоставлять доступ к транковому каналу нетранковым подключениям
Б) чтобы позволить клиентам видеть заголовок 802.1Q
В) чтобы обеспечить соединение сетей VLAN посредством моста
Г) для выравнивания нагрузки между параллельными каналами с помощью STP
Д) чтобы обеспечить транкинг между коммутаторами Cisco и коммутаторами других производителей

В4) Каково главное преимущество VTP? (Источник: внедрение сетей VLAN и транковых подключений)

А) обеспечивает транкинг для резервирования
Б) минимизирует резервирование в коммутируемой сети
В) позволяет использовать несколько VLAN в одном канале
Г) сводит к минимуму число ошибок конфигурации и несогласованных параметров

В5) Сколько доменов VTP можно настроить на коммутаторе? (Источник: внедрение сетей VLAN и транковых подключений)

А) один
Б) два
В) четыре
Г) восемь

В6) Какая команда используется для перевода коммутатора в прозрачный режим в домене VTP "switchlab"? (Источник: внедрение сетей VLAN и транковых подключений)

А) vtp mode trunk on
Б) **vtp mode transparent**
В) **vtp domain switchlab**
Г) **vtp domain switchlab transparent**

B7) Какой режим VTP используется по умолчанию на коммутаторе Cisco Catalyst? (Источник: внедрение сетей VLAN и транковых подключений)

А) выкл.
Б) клиент
В) сервер
Г) прозрачный режим

B8) Какие сведения выводит команда **show vlan**? (Источник: внедрение сетей VLAN и транковых подключений)

А) Параметры домена VTP
Б) Параметры конфигурации VMPS-сервера
В) Данные о портах, настроенных в качестве транковых
Г) Имена VLAN и порты, назначенные в эти VLAN

B9) Какая команда выводит данные о состоянии конфигурации протокола "spanning tree" для портов коммутатора серии Cisco Catalyst 2960? (Источник: внедрение сетей VLAN и транковых подключений)

А) **show vlan**
Б) **show trunk**
В) **show spanning-tree**
Г) **show spantree config**

B10) Где выполняется удаление VLAN из домена VTP? (Источник: внедрение сетей VLAN и транковых подключений)

А) на коммутаторе в режиме VTP-сервера
Б) на всех коммутаторах в режиме VTP-клиента
В) на коммутаторе в прозрачном режиме VTP
Г) на всех коммутаторах независимо от режима VTP mode

B11) Какие меры предосторожности следует предпринять при повторном развертывании коммутатора в новом домене VTP? (Источник: внедрение сетей VLAN и транковых подключений)

А) Задать на коммутаторе уникальный пароль VTP для безопасности.
Б) Предварительно настроить VLAN нового домена VTP на коммутаторе.
В) Убедиться, что номер версии конфигурации VTP ниже, чем у существующего домена.
Г) Перевести коммутатор в прозрачный режим VTP для минимизации негативного эффекта.

B12) Предположим, что VTP не обновляет конфигурацию на других коммутаторах при внесении в конфигурацию VLAN. Какую команду следует ввести, чтобы узнать, не находится ли коммутатор в прозрачном режиме VTP? (Источник: внедрение сетей VLAN и транковых подключений)

А) **show trunk**
Б) **show spantree**
В) **show interfaces**
Г) **show vtp status**

В13) Какие три типа кадров рассылаются по всем портам коммутатора, кроме порта источника? (Выберите три варианта.) (Источник: улучшение производительности с помощью протокола "spanning tree")

А) одноадресные кадры
Б) многоадресные кадры
В) широковещательные кадры
Г) кадры с известным адресом назначения
Д) кадры с неизвестным адресом назначения
Е) кадры с неизвестным адресом источника

В14) Какой термин используется для описания бесконечной рассылки кадров (образование бесконечных петель)? (Источник: улучшение производительности с помощью протокола "spanning tree")

А) шторм рассылки
Б) перегрузка петли
В) широковещательный шторм
Г) широковещательная перегрузка

В15) Какой термин используется для описания ситуации, когда несколько копий кадра прибывают на разные порты коммутатора? (Источник: улучшение производительности с помощью протокола "spanning tree")

А) шторм рассылки
Б) множественная передача кадров
В) нестабильность базы данных MAC-адресов
Г) перегрузка петли

В16) Когда протокол STP выполняет автоматическую перенастройку портов коммутатора или маршрутизатора? (Источник: улучшение производительности с помощью протокола "spanning tree")

А) при изменении топологии сети
Б) при истечении таймера задержки пересылки
В) когда администратор выбирает повторный расчет
Г) когда очередной блок BPDU не приходит в течение периода времени, определяемого задержкой пересылки

В17) Как протокол STP обеспечивает защиту от образования петель? (Источник: улучшение производительности с помощью протокола "spanning tree")

А) он помещает все порты в блокирующий режим
Б) он помещает все мосты в блокирующий режим
В) он помещает некоторые порты в блокирующий режим
Г) он помещает некоторые мосты в блокирующий режим

В18) Какой порт представляет маршрут с наименьшей стоимостью от некорневого моста к корневому? (Источник: улучшение производительности с помощью протокола "spanning tree")

А) корневой
Б) блокирующий
В) выделенный
Г) невыделенный

В19) По какому критерию протокол STP выбирает выделенный порт для сегмента? (Источник: улучшение производительности с помощью протокола "spanning tree")

А) наименьшая стоимость маршрута к корневому мосту
Б) наибольшая стоимость маршрута к корневому мосту
В) наименьшая стоимость маршрута к ближайшему некорневому мосту
Г) наибольшая стоимость маршрута к ближайшему некорневому мосту

В20) Какое утверждение является справедливым для режима прослушивания? (Источник: улучшение производительности с помощью протокола "spanning tree")

А) Порт может принимать блоки BPDU и заполнять таблицу MAC-адресов.
Б) Порт может принимать блоки BPDU, но пока не может заполнять таблицу MAC-адресов.
В) Порт может заполнять таблицу MAC-адресов, но пока не может пересылать пользовательские кадры.
Г) Порт может пересылать пользовательские кадры, но пока не может заполнять таблицу MAC-адресов.

В21) Каков режим невыделенного порта с точки зрения STP? (Источник: улучшение производительности с помощью протокола "spanning tree")

А) блокирующий
Б) режим обучения
В) режим прослушивания
Г) режим пересылки

В22) Каков режим корневого порта с точки зрения STP? (Источник: улучшение производительности с помощью протокола "spanning tree")

А) блокирующий
Б) режим обучения
В) режим прослушивания
Г) режим пересылки

В23) На каком мосту STP все порты являются выделенными? (Источник: улучшение производительности с помощью протокола "spanning tree")

А) корневой мост
Б) некорневой мост
В) мост с наименьшим приоритетом
Г) мост с наибольшим идентификатором моста

В24) При каком событии протокол STP обнаруживает изменение топологии? (Источник: улучшение производительности с помощью протокола "spanning tree")

А) Блок BPDU не получен в течение двух секунд.
Б) Устройство не отвечает на сообщение согласования подключения.
В) Таймер max_age истек и блок BPDU не получен.
Г) Устройство не отвечает на сообщение согласования подключения в течение заданного периода времени.

В25) Какие проблемы коммутируемой сети решает протокол RSTP? (Источник: улучшение производительности с помощью протокола "spanning tree")

А) сетевая безопасность
Б) размер сети
В) резервируемая топология
Г) скорость конвергенции

В26) Какой эквивалент режима прослушивания STP используется в RSTP? (Источник: улучшение производительности с помощью протокола "spanning tree")

А) блокирующий
Б) режим прослушивания
В) режим отбрасывания
Г) режим пересылки

В27) Порты с какими ролями RSTP включаются в активную топологию? (Источник: улучшение производительности с помощью протокола "spanning tree")

А) корневой и альтернативный
Б) корневой и выделенный
В) альтернативный и резервный
Г) выделенный и резервный

В28) Какая команда назначает субинтерфейс сети VLAN 50 с использованием транкового режима 802.1Q? (Источник: маршрутизация между VLAN)

А) Router(config) # **encapsulation 50 dot1Q**
Б) Router(config) # **encapsulation 802.1Q 50**
В) Router(config-if) # **encapsulation dot1Q 50**
Г) Router(config-if) # **encapsulation 50 802.1Q**

В29) Какая команда разрешает использование порта максимум 10-ю устройствами? (Источник: обеспечение безопасности расширенной сети)

А) **switchport secure 10**
Б) **switchport max-mac-count 10**
В) **switchport port-security maximum 10**
Г) **switchport port-security 10 max-mac**

В30) Что происходит с портом коммутатора при удалении VLAN, к которой он принадлежит? (Источник: устранение неполадок в коммутируемых сетях)

А) Порт переходит в сеть VLAN по умолчанию (VLAN 1).
Б) Порт переходит в сеть VLAN по умолчанию (VLAN 1) и становится неактивным.
В) Порт остается в удаленной VLAN и становится неактивным.
Г) VLAN нельзя удалить, если в нее назначены порты.

В31) Что происходит, когда администратор пытается создать транковый канал между двумя портами, порты которых находятся в режиме "dynamic auto"? (Источник: устранение неполадок в коммутируемых сетях)

А) Канал становится транковым.
Б) Канал становится нетранковым.
В) Оба порта будут настроены как порты доступа.
Г) Оба порта станут неактивными.

В32) Коммутатор A находится в режиме VTP-клиента, в его базе данных VLAN заданы VLAN с номерами от 1 до 5. Коммутатор B добавляется в тот же домен VTP в режиме VTP-сервера, в его базе данных заданы VLAN с номерами от 6 до 10. Как базы данных VLAN на коммутаторах A и B будут выглядеть после добавления коммутатора B в сеть? (Источник: устранение неполадок в коммутируемых сетях)

А) Обе базы данных VLAN будут включать VLAN с номерами 1 до 10.
Б) Обе базы данных VLAN будут включать VLAN с номерами 1 до 5.
В) Обе базы данных VLAN будут включать VLAN с номерами 6 до 10.
Г) Это зависит от того, какой коммутатор имеет более высокий номер версии конфигурации.

Ответы на вопросы для самопроверки по модулю

В1) А

В2) Г

В3) А, Е

В4) Г

В5) А

В6) Б

В7) В

В8) Г

В9) В

В10) А

В11) В

В12) Г

В13) Б, В, Е

В14) В

В15) В

В16) А

В17) В

В18) А

В19) А

В20) Б

В21) А

В22) Г

В23) А

В24) В

В25) Г

В26) В

В27) Б

В28) В

В29) В

В30) В

В31) Б

В32) Г

Модуль 3

Создание маршрутизируемой сети среднего размера

Обзор

Маршрутизация — это процесс передачи информации из одного места в другое. Очень важно понимать принципы динамической маршрутизации и методы, которые различные протоколы маршрутизации (на основе вектора расстояния и состояния канала) используют для определения IP-маршрутов.

Бесклассовые протоколы маршрутизации, например RIPv2, EIGRP и OSPF масштабируются лучше, чем классовые протоколы, так как они поддерживают маски подсети переменной длины VLSM и суммирование маршрутов.

Задачи модуля

По окончании этого модуля вы сможете описывать концепции маршрутизации в применении к сети среднего размера и обсуждать факторы, которые учитываются при внедрении маршрутизации в сети. Это значит, что вы сможете выполнить следующие задачи:

- описывать способы применения и ограничения динамической маршрутизации, в том числе классовой маршрутизации на основе векторов расстояния и бесклассовой маршрутизации на основе состояний каналов, в маршрутизируемой сети среднего размера;
- описывать принцип работы VLSM и бесклассовой внутридоменной маршрутизации (CIDR) на маршрутизаторах Cisco и объяснять, как маршрутизаторы Cisco реализуют суммирование маршрутов.

Занятие 1

Повторение пройденного материала по принципам маршрутизации

Обзор

Маршрутизация — это процесс определения места назначения для отправки пакетов данных, направленных за пределы локальной сети. Маршрутизаторы собирают и хранят данные маршрутизации, чтобы обеспечивать прием и передачу этих пакетов. Данные маршрутизации обрабатываются в виде записей в таблице маршрутизации, при этом каждая запись соответствует идентифицированному маршруту. Маршрутизатор может использовать протокол маршрутизации для динамического создания и поддержки таблицы маршрутизации, что позволяет записывать и учитывать изменения в сети, когда бы они не происходили.

Для эффективного управления IP-сетью вы должны понимать принцип работы протоколов динамической маршрутизации и их влияния на IP-сеть. В этом занятии описывается принцип работы и ограничения протоколов маршрутизации на основе векторов расстояния и состояния канала.

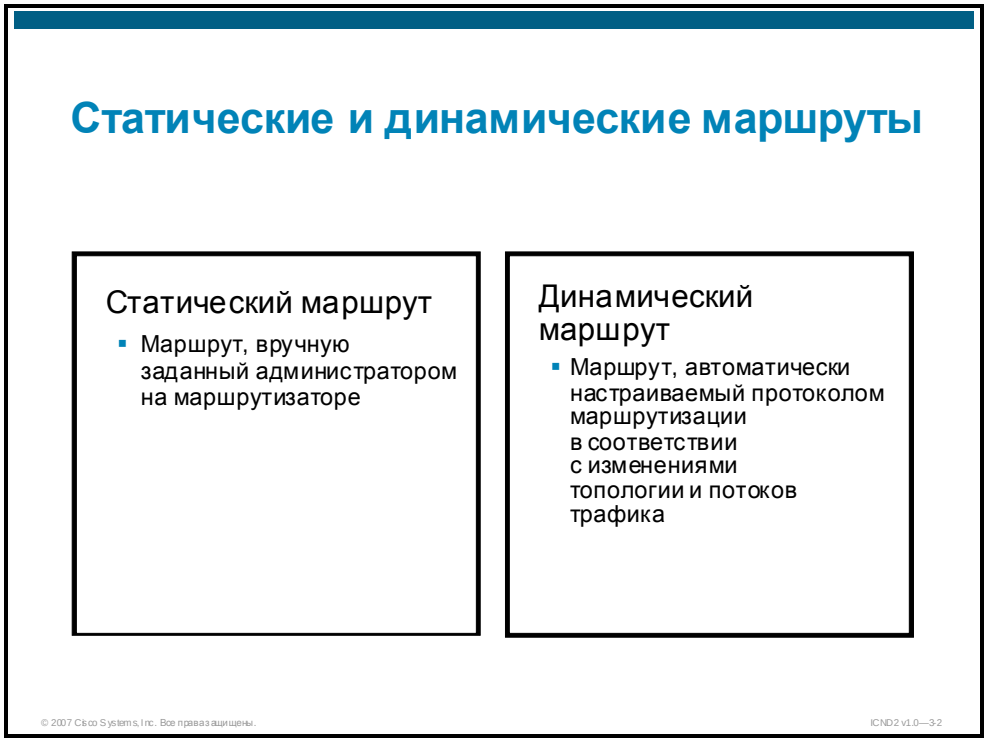
Задачи

По окончании этого занятия вы сможете описывать способы применения и ограничения динамической маршрутизации в маршрутизируемой сети среднего размера. Это значит, что вы сможете выполнить следующие задачи:

- описывать назначение и типы протоколов динамической маршрутизации;
- описывать принцип работы и внедрение протоколов на основе вектора расстояния;
- описывать принцип работы и внедрение протоколов на основе состояния канала.

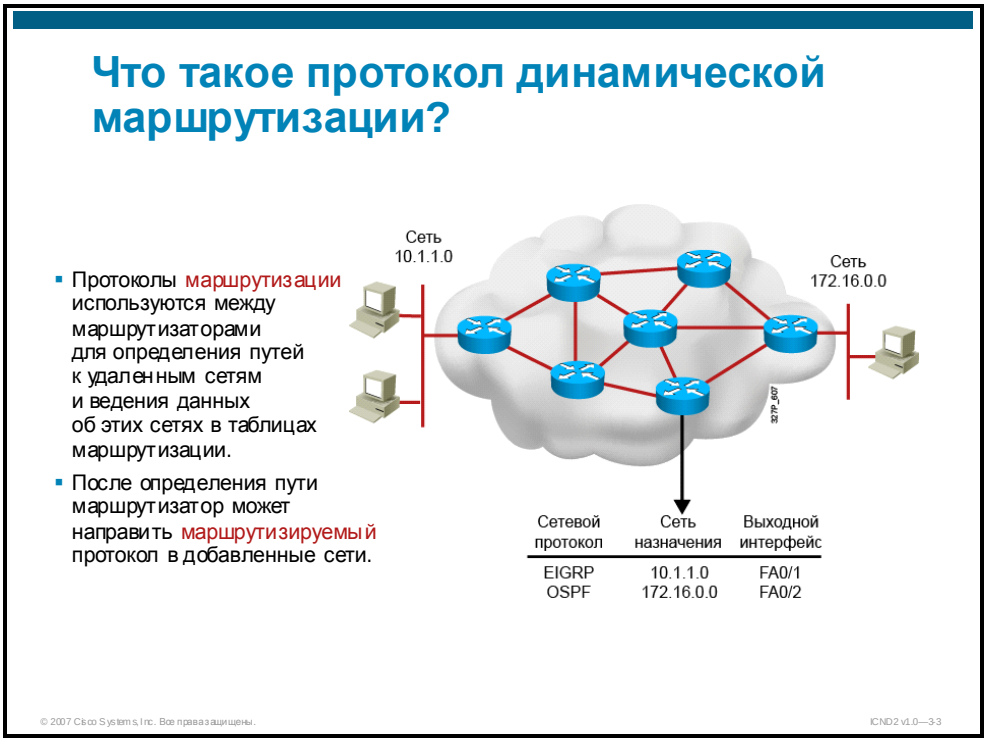
Повторение пройденного материала по динамической маршрутизации

В этом разделе описывается назначение, типы и классы протоколов динамической маршрутизации.



Маршрутизаторы могут пересылать пакеты через статические или динамические маршруты, в зависимости от конфигурации маршрутизатора. Существует два способа сообщить маршрутизатору, как пересылать пакеты в сети, не имеющие прямого подключения к нему.

- **Статический.** Маршрутизатор добавляет статический маршрут, вручную настроенный маршрутизатором. Администратор должен вручную обновлять запись статического маршрута при каждом изменении топологии интерсети. Статические маршруты задаются пользователем и определяют путь, который пакеты проходят при перемещении из источника в место назначения. Эти настраиваемые администратором маршруты обеспечивают высокую степень контроля на маршрутизацией в IP-интерсети.
- **Динамический.** Маршрутизатор динамически добавляет маршруты после того, как администратор настраивает протокол маршрутизации, используемый для определения маршрутов. В отличие от статических маршрутов, при использовании динамической маршрутизации процесс маршрутизации автоматически обновляет данные о маршрутах каждый раз при получении новых данных о топологии. Маршрутизатор добавляет и поддерживает маршруты к удаленным местам назначения, обмениваясь обновлениями маршрутизации с другими маршрутизаторами в интерсети.



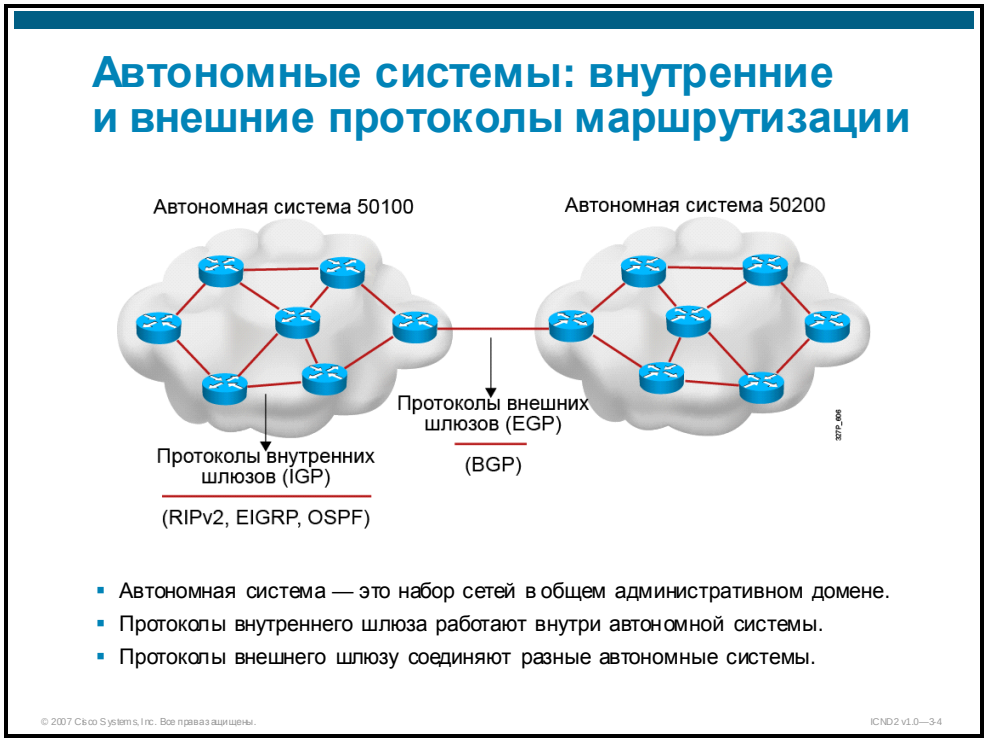
При динамической маршрутизации для распространения информации используется протокол маршрутизации. Протокол маршрутизации задает правила, которые маршрутизатор использует при взаимодействии с соседними маршрутизаторами для определения путей в удаленные сети и ведения записей об этих сетях в таблице маршрутизации.

Ниже приводятся различия между маршрутизируемыми протоколами и протоколами маршрутизации.

- **Маршрутизируемый протокол.** Любой сетевой протокол с адресом сетевого уровня, который поддерживает пересылку пакетов с одного хоста на другой в зависимости от схемы адресации, не имея информации о полном маршруте от источника к месту назначения. Как правило, пакеты передаются из одной системы в другую. Пример маршрутизируемого протокола — IP.
- **Протокол маршрутизации.** Обеспечивает обмен данными маршрутизации между сетями и позволяет маршрутизаторам создавать динамические таблицы маршрутизации. Традиционная IP-маршрутизация остается простой, так как использует метод следующего перехода (следующего маршрутизатора). Маршрутизатор должен знать, куда отправить пакет, но не последующий путь пакета по оставшимся переходам (маршрутизаторам).

Протоколы маршрутизации предоставляют следующие сведения:

- способ передачи обновлений;
- передаваемые данные;
- время передачи данных;
- методы определения получателей обновлений.

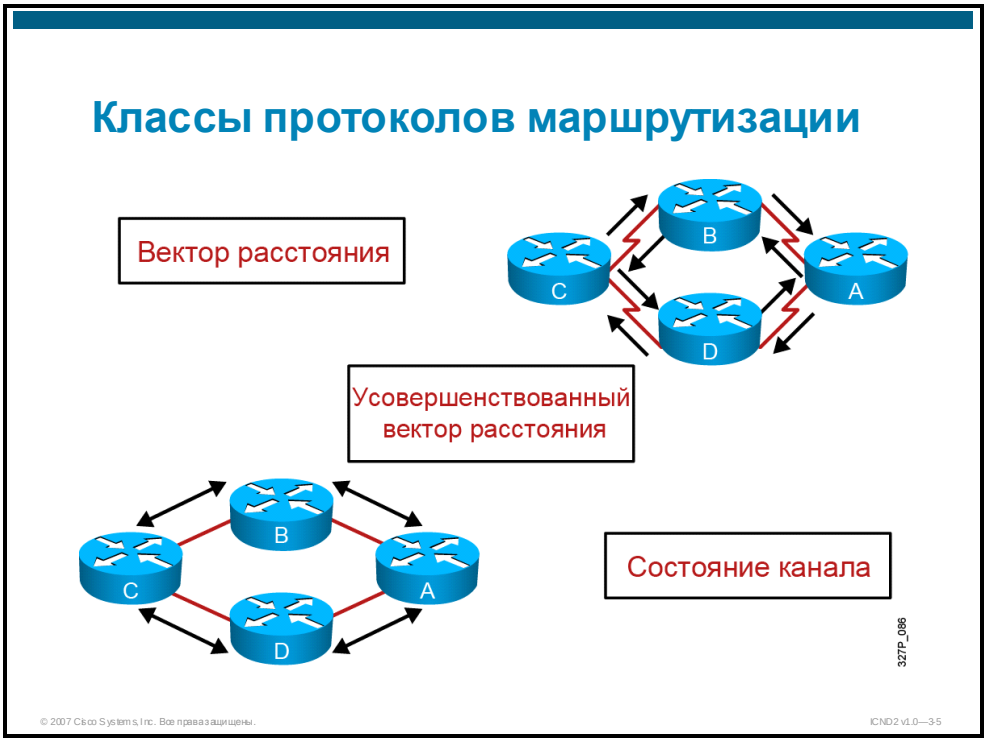


Автономная система — это совокупность сетей с общим управлением, использующих общую стратегию маршрутизации.

Существует два типа протоколов маршрутизации.

- **Протоколы внутреннего шлюза (IGP).** Эти протоколы маршрутизации используются для обмена данными маршрутизации внутри автономной системы. примеры IGP: RIPv2, EIGRP и OSPF.
- **Протоколы внешнего шлюза (EGP).** Эти протоколы используются для маршрутизации между автономными системами. В современных сетях в качестве протокола внешнего шлюза используется протокол BGP.

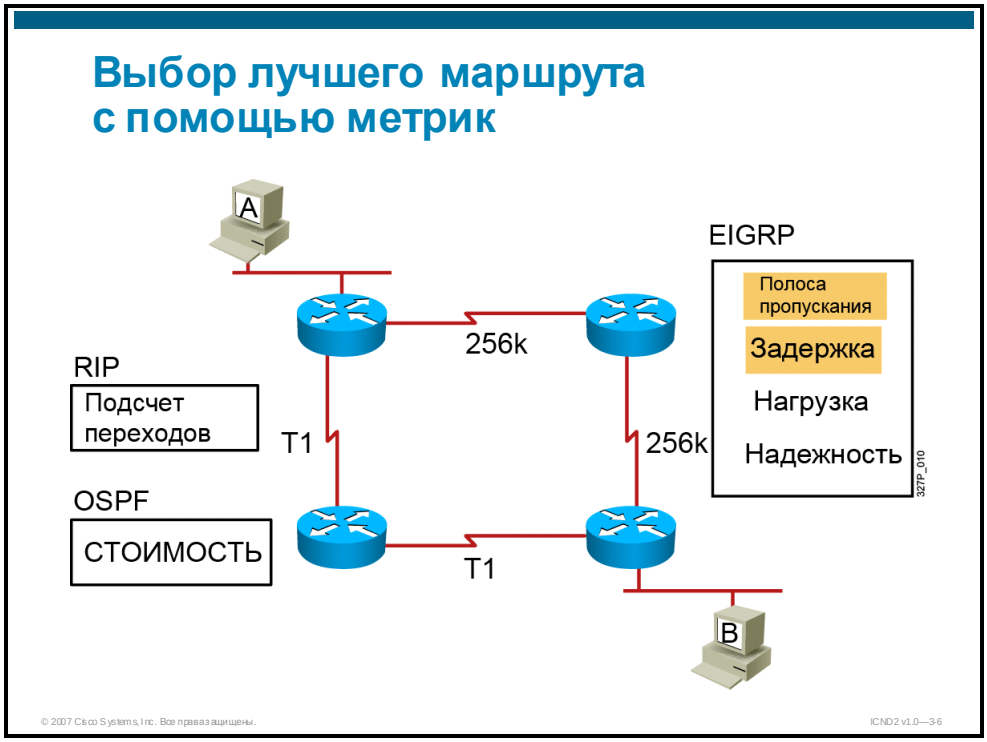
Примечание	Организация IANA (полномочный орган по цифровым адресами Интернета) назначает номера автономных систем во многих юрисдикциях. Нумерация IANA является обязательной, если ваша организация планирует использовать BGP. Однако мы рекомендуем студентам ознакомиться с различиями между открытой и закрытой системами нумерации.



Внутри автономной системы большинство протоколов маршрутизации внутреннего шлюза можно классифицировать по использованию одного из следующих алгоритмов.

- **Векторы расстояния.** Метод маршрутизации на основе векторов расстояния определяет направление (вектор) и расстояние (например, количество переходов) к любому каналу интерсети.
- **Состояние канала.** В маршрутизации на основе состояния канала используется алгоритм определения кратчайших путей (SPF). Он подразумевает создание абстракции точной топологии полной интерсети или ее отдела, в котором работает маршрутизатор.
- **Расширенный вектор расстояния.** Расширенный метод векторов состояния объединяет отдельные аспекты алгоритмов состояния канала и вектора расстояния.

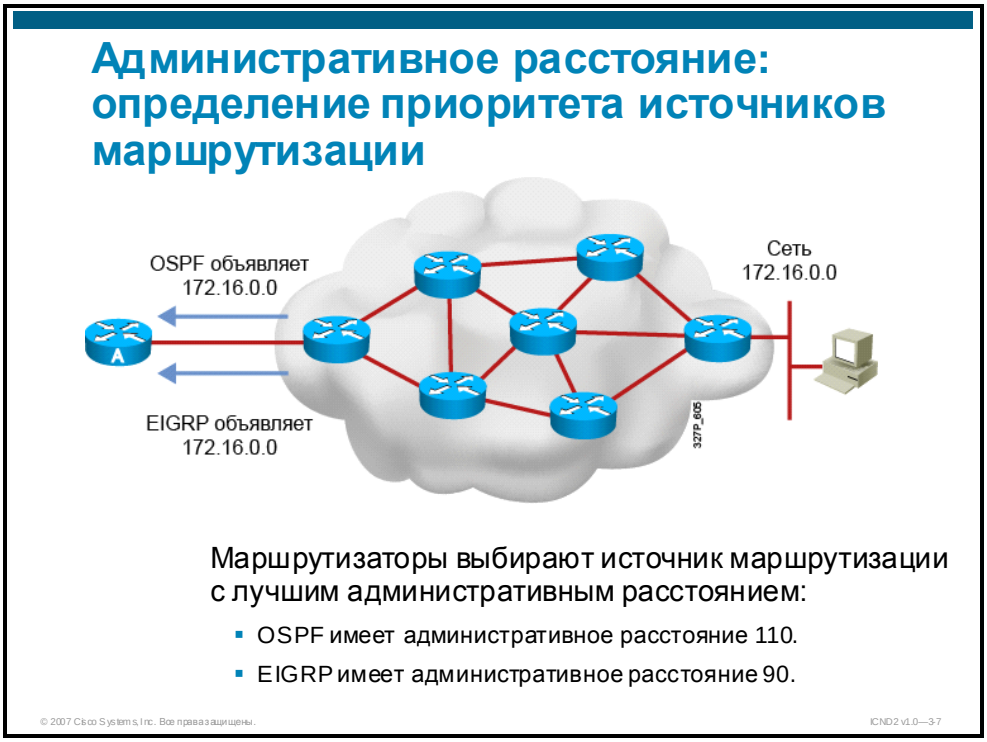
Не существует идеального алгоритма маршрутизации, подходящего для всех интерсетей. Все протоколы маршрутизации предоставляют информацию разными способами.



К месту назначения может существовать несколько маршрутов. Когда алгоритм протокола маршрутизации обновляет таблицу маршрутизации, его главной целью является определение наилучшего маршрута для включения в таблицу. Протоколы вектора расстояния используют разные метрики маршрутизации для определения наилучшего маршрута. Для каждого пути через сеть алгоритм генерирует число, которое называется метрикой. В большинстве случаев меньшая метрика означает лучший путь.

Метрики могут рассчитываться на основе одной из характеристик пути. Более сложные метрики рассчитываются на основе комбинации нескольких характеристик пути. Ниже перечислены метрики, которые используются протоколами маршрутизации.

- **Количество переходов.** Количество переходов пакета через выходной порт маршрутизатора.
- **Полоса пропускания.** Скорость передачи данных канала, например Ethernet-канал с полосой пропускания 10 Мбит/с является более предпочтительным, чем выделенный канала 64 Кбит/с.
- **Задержка.** Период времени, который требуется для передачи пакета от источника к месту назначения.
- **Загрузка.** Активность сетевого ресурса, например маршрутизатора или канала.
- **Надежность.** Как правило, относится к частоте возникновения ошибочных битов в сетевом канале.
- **Стоимость.** Настраиваемое значение. На маршрутизаторах Cisco определяется полосой пропускания интерфейса (по умолчанию).



Большинство протоколов маршрутизации можно использовать вместе со статическими маршрутами. Если в сети доступно несколько источников данных маршрутизации, для определения степени доверия к этим источником используется административное расстояние. Значения административного расстояния позволяют ПО Cisco IOS выбирать источники данных маршрутизации.

Пример: административное расстояние

Административное расстояние — это целое число от 0 до 255. Протокол маршрутизации с меньшим административным расстоянием считается более надежным, чем протокол с более высоким административным расстоянием. Как показано на рисунке, если маршрутизатор A одновременно получит маршруты к сети 172.16.0.0, объявленные протоколами EIGRP и OSPF, он определит, что протокол EIGRP более надежен, с помощью административного расстояния. Затем маршрутизатор A добавит маршрут EIGRP в таблицу маршрутизации.

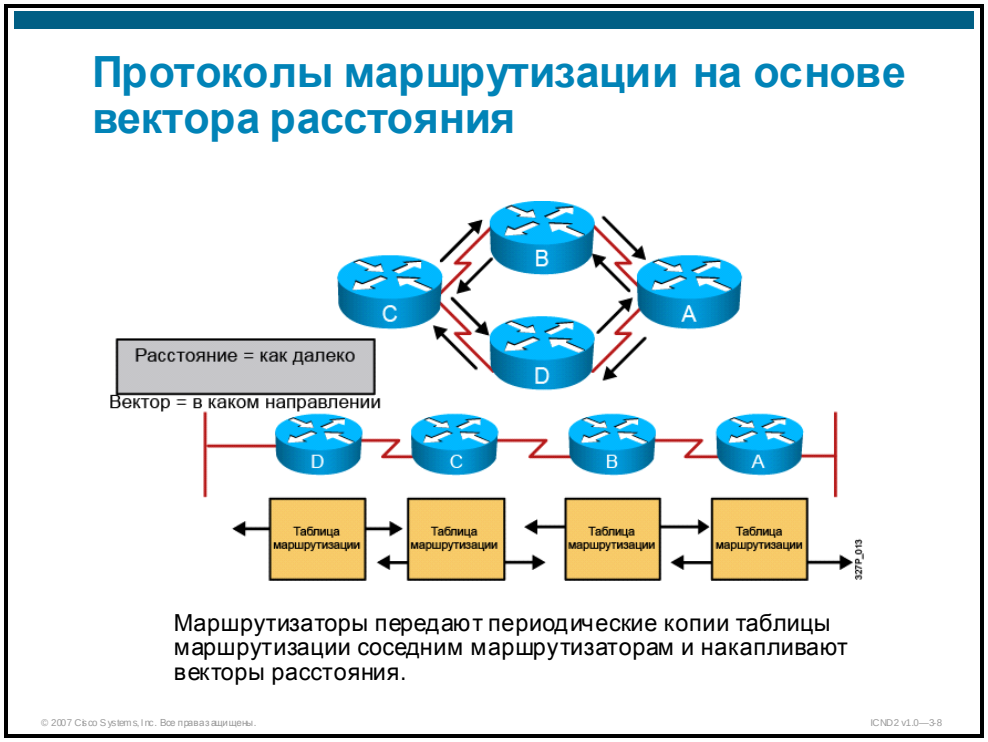
В таблице приводятся административные расстояния по умолчанию для некоторых источников данных маршрутизации.

Источник маршрутов	Расстояние по умолчанию
Подключенная сеть	0
Статический маршрут	1
EIGRP	90
OSPF	110
RIPv2	120
External EIGRP	170
Неизвестный или непредусмотренный	255 (не будет использоваться для передачи трафика)

Если необходимы значения, отличные от стандартных, вы можете настроить административное расстояние для отдельных маршрутизаторов, протоколов и маршрутов с помощь ПО Cisco IOS.

Общие сведения о протоколах вектора расстояния

В этом разделе описывается принцип работы и внедрение протоколов маршрутизации на основе вектора расстояния.



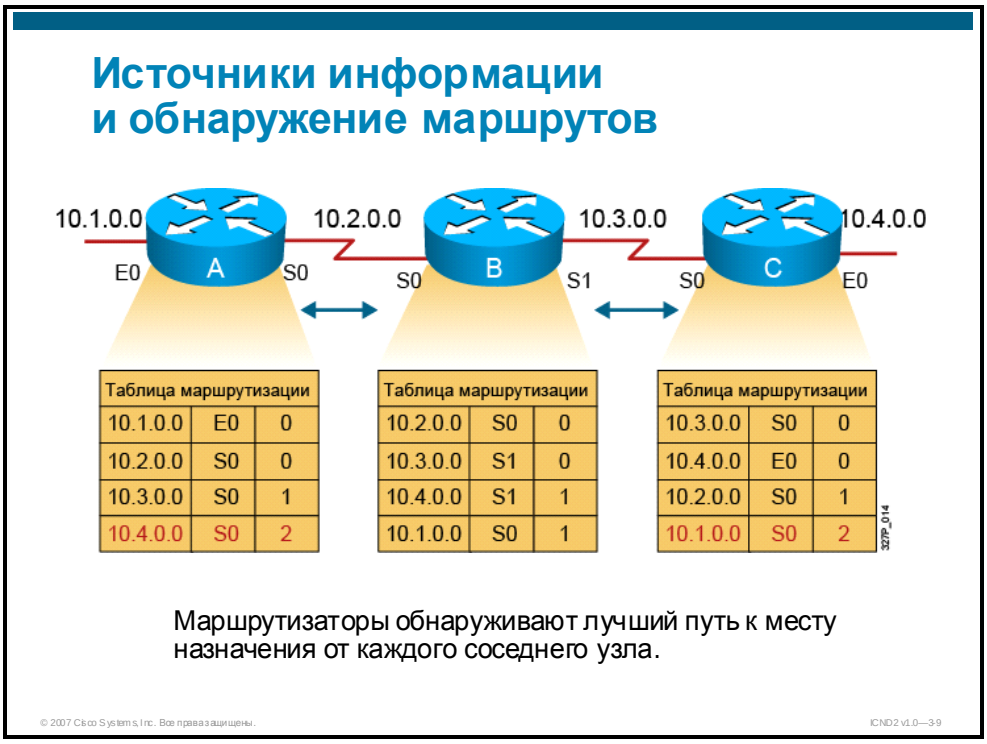
Периодические обновления данных маршрутизации большинства протоколов маршрутизации на основе векторов расстояния направляются только маршрутизаторам с прямым подключением. В качестве схемы адресации используется логическая широковещательная рассылка. Маршрутизаторы под управлением протоколов на основе векторов расстояния рассылают периодические обновления, даже если в сеть не вносились изменения.

В средах, использующих только алгоритм векторов расстояния, периодические обновления включают полную таблицу маршрутизации. Получив полную таблицу маршрутизации от соседнего узла, маршрутизатор может проверить все известные маршруты и изменить локальную таблицу маршрутизации в соответствии с обновленными данными. Этот процесс также называется "маршрутизацией по слухам", так как маршрутизатор получает данные о сети топологии сети с точки зрения соседнего маршрутизатора.

Пример: протоколы маршрутизации на основе вектора расстояния

Маршрутизатор B получает периодическое обновление от маршрутизатора A. Маршрутизатор B добавляет метрику вектора расстояния (например, число переходов) для каждого маршрута, полученного от маршрутизатора A, повышая вектор расстояния. Затем маршрутизатор B передает полную таблицу маршрутизации своему соседнему узлу, маршрутизатору C. Этот поэтапный процесс выполняется во всех направлениях между соседними маршрутизаторами, с прямым подключением друг к другу.

Традиционно протоколы вектора расстояния также являлись классовыми протоколами. Протоколы RIPv2 и EIGRP — примеры более совершенных протоколов вектора расстояния, работающих в бесклассовом режиме. EIGRP также имеет ряд характеристик протоколов, использующих алгоритм состояния канала.



На рисунке интерфейсы сетей с прямым подключением имеют расстояние 0.

На последующих этапах процесса обнаружения сети по алгоритму векторов расстояния, маршрутизаторы обнаруживают сети назначения, не имеющие прямого подключения к ним, с помощью накопительных метрик, полученных от каждого соседнего узла. Соседние маршрутизаторы предоставляют сведения о маршрутах, не имеющих прямого подключения к данному маршрутизатору.

Пример: источники информации для обнаружения маршрутов

Маршрутизатор A получает сведения о сетях, которые не имеют прямого подключения к нему (10.3.0.0 и 10.4.0.0), используя информацию, полученную от маршрутизатора B. Во всех записях сетей в таблице маршрутизации задается накопительный вектор расстояния, который указывает расстояние до сети в выбранном направлении.

Обслуживание данных маршрутизации

Таблицы маршрутизации должны обновляться при изменениях топологии интерсети. Как и процесс обнаружения сети, процесс обновления топологии выполняется поэтапно от маршрутизатора к маршрутизатору.

Алгоритмы вектора расстояния заставляют каждый маршрутизатор отправить полную таблицу маршрутизации всем своим соседям. Обновления маршрутизации по алгоритму векторов расстояния рассылаются через регулярные интервалы. Кроме того, таблица маршрутизации может быть отправлена немедленно с помощью триггерных обновлений, которые рассылаются, когда маршрутизатор обнаруживает изменение топологии.

Когда маршрутизатор получает обновление от соседнего маршрутизатора, он сравнивает его со своей таблицей маршрутизации. Чтобы сформировать новую метрику, маршрутизатор добавляет стоимость перехода к соседнему маршрутизатору к стоимости пути, о которой сообщил маршрутизатор. Если маршрутизатор получает данные о лучшем маршруте (с меньшей совокупной метрикой) от соседа, он обновляет свою таблицу маршрутизации. Каждая запись таблицы маршрутизации включает данные о совокупной стоимости пути (определяется метрикой таблицы маршрутизации) и логические адреса первых маршрутизаторов путей ко всем сетям, заданным в таблице маршрутизации.

Пример: обслуживание данных маршрутизации

На рисунке стоимость канала от маршрутизатора B к маршрутизатору A равняется 1. Маршрутизатор B добавляет единицу к совокупной стоимости, переданной маршрутизатором A, когда маршрутизатор B запустил процессы вектора расстояния для обновления своей таблицы маршрутизации.

Пример: счет до бесконечности

Перед отказом сети 10.4.0.0 у всех маршрутизаторов были верные таблицы маршрутизации и согласованные данные. Состояние такой сети называется конвергенцией. Маршрутизатор C имеет прямое подключение к сети 10.4.0.0, расстояние равно 0 (переход). Путь от маршрутизатора A к сети 10.4.0.0 проходит через маршрутизатор B, количество переходов равняется двум.

Счет до бесконечности

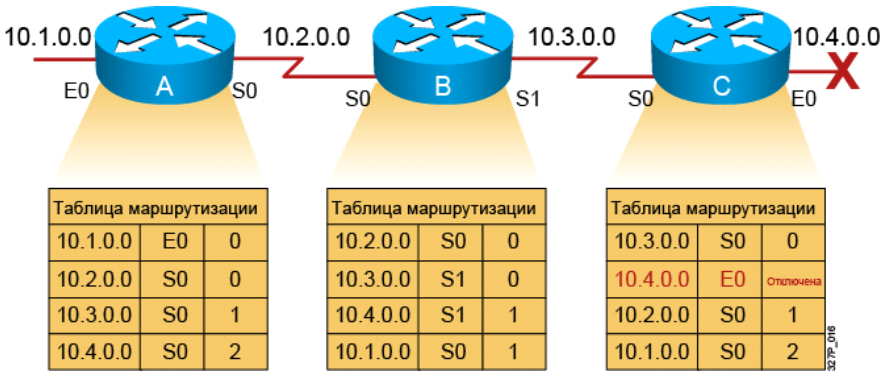


Таблица маршрутизации		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

Таблица маршрутизации		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	S0	1

Таблица маршрутизации		
10.3.0.0	S0	0
10.4.0.0	E0	Отключена
10.2.0.0	S0	1
10.1.0.0	S0	2

327P_016

Медленная конвергенция является причиной несогласованной маршрутизации.

Когда сеть 10.4.0.0 отказывает, маршрутизатор C обнаруживает отказ и прекращает маршрутизацию пакетов из интерфейса E0. Однако на этом этапе маршрутизаторы A и B не получают уведомления об отказе. Маршрутизатор A продолжает считать, что у него есть доступ к сети 10.4.0.0 через маршрутизатор B. Таблица маршрутизации маршрутизатора A все еще содержит путь к сети 10.4.0.0 с расстоянием 2.

Счет до бесконечности (прод.)

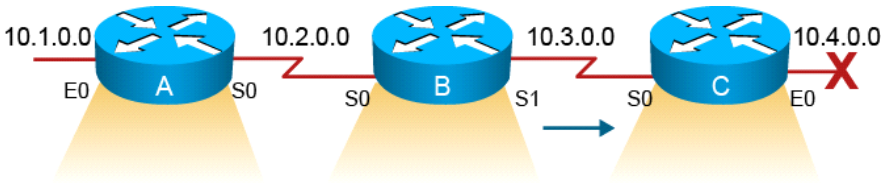


Таблица маршрутизации		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

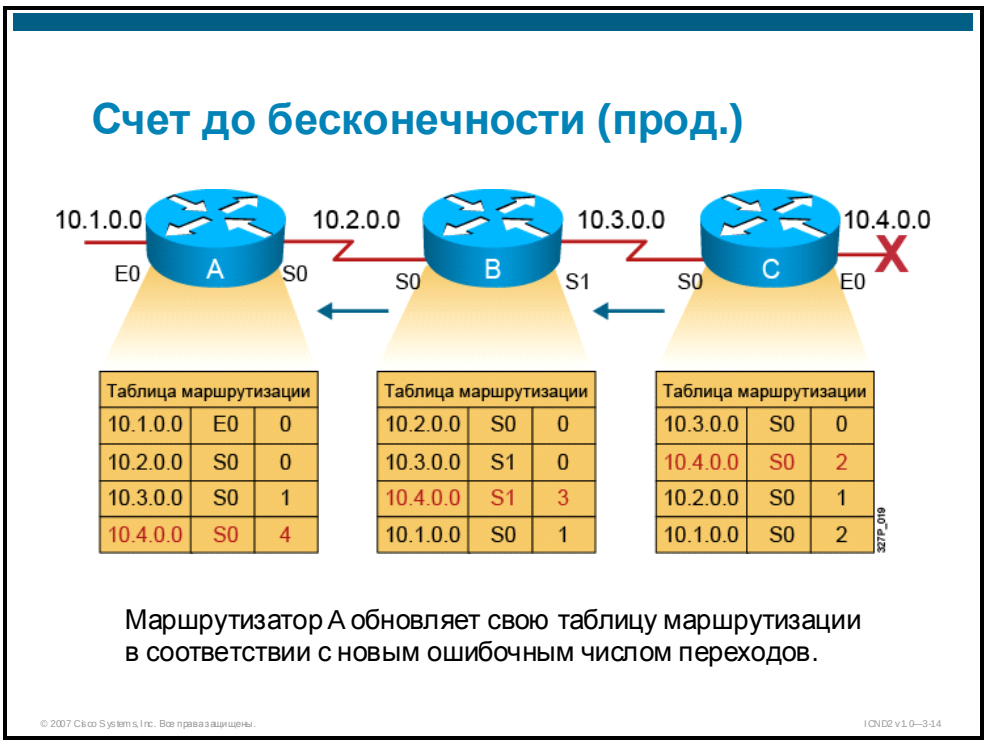
Таблица маршрутизации		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	S0	1

Таблица маршрутизации		
10.3.0.0	S0	0
10.4.0.0	S0	2
10.2.0.0	S0	1
10.1.0.0	S0	2

327P_016

Маршрутизатор C заключает, что лучший путь к сети 10.4.0.0 лежит через маршрутизатор B.

Когда маршрутизатор B отправляет периодическую копию своей таблицы маршрутизации в маршрутизатор C, маршрутизатор C считает, что он имеет исправный путь к сети 10.4.0.0 через маршрутизатор B. Маршрутизатор C обновляет свою таблицу маршрутизации, чтобы добавить путь к сети 10.4.0.0 через маршрутизатор B с количеством переходов равным 2.



Маршрутизатор B получает новое обновление от маршрутизатора C и обновляет свою таблицу, добавляя новую стоимость (3 перехода). Маршрутизатор A получает новую таблицу маршрутизации от маршрутизатора B, обнаруживает обновленный вектор расстояния к сети 10.4.0.0 и перерассчитывает свой собственный вектор расстояния до 10.4.0.0. Новое значение равняется 4.

Счет до бесконечности (прод.)

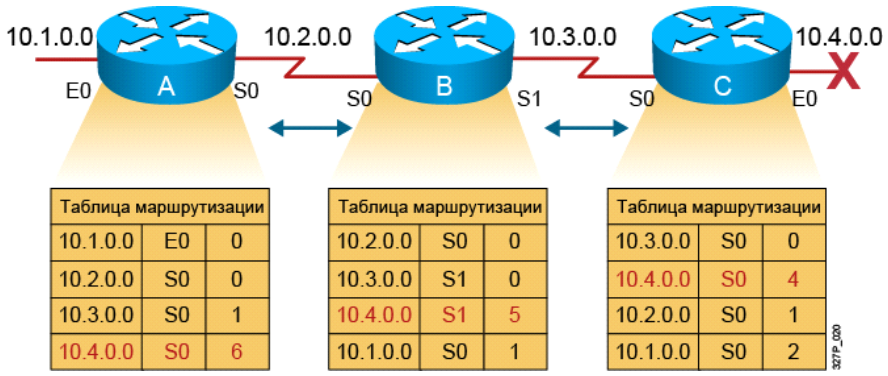


Таблица маршрутизации		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	6

Таблица маршрутизации		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	5
10.1.0.0	S0	1

Таблица маршрутизации		
10.3.0.0	S0	0
10.4.0.0	S0	4
10.2.0.0	S0	1
10.1.0.0	S0	2

3279_080

Число переходов к сети 10.4.0.0 увеличивается до бесконечности.

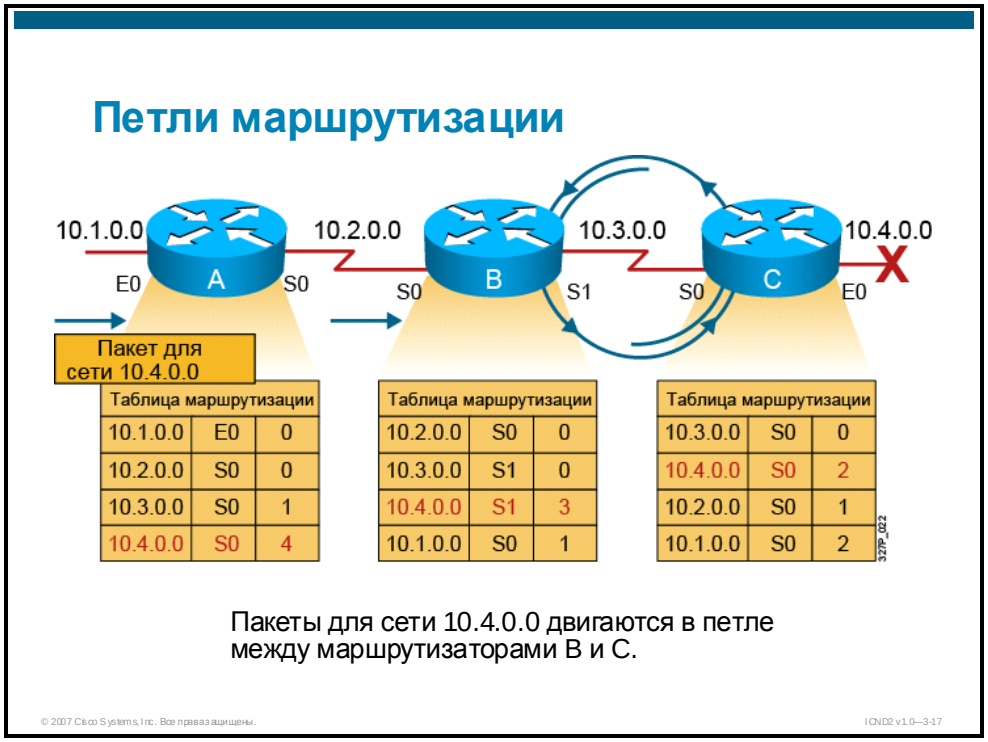
На этот момент таблицы маршрутизации всех трех маршрутизаторов неверны. Они показывают, что сеть 10.4.0.0 достижима через пути, которые не существуют, с количествами переходов, которые не имеют смысла. Рассылка обновлений таблицы маршрутизации продолжится, и количество переходов будет расти (проблема счета до бесконечности). Пакеты, направленные в сеть 10.4.0.0, никогда не достигнут места назначения. Вместо этого они будут непрерывно двигаться между маршрутизаторами, создавая петлю маршрутизации.

Если другой процесс не остановит образование петли, маршрутизаторы будут обновлять друг друга некорректными данными, не осознавая, что сеть 10.4.0.0 отключена. Без контрмер, которые могли бы остановить этот процесс, количество переходов вектора расстояния будет увеличиваться при каждой передаче обновления таблицы маршрутизации в другой маршрутизатор. Обновления продолжат распространяться, поскольку место назначения никогда не будет отмечено как недоступное.

Решение проблемы счета до бесконечности — задание максимума. Протоколы вектора расстояния определяют бесконечность как некое максимальное число. Это число относится к одной из метрик маршрутизации, например к количеству переходов.

Пример: задание максимума предотвращает счет до бесконечности

На рисунке ниже показано максимальное значение в 16 переходов. Когда метрика превышает максимально допустимое значение, сеть 10.4.0.0 объявляется недоступной, и распространение обновлений маршрутизации, увеличивающих метрику, прекращается.



Задание максимального значение решает проблемы бесконечного роста метрики, но также необходимо предотвратить образование петли маршрутизации. Петля маршрутизации образуется, когда два или более маршрутизаторов имеют данные маршрутизации, которые неверно указывают на действующий путь к недоступному месту назначения через другие маршрутизаторы.

Существует несколько методов предотвращения образования петель маршрутизации. В их числе: Split horizon, Route poisoning, Poison reverse, таймеры удержания и триггерные обновления.

Пример: петли маршрутизации

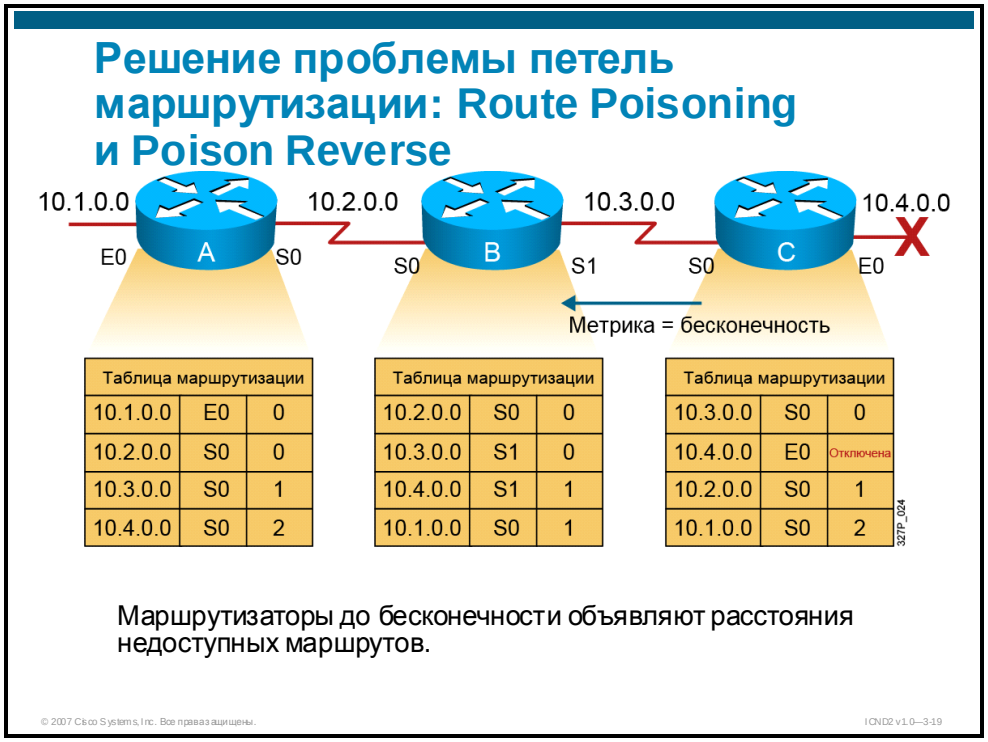
В этом примере пакет направленный в сеть 10.4.0.0 прибывает на маршрутизатор A. В соответствии со своей таблицей маршрутизации маршрутизатор A пересылает пакет через интерфейс S0. Пакет прибывает на маршрутизатор B, который пересылает его через интерфейс S1, в соответствии со своей таблицей маршрутизации. Маршрутизатор C получает этот пакет и проверяет его таблицу маршрутизации, которая указывает, что пакет следует переслать через интерфейс S0. Таким образом пакет возвращается в маршрутизатор B, который снова пересылает пакет в маршрутизатор C через интерфейс S1. Пакет попадает в бесконечную петлю между маршрутизаторами B и C.

Один из методов, позволяющих исключить образование петель маршрутизации и ускорить конвергенцию, называется Split horizon (горизонт разделения). Основное правило Split horizon — не следует посылать информацию о маршруте в обратном направлении, т. е. к источнику исходных данных.

Пример: Split Horizon

На рисунке описывается, как метод Split horizon исключает образование петель маршрутизации.

- Маршрутизатор B имеет доступ к сети 10.4.0.0 через маршрутизатор C. Маршрутизатору B нет никакого смысла объявлять маршрутизатору C, что маршрутизатор B имеет доступ к сети 10.4.0.0 через маршрутизатор C.
- Если маршрутизатор B передал объявление о своем маршруте к сети 10.4.0.0 в маршрутизатор A, маршрутизатору A не имеет смысла объявлять о расстоянии от сети 10.4.0.0 до маршрутизатора B.
- Когда маршрутизатор C объявляет о том, что его подключение к сети 10.4.0.0 недоступно, маршрутизатор B видит, что альтернативный путь к сети 10.4.0.0 отсутствует и заключает, что она недоступна. Маршрутизатор C не использует маршрутизатор B, чтобы достичь сети 10.4.0.0.



Route poisoning — еще один механизм, предотвращающий образование петель маршрутизации. При использовании этой функции маршрутизатор создает запись таблицы, которая поддерживает согласованность состояния сети, пока на других маршрутизаторах выполняется конвергенция изменения топологии.

Пример: Route Poisoning

Когда сеть 10.4.0.0 перестает быть доступной, маршрутизатор C «отравляет» свой канал к сети 10.4.0.0, отправляя обновление для этого канала, которое сообщает, что канал имеет бесконечную метрику и количество переходов равное 16 (это значит, что сеть недоступна). Благодаря отравлению маршрута маршрутизатора C к сети 10.4.0.0 этот маршрутизатор становится невосприимчивым к неверным обновлением, относящимся к сети 10.4.0.0 и поступающих от соседних маршрутизаторов, которые могут объявлять о действующем альтернативном пути.

Решение проблемы петель маршрутизации: Route Poisoning и Poison Reverse (прод.)

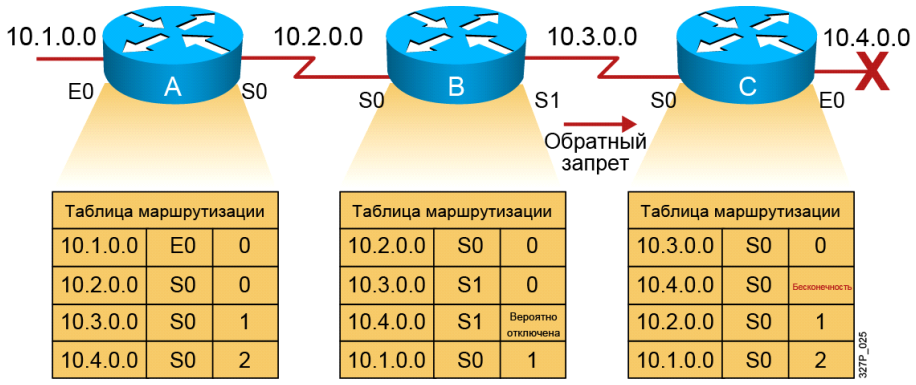


Таблица маршрутизации		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

Таблица маршрутизации		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	Вероятно отключена
10.1.0.0	S0	1

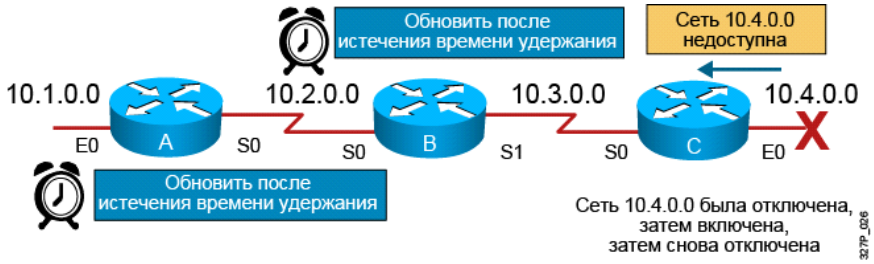
Таблица маршрутизации		
10.3.0.0	S0	0
10.4.0.0	S0	Бесконечность
10.2.0.0	S0	1
10.1.0.0	S0	2

327P_025

Функция Poison reverse переопределяет метод Split horizon.

Когда маршрутизатор B видит, что метрика сети 10.4.0.0 стала бесконечно, он отправляет обновление, которое называется Poison reverse, в обратно в маршрутизатор C. Обновление Poison reverse указывает, что сеть 10.4.0.0 недоступна. Poison reverse является особым состоянием, переопределяющим метод Split horizon. Оно обеспечивает невосприимчивость маршрутизатора C к неверным обновлениям, относящимся к сети 10.4.0.0.

Решение проблемы петель маршрутизации: таймеры удержания



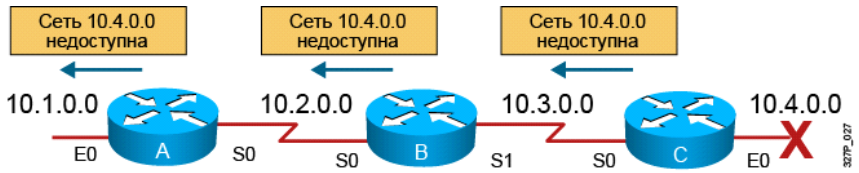
Маршрутизатор поддерживает запись о том, что сеть находится в состоянии «предположительно недоступна», что дает другим маршрутизаторам достаточно времени для повторного вычисления маршрутов с учетом изменения топологии.

Таймеры удержания используются для предотвращения регулярных обновлений, указывающих на маршрут, который может быть недоступен. Таймеры удержания не позволяют маршрутизаторам применять изменения маршрутов в течение определенного периода времени. Период удержания зависит от протокола маршрутизации, но как правило равен трем интервалам периодического обновления протокола векторного расстояния.

Таймеры удержания работают следующим образом.

- Когда маршрутизатор получает обновление от соседнего узла, которое указывает, что доступная сеть стала недоступной, маршрутизатор отмечает маршрут как "предположительно недоступный" и запускает таймер удержания.
- Если от соседнего маршрутизатора приходит обновление с лучшей метрикой, чем исходная метрика сети, маршрутизатор отмечает сеть как «доступную» и удаляет таймер удержания.
- Если во время работы таймера приходит обновление от другого соседнего маршрутизатора с худшей или такой же метрикой, обновление игнорируется. Пропуск обновлений с худшей или такой же метрикой во время работы таймера удержания дает больше времени для распространения изменения на всю сеть.
- Во время периода удержания маршруты заносятся в таблицу маршрутизации как "предположительно недоступные". Маршрутизатор будет направлять пакеты в предположительно недоступные сети (если проблемы сети с подключением носят прерывистый характер, такая ситуация называется периодическим пропаданием канала).

Триггерные обновления



Маршрутизатор отправляет обновления при изменении таблицы маршрутизации.

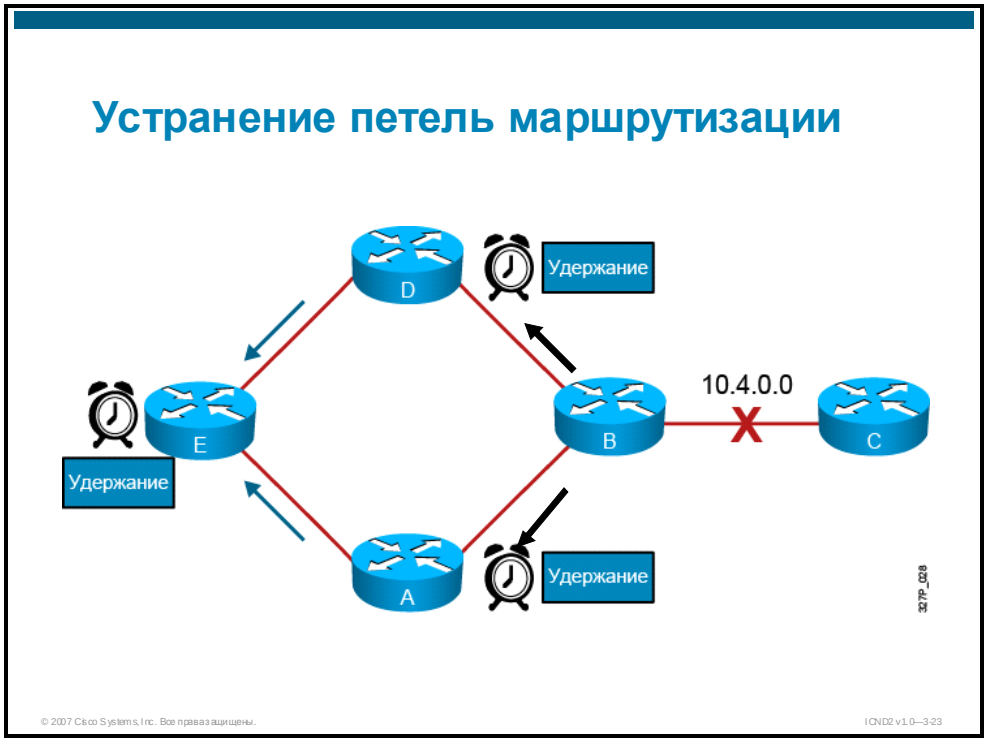
В предыдущем примере петли маршрутизации были вызваны циркуляцией ошибочной информации, рассчитанной в результате несогласованных обновлений, медленной конвергенции и задержек. Кроме того, проблема медленной конвергенции может возникнуть, если маршрутизаторы ждут регулярных плановых обновлений перед оповещением соседних коммутаторов об изменениях сети.

Как правило, обновления таблицы маршрутизации отправляются в соседние маршрутизаторы через регулярные интервалы. Триггерное обновление таблицы маршрутизации отправляется немедленно в ответ на определенное изменение. Маршрутизатор, обнаруживший изменение, немедленно отправляет обновление смежным маршрутизаторам, которые, в свою очередь, генерируют триггерные обновления, оповещающие их соседей об изменении. Эта волна оповещений распространяется по всему фрагменту сети, маршруты которого проходят через измененный канал.

Триггерные обновления были бы достаточной мерой, если бы гарантировали своевременную доставку оповещений всем нужным маршрутизаторам. Однако здесь возникает две проблемы.

- Пакеты с обновлением могут быть отброшены или повреждены одним из каналов сети.
- Триггерные обновления не применяются мгновенно. Существует вероятность, что маршрутизатор, который еще не получил триггерного обновления, отправит регулярное обновление в неудачное время, что приведет к повторной установке маршрута в соседний узел, который уже получил триггерное обновление.

Эту проблему можно предотвратить, объединив таймеры удержания и триггерные обновления. Правило удержания запрещает добавление маршрутов с метрикой, равной или худшей, чем метрика маршрута на удержании (предположительно недоступного). Это даст триггерному обновлению достаточно времени для распространения по сети.



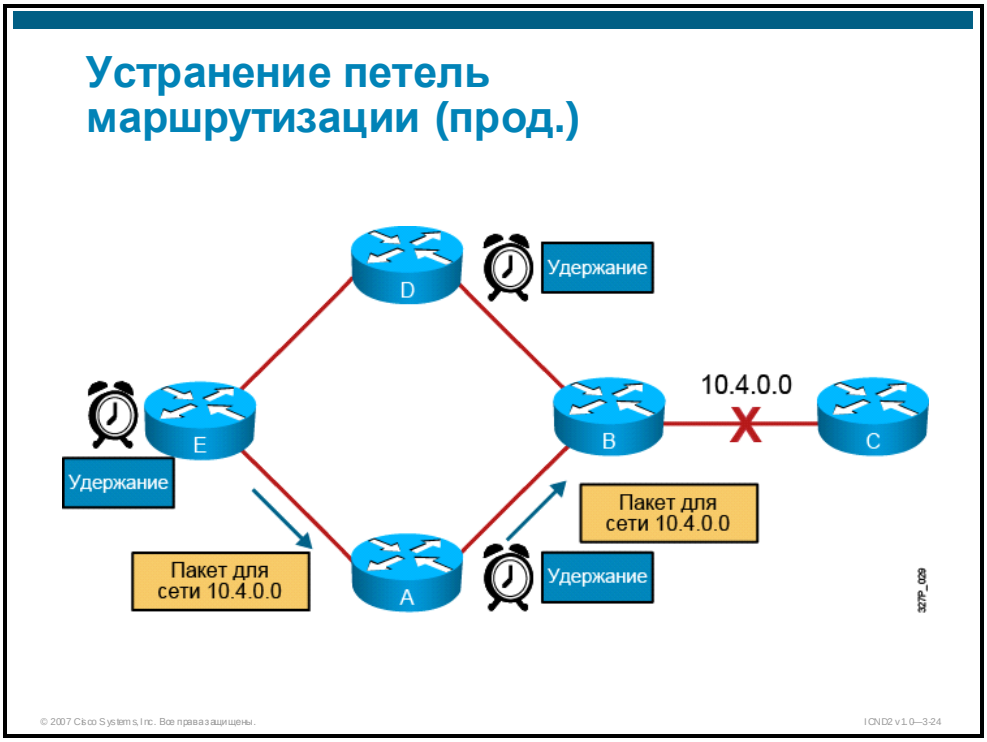
Пример: методики исключения петель маршрутизации

Маршрутизатор A, D и E имеют несколько маршрутов к сети 10.4.0.0. Как только маршрутизатор B обнаруживает отказ сети 10.4.0.0, он удаляет свой маршрут к этой сети. Маршрутизатор B отправляет триггерное обновление маршрутизаторам A и D, "отравляя" маршрут к сети 10.4.0.0 путем задания бесконечной метрики для этой сети.

Маршрутизаторы D и A получают триггерное обновление и устанавливают свои таймеры удержания, указывающие, что сеть 10.4.0.0 предположительно недоступна. Маршрутизаторы D и A в свою очередь отправляют триггерное обновление маршрутизатору E, указывая на возможную недоступность сети 10.4.0.0. Маршрутизатор E также переводит маршрут к сети 10.4.0.0 в состояние удержания.

Маршрутизаторы A и D отправляют обновление Poison reverse маршрутизатору B. Обновление указывает на то, что сеть 10.4.0.0 недоступна.

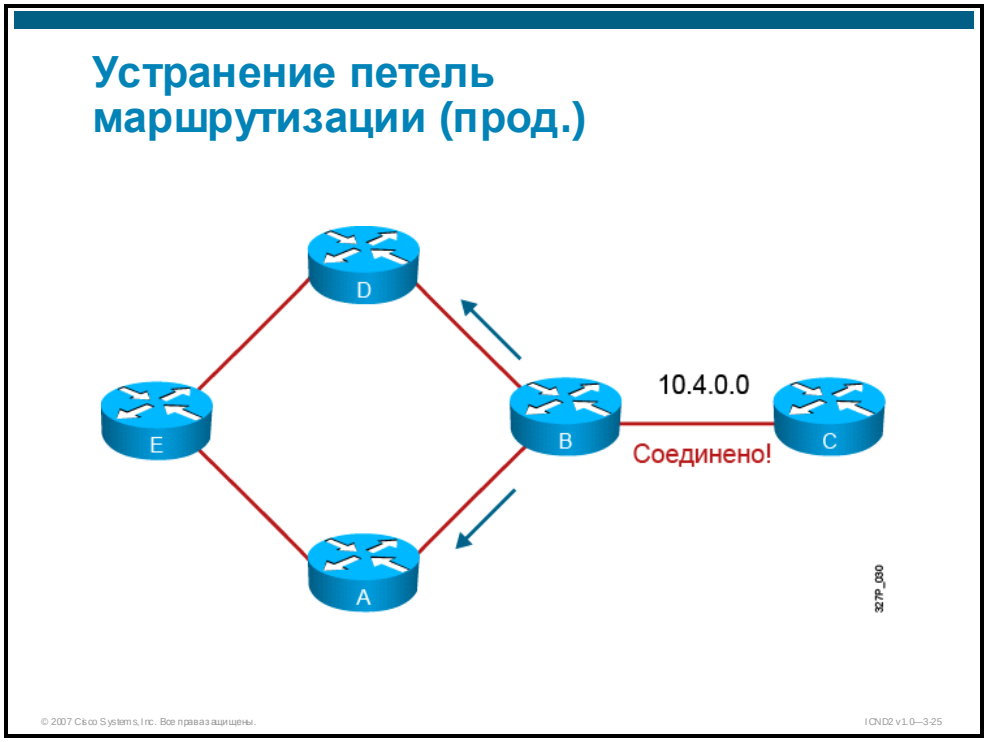
Поскольку маршрутизатор E получил триггерное обновление от маршрутизаторов A и D, маршрутизатор E также отправляет обновление Poison reverse маршрутизаторам A и D.



Маршрутизаторы A, D и E останутся на удержании, пока не произойдет одно из следующих событий.

- Таймер удержания истекает.
- Приходит обновление, указывающее на новый маршрут с лучшей метрикой.
- Таймер сброса удаляет маршрут из таблицы маршрутизации.

Во время периода удержания маршрутизаторы A, D и E заключают, что сеть предположительно недоступна и пытаются направить пакеты в сеть 10.4.0.0. На рисунке ниже показана попытка маршрутизатора E переслать пакет в сеть 10.4.0.0. Этот пакет дойдет до маршрутизатора B. Однако поскольку маршрутизатор B не имеет маршрута 10.4.0.0, он отбросит пакет и отправит сообщение ICMP «network unreachable».



Когда канал 10.4.0.0 становится активным, маршрутизатор B отправляет триггерное обновление для оповещения маршрутизаторов A и D. После истечения таймера удержания, маршрутизаторы A и D изменяют состояние маршрутов к 10.4.0.0 с "предположительно недоступен" на "доступен"..

Маршрутизаторы A и D отправляют маршрутизатору E обновление, которое указывает, что сеть 10.4.0.0 доступна. Маршрутизатор E обновляет свою таблицу маршрутизации по истечении таймера удержания.

Общие сведения о протоколах маршрутизации на основе состояния канала

Для обслуживания данных маршрутизации алгоритм состояния канала использует объявления состояния канала (LSA), топологическую базу данных, алгоритм SPF, дерево SPF и таблицу маршрутизации с путями и портами для каждой сети. Примеры протоколов состояния канала: OSPF и IS-IS (транзитная система — транзитная система). IS-IS — это протокол маршрутизации, который как правило используется крупными поставщиками услуг Интернета (ISP). Он не рассматривается в этом курсе. В этом разделе описывается принцип работы и внедрение протоколов маршрутизации на основе состояния канала, и в частности протокола OSPF.

OSPF классифицируется как протокол маршрутизации на основе состояния канала. Концепции и принципы работы состояния канала OSPF описываются в стандарте RFC 2328. Протоколы маршрутизации на основе состояния канала собирают данные маршрутизации от всех других маршрутизаторов в сети или от маршрутизаторов в заданной области сети. После сбора всех необходимых данных, каждый маршрутизатор, независимо от других маршрутизаторов, рассчитывает оптимальные маршруты ко всем местам назначения в сети. Поскольку каждый маршрутизатор поддерживает собственное представление сети, вероятность того, что маршрутизатор начнет распространять неверные сведения, полученные от другого маршрутизатора, невысока.

Канал аналогичен интерфейсу маршрутизатора. Состояние канала — это описание интерфейса и его отношений с соседними маршрутизаторами. Описание интерфейса должно включать, например, его IP-адрес, маску, тип сети, к которой он подключен, маршрутизаторы, подключенные к этой сети и т. п. Набор состояний канала формирует базу данных состояний канала или топологическую базу данных. База данных состояний канала используется для расчета наилучших путей через сеть. Маршрутизаторы, работающие по алгоритму состояния канала, находят наилучшие пути к местам назначения, применяя алгоритм Дийкстра к базе данных состояний канала, чтобы создать дерево SPF. Затем наилучшие пути выбираются из дерева SPF и помещаются в таблицу маршрутизации.

Способность протоколов состояния канала, таких как OSPF, разделять большую автономную систему на малые группы маршрутизаторов, которые называются областями, называется иерархической маршрутизацией.

При использовании этого метода маршрутизация выполняется и между областями (это называется межобластной маршрутизацией), однако многие частые внутренние операции, такие как повторный расчет базы данных, выполняются внутри области.

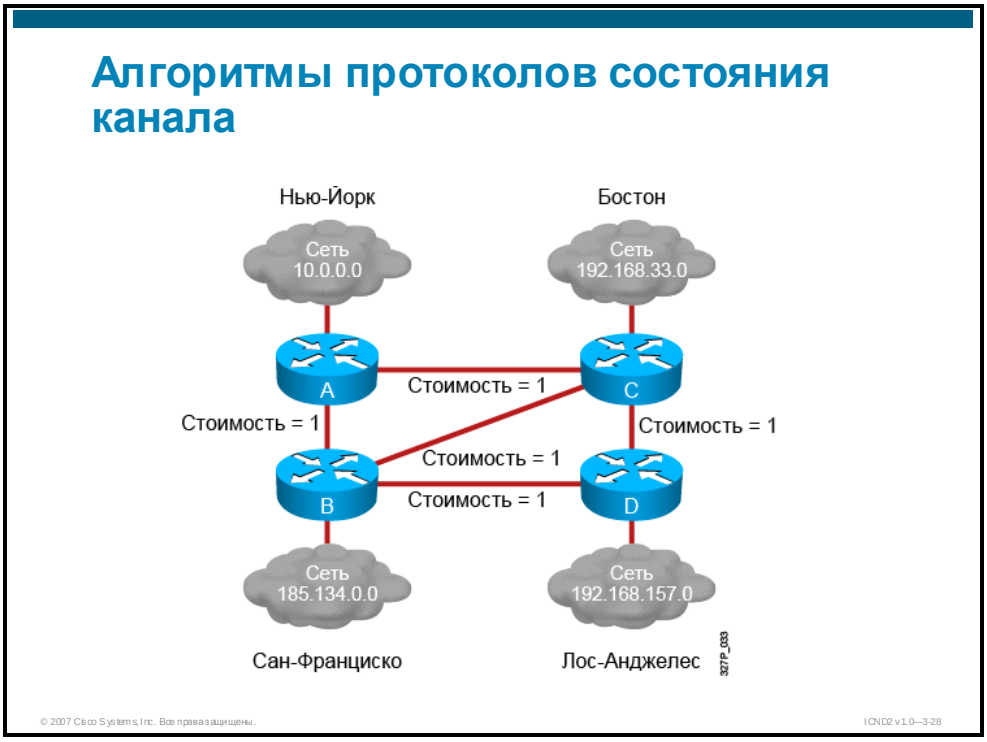
Когда в сети происходит отказ, например когда соседний маршрутизатор становится недоступным, протоколы состояния канала рассылают объявления состояния канала по области, используя особый адрес многоадресной рассылки. Каждый маршрутизатор, работающий по алгоритму состояния канала, принимает копию сообщения о состоянии канала, обновляет свою базу данных состояний канала (топологическую базу данных) и пересылает обновление соседним устройствам. Обновления состояния канала заставляют все маршрутизаторы в области перерассчитывать маршруты. Поскольку объявления состояния канала рассылаются по всей области, и все маршрутизаторы в области должны перерассчитывать свои таблицы маршрутизации, количество маршрутизаторов в области, работающих по алгоритму состояния канала, должно быть ограничено.

Пример: иерархическая маршрутизация OSPF

См. рисунок. Если область 1 испытывает проблемы пропадания канала, маршрутизаторы в других областях не должны постоянно выполнять перерасчет дерева SPF, поскольку они изолированы от проблемы области 1.

Иерархическая топология протокола OSPF предлагает следующие важные преимущества:

- сниженная частота расчета SPF;
- меньшая таблица маршрутизации;
- меньший объем служебных состояния канала.



Алгоритмы протоколов состояния канала

Алгоритмы маршрутизации по методу состояния канала, также известные как протоколы SPF, ведут комплексную базу данных сетевой топологии. В отличие от протоколов вектора расстояния, протоколы состояния канала создают и поддерживают полное представление маршрутизаторов и их соединений. Это представление обеспечивается благодаря обмену объявлениями состояния канала с другими маршрутизаторами сети.

Каждый маршрутизатор, участвующий в обмене объявлениями состояния канала, создает топологическую базу данных с использованием всех полученных объявлений. Затем алгоритм SPF используется для вычисления доступности мест назначения в сети. Эта информация используется для обновления таблицы маршрутизации. Этот процесс обнаруживает изменения в топологии сети, вызванные отказом компонентов или увеличением сети.

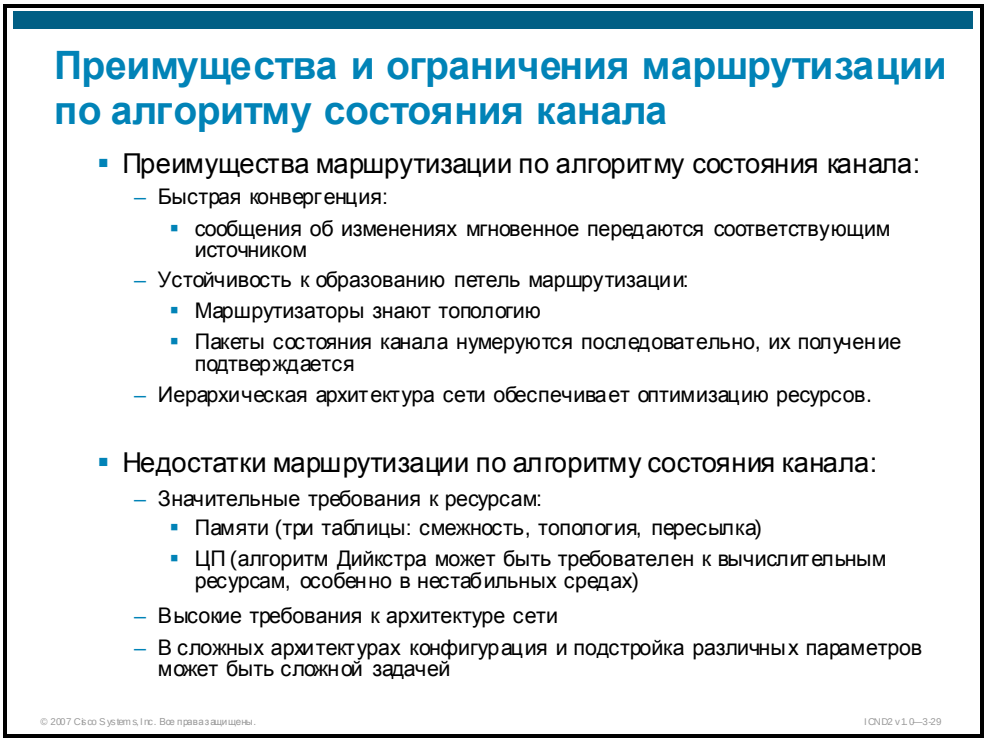
В отличие от периодических обновлений, обмен объявлениями состояния канала инициируется событием в сети. Это может значительно ускорить конвергенцию, поскольку маршрутизаторам не приходится ждать истечения последовательности таймеров, чтобы начать конвергенцию.

Пример: алгоритмы протоколов состояния канала

Если сеть, показанная на рисунке, использует протокол состояния канала, между Нью-Йорком и Сан-Франциско не будет проблем подключения. В зависимости от фактически используемого протокола и выбранных метрик, протокол маршрутизации с высокой долей вероятности выберет лучший из двух путей. В таблице приводится сводка содержимого таблиц маршрутизации.

Маршрутизатор	Назначение	Следующий переход	Стоимость
A	185.134.0.0	B	1
A	192.168.33.0	C	1
A	192.168.157.0	B	2
A	192.168.157.0	C	2
B	10.0.0.0	A	1
B	192.168.33.0	C	1
B	192.168.157.0	D	1
C	10.0.0.0	A	1
C	185.134.0.0	B	1
C	192.168.157.0	D	1
D	10.0.0.0	B	2
D	10.0.0.0	C	2
D	185.134.0.0	B	1
D	192.168.33.0	C	1

Записи таблицы маршрутизации для Нью-Йорка (маршрутизатор A) и Лос-Анжелеса (маршрутизатор D) показывают, что протокол маршрутизации запомнил бы оба маршрута. Некоторые протоколы состояния канала предоставляют способ оценки производительности этих двух маршрутов и дают приоритет пути с лучшей производительностью. Если протокол с лучшей производительностью, например маршрут через Бостон (маршрутизатор C), испытывает какие либо трудности, например перегрузку или отказ компонентов, протокол состояния канала обнаружит это и начнет пересылать пакеты через Сан-Франциско (маршрутизатор B).



Преимущества и ограничения маршрутизации по алгоритму состояния канала

Ниже описываются некоторые из многочисленных преимуществ протоколов маршрутизации на основе состояния канала по сравнению с традиционными протоколами вектора расстояния.

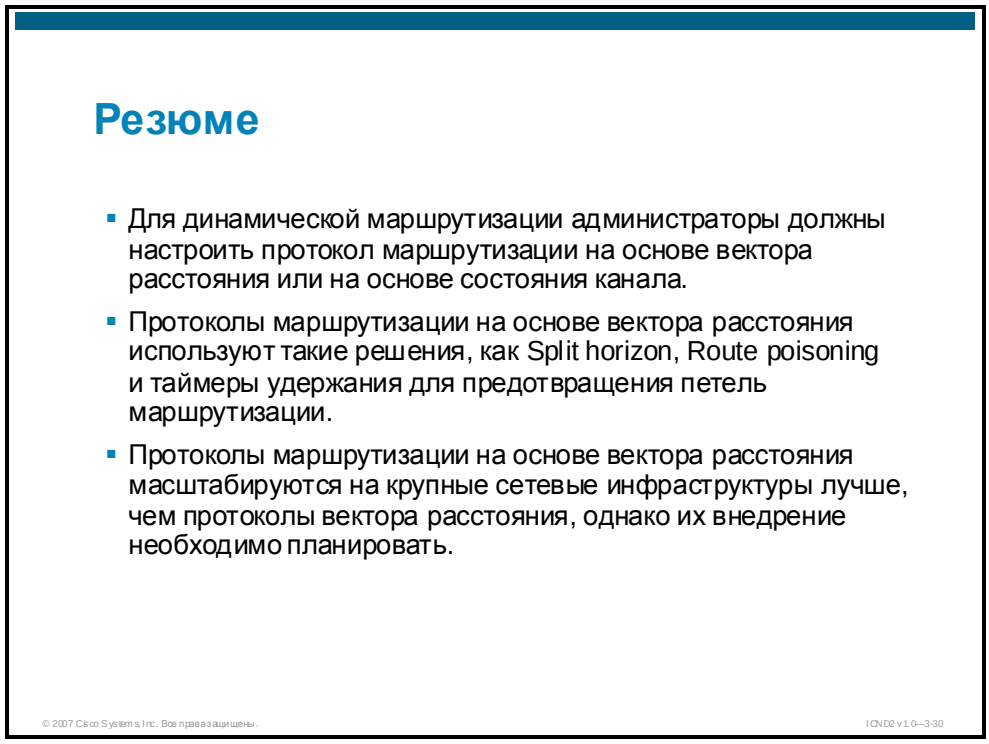
- Протоколы состояния канала используют метрики стоимости для выбора между путями через сеть. Метрика стоимости отражает полосу пропускания каналов, которые входят в эти пути.
- Обновления маршрутизации происходят реже.
- Как правило, протоколы состояния канала масштабируются на сети большего размера, чем протоколы вектора расстояния, такие как RIPv2.
- Сеть можно сегментировать в иерархии областей, ограничивая зону распространения изменений маршрутизации.
- Протоколы состояния канала отправляют обновления только при изменении топологии. Благодаря рассылке триггерных обновлений, протоколы состояния канала немедленно сообщают об изменениях топологии всем маршрутизаторам в сети. Это позволяет ускорить конвергенцию.
- Поскольку каждый маршрутизатор имеет полное и синхронизированное представление о сети, возникновение петель маршрутизации крайне маловероятно.
- Поскольку объявления состояния канала нумеруются последовательно и устаревают со временем, решения о маршрутизации принимаются на основе самой последней информации.
- В качественно спроектированной сети размер базы данных состояний канала можно свести к минимуму, что позволит уменьшить объем расчетов по алгоритму Дийкстра и ускорить конвергенцию.

Протоколы состояния канала имеют следующие ограничения.

- В дополнение к таблице маршрутизации, протоколы состояния канала требуют базу данных топологии и базу данных смежности. Все эти базы данных могут потребовать значительного объема памяти в крупных или сложных сетях.
- Алгоритм Дийкстра потребляет циклы ЦП при расчете наилучших путей через сеть. В крупных и сложных сетях (со сложным вычислением по алгоритму Дийкстра), а также в нестабильных сетях (вычисление по алгоритму Дийкстра выполняется регулярно), протоколы состояния канала могут требовать значительной вычислительной мощности.
- Создание иерархии областей может стать причиной проблем, так как области должны оставаться непрерывными. Маршрутизаторы в области должны иметь возможность получать объявления состояния канала от всех прочих маршрутизаторов этой области. В архитектуре, включающей несколько областей, маршрутизатор всегда должен иметь путь к магистрали, или он потеряет подключение к другим частям сети. Кроме того, магистральная область всегда должна оставаться непрерывной, чтобы избежать изоляции (разбиения) областей.
- В сетях со сложной архитектурой протокол состояния канала должен быть настроен для поддержки этой архитектуры. Настройка протокола состояния канала в крупной сети может быть сложной задачей.
- Интерпретация данных, сохраненных в топологии, баз данных соседних узлов и таблицы маршрутизации требует понимания концепций маршрутизации на основе состояния канала.

Резюме

В этом разделе приводится резюме основных вопросов, рассмотренных в занятии.



Занятие 2

Внедрение VLSM

Обзор

Маски подсети переменной длины (VLSM) были разработаны для обеспечения нескольких уровней IP-адресов в подсетях в одной сети. Эту стратегию можно использовать только если она поддерживается протоколом маршрутизации, например RIPv2, OSPF и EIGRP. VLSM является одной из ключевых технологий в крупных коммутируемых сетях. Понимание возможностей VLSM очень важно при планировании крупных сетей. В этом анятии рассматриваются возможности VLSM.

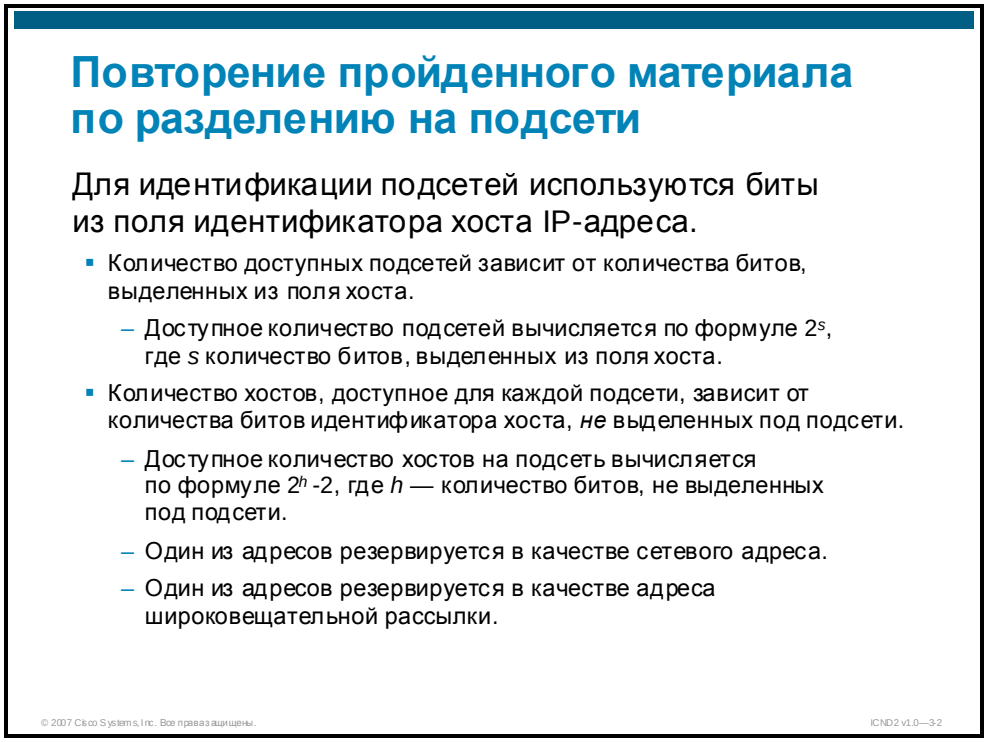
Задачи

По окончании этого занятия вы сможете описывать принцип работы VLSM и бесклассовой маршрутизации между доменами (CIDR) на маршрутизаторах Cisco, а также рассказывать, как маршрутизаторы Cisco реализуют суммирование маршрутов. Это значит, что вы сможете выполнить следующие задачи:

- описывать расчет маски подсети;
- описывать назначение масок VLSM и рассчитывать эти маски;
- описывать процесс суммирования маршрутов и методы, которые используются маршрутизаторами для управления суммированием маршрутов.

Повторение пройденного материала по подсетям

При создании подсетей необходимо определить оптимальное число подсетей и хостов. В этом разделе мы повторим процесс планирования подсетей.



Расчет числа доступных подсетей и хостов

Как вы помните, IP-адрес включает 32 бита и состоит из двух частей: идентификатор сети и идентификатор хоста. Длины сетевого идентификатора и идентификатора хоста зависят от класса IP-адреса. Доступное количество хостов также зависит от класса IP-адреса.

Стандартное количество бит в идентификаторе сети называется длиной классового префикса. Таким образом, адрес класса A имеет длину классового префикса /8, адрес класса B — /16, и адрес класса C — /24.

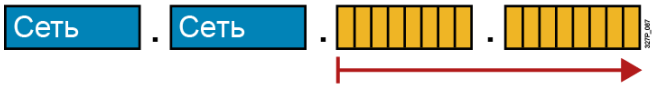
Доступные количества подсетей и хостов для сети класса C

Количество заимствованных битов (s)	Количество возможных подсетей (2s)	Количество бит, оставшихся в идентификаторе узла (8 - s = h)	Количество узлов, допустимых в подсети (2h - 2)
1	2	7	126
2	4	6	62
3	8	5	30
4	16	4	14
5	32	3	6
6	64	2	2
7	128	1	0

Адрес подсети создается из битов части адреса класса A, B или C, выделенной под хоста. Как правило сетевой администратор назначает адреса подсети локально. Как и IP-адреса, адреса подсети должны быть уникальны.

Каждый раз, когда бит берется из поля хоста, количество битов в поле, которое можно использовать для номеров хостов, уменьшается. При этом число адресов хостов, доступных для назначения, уменьшается на два.

Доступные количества подсетей и хостов для сети класса B



Биты, которые необходимо позаимствовать

Количество заимствованных битов (s)	Количество возможных подсетей (2s)	Количество битов, оставшихся в идентификаторе узла (16 - s = h)	Количество узлов, допустимых в подсети (2h - 2)
1	2	15	32,766
2	4	14	16,382
3	8	13	8,190
4	16	12	4,094
5	32	11	2,046
6	64	10	1,022
7	128	9	510
...	...	...	...

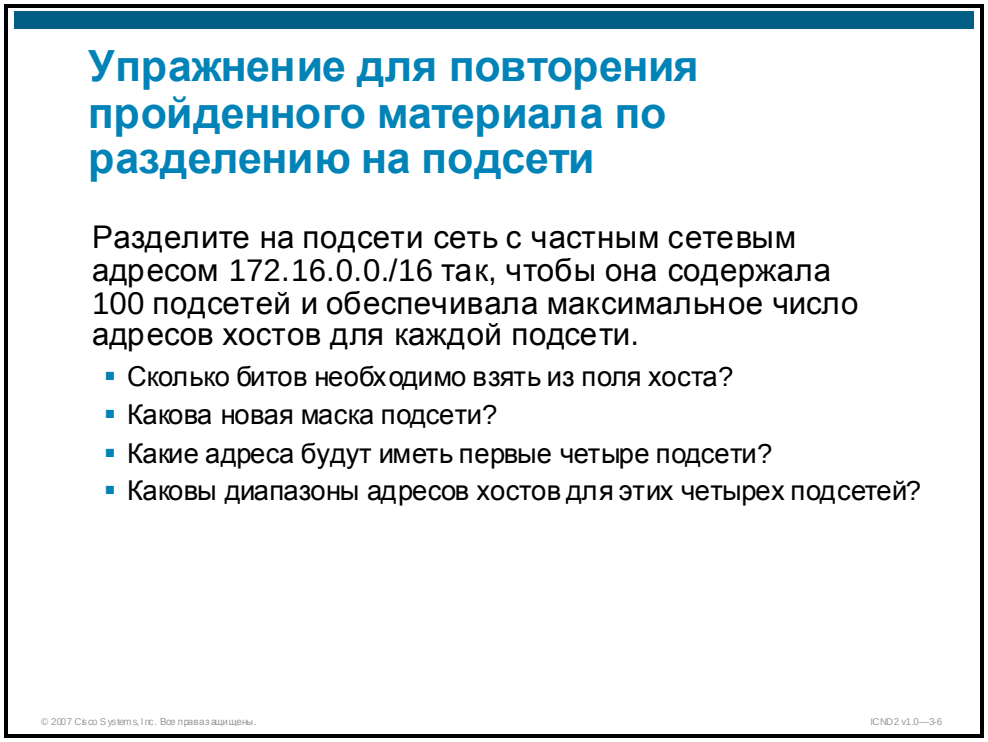
Когда вы берете биты из поля хоста, важно отметить число дополнительных подсетей, которые можно создать из каждого бита. Два бита из поля хоста позволяют создать 4 подсети (22 = 4). Каждый раз, когда вы берете бит из поля хоста, количество возможных подсетей увеличивается на 2, а количество отдельных адресов хостов уменьшается на 2.

Ниже приводятся примеры количества подсетей в зависимости от количества битов, взятых из поля хоста.

- Использование 3-х битов для поля подсети позволяет создать 8 подсетей (23 = 8).
- Использование 4-х битов для поля подсети позволяет создать 16 подсетей (24 = 16).
- Использование 5-х битов для поля подсети позволяет создать 32 подсетей (25 = 32).
- Использование 6-х битов для поля подсети позволяет создать 64 подсетей (26 = 64).

Как правило, для расчета числа доступных подсетей в зависимости от числа битов можно использовать следующую формулу:

- Число подсетей = 2s (где s — количество битов, используемых для подсетей)

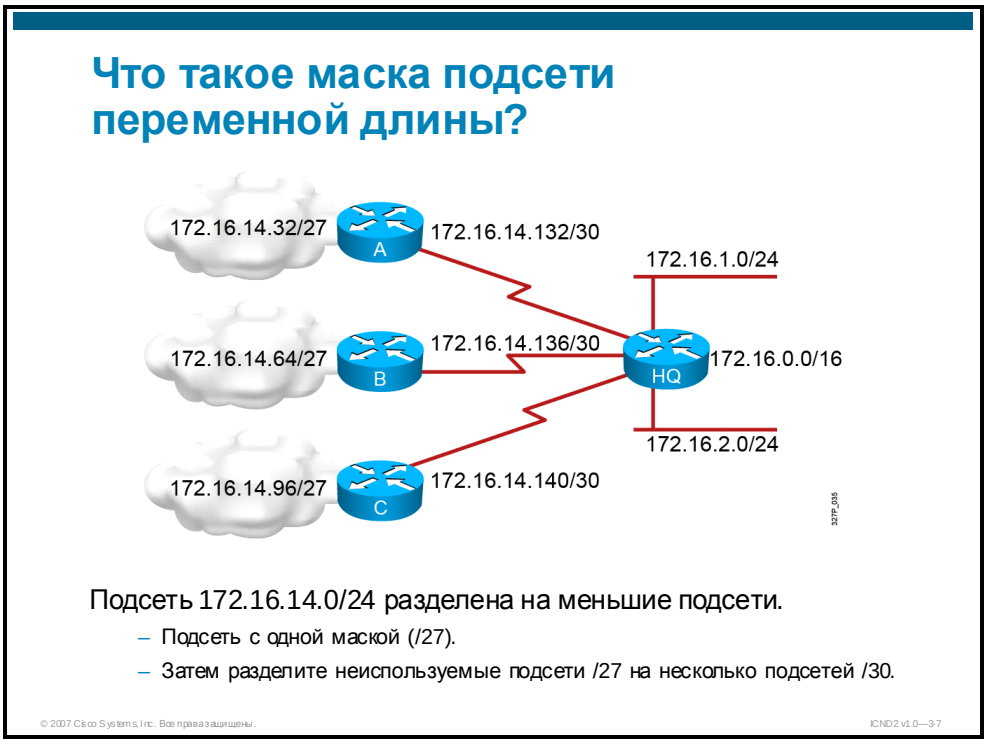


Разделите на подсети сеть с частным сетевым адресом 172.16.0.0/16 так, чтобы она содержала 100 подсетей и обеспечивала максимальное число адресов хостов для каждой подсети.

- Сколько битов необходимо взять из поля хоста?
  - 2s = 27 = 128 подсетей (s = 7 бит)
- Какова новая маска подсети?
  - Для 7 битов хоста = 255.255.254.0 или /23
- Какие адреса будут иметь первые четыре подсети?
  - 172.16.0.0, 172.16.2.0, 172.16.4.0 и 172.16.6.0
- Каковы диапазоны адресов хостов для этих четырех подсетей?
  - 172.16.0.1–172.16.1.254
  - 172.16.2.1–172.16.3.254
  - 172.16.4.1–172.16.5.254
  - 172.16.6.1–172.16.7.254

Общие сведения о VLSM

В этом разделе рассматриваются преимущества VLSM.



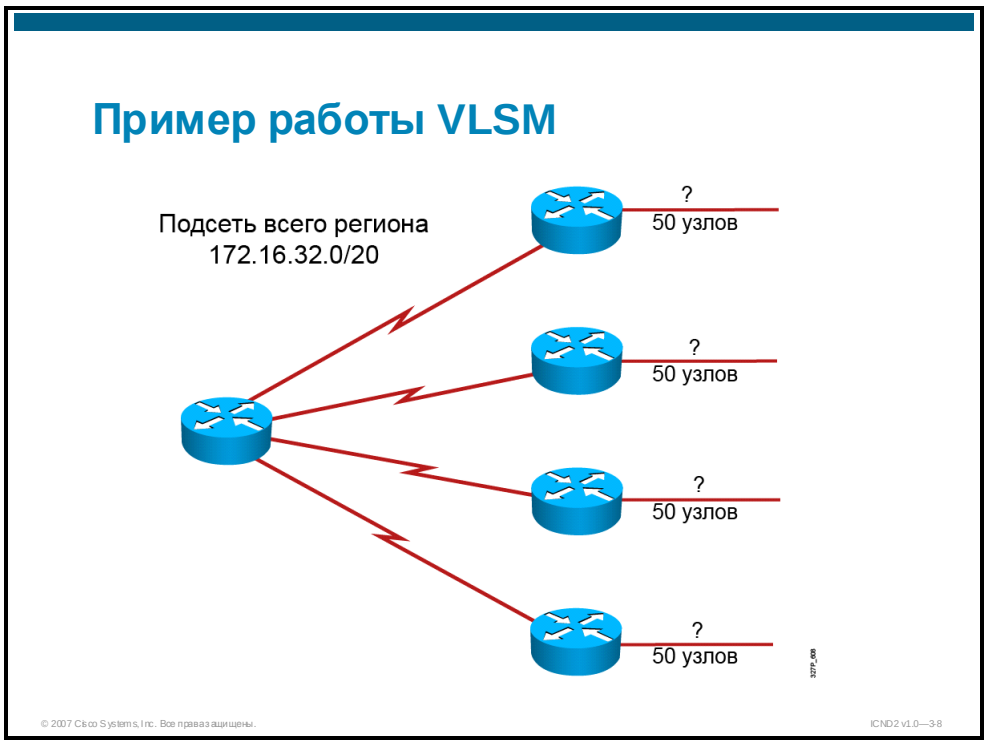
VLSM позволяет создавать несколько масок подсети в одной сети и создавать подсети для адреса, который уже разделен на подсети. VLSM предлагает следующие преимущества.

- Более эффективное использование IP-адресов. Без VLSM компании могут внедрять только одну маску подсети для сетевого номера класса Class A, B или C.

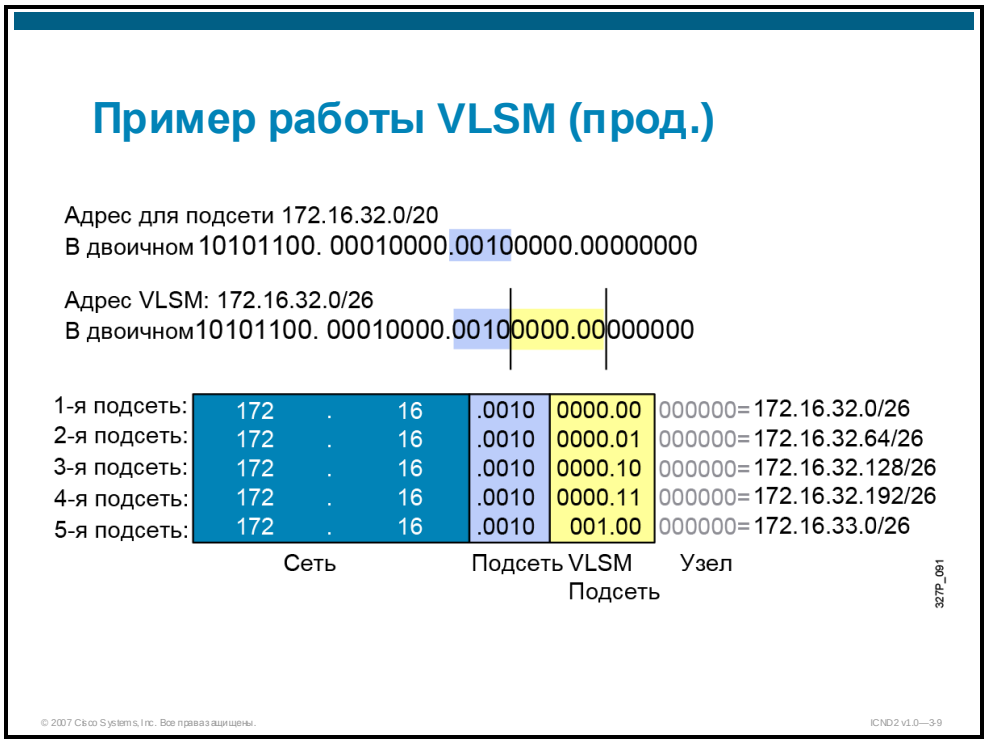
  Предположим, что сетевой адрес 172.16.0.0/16 разделен на подсети по маске /24. Одна из подсетей этого диапазона, 172.16.14.0/24, разделена на меньше подсети по маске /27, как показано на рисунке. Эти малые подсети находятся в диапазоне от 172.16.14.0/27 до 172.16.14.224/27. На рисунке одна их этих подсетей, 172.16.14.128/27, разделена на еще меньшие подсети с префиксом /30, что позволяет использовать для каналов WAN подсети всего с двумя хостами. Подсети /30 находятся в диапазоне от 172.16.14.128/30 до 172.16.14.156/30. На рисунке для каналов WAN используются подсети 172.16.14.132/30, 172.16.14.136/30 и 172.16.14.140/30 из этого диапазона.

- Улучшенная возможность суммирования маршрутов. VLSM позволяет использовать больше уровней иерархии в плане адресации, что обеспечивает улучшенное суммирование маршрутов в таблице маршрутизации. Например, на рисунке подсеть 172.16.14.0/24 суммирует все адреса, которые относятся к подсетям 172.16.14.0, включая адреса из подсети 172.16.14.0/27 и 172.16.14.128/30.

- Изоляция изменений топологии от других маршрутизаторов. Другое преимущество суммирования маршрутов в крупных и сложных сетях заключается в изоляции изменений топологии от других маршрутизаторов. Например, когда состояние канала в домене 172.16.27.0/24 начинает быстро меняться между активным и неактивным (пропадание канала), суммарный маршрут не меняется. Поэтому маршрутизаторам, которые не входят в домен, не приходится изменять свои таблицы маршрутизации при пропадании канала.

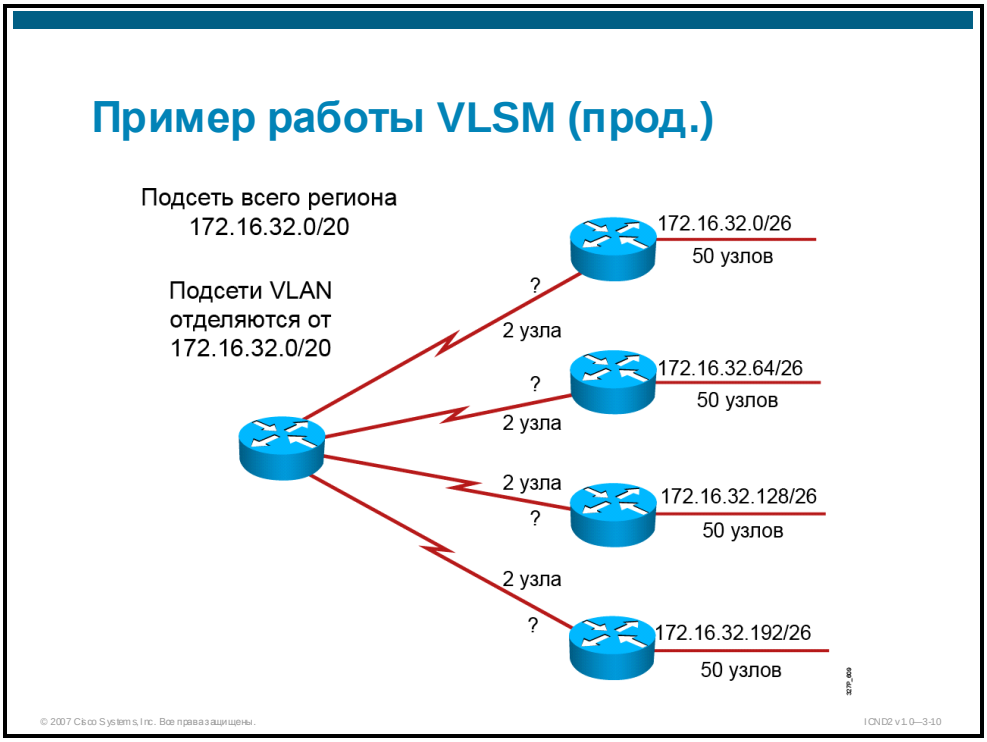


На этом рисунке адрес подсети 172.16.32.0/20, используемый для данной части корпоративной сети, создан путем разделения сети класса B 172.16.0.0/16 на несколько подсетей /20.

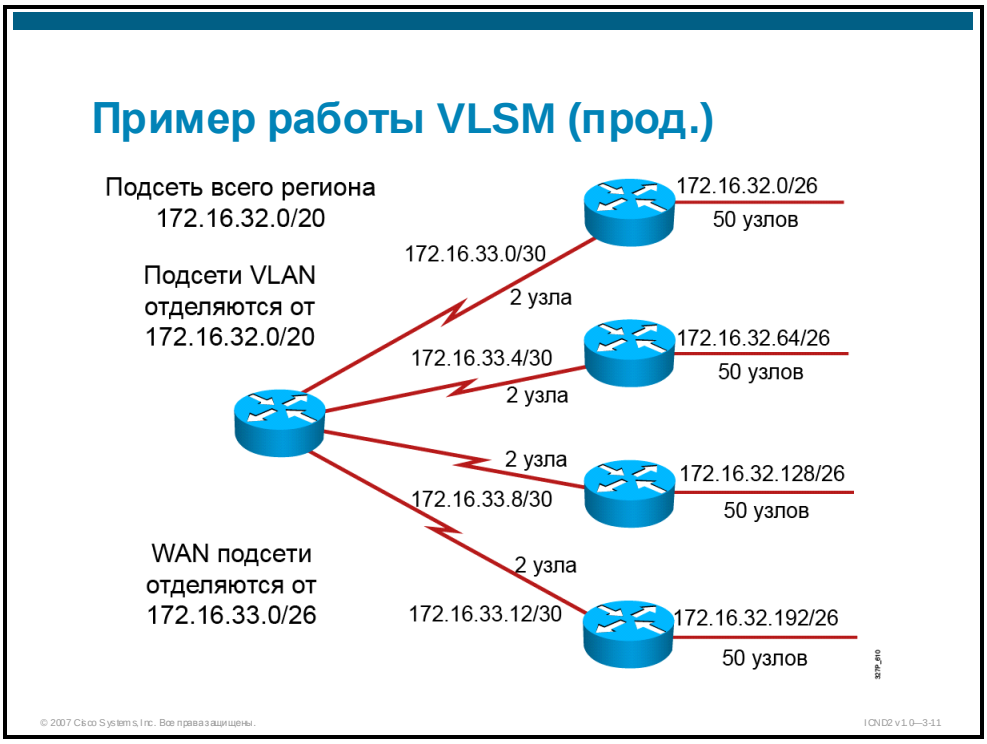


VLSM позволяет разделить на подсети адреса, которые уже разделены на подсети. Предположим, что область корпоративной сети имеет адрес 172.16.32.0/20 и вам необходимо назначить адреса нескольким локальным сетям на 50 хостов каждая внутри этой области. VLSM позволяет разделить на подсети уже разделенный адрес 172.16.32.0/20, что увеличит число сетевых адресов и уменьшит число хостов на сеть.

Например, если вы разделите подсети 172.16.32.0/20 по маске 172.16.32.0/26, вы получите 64 (26) подсети, каждая из которых будет поддерживать 62 (26 – 2) хоста.



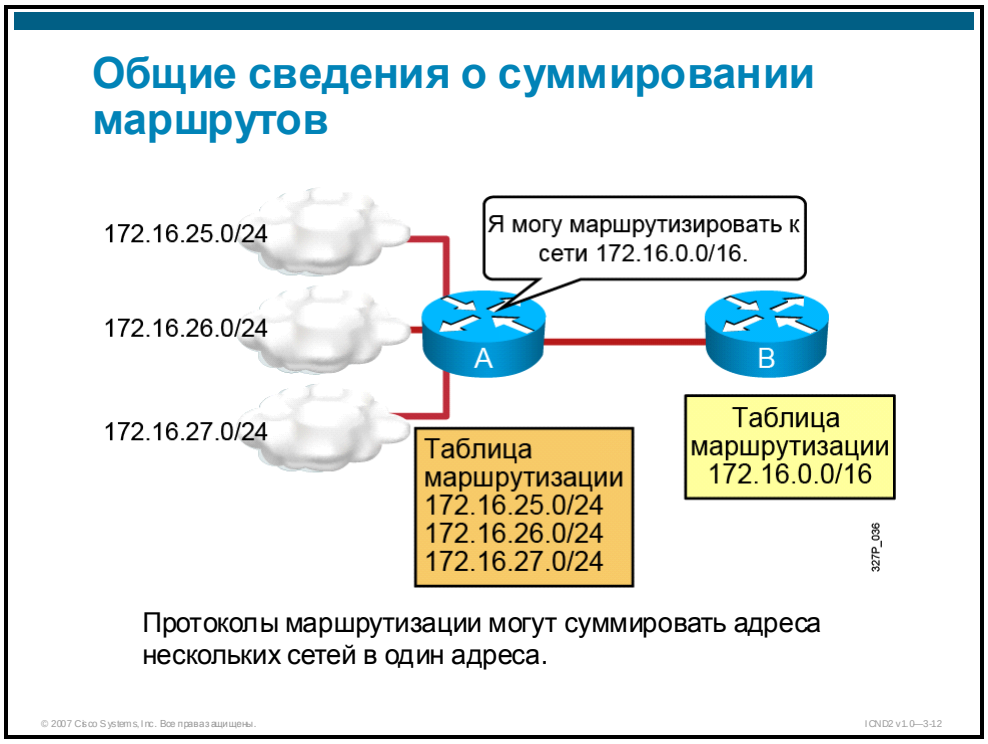
На рисунке адреса подсети, которые используются в локальных сетях Ethernet, получены при разделении подсети 172.16.32.0/20 на несколько подсетей /26.



Чтобы рассчитать адреса подсети, используемые для каналов WAN, разделите неиспользуемые подсети /26. На рисунке адреса подсети, которые используются для каналов WAN, получены при разделении подсети 172.16.33.0/26 на несколько подсетей /30. Это обеспечивает 16 (24) подсетей и 2 (22 – 2) хоста для каждой WAN.

Общие сведения о суммировании маршрутов

В этом разделе описывается процесс суммирования маршрутов.



Пример: суммирование маршрутов

Как показано на рисунке, маршрутизатор A может отправить три записи обновления маршрутизации или суммировать адреса в один номер сети. На рисунке изображен суммарный маршрут на базе полного октета: 172.16.25.0/24, 172.16.26.0/24 и 172.16.27.0/24 суммируется в 172.16.0.0/16.

Примечание Маршрутизатор A на рисунке может направлять пакеты в сеть 172.16.0.0/16, включая все ее подсети. Однако, если в сети присутствуют другие подсети 172.16.0.0 (например, если сеть 172.16.0.0 не является непрерывной), такое суммирование может быть некорректным.

Суммирование маршрутов (также известно как объединение маршрутов), уменьшает количество маршрутов, которые должны поддерживаться маршрутизатором, представляя последовательность номеров сетей как один суммарный адрес.

Суммирование маршрутов будет наиболее эффективно в средах подсетей, в которых сетевые адреса представлены непрерывными блоками в степенях двойки. Например, 4, 16 или 512 адресов можно представить одной записью таблицы маршрутизации поскольку суммарные маски, как и маски подсети, являются двоичными числами поэтому суммирование должно выполняться по двоичным границами (степеням двойки).

Обзор классовой маршрутизации

- Классовые протоколы маршрутизации не добавляют маску подсети в объявления маршрутизации.
- Внутри одной сети предполагается согласованность масок подсети, одна маска подсети должна использоваться для всей сети.
- Обмен суммарными маршрутами происходит между удаленными сетями.
- Примеры классовых протоколов маршрутизации:
  - RIPv1
  - IGRP

Примечание. Классовые протоколы маршрутизации — это старые протоколы, которые используются для решения проблем совместимости. Протоколы RIPv1 и IGRP приводятся в качестве примера.

Классовая маршрутизация основывается на факте, что большинство протоколов маршрутизации на базе вектора расстояния не включают маски подсети в объявления маршрутизации, которые они генерируют.

При использовании классового протокола все подсети в одной основной сети (класса A, B или C) должны использовать одну маску подсети. Маршрутизаторы под управлением классового протокола маршрутизации выполняют автоматическое суммирование маршрутов через границы сети.

При получении пакета обновления маршрутизации маршрутизатор под управлением классового протокола выполняет одно из следующих действий, чтобы определить сетевую часть маршрута.

- Если данные обновления маршрутизации содержат номер основной сети, совпадающий с номером, заданным на принимающем интерфейсе, маршрутизатор применяет маску подсети, настроенную на принимающем интерфейсе.
- Если данные обновления маршрутизации содержат номер основной сети, не совпадающий с номером, заданным на принимающем интерфейсе, маршрутизатор применяет маску подсети по умолчанию следующим образом:
  - Для адресов класса A маска по умолчанию будет 255.0.0.0.
  - Для адресов класса B маска по умолчанию будет 255.255.0.0.
  - Для адресов класса C маска по умолчанию будет 255.255.255.0.

Примечание Протоколы RIPv1 и IGRP — старые протоколы вектора расстояния, которые используются для решения проблем совместимости. Новое ПО Cisco IOS не будет поддерживать IGRP. RIPv1 и IGRP приводятся в качестве примеров классового протокола маршрутизации.

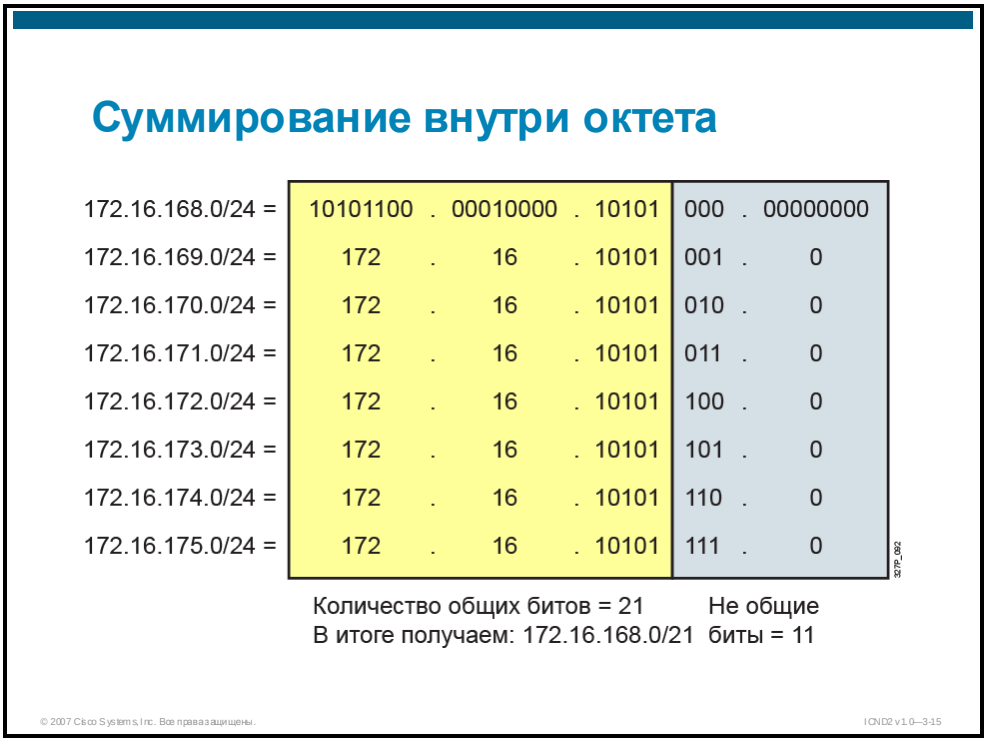
Обзор бесклассовой маршрутизации

- Бесклассовые протоколы маршрутизации добавляют маску подсети в объявления маршрутизации.
- Бесклассовые протоколы маршрутизации поддерживают VLSM, одна подсети может иметь несколько масок.
- Суммарные маршруты должны вручную контролироваться внутри сети.
- Примеры бесклассовых протоколов маршрутизации:
  - RIPv2
  - EIGRP
  - OSPF
- По умолчанию протоколы RIPv2 и EIGRP действуют как классовые и выполняют обмен суммарными маршрутами между удаленными сетями.
  - Команда no auto-summary переводит эти протоколы в бесклассовый режим.

Бесклассовые протоколы маршрутизации можно считать протоколами второго поколения, так как они разработаны для устранения некоторых ограничений классовых протоколов маршрутизации. Одно из самых серьезных ограничений классовой среды заключается в том, что во время обновления маршрутизации не происходит обмена масками подсети. Поэтому одна маска подсети использовалась во всех подсетях основной сети.

Другое ограничение классового метода — потребность в автоматическом суммировании по границам классовой сети на границах основной сети.

В бесклассовой среде процесс суммирования контролируются вручную и как правило может выполняться для любого бита в адресе. Поскольку маршруты подсетей распространяются в домене маршрутизации, может потребоваться суммирование вручную, чтобы сохранить размер таблиц маршрутизации на управляемом уровне. Среди бесклассовых протоколов маршрутизации можно упомянуть RIPv2, EIGRP и OSPF.

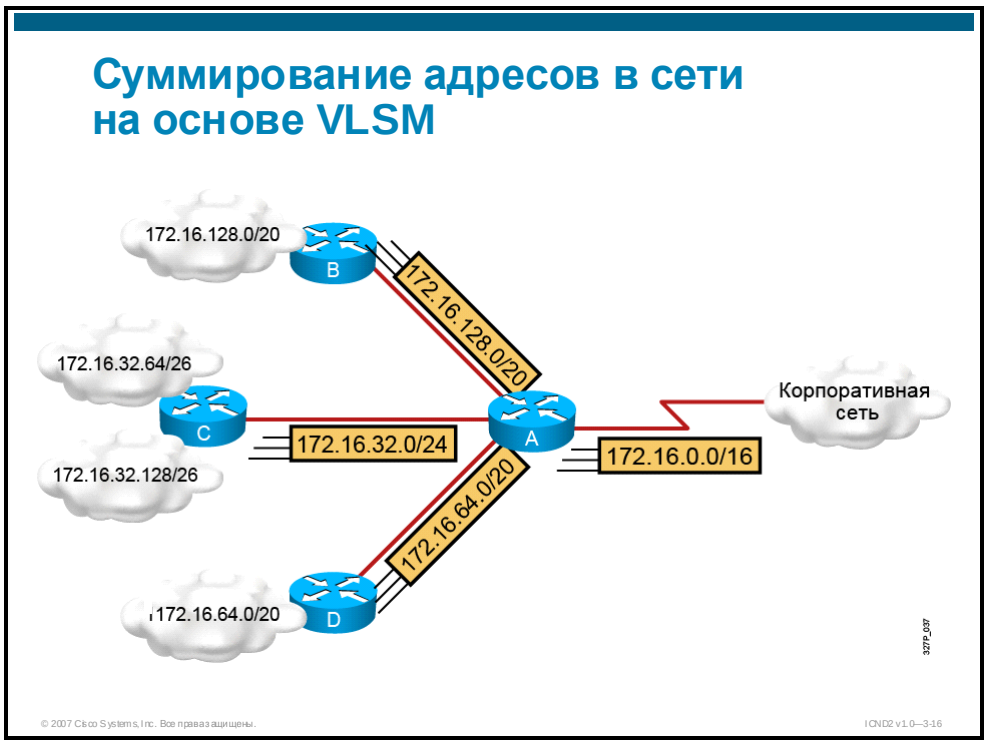


Пример: суммирование внутри октета

В примере ниже иллюстрируется процесс суммирования маршрута внутри октета. Маршрутизатор получает обновления для следующих маршрутов:

- 172.16.168.0/24
- 172.16.169.0/24
- 172.16.170.0/24
- 172.16.171.0/24
- 172.16.172.0/24
- 172.16.173.0/24
- 172.16.174.0/24
- 172.16.175.0/24

Чтобы определить суммарный маршрут, маршрутизатор определяет количество старших битов, которые совпадают во всех адресах. Преобразуя IP-адреса в двоичный формат вы можете определить число битов, общих для этих IP-адресов. На рисунке старшие 21 бит являются общими для представленных IP-адресов Поэтому суммарный маршрут будет 172.16.168.0/21. Вы можете суммировать адреса, если их число равняется степени двойки. Если количество адресов не является степенью двойки, адреса можно разделить на группы и суммировать эти группы по отдельности.



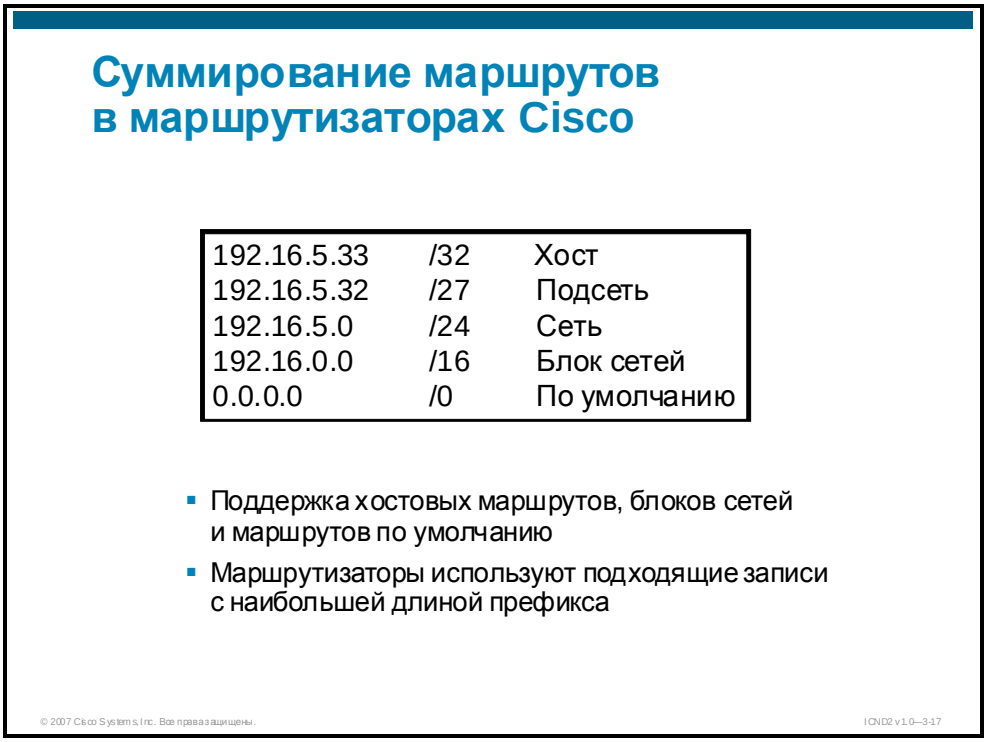
Чтобы маршрутизатор мог объединить максимальное число IP-адресов в один суммированный маршрут, план IP-адресации должен быть иерархическим. Этот подход особенно важен при использовании VLSM. При использовании IP-адресации архитектура VLSM обеспечивает максимальное использование IP-адресов и более эффективное обновление маршрутизации.

На этом рисунке суммирование маршрутов выполняется на двух уровнях:

- Маршрутизатор C суммирует два обновления маршрутизации из сетей 172.16.32.64/26 и 172.16.32.128/26 в одно обновление 172.16.32.0/24.
- Маршрутизатор A получает три разных обновления маршрутизации, но суммирует их в одно обновление, а затем распространяет это обновление по корпоративной сети.

Суммирование маршрутов снижает использование памяти на маршрутизаторах и сетевой трафик протоколов маршрутизации. Для корректной работы суммирования необходимо следующее:

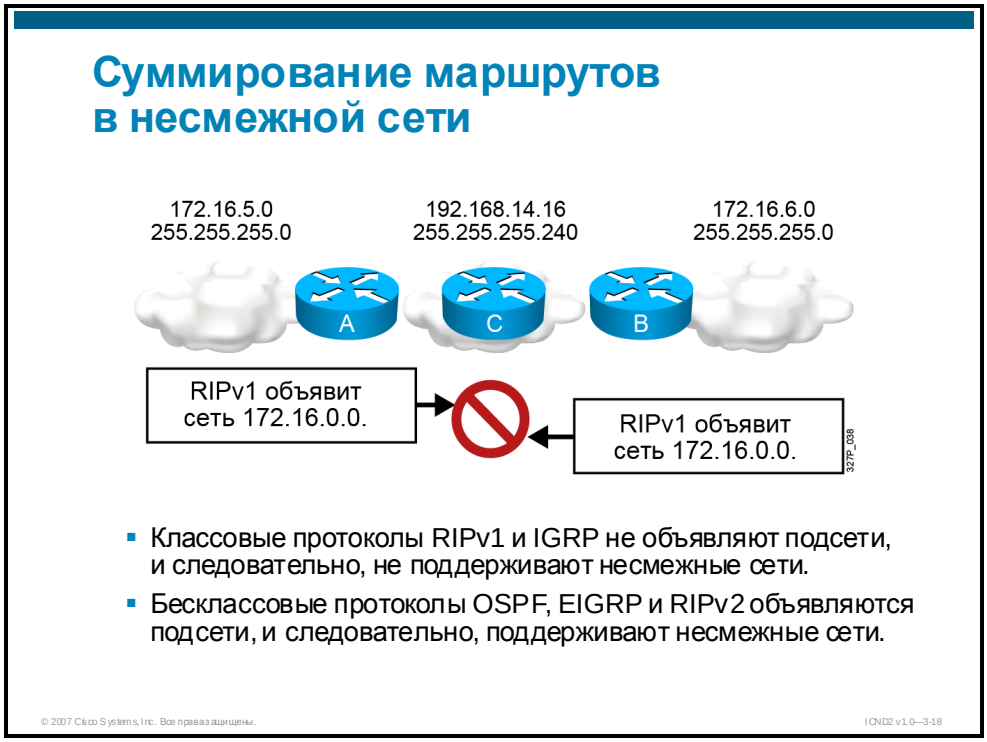
- несколько IP-адресов должны иметь одинаковые старшие биты;
- протоколы маршрутизации должны принимать решения о маршрутизации на основе 32-битного IP-адреса и длины префикса до 32 бит;
- протоколы маршрутизации должны переносить длину префикса (маску подсети) вместе с 32-битным IP-адресом.



Выделение маршрутов из суммированных маршрутов

Если указанному месту назначения соответствует несколько записей таблицы маршрутизации, используется запись с наибольшим префиксом. Несколько маршрутов могут указывать на одно место назначение, но используется префикс с максимальной длиной.

Например, если таблица маршрутизации включает разные пути к 192.16.0.0/16 и 192.16.5.0/24, пакеты, адресованные сети 192.16.5.99, направляются по пути 192.16.5.0/24, поскольку его адрес максимально совпадает с адресом назначения.



Классовые протоколы маршрутизации выполняют автоматическое суммирование на границах сети. Это поведение, которые вы не можете изменить, имеет два важных последствия:

- подсети не объявляются в другой основной сети;
- несмежные подсети невидимы друг для друга.

Пример: суммирование маршрутов в несмежной сети

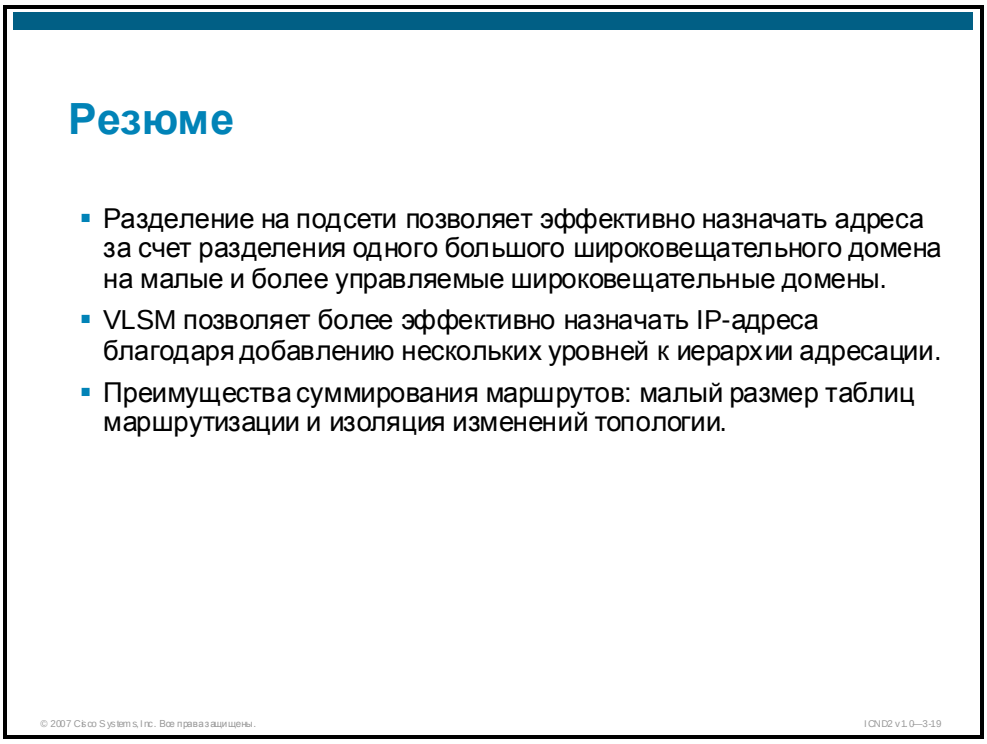
На рисунке протокол RIPv1 не объявляет подсети 172.16.5.0 255.255.255.0 и 172.16.6.0 255.255.255.0, так как не поддерживает объявление подсетей между удаленными сетями. Маршрутизаторы A и B объявляют 172.16.0.0. Неспособность протокола RIPv1 объявлять подсети приводит к путанице при маршрутизации в сети 192.168.14.0. В этом примере маршрутизатор C получает маршруты 172.16.0.0 из двух направлений и не может принять верное решение о маршрутизации.

Это проблему можно решить с помощью бесклассового протокола маршрутизации;

- OSPF;
- RIPv2 с командой **no auto-summary**;
- EIGRP с командой **no auto-summary**.

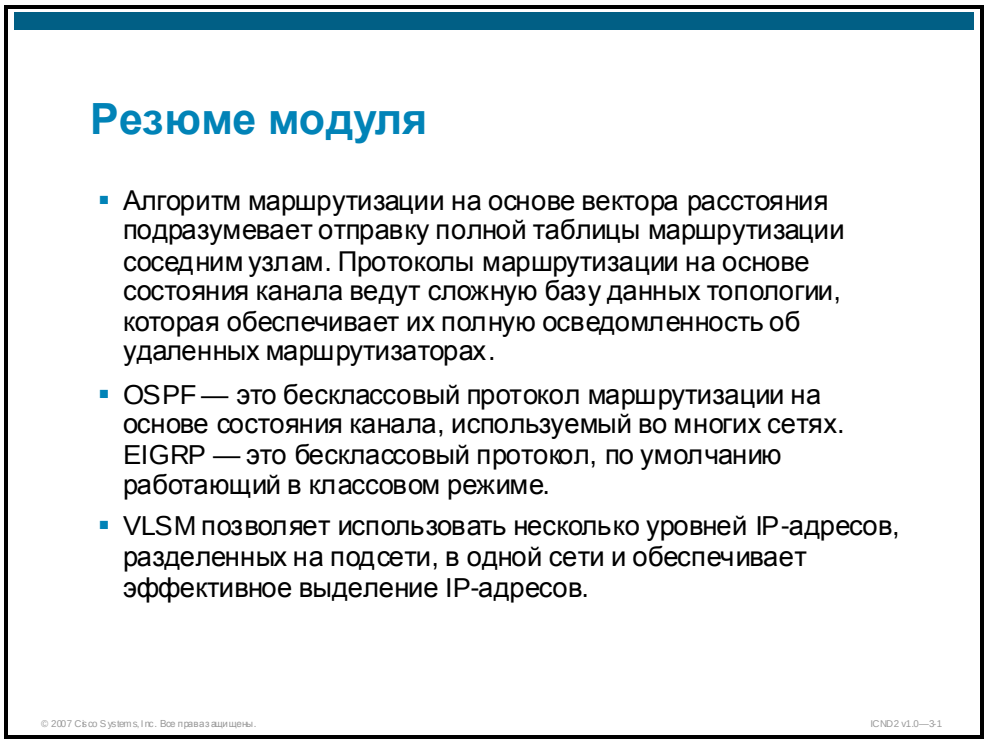
Резюме

В этом разделе приводится резюме основных вопросов, рассмотренных в занятии.



Резюме модуля

В этом разделе приводится резюме вопросов, рассмотренных в модуле.



Маршрутизаторы собирают и хранят данные маршрутизации, чтобы обеспечивать прием и передачу пакетов данных. Различные классы протоколов маршрутизации обеспечивают поддержку разных функций для каждой сети. Протоколы маршрутизации EIGRP и OSPF предоставляют разные функции и возможности.

Работу этих протоколов можно подстроить с помощью масок подсети переменной длины и суммирования маршрутов. Администраторы сети должны знать все протоколы, чтобы внедрить протокол, максимально соответствующий требованиям их сети.

Вопросы для самопроверки по модулю

Используйте эти вопросы, чтобы проверить, насколько хорошо вы освоили материал, представленный в данном модуле. Верные ответы и решения можно найти в разделе "Ответы на вопросы для самопроверки".

В1) Какое утверждение наилучшим образом описывает статические и динамические маршруты? (Источник: повторение пройденного материала по принципам маршрутизации)

А) Динамические маршруты вручную задаются администратором сети, статические маршруты автоматически добавляются и подстраиваются протоколом маршрутизации.
Б) Статические маршруты вручную задаются администратором сети, динамические маршруты автоматически добавляются и подстраиваются протоколом маршрутизации.
В) Статические маршруты сообщают маршрутизатору, как пересылать пакеты в сети, не имеющие прямого подключения к этому маршрутизатору, динамические маршруты сообщают, как пересылать пакеты в сети с прямым подключением.
Г) Динамические маршруты сообщают маршрутизатору, как пересылать пакеты в сети, не имеющие прямого подключения к этому маршрутизатору, статические маршруты сообщают, как пересылать пакеты в сети с прямым подключением.

В2) Какой из следующих протоколов может служить примером протокола внешнего шлюза? (Источник: повторение пройденного материала по принципам маршрутизации)

А) RIP
Б) BGP
В) IGRP
Г) EIGRP

В3) В каких ситуациях используется административное расстояние? (Источник: повторение пройденного материала по принципам маршрутизации)

А) при определении статических маршрутов
Б) при включении динамической маршрутизации
В) когда данные об одном маршруте получаются из нескольких источников маршрутизации
Г) когда к месту назначения доступно несколько путей, полученных от одного протокола маршрутизации

В4) Как маршрутизатор, работающий по алгоритму вектора расстояния, получает сведения о сетях без прямого подключения к нему. (Источник: повторение пройденного материала по принципам маршрутизации)

А) от исходного маршрутизатора
Б) от соседних маршрутизаторов
В) от маршрутизатора назначения
Г) вектор расстояния может быть получен только от сетей с прямым подключением

B5) Что маршрутизатор, работающий по алгоритму вектора расстояния, посылает соседним маршрутизаторам в периодических обновлениях таблицы маршрутизации? (Источник: повторение пройденного материала по принципам маршрутизации)

А) полную таблицу маршрутизации
Б) сведения о новых маршрутах
В) сведения об измененных маршрутах
Г) сведения о маршрутах, прекративших существование

B6) При использовании маршрутизации на основе вектора расстояния, ограничение какой величины позволяет предотвратить счет до бесконечности? (Источник: повторение пройденного материала по принципам маршрутизации)

А) метрика
Б) время обновления
В) время удержания
Г) административное расстояние

B7) В чем заключается правило горизонта разделения? (Источник: повторение пройденного материала по принципам маршрутизации)

А) информация о маршруте не должна отправляться в каком-либо направлении
Б) информация о маршруте не должна отправляться в направлении, с которого была получена исходная информация
В) информация о маршруте всегда должна отправляться в направлении, с которого была получена исходная информация
Г) информация о маршруте должна отправляться только в направлении, с которого была получена исходная информация

B8) Когда маршрутизатор задает максимальное значение метрики для недоступной сети, какую операцию он выполняет? (Источник: повторение пройденного материала по принципам маршрутизации)

А) инициация маршрута
Б) отравление маршрута
В) применение горизонта разделения
Г) перевод маршрута на удержание

B9) Если маршрут к сети находится на удержании, и от соседнего маршрутизатора приходит метрика, равная метрике, изначально записанной для данной сети, какую операцию выполняет маршрутизатор? (Источник: повторение пройденного материала по принципам маршрутизации)

А) игнорирует обновление
Б) увеличивает значение таймера удержания
В) помечает сеть как "доступную" и удаляет таймер удержания
Г) помечает сеть как "доступную", но сохраняет таймер удержания

B10) Если маршрутизатор имеет путь к сети на удержании, и от соседнего маршрутизатора приходит метрика, лучшая, чем метрика, изначально записанная для данной сети, какие операции выполняет маршрутизатор. (Выберите два варианта.) (Источник: повторение пройденного материала по принципам маршрутизации)

А) удаляет таймер удержания
Б) продолжает удержание
В) отмечает сеть как "доступную"
Г) отмечает сеть как "недоступную"
Д) отмечает сеть как "предположительно недоступную"

B11) Как протоколы на основе состояния канала ограничивают область распространения изменений маршрутизации? (Источник: повторение пройденного материала по принципам маршрутизации)

А) благодаря поддержке бесклассовой маршрутизации
Б) путем отправки маски вместе с адресом
В) путем отправки обновлений только при изменении топологии
Г) путем разделения сети на иерархии областей

B12) Каково назначение объявлений состояния канала? (Источник: повторение пройденного материала по принципам маршрутизации)

А) создание топологической базы данных
Б) задание стоимости достижения места назначения
В) определение наилучшего пути к месту назначения
Г) подтверждение работы соседнего хоста

B13) Каковы две характеристики протокола OSPF? (Выберите два варианта.) (Источник: повторение пройденного материала по принципам маршрутизации)

А) иерархический
Б) проприетарный
В) открытый стандарт
Г) аналогичен RIP
Д) протокол вектора расстояния

B14) OSPF направляет пакеты внутри одной/одного _____. (Источник: повторение пройденного материала по принципам маршрутизации)

А) области
Б) сети
В) сегменте
Г) автономной системе

B15) Сколько подсетей можно получить при разделении подсети 172.17.32.0/20 на подсети /28? (Источник: внедрение VLSM)

А) 16
Б) 32
В) 256
Г) 1024

В16) Сколько хостов могут адресоваться в подсети, включающей 7 битов из поля хоста? (Источник: внедрение VLSM)

А) 7
Б) 62
В) 126
Г) 252

В17) Сколько хостов могут адресоваться в подсети с префиксом /30? (Источник: внедрение VLSM)

А) 1
Б) 2
В) 4
Г) 30

В18) Какую маску подсети следует использовать для адреса класса C, используемого для 9 локальных сетей на 12 хостов каждая? (Источник: внедрение VLSM)

А) 255.255.255.0
Б) 255.255.255.224
В) 255.255.255.240
Г) 255.255.255.252

В19) Как можно эффективно суммировать диапазон IP-адресов от 10.1.32.0 до 10.1.35.255? (Источник: внедрение VLSM)

А) 10.1.32.0/23
Б) 10.1.32.0/22
В) 10.1.32.0/21
Г) 10.1.32.0/20

В20) Какая из нижеперечисленных команд переводит протоколы RIPv2 и EIGRP в бесклассовый режим? (Source: Implementing VLSM)

А) **ip classless**
Б) **no ip classful**
В) **no auto-summary**
Г) эти протоколы не работают в бесклассовом режиме

В21) Как можно эффективно суммировать диапазон IP-адресов от 172.168.12.0/24 до 172.168.13.0/24 (Источник: внедрение VLSM)

А) 172.168.12.0/23
Б) 172.168.12.0/22
В) 172.168.12.0/21
Г) 172.168.12.0/20

Ответы на вопросы для самопроверки по модулю

В1 Б

В2 Б

В3 В

В4 Б

В5 А

В6 А

В7 Б

В8 Б

В9 А

В10 А, В

В11 Г

В12 А

В13 А, В

В14 Г

В15 В

В16 В

В17 Б

В18 В

В19 Б

В20 В

В21 А

Модуль 4

Внедрение сети OSPF с одной областью

Обзор

В этом модуле рассматривается протокол OSPF, один из самых распространенных протоколов внутреннего шлюза для IP-сетей. OSPF — открытый протокол, основанный в основном на стандарте RFC 2328. Протокол OSPF достаточно сложен, поэтому получение навыков по настройке и проверке протокола OSPF на маршрутизаторе Cisco является основной задачей обучения.

Задачи модуля

По окончании этого модуля вы сможете настраивать, проверять и устранять неполадки OSPF. Это значит, что вы сможете выполнять следующие задачи:

- описывать принцип работы и конфигурацию протоколов на основе состояния канала и сети OSPF с одной областью, включая выравнивание нагрузки и аутентификацию;
- определять методы выявления распространенных проблем OSPF и предлагать решения этих проблем.

Занятие 1

Внедрение OSPF

Обзор

Протокол OSPF — это бесклассовый протокол внутреннего шлюза (IGP). В сетях с крупными автономными системами этому протоколу отдается предпочтение по сравнению со старыми протоколами на основе вектора расстояния. IETF определяет протокол OSPF как один из нескольких протоколов внутреннего шлюза. Поскольку OSPF является широко распространенным стандартным протоколом, знания по его конфигурации и обслуживанию абсолютно необходимы. В этом занятии описывается функционирование протокола OSPF, а также настройка сети OSPF с одной областью на маршрутизаторе Cisco.

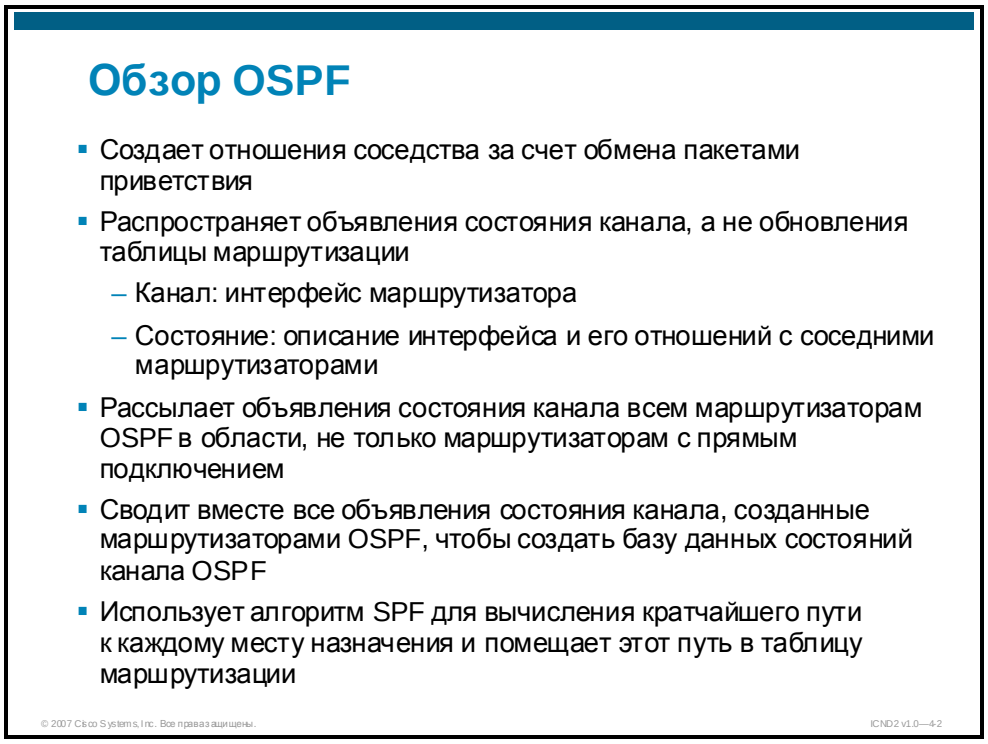
Задачи

По окончании этого занятия вы сможете описывать принцип работы и конфигурации сети OSPF с одной областью, включая выравнивание нагрузки и аутентификацию. Это значит, что вы сможете выполнять следующие задачи:

- описывать функции OSPF;
- описывать формирование смежности между соседними узлами OSPF;
- описывать алгоритм SPF, используемый протоколом OSPF;
- настраивать сеть OSPF с одной областью;
- настраивать интерфейс возвратной петли для использования в качестве идентификатора маршрутизатора;
- проверять конфигурацию сети OSPF с одной областью;
- использовать команды debug протокола OSPF для поиска и устранения неполадок среды OSPF;
- настраивать выравнивание нагрузки с использованием OSPF;
- настраивать аутентификацию для OSPF.

Общие сведения о OSPF

В этом разделе описываются функции протокола OSPF.

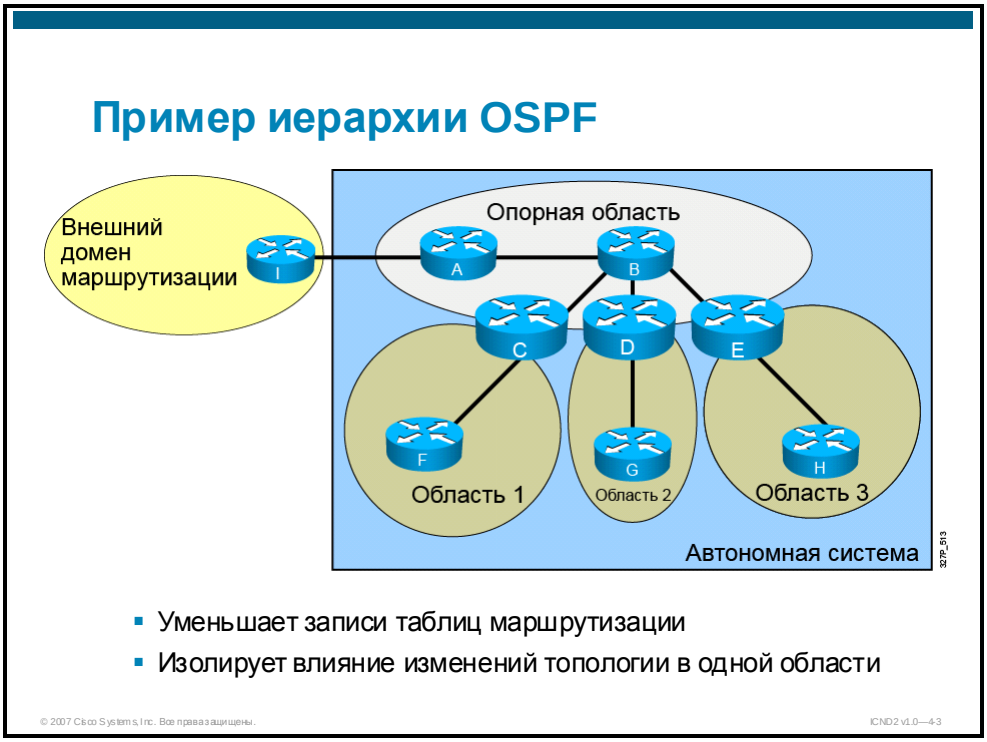


OSPF основывается на алгоритме состояния канала. Канал можно представить как интерфейс маршрутизатора. Состояние канала — это описание интерфейса и его отношений с соседними маршрутизаторами. Описание интерфейса должно включать, такие параметры, как IP-адрес, маску, тип сети, к которой подключен интерфейс, маршрутизаторы, подключенные к этой сети и т. п. Набор всех состояний каналов формирует базу данных состояний каналов.

Маршрутизатор отправляет пакеты объявления состояния канала (LSA), чтобы объявить о своем состоянии, через регулярные интервалы (30 минут) или немедленно при изменении состояния маршрутизатора. В объявления состояния канала OSPF включаются данные о подключенных интерфейсах, используемых метриках и других параметрах. Накопив данные о состоянии каналов, маршрутизаторы OSPF используют алгоритм SPF для расчета кратчайшего пути к каждому из узлов.

Топологическая база данных (база данных состояния каналов) содержит общее представление сетей с точки зрения маршрутизаторов. Топологическая база данных содержит набор объявлений состояния канала, полученных от всех маршрутизаторов в области. Поскольку маршрутизаторы в одной области используют одинаковые данные, их топологические базы данных идентичны.

Примечание Протокол OSPF может работать в иерархии. Самая крупная сущность иерархии — автономная система (набор сетей под общим управлением и с общей стратегией маршрутизации). Автономную систему можно разделить на несколько областей, которые представляют собой группы смежных сетей и подключенных к ним узлов.



OSPF использует двухуровневую иерархию сети. Эта иерархия включает два основных элемента.

- **Область.** Область — это группа смежных сетей. Области представляют собой логические разделы автономной системы.
- **Автономная система.** Автономная система — это совокупность сетей с общим управлением и с общей стратегией маршрутизации. Автономные системы, также известные как домены, можно логически разделить на несколько областей.

В каждой автономной системе необходимо задать непрерывную магистральную область. Все немагистральные области соединяются через магистральную область. Магистральная область является транзитной, поскольку все остальные области взаимодействуют через нее. В сети OSPF немагистральные области могут быть настроены в качестве шлейфных, полностью шлейфных или не слишком шлейфных (NSSA), чтобы уменьшить размеры баз данных состояния канала и таблиц маршрутизации.

Маршрутизаторы, работающие в двухуровневой сетевой иерархии, могут выполнять разные роли и функции в среде OSPF. Ниже приводятся примеры этих ролей (см. рисунок).

- Маршрутизатор B является магистральным маршрутизатором. Магистральный маршрутизатор обеспечивает соединение областей.
- Маршрутизаторы C, D и E — пограничные маршрутизаторы области (ABR). ABR подключаются к нескольким областям, ведут отдельную базу данных состояний канала для каждой области, к которой они подключены, и маршрутизируют трафик, направленный в другие области или прибывающий из них.
- Маршрутизаторы F, G и H — немагистральные, внутренние маршрутизаторы. Немагистральные внутренние маршрутизаторы имеют данные о топологии областей, в которых они находятся, и ведут одинаковые базы данных состояния каналов для этих областей.

- В зависимости от конфигурации немагистральной области OSPF (шлейфной области, полностью шлейфной области или NSSA) маршрутизатор ABR объявляет маршрут по умолчанию внутреннему немагистральному маршрутизатору. Внутренний немагистральный маршрутизатор использует маршрут по умолчанию для пересылки всего межобластного или междоменного трафика в маршрутизатор ABR.
- Маршрутизатор A является пограничным маршрутизатором автономной системы (ASBR) и служит для соединения с внешним доменом маршрутизации или автономной системой.
- Маршрутизатор I принадлежит другому домену маршрутизации или автономной системе.

Формирование смежности между соседними узлами OSPF

В этом разделе описывается формирование смежности между соседними узлами OSPF.

Соседние маршрутизаторы OSPF должны опознать друг друга в сети перед тем, как смогут обмениваться информацией, так как маршрутизация OSPF зависит от состояния канала между двумя маршрутизаторами. Этот процесс реализуется с помощью протокола приветствия (Hello). Протокол приветствия создает и поддерживает отношения соседства, обеспечивая двунаправленное соединение между коммутаторами. Двунаправленной соединение имеет место, когда маршрутизатор находит себя в пакете приветствия, полученном от соседнего узла.

Каждый интерфейс в среде OSPF периодически отправляет пакеты приветствия по адресу многоадресной рассылки 224.0.0.5. Пакет приветствия включает следующие сведения.

- **Идентификатор маршрутизатора.** Идентификатор маршрутизатора — это 32-битный номер, уникальный для маршрутизатора. По умолчанию выбирается самый высокий IP-адрес активного интерфейса, если не настроен интерфейс возвратной петли или идентификатор маршрутизатора, например IP-адресу 172.16.12.1 будет отдано предпочтение над 172.16.1.1. Эта идентификация важна для установления отношений соседства и устранения неполадок в них, а также для координации обмена данными маршрутизации.

- **Интервалы приветствия и простоя.** Интервал приветствия определяет период отправки пакетов приветствия маршрутизатором. Интервал приветствия по умолчанию составляет 10 секунд. Интервал простоя — это время в секундах, в течение которого маршрутизатор ожидает пакета приветствия от соседнего маршрутизатора, прежде чем объявить его неисправным. По умолчанию интервал простоя в 4 раза превышает интервал приветствия. Эти таймеры должны быть одинаковы на соседних маршрутизаторах, в противном случае смежность не будет сформирована.
- **Соседи.** В поле соседей перечисляются смежные маршрутизаторы, с которыми установлено двусторонне соединение. Это двустороннее соединение устанавливается, когда маршрутизатор опознает себя в поле соседей пакета приветствия, полученного от соседнего маршрутизатора.
- **Идентификатор области.** Для успешного взаимодействия маршрутизаторы должны находиться в одном сегменте и их интерфейсы должны принадлежать к одной области OSPF в этом сегменте. Кроме того, соседние узлы должны использовать одинаковую подсеть и маску. Все эти маршрутизаторы будут иметь одинаковые данные о состоянии канала.
- **Приоритет маршрутизатора.** Приоритет маршрутизатора — это 8-битное число, определяющее приоритет маршрутизатора. OSPF использует приоритет для выбора выделенного маршрутизатора (DR) и резервного выделенного маршрутизатора (BDR).
- **IP-адреса DR и BDR.** IP-адреса маршрутизаторов DR и BDR в сети (если они известны).

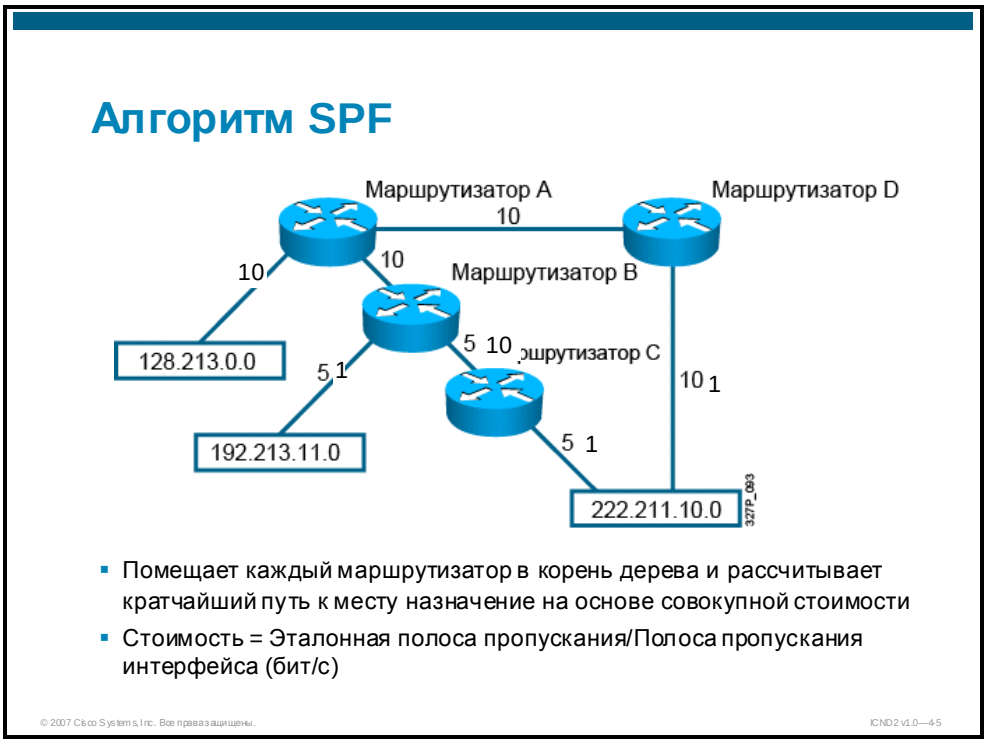
Примечание Маршрутизаторы DR и BDR рассматриваются в курсе Cisco CCNP®.

- **Пароль для аутентификации.** Если включена аутентификация маршрутизаторов, два маршрутизатора должны передать друг другу одинаковый пароль. Аутентификация не является обязательной, однако если она включена, на всех маршрутизаторах должен быть задан одинаковый пароль.
- **Флаг шлейфной области.** Шлейфная область — особая область среды OSPF. Два маршрутизатора должны согласовать флаг шлейфной области в пакетах приветствия. Назначение шлейфной области позволяет уменьшить число обновлений маршрутизации, заменив их на маршрут по умолчанию.

Примечание Особые области OSPF, такие как шлейфные области, рассматриваются в курсе CCNP.

Алгоритм SPF

В этом разделе описывается алгоритм SPF.



Алгоритм SPF помещает все маршрутизаторы в корень дерева и рассчитывает кратчайший путь к каждому месту назначения по алгоритму Дийкстра на основе совокупной стоимости доступа к этому месту назначения. Объявления состояния канала рассылаются по области с использованием надежного алгоритма, который гарантирует, что у все маршрутизаторы в области используют одинаковые топологические базы данных. Каждый маршрутизатор использует информацию своей топологической базы данных для расчета дерева кратчайших путей, принимая себя за корневой узел. Затем маршрутизатор использует это дерево для маршрутизации сетевого трафика. На этом рисунке маршрутизатор A — корневой узел.

Каждый маршрутизатор имеет собственное представление топологии, но при этом все маршрутизаторы используют одну базу данных состояний канала для вычисления дерева кратчайших путей.

Стоимость (метрика) интерфейса обозначает издержки отправки пакетов через определенный интерфейс. Стоимость интерфейса обратно пропорциональна полосе пропускания интерфейса, т. е. чем выше полоса пропускания, тем ниже стоимость. При передаче данных через последовательный канал T1 издержки (стоимость) и временные задержки выше, чем при передачи через канал Ethernet 10 Мбит/с.

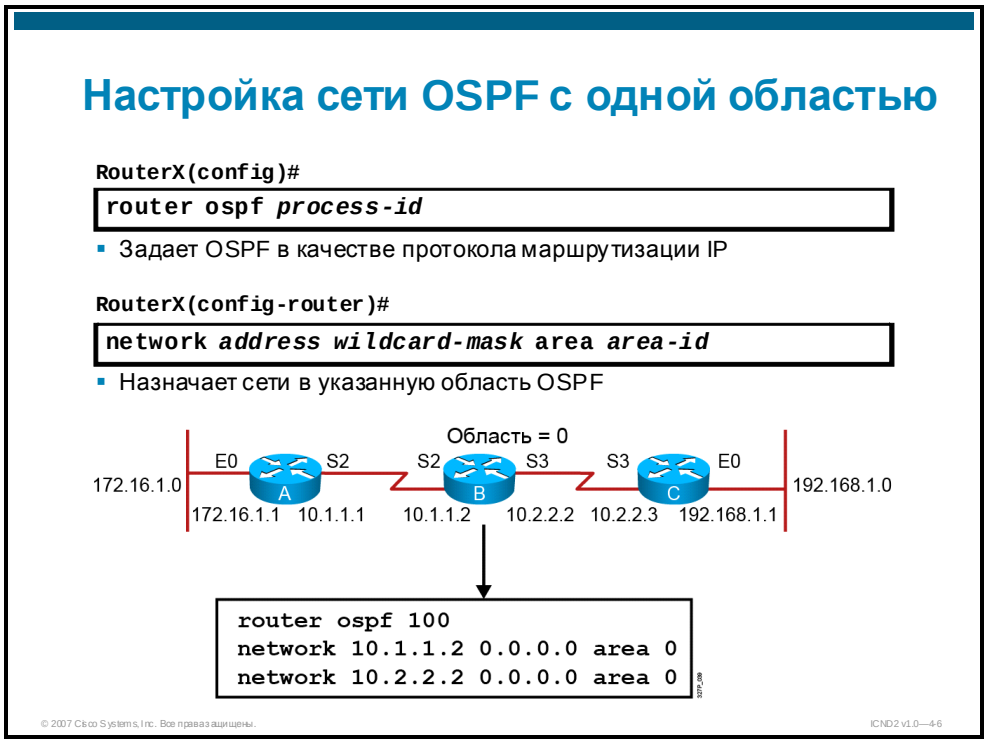
Формула расчета стоимости OSPF: стоимость = эталонная полоса пропускания/полоса пропускания интерфейса (в бит/с).

Эталонная полоса пропускания — 108 или 100 000 000, что эквивалентно полосе пропускания Fast Ethernet. Поэтому стоимость по умолчанию канала Ethernet 10 Мбит/с будет 108 / 107 = 10, стоимость канала T1 будет 108 / 1 544 000 = 64.

Чтобы отрегулировать эталонную полосу пропускания для каналов с полосой пропускания выше, чем у Fast Ethernet, используйте команду **ospf auto-cost reference-bandwidth** эталонная полоса пропускания.

Настройка и проверка OSPF

В этом разделе описывается настройка и проверка сети OSPF с одной областью.



В качестве аргумента команды router ospf используется идентификатор процесса. Идентификатор процесса — уникальный случайный номер, который применяется для идентификации процесса маршрутизации. Идентификатор процесса не обязательно должен совпадать с идентификатором процесса OSPF на других маршрутизаторах OSPF.

Команда network определяет, какие IP-сети маршрутизатора являются частью сети OSPF. Кроме того, необходимо задать область OSPF, к которой принадлежат сети. Команда network использует три аргумента, перечисленные в таблице.

В таблице ниже перечислены параметры команды network.

Параметры команды router ospf	Описание
адрес	Адрес сети, подсети или интерфейса
шаблонная маска	Шаблонная маска. Эта маска определяет часть IP-адреса, которая должна совпадать, 0 означает совпадение, 1 — «все равно». Например, шаблонная маска 0.0.0.0 предполагает совпадение всех 32 битов.
идентификатор области	Область, которую необходимо связать с диапазоном адресов OSPF. Может указываться как десятичное значение или как десятичное представление, разделенное точками.

Расчет шаблонных масок для границ, не соответствующих 8 битам, может привести к ошибкам. Расчета шаблонных масок можно избежать с помощью сетевого оператора, соответствующего IP-адресам всех интерфейсов и использующего маску 0.0.0.0.

Интерфейсы возвратной петли

В этом разделе описывается изменение идентификатора маршрутизатора OSPF на адрес возвратной петли.

Чтобы изменить идентификатор маршрутизатора OSPF на адрес возвратной петли, задайте интерфейс возвратной петли с помощью следующей команды:

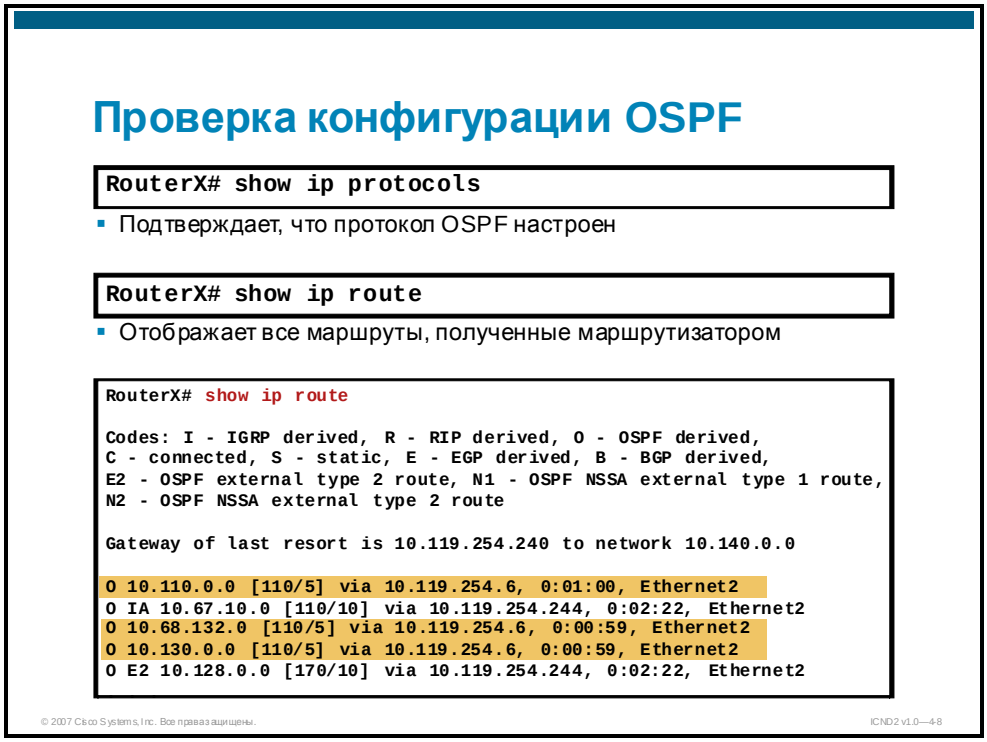
```
RouterX(config)# interface loopback <number>
```

Самый высокий IP-адрес, используемый в качестве идентификатора маршрутизатора, можно переопределить, настроив IP-адрес интерфейса возвратной петли. Надежность OSPF повышается при использовании интерфейса возвратной петли, поскольку он всегда активен и не может перейти в недоступное состояние, как «настоящий» интерфейс. Поэтому интерфейс возвратной петли следует использовать на всех ключевых маршрутизаторах. Если интерфейс возвратной петли будет опубликован с помощью команды **network area**, использование частного IP-адреса позволит сэкономить зарезервированное адресное пространство IP. Обратите внимание, что интерфейс возвратной петли требует использования разных подсетей на всех маршрутизаторах, если не объявляется адрес хоста.

Использование необъявляемого адреса позволяет сэкономить адресное пространство IP, но в отличии от объявляемого адреса, необъявляемый адрес не добавляется в таблицу OSPF и поэтому к нему нельзя обращаться через сеть. Таким образом, использование частного IP-адреса обеспечивает компромисс между простотой отладки сети и экономией адресного пространства.

Проверка конфигурации OSPF

В этом разделе описывается проверка конфигурации OSPF с помощью нескольких команд show.

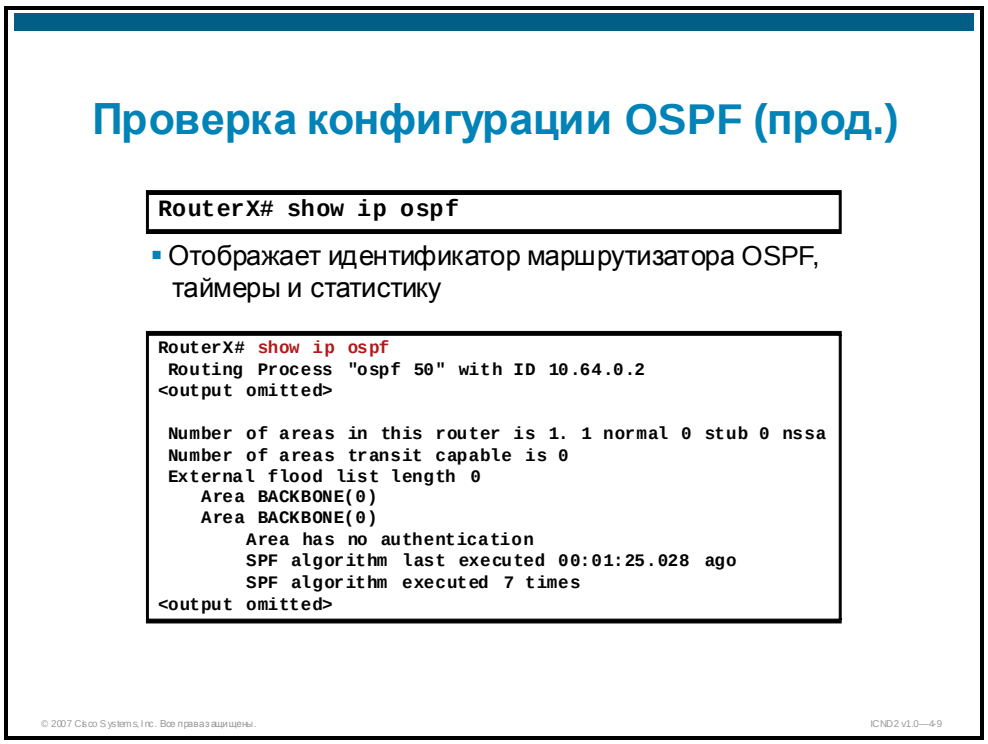


Для вывода информации о конфигурации OSPF можно использовать любое количество команд **show**. Команда **show ip protocols** выводит параметры таймеров, фильтров, метрик, сетей, а также другие данные для маршрутизатора в целом.

Команда **show ip route** отображает маршруты, известные маршрутизатору, а также сведения о том, как были получены эти маршруты. Эта команда предлагает один из лучших способов определить соединение между локальным маршрутизатором о остальной частью интерсети.

В таблице описываются значимые поля вывода команды **show ip route**.

Значение	Описание
O	В этом поле указывается способ получения маршрута. Оно может принимать следующие значения. ■ **I:** маршрут получен от протокола IGRP ■ **R:** маршрут получен от протокола RIP ■ **O:** маршрут получен от протокола OSPF (это значение отображается в примере) ■ **C:** подключен ■ **S:** статический ■ **E:** маршрут получен от протокола EGP ■ **B:** маршрут получен от протокола BGP ■ **D:** маршрут получен от протокола EIGRP ■ **EX:** внешний маршрут EIGRP ■ **i:** маршрут получен от протокола IS-IS ■ **ia:** IS-IS ■ **M:** мобильный ■ **P:** периодически загружаемый статический маршрут ■ **U:** пользовательский статический маршрут ■ **o:** маршрутизация по требованию
E2 IA	В этом поле указывается тип маршрута. Оно может принимать следующие значения. ■ ***:** Указывает последний путь, использованный для пересылки маршрутов. Значение сохраняется только для пакетов без быстрой коммутации. Однако это поле не указывает, какой путь будет использоваться при следующей пересылке пакета без быстрой коммутации, за исключением путей с одинаковой стоимостью. ■ **IA:** межобластной маршрут OSPF ■ **E1:** внешний маршрут OSPF первого типа ■ **E2:** внешний маршрут OSPF второго типа (это значение отображается в примере) ■ **L1:** маршрут IS-IS первого уровня ■ **L2:** маршрут IS-IS второго уровня ■ **N1:** внешний маршрут OSPF NSSA первого типа ■ **N2:** внешний маршрут OSPF NSSA второго типа
172.150.0.0	Адрес удаленной сети.
[110/5]	Первое число в скобках — административное расстояние источника информации, второе число — метрика маршрута.
via 10.119.254.6	Адрес следующего маршрутизатора в удаленной сети.
0:01:00	Время последнего обновления маршрутизатора (часы:минуты:секунды).
Ethernet2	Интерфейс, через который можно получить доступ к указанной сети.



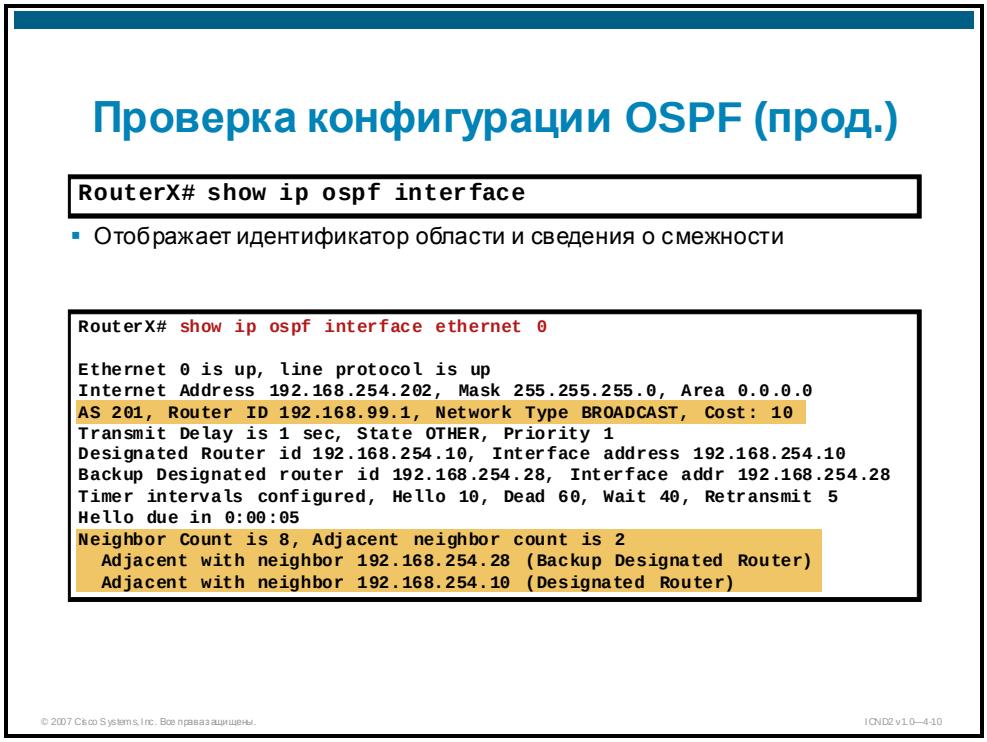
Используйте команду show ip ospf для проверки идентификатора маршрутизатора OSPF. Эта команда также отображает параметры таймера OSPF и другие характеристика, включая количество выполнений алгоритма SPF. Кроме того, команда имеет дополнительные параметры, которые позволяют уточнить данные, которые необходимо вывести.

На рисунке приводится часть вывода этой команды, выполненной на маршрутизаторе X. Полный вывод выглядит следующим образом:

```
RouterX# sh ip ospf
 Routing Process "ospf 50" with ID 10.64.0.2
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Supports area transit capability
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Incremental-SPF disabled
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
```



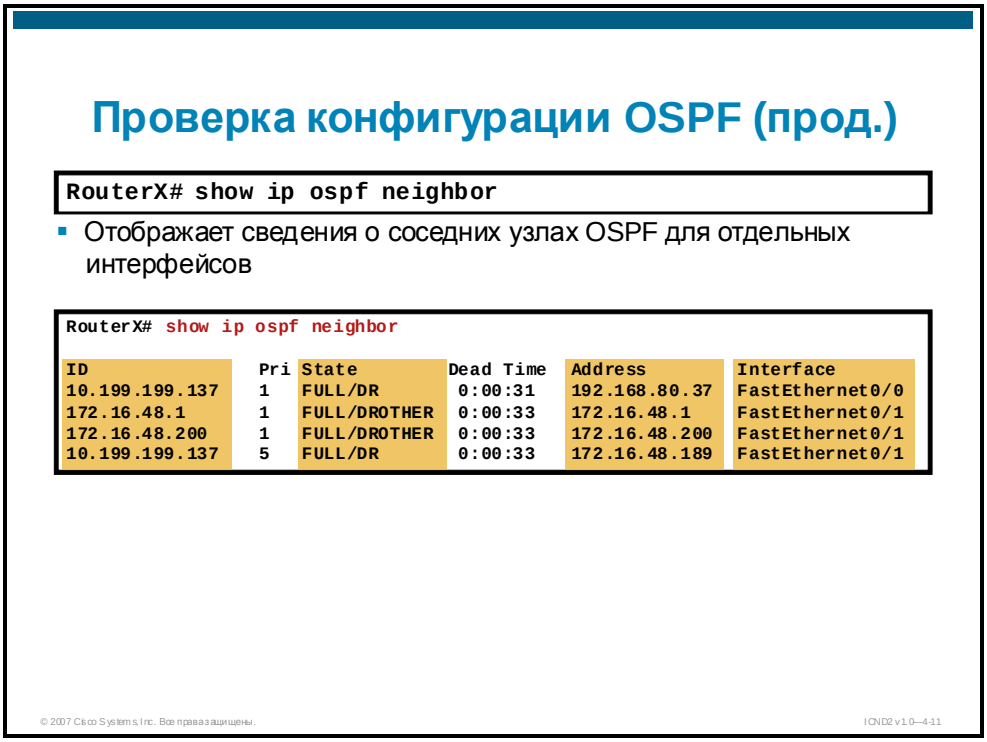
```
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Number of areas transit capable is 0
External flood list length 0
   Area BACKBONE(0)
   Area BACKBONE(0)
       Area has no authentication
       SPF algorithm last executed 00:01:25.028 ago
       SPF algorithm executed 7 times
       Area ranges are
       Number of LSA 6. Checksum Sum 0x01FE3E
       Number of opaque link LSA 0. Checksum Sum 0x000000
       Number of DCbitless LSA 0
       Number of indication LSA 0
       Number of DoNotAge LSA 0
       Flood list length 0
```



Команда show ip ospf interface позволяет убедиться, что интерфейсы настроены в верных областях. Если адрес возвратной петли не задан, в качестве идентификатора маршрутизатора используется интерфейс с наибольшим IP-адресом. Кроме того, эта команда отображает интервалы таймеров, включая интервал приветствия, и отношения смежности между соседними узлами.

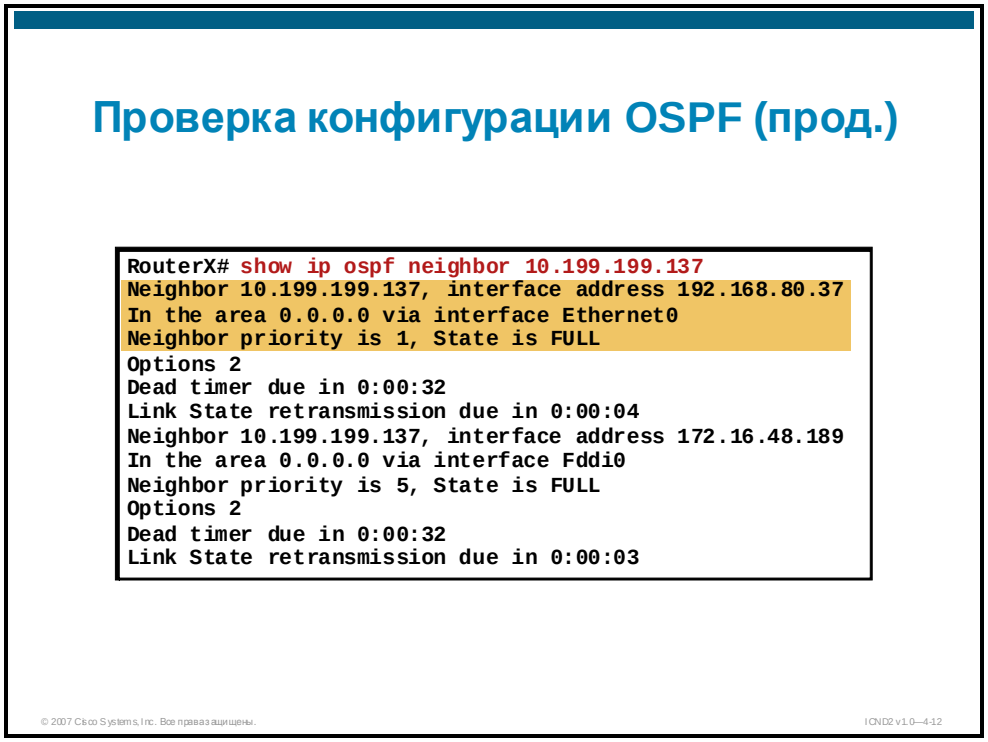
Вывод команды show ip ospf interface

Поле	Описание
Ethernet	Состояние физического канала и операционное состояние протокола.
Internet Address	IP-адрес интерфейса, маска подсети и адрес области.
AS	Номер автономной системы (идентификатор процесса OSPF), идентификатор маршрутизатора, тип сети, стоимость состояния канала.
Transmit Delay	Задержка при передаче, состояние интерфейса и приоритет маршрутизатора
Designated Router	Идентификатор выделенного маршрутизатора и IP-адрес соответствующего интерфейса.
Backup Designated router	Идентификатор резервного выделенного маршрутизатора и IP-адрес соответствующего интерфейса.
Timer intervals configured	Конфигурация интервалов таймеров.
Hello	Интервал отправки пакетов приветствия из интерфейса (в секундах)
Neighbor Count	Число соседних узлов и список смежных соседних узлов.



Команда **show ip ospf neighbor** выводит сведения о соседних узлах OSPF для каждого интерфейса.

На рисунке приводится пример вывода команды **show ip ospf neighbor** с одной сводной строкой для каждого соседнего узла.



На таблице описываются значимые поля вывода команды show ip ospf neighbor.

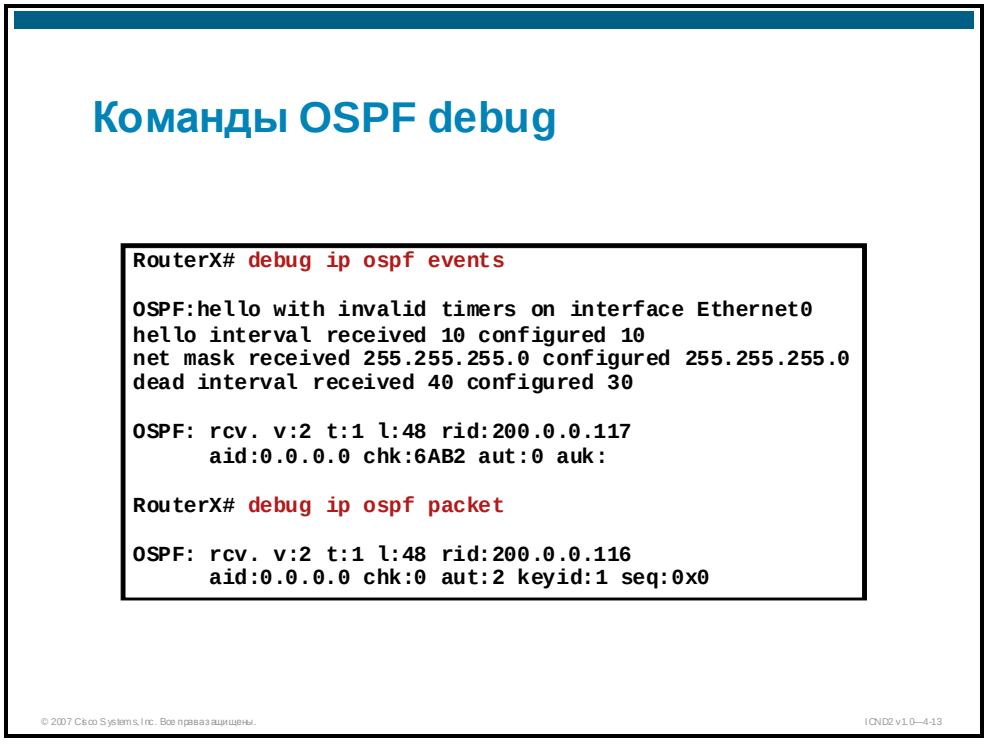
Вывод команды show ip ospf neighbor

Поле	Описание
Neighbor	Идентификатор соседнего маршрутизатора.
interface address	IP-адрес интерфейса.
In the area	Область и интерфейс, через которые были получены данные о соседнем узле OSPF.
Neighbor priority	Приоритет соседнего узла, состояние соседнего узла.
State	Состояние OSPF.
state changes	Количество изменений состояния с момента установления соседства. Это значение можно сбросить с помощью команды **clear ip ospf counters neighbor**.
DR is	Идентификатор выделенного маршрутизатора для данного интерфейса.
BDR is	Идентификатор резервного выделенного маршрутизатора для данного интерфейса.
Options	Содержимое поля параметров пакетов приветствия. (Только бит E. Доступные значения: 0 и 2. 2 означает, что область не является шлейфной, 0 — что область шлейфная.)
LLS Options..., last OOB-Resync	Локальная (LLS) и внеполосная (OOB) ресинхронизация баз данных выполнена часы:минуты:секунды назад (данные Cisco Nonstop Forwarding [NSF]). Это поле обозначает время последней успешной внеполосной ресинхронизации с NSF-совместимым маршрутизатором
Dead timer due in	Период ожидания, по истечении которого ПО Cisco IOS объявит соседний узел неисправным.

Поле	Описание
Neighbor is up for	Количество часов:минут:секунд с момента перехода соседнего узла в двусторонний режим.
Index	Положение узла в очередях повторной передачи области и автономной системы.
retransmission queue length	Количество элементов в очереди повторной передачи.
number of retransmission	Количество операций повторной отправки пакетов обновления во время лавинной рассылки.
First	Расположение данных лавинной рассылки в памяти.
Next	Расположение данных лавинной рассылки в памяти.
Last retransmission scan length	Количество объявлений состояния канала в последнем пакете повторной передачи.
maximum	Максимальное количество объявлений состояния канала, которое можно отправить в любом пакете повторной передачи.
Last retransmission scan time	Время, затраченное на формирование последнего пакета повторной передачи.
maximum	Максимальное время, затраченное на формирование пакета повторной передачи.

Использование команд debug протокола OSPF

В этом разделе описывается использование команд debug протокола OSPF для поиска и устранения распространенных проблем.



Вывод команды debug ip ospf events, представленный на рисунке, может отображаться в любой из следующих ситуаций:

- маски IP-подсетей для маршрутизаторов в одной сети не совпадают;
- интервал приветствия OSPF маршрутизатора не совпадает с интервалом приветствия OSPF, настроенным на соседнем узле;
- интервал простоя OSPF маршрутизатора не совпадает с интервалом простоя OSPF, настроенным на соседнем узле.

Если маршрутизатор OSPF не видит соседний узел OSPF в подключенной сети, выполните следующие действия:

- убедитесь, что маски IP-подсети, а также интервалы приветствия и простоя OSPF, настроенные на маршрутизаторах, совпадают;
- убедитесь, что обоим соседним узлам назначены одинаковые номера и типы области.

Ниже приводится пример вывода команды **debug ip ospf events**, которые отображаются, если данный маршрутизатор или соседний маршрутизатор не являются частью шлейфной области. Т. е. один маршрутизатор настроен для работы в транзитной области, а другой — в шлейфной области, согласно определению стандарта RFC 1247.

```
OSPF: hello packet with mismatched E bit
```

Чтобы вывести сведения обо всех полученных пакетах OSPF, используйте команду **debug ip ospf packet** привилегированного режима EXEC. Используйте версию «**no**» этой команды, чтобы отключить вывод данных отладки.

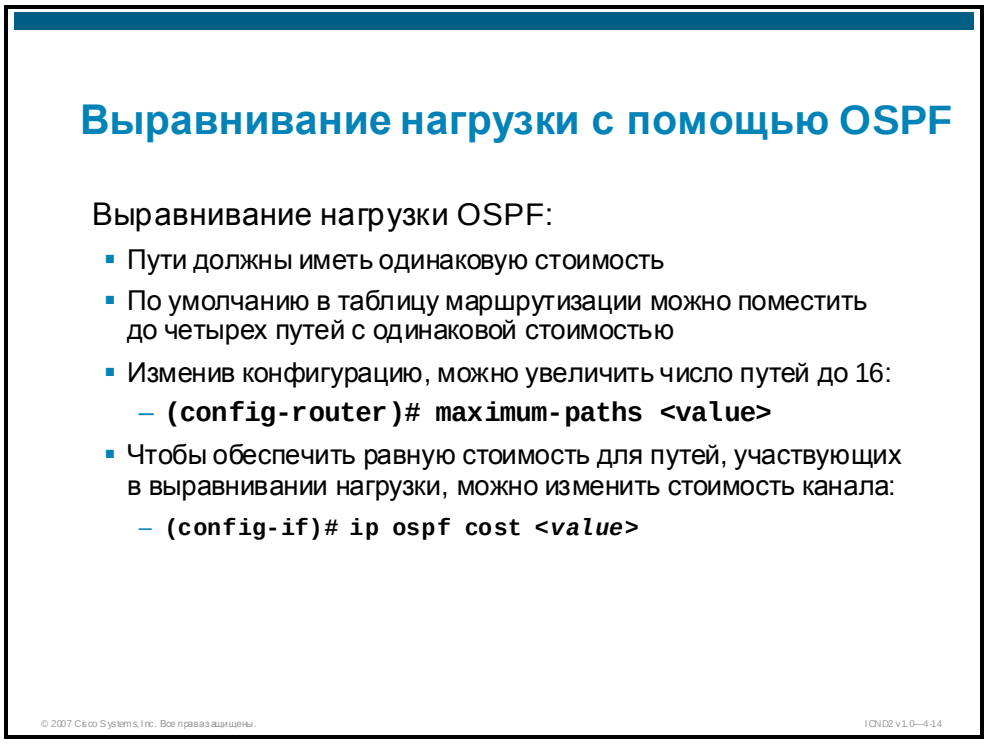
Команда **debug ip ospf packet** выводит один набор данных для каждого полученного пакета. Вывод может незначительно меняться в зависимости от метода аутентификации. В таблице приводится пример вывода команды **debug ip ospf packet** при использовании аутентификации Message Digest 5 (MD5).

Пол**я вывода кома**нды debug ip ospf packet

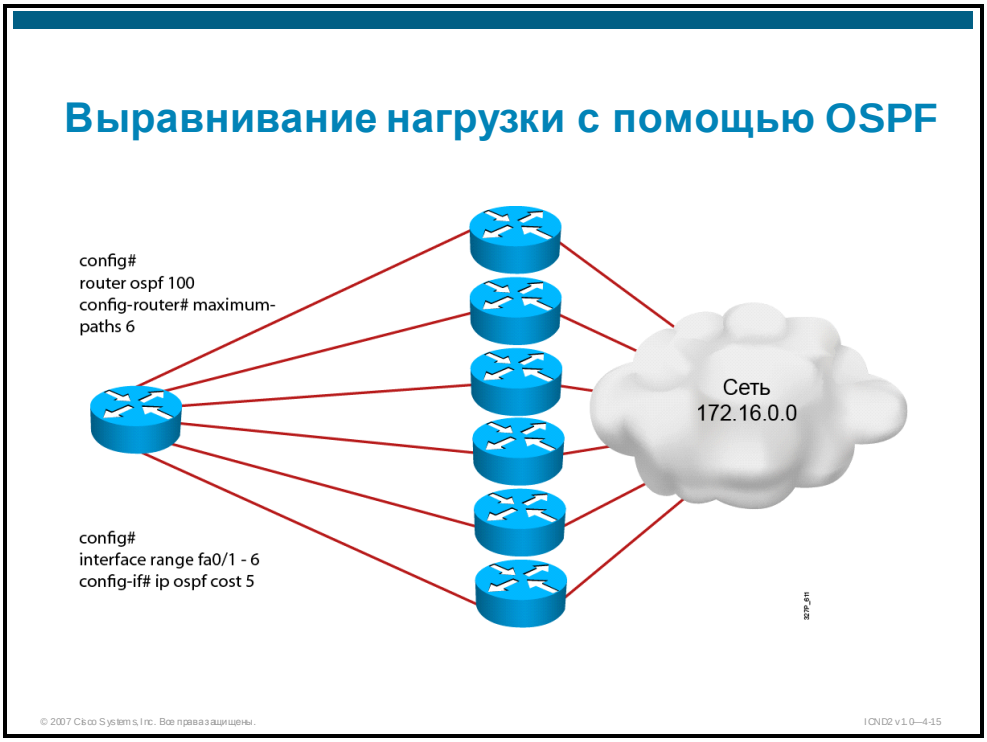
Поле	Описание
v:	Версия OSPF
t:	Тип пакета OSPF, возможные типы: ■ **1:** Пакет приветствия ■ **2:** Описание данных ■ **3:** Запрос состояния канала ■ **4:** Обновление состояния канала ■ **5:** Подтверждение состояния канала
l:	Длина пакета OSPF в байтах
rid:	Идентификатор маршрутизатора OSPF
aid:	Идентификатор области OSPF
chk:	Контрольная сумма OSPF
aut:	Тип аутентификации OSPF, возможные типы аутентификации: ■ **0:** Аутентификация не используется ■ **1:** Нешифрованный пароль ■ **2:** MD5
auk:	Ключ аутентификации OSPF
keyid:	Идентификатор ключа MD5
seq:	Последовательный номер

Выравнивание нагрузки с помощью OSPF

В этом разделе описывается настройка выравнивания нагрузки с помощью OSPF.



Выравнивание нагрузки — это стандартная функция ПО Cisco IOS, она доступна во всех платформах маршрутизаторов. Функция основана на процессе пересылки и позволяет маршрутизатору использовать несколько путей к месту назначения при пересылке пакетов. Количество используемых путей ограничивается числом записей, которое протокол маршрутизации добавляет в таблицу маршрутизации. По умолчанию для протоколов маршрутизации IP в ПО Cisco IOS создается 4 записи (за исключением BGP). Значением по умолчанию для BGP — одна запись. Максимальное количество путей, которое можно настроить, равняется 16.



Стоимость OSPF

Стоимость (метрика) интерфейса обозначает издержки отправки пакетов через определенный интерфейс. Стоимость интерфейса обратно пропорциональна его полосе пропускания. Более высокая полоса пропускания подразумевает более низкую стоимость. По умолчанию маршрутизаторы Cisco рассчитывают стоимость интерфейса на основе полосы пропускания. Однако вы можете принудительно назначить стоимость интерфейса с помощью команды ip ospf cost {значение} в режиме конфигурации интерфейса.

Если к месту назначения доступно несколько путей с одинаковой стоимостью, версия протокола OSPF от Cisco может отслеживать до 16 последующих переходов в таблице маршрутизации (это называется выравниванием нагрузки). По умолчанию маршрутизаторы Cisco поддерживают до 4 путей OSPF к месту назначения. С помощью команды maximum-paths в режиме конфигурации процесса маршрутизатора OSPF можно задать число путей с одинаковой стоимостью в таблице маршрутизации.

```
RouterX(config)#router ospf 1
RouterX(config-router)#maximum-paths ?
<1-16>  Number of paths
RouterX(config-router)#maximum-paths 3
```

Для поиска маршрутов с одинаковой стоимостью используется команда show ip route. Ниже приводится пример вывода команды show ip route для подсети, для которой доступно несколько маршрутов в таблице маршрутизации. В примере выводится три пути к сети 194.168.20.0 с одинаковой стоимостью.

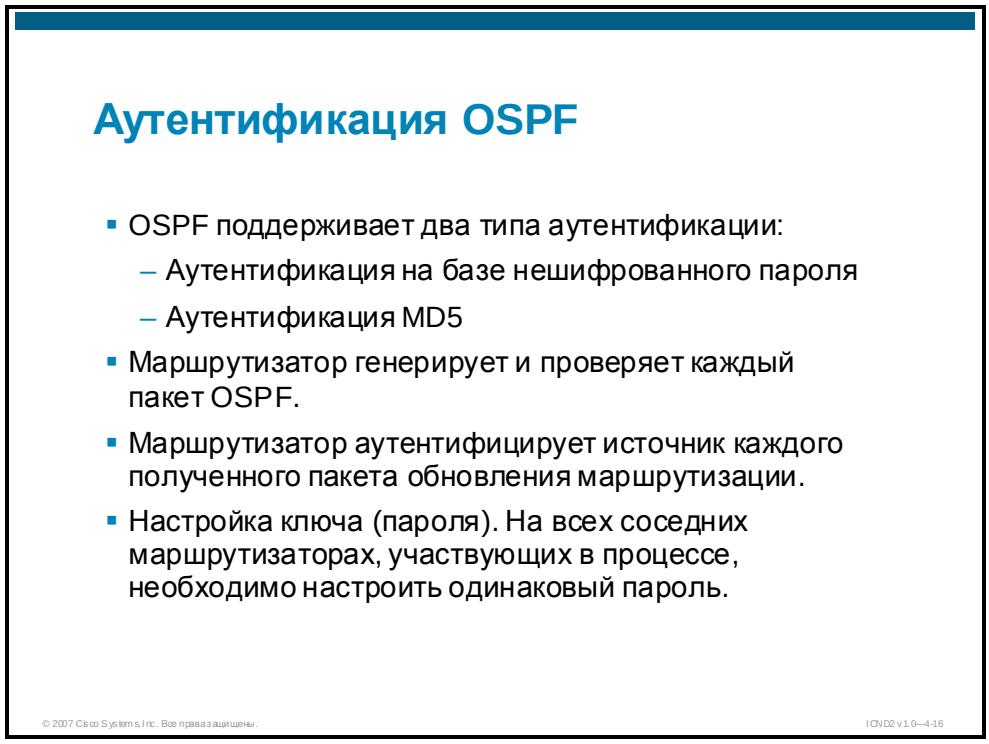
```
RouterX# show ip route 194.168.20.0
 Routing entry for 194.168.20.0/24
  Known via "ospf 1", distance 110, metric 74, type intra area
```

```
Redistributing via ospf 1
Last update from 10.10.10.1 on Serial1, 00:00:01 ago
Routing Descriptor Blocks:
* 20.20.20.1, from 204.204.204.1, 00:00:01 ago, via Serial2
    Route metric is 74, traffic share count is 1
  30.30.30.1, from 204.204.204.1, 00:00:01 ago, via Serial3
    Route metric is 74, traffic share count is 1
  10.10.10.1, from 204.204.204.1, 00:00:01 ago, via Serial1
    Route metric is 74, traffic share count is 1
```

Обратите внимание, что вывод содержит три блока дескрипторов маршрутизации. Каждый блок представляет один из доступных маршрутов. Кроме того, один из блоков обозначен астериском (*). Астериск указывает на активный маршрут, используемый для нового трафика. Термин «новый трафик» обозначает одиночный пакет или поток данных, направленный к месту назначения, в зависимости от того, в каком режиме выравнивания нагрузки работает маршрутизатор — выравнивание по месту назначения или выравнивания по пакету.

Аутентификация OSPF

В этом разделе описывается настройка аутентификации для OSPF.



Типы аутентификации

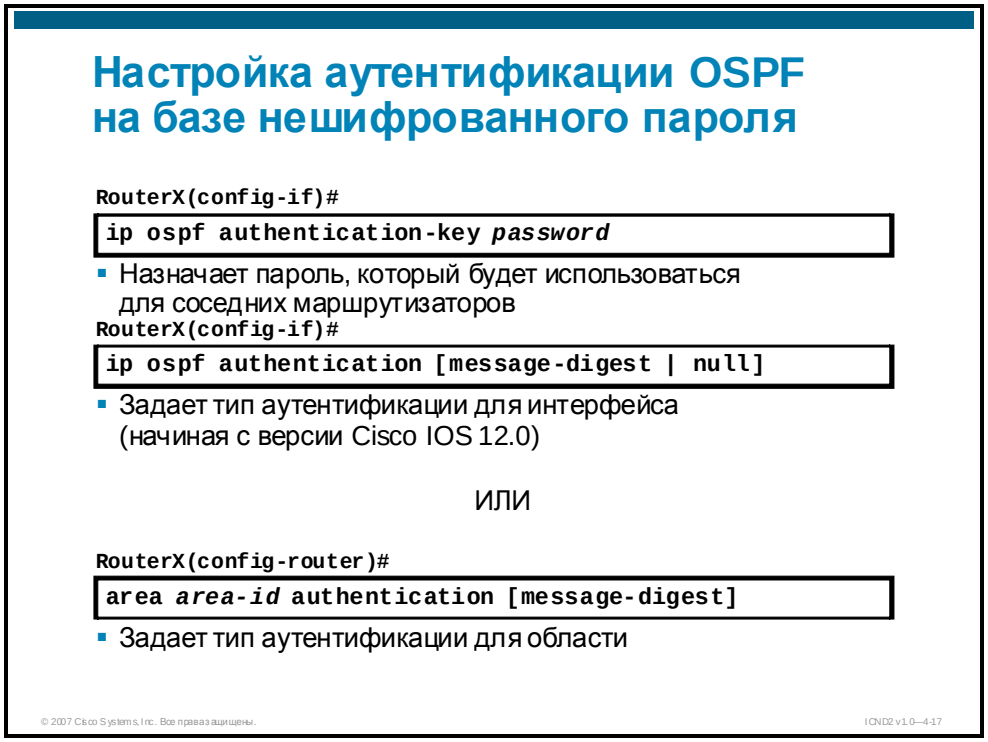
Аутентификация соседних узлов OSPF (также известная как аутентификация соседних маршрутов или аутентификация маршрутов) настраивается, чтобы маршрутизаторы могли принимать участие в процессе маршрутизации только при наличии пароля.

Маршрутизатор, на котором настроена аутентификация соседних узлов, аутентифицирует источник каждого полученного пакета обновления маршрутизации. Эта аутентификация реализуется путем обмена копиями ключа аутентификации (другое название — пароль), известного маршрутизатору-отправителю и маршрутизатору-получателю.

По умолчанию маршрутизатор выполняет нулевую аутентификацию, это означает, что при обмене данными маршрутизации по сети аутентификация не выполняется. OSPF поддерживает два метода аутентификации:

- аутентификация на базе нешифрованного пароля;
- аутентификация MD5;

Аутентификация OSPF MD5 включает неуменьшаемый последовательный номер в каждый пакет OSPF для защиты от атак повтора.



Настройка аутентификации на базе нешифрованного пароля

Для настройки аутентификации OSPF на базе нешифрованного пароля, выполните следующие действия:

Действие 1 С помощью команды **ip ospf authentication-key** *пароль* назначьте пароль, который будет использоваться соседними маршрутизаторами при аутентификации OSPF на базе нешифрованного пароля.

Параметр команды ip ospf authentication-key

Параметр	Описание
пароль	Любая непрерывная строка символов, которые можно ввести с клавиатуры, длиной до 8-ми символов.

Примечание В ПО Cisco IOS версии 12.4 маршрутизатор выдаст предупреждение при попытке настроить пароль с длиной, превышающей 8 символов. В пароле будут использоваться только первые 8 символов. Некоторые старые версии ПО Cisco IOS не выводят это предупреждение.

Пароль, заданный с помощью этой команды, используется в качестве «ключа», который вставляется в заголовок OSPF, когда ПО Cisco IOS создает пакеты протокола маршрутизации. Для каждой сети можно назначить отдельный пароль (на каждом интерфейсе). На всех соседних маршрутизаторах в одной сети должен быть задан одинаковый пароль, чтобы они могли обмениваться данными OSPF.

Примечание Если при настройке аутентификации OSPF не была использована команда **service password-encryption**, ключ будет сохранен в конфигурации маршрутизатора в виде нешифрованного текста. Если команда **service password-encryption** была введена, ключ сохраняется и отображается в зашифрованном виде. Когда пароль выводится, перед ним отображается тип шифрования 7.

Укажите тип аутентификации с помощью команды **ip ospf authentication**.

Параметры команды ip ospf authentication

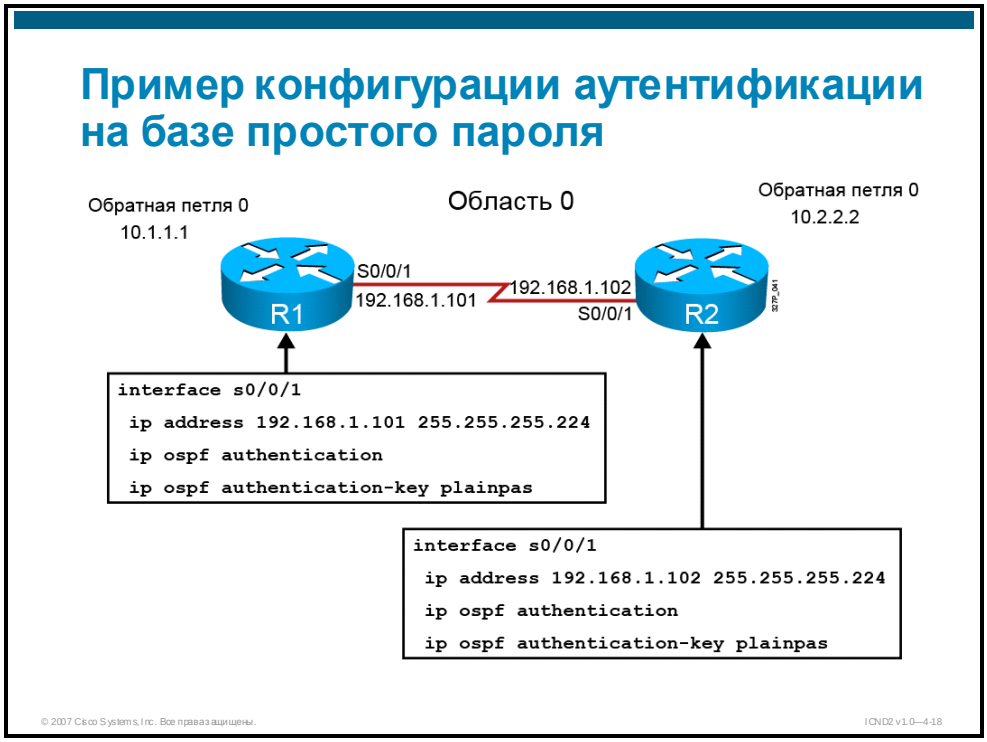
Параметр	Описание
`message-digest`	(Необязательно) Активирует аутентификацию MD5.
`null`	(Необязательно) Отключает аутентификацию. Этот параметр может быть полезен для переопределения аутентификации на основе пароля или MD5, если она настроена в области.

Чтобы включить аутентификацию на базе нешифрованного пароля, введите команду **ip ospf authentication** без параметров. Перед вводом этой команды, задайте пароль для интерфейса с помощью команды **ip ospf authentication-key**.

Команда **ip ospf authentication** была добавлена в версии Cisco IOS 12.0. Для обратной совместимости поддержка типа аутентификации для области сохранена. Если тип аутентификации для интерфейса не указан, используется тип аутентификации, заданный для области (по умолчанию для области задается нулевая аутентификация). Чтобы включить аутентификацию для области OSPF, используйте команду конфигурации маршрутизатора **area** *идентификатор области* **authentication [message-digest]**.

Параметры команды area authentication

Параметр	Описание
`идентификатор области`	Идентификатор области, для которой необходимо включить аутентификацию. В качестве идентификатора можно указать десятичное значение или IP-адрес.
`message-digest`	(Необязательно) Включает аутентификацию MD5 для области, указанной в аргументе *идентификатор области*.

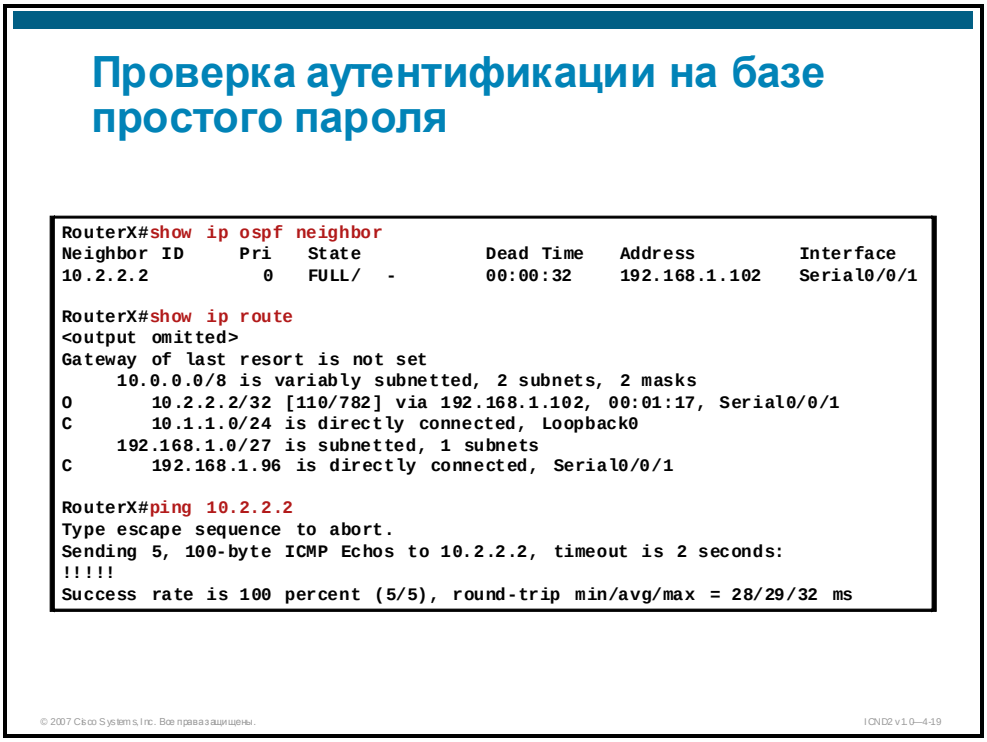


Пример: конфигурация аутентификации на базе нешифрованного пароля

На рисунке изображена сеть, которая используется для демонстрации настройки, проверки и устранения неполадок аутентификации на базе нешифрованного пароля.

Аутентификация на базе простого пароля настраивается на последовательном интерфейсе 0/0/1 с помощью команды ip ospf **authentication**. Для интерфейса задается ключ аутентификации "plainpas".

Обратите внимание, что для соединенных интерфейсов маршрутизаторов X и Y настраиваются одинаковые ключи аутентификации.



Проверка аутентификации на базе нешифрованного ключа

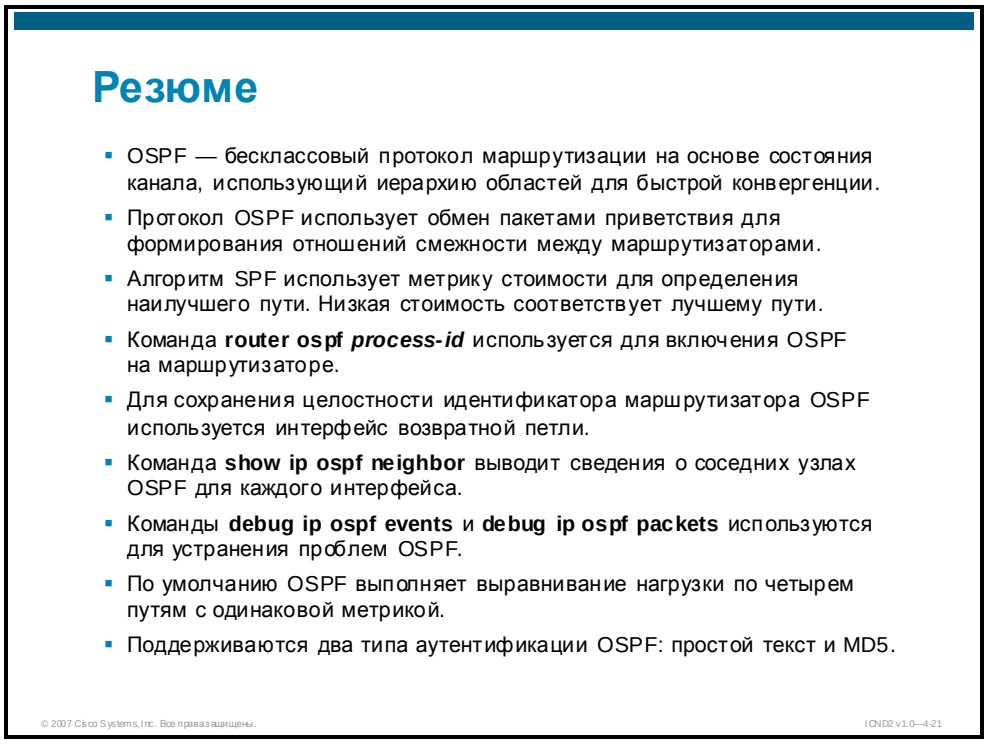
На рисунке приводится вывод команд show ip ospf neighbor и show ip route.

Обратите внимание, что если маршрутизатор имеет состояние FULL, это значит, что два маршрутизатора успешно сформировали смежность OSPF. Таблица маршрутизации подтверждает, что адрес 10.2.2.2 был получен через протокол OSPF от последовательного подключения.

В результате отправки эхо-запрос в маршрутизатор Y также отображается адрес интерфейса возвратной петли, что доказывает работоспособность канала.

Резюме

В этом разделе приводится резюме основных вопросов, рассмотренных в занятии.



Занятие 2

Устранение неполадок OSPF

Обзор

Будучи протоколом состояния канала, OSPF масштабируется с ростом сети. Но эта масштабируемость усложняет проектирование, настройку и обслуживание сети. В этом занятии описывается несколько общих проблем, возникающих в сети OSPF, а также метод поиска и устранения этих проблем на основе рабочей диаграммы.

Задачи

По окончании этого занятия вы сможете определять методы поиска и изоляции распространенных проблем OSPF, а также предлагать решения этих проблем. Это значит, что вы сможете выполнять следующие задачи:

- описывать основные составляющие процедуры поиска и устранения неполадок OSPF;
- выявлять и устранять ошибки, связанные с отношениями смежности между соседними узлами OSPF;
- выявлять и устранять ошибки, связанные с таблицами маршрутизации OSPF;
- выявлять и устранять проблемы аутентификации.

Составляющие процедуры поиска и устранения неполадок OSPF

В этом разделе описываются основные составляющие процедуры поиска и устранения неполадок OSPF.

Основные составляющие процедуры поиска и устранения неполадок OSPF:

- смежность между соседним маршрутизаторами OSPF;
- таблица маршрутизации OSPF;
- аутентификация OSPF.

Поиск и устранение неполадок смежности между соседними маршрутизаторами OSPF

В этом разделе описывается выявление и устранение ошибок, связанных с отношениями смежности между соседними маршрутизаторами OSPF.

Исправное состояние соседства OSPF — "Full". Любое другое состояние соседства OSPF указывает на проблему. Ниже приводится пример вывода команды **show ip ospf neighbor**:

```
RouterX# sh ip ospf neighbor
Neighbor ID     Pri   State   Dead Time   Address         Interface
172.16.31.100     0   Full/   - 00:00:31    10.140.1.1      Serial0/0/0
192.168.1.81      0   Full/   - 00:00:31    10.23.23.2      Serial0/0/1
```

Чтобы определить, существует ли проблема подключения на первом или втором уровнях, выведите сведения о состоянии интерфейса с помощью команды **show ip ospf neighbor**. Состояние "Administratively Down" указывает на то, что интерфейс не включен. Если состояние интерфейса отлично от "up/up", смежность между соседними узлами OSPF сформирована не будет. В этом примере последовательный интерфейс 0/0/1 находится в состоянии "up/up".

```
RouterX# sh ip ospf interface
Serial0/0/1 is up, line protocol is up
  Internet Address 10.23.23.1/24, Area 0
  Process ID 100, Router ID 192.168.1.65, Network Type POINT_TO_POINT,
Cost: 1562
```

Чтобы протокол OSPF мог сформировать смежность с соседним маршрутизатором, подключенным напрямую, два маршрутизатора должны иметь одинаковые размеры MTU. Чтобы проверить размер MTU интерфейса используйте команду **show interface**. В этом примере размер MTU составляет 1 500 байт.

```
RouterX# sh ip int fa0/0
FastEthernet0/0 is up, line protocol is up
  Internet address is 10.2.2.3/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
```

Команда **network**, выполненная для процесса маршрутизации OSPF, выводит данные о том, какие интерфейсы маршрутизатора участвуют в процессе OSPF и к какой области они принадлежат. Если интерфейс отображается в выводе команды **show ip ospf interface**, значит он работает под управлением протокола OSPF. В этом примере под управлением OSPF работают последовательные интерфейсы 0/0/1 и 0/0/0.

```
RouterX# sh ip ospf interface
Serial0/0/1 is up, line protocol is up
  Internet Address 10.23.23.1/24, Area 0
  Process ID 100, Router ID 192.168.1.65, Network Type POINT_TO_POINT,
Cost: 1562
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:04
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.1.81
  Suppress hello for 0 neighbor(s)
  Simple password authentication enabled

Serial0/0/0 is up, line protocol is up
  Internet Address 10.140.1.2/24, Area 0
  Process ID 100, Router ID 192.168.1.65, Network Type POINT_TO_POINT,
Cost: 1562
  Transmit Delay is 1 sec, State POINT_TO_POINT,
```

Маршрутизаторы OSPF обмениваются пакетами приветствия для формирования смежности. Пакет приветствия OSPF включает 4 информационных элемента, которые должны совпасть для формирования смежности OSPF:

- идентификатор области;
- интервалы приветствия и простоя;
- пароль для аутентификации;
- флаг шлейфной области.

Чтобы определить, совпадают ли эти параметры используйте команду **debug ip ospf adj**. Вывод ниже иллюстрирует успешное формирование смежности на интерфейсе 0/0/1.

```
*Feb 17 18:41:51.242: OSPF: Interface Serial0/0/1 going Up

*Feb 17 18:41:51.742: OSPF: Build router LSA for area 0,
router ID 10.1.1.1, seq 0x80000013

*Feb 17 18:41:52.242: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Serial0/0/1, changed state to up

*Feb 17 18:42:01.250: OSPF: 2 Way Communication to 10.2.2.2 on
Serial0/0/1, state 2WAY

*Feb 17 18:42:01.250: OSPF: Send DBD to 10.2.2.2 on
Serial0/0/1 seq 0x9B6 opt 0x52 flag 0x7 len 32

*Feb 17 18:42:01.262: OSPF: Rcv DBD from 10.2.2.2 on
Serial0/0/1 seq 0x23ED opt0x52 flag 0x7 len 32  mtu 1500 state
EXSTART

*Feb 17 18:42:01.262: OSPF: NBR Negotiation Done. We are the
SLAVE

*Feb 17 18:42:01.262: OSPF: Send DBD to 10.2.2.2 on
Serial0/0/1 seq 0x23ED opt 0x52 flag 0x2 len 72

*Feb 17 18:42:01.294: OSPF: Rcv DBD from 10.2.2.2 on
Serial0/0/1 seq 0x23EE opt0x52 flag 0x3 len 72  mtu 1500 state
EXCHANGE

*Feb 17 18:42:01.294: OSPF: Send DBD to 10.2.2.2 on
Serial0/0/1 seq 0x23EE opt 0x52 flag 0x0 len 32

*Feb 17 18:42:01.294: OSPF: Database request to 10.2.2.2

*Feb 17 18:42:01.294: OSPF: sent LS REQ packet to
192.168.1.102, length 12

*Feb 17 18:42:01.314: OSPF: Rcv DBD from 10.2.2.2 on
Serial0/0/1 seq 0x23EF opt0x52 flag 0x1 len 32  mtu 1500 state
EXCHANGE

*Feb 17 18:42:01.314: OSPF: Exchange Done with 10.2.2.2 on
Serial0/0/1

*Feb 17 18:42:01.314: OSPF: Send DBD to 10.2.2.2 on
Serial0/0/1 seq 0x23EF opt 0x52 flag 0x0 len 32

*Feb 17 18:42:01.326: OSPF: Synchronized with 10.2.2.2 on
Serial0/0/1, state FULL

*Feb 17 18:42:01.330: %OSPF-5-ADJCHG: Process 10, Nbr 10.2.2.2
on Serial0/0/1 from LOADING to FULL, Loading Done

*Feb 17 18:42:01.830: OSPF: Build router LSA for area 0,
router ID 10.1.1.1, seq 0x80000014
```

Поиск и устранение неполадок таблиц маршрутизации OSPF

В этом разделе описывается выявление и устранение ошибок таблиц маршрутизации OSPF.

Запись маршрута OSPF в таблице маршрутизации может включать различные коды:

- **O:** внутриобластной маршрут OSPF от маршрутизатора в той же области OSPF;
- **O IA:** межобластной маршрут OSPF от маршрутизатора в другой области OSPF;
- **O E1 or E2:** внешний маршрут OSPF из другой автономной системы.

В сети с одной областью OSPF в таблице маршрутизации не должно быть маршрутов O IA. В этом примере присутствуют маршруты O IA и O E2.

```
RouterX# sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       ia - IS-IS inter area, * - candidate default,       o - ODR, P
- periodic downloaded static route
Gateway of last resort is not set
     172.16.0.0/32 is subnetted, 1 subnets
O       172.16.31.100 [110/1563] via 10.140.1.1, 00:03:15, Serial0/0/0
     10.0.0.0/24 is subnetted, 5 subnets
C       10.2.2.0 is directly connected, FastEthernet0/0
```



```
O IA       10.1.1.0 [110/1563] via 10.140.1.1, 00:03:15, Serial0/0/0
O       10.140.2.0 [110/3124] via 10.140.1.1, 00:03:15, Serial0/0/0
                   [110/3124] via 10.23.23.2, 00:03:15, Serial0/0/1
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.64/28 is directly connected, Loopback0
O E2  192.168.1.81/32 [110/1563] via 10.23.23.2, 00:03:17, Serial0/0/1
```

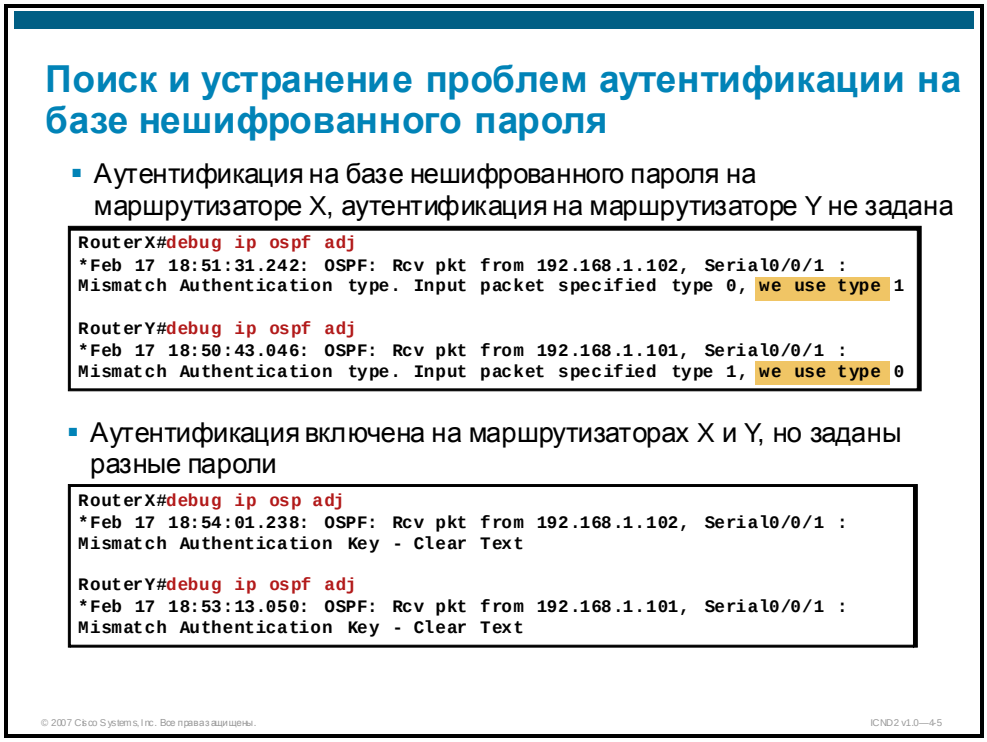
Кроме того, команда **network** процесса маршрутизации OSPF отображает сведения о сетях, которые объявляются OSPF.

Команда **show ip protocols** позволяет узнать, заданы ли фильтры маршрутов, которые влияют на маршруты, отображаемые в таблице маршрутизации. Кроме того, эта команда, как показано в следующем примере, отображает сети, которые настроены для объявления другим маршрутизаторам.

```
RouterX# sh ip protocols
Routing Protocol is "ospf 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.1.65
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.2.2.3 0.0.0.0 area 0
    10.23.23.1 0.0.0.0 area 0
    10.140.1.2 0.0.0.0 area 0
    192.168.1.65 0.0.0.0 area 0
 Reference bandwidth unit is 100 mbps
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.1.81         110      00:04:52
    172.16.31.100        110      00:04:52
  Distance: (default is 110)
```

Устранение неполадок аутентификации на базе нешифрованного пароля

В этом разделе описывается поиск и устранение неполадок аутентификации на базе нешифрованного пароля.



Команда **debug ip ospf adj** используется для вывода событий OSPF, связанных со смежностью. Она очень полезна при поиске и устранении неполадок аутентификации.

Пример: устранение проблем аутентификации на базе нешифрованного пароля

Если аутентификация на базе нешифрованного пароля настроена на последовательном интерфейсе 0/0/1 маршрутизатора X, но не настроена на последовательном интерфейсе 0/0/1 маршрутизатора Y, эти маршрутизаторы не смогут сформировать смежность на данном канале. В соответствии с выводом команды **debug ip ospf adj** в верхней части рисунка, маршрутизаторы сообщают о несовпадении типа аутентификации. Пакеты OSPF не будут отправляться между соседними маршрутизаторами.

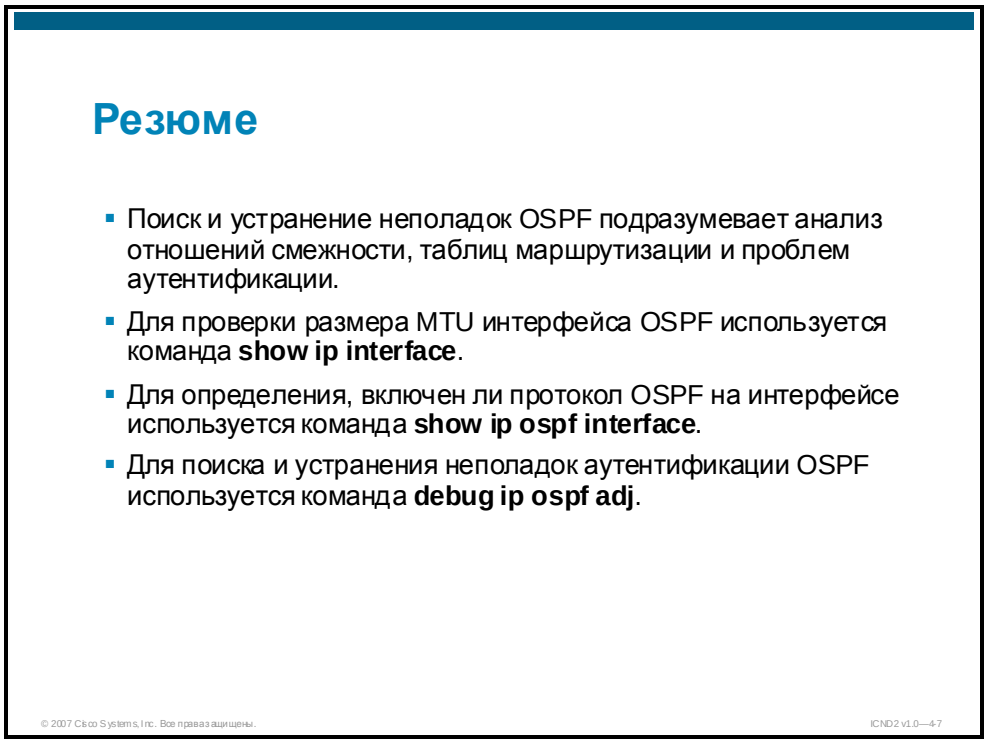
Примечание	Типы аутентификации имеют следующие коды: нулевая аутентификация — тип 0, нешифрованный пароль — тип 1, MD5 — тип 2.

Если аутентификация на базе нешифрованного пароля настроена на последовательном интерфейсе 0/0/1 маршрутизатора X и на последовательном интерфейсе 0/0/1 маршрутизатора Y, но для них заданы разные пароли, эти маршрутизаторы не смогут сформировать смежность на данном канале.

В соответствии с выводом команды debug ip ospf adj в нижней части рисунка, маршрутизаторы сообщают о несовпадении ключа аутентификации. Пакеты OSPF не будут отправляться между соседними маршрутизаторами.

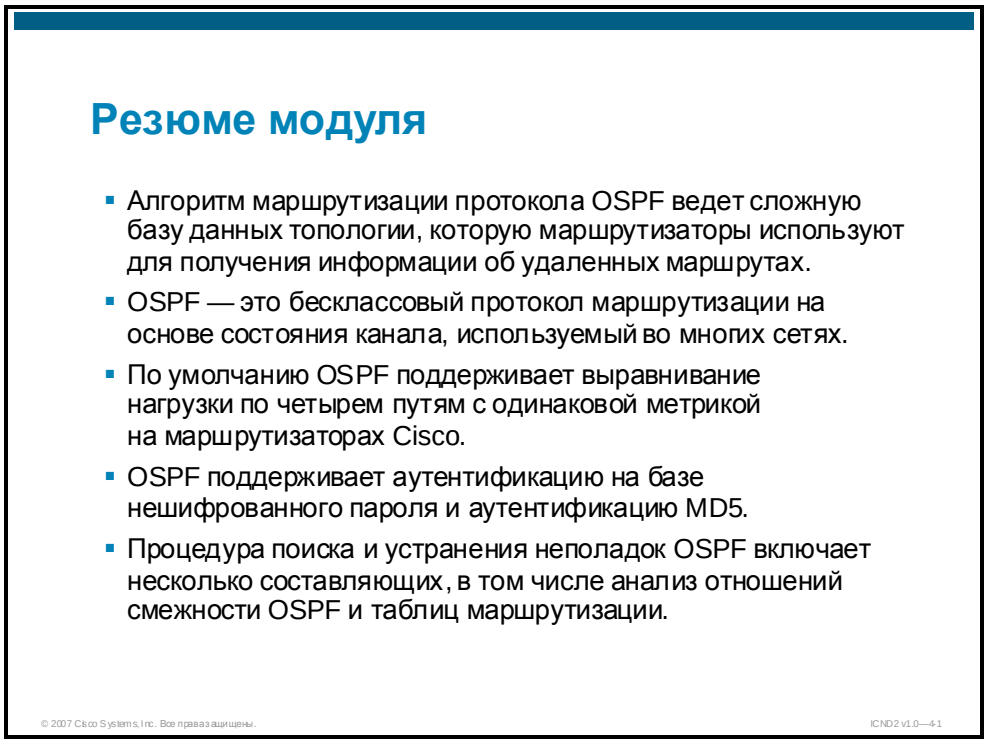
Резюме

В этом разделе приводится резюме основных вопросов, рассмотренных в занятии.



Резюме модуля

В этом разделе приводится резюме вопросов, рассмотренных в модуле.



В этом модуле рассматривается протокол OSPF, один из самых распространенных протоколов внутреннего шлюза для IP-сетей. OSPF — сложный протокол на основе открытых стандартов, определяющий несколько процедур установления связи, объявлений БД и типов пакетов.

Вопросы для самопроверки по модулю

Используйте эти вопросы, чтобы проверить, насколько хорошо вы освоили материал, представленный в данном модуле. Верные ответы и решения можно найти в разделе "Ответы на вопросы для самопроверки".

B1 Каковы две характеристики протокола OSPF? (Выберите два варианта.) (Источник: внедрение OSPF)

А) OSPF использует двухуровневую иерархию сети;
Б) OSPF — проприетарный протокол маршрутизации.
В) OSPF является открытым стандартом.
Г) Протокол OSPF аналогичен протоколу RIP.
Д) OSPF протокол маршрутизации на основе вектора расстояния.

B2 OSPF направляет пакеты внутри одной/одного _____. (Источник: внедрение OSPF)

А) области
Б) сети
В) сегменте
Г) автономной системе

B3 В ходе процесса OSPF каждый маршрутизатор создает свое дерево SPF на основе одинаковых данных о состоянии канала, но каждый будет иметь собственное/собственную _____ топологии. (Источник: внедрение OSPF)

А) состояние
Б) представление
В) версию
Г) конфигурацию

B4 Какой компонент алгоритма SPF обратно пропорционален полосе пропускания? (Источник: внедрение OSPF)

А) стоимость
Б) стоимость корня
В) состояние канала
Г) количество переходов

B5 Какая команда запускает процесс маршрутизации OSPF с идентификатором 191? (Source: Implementing OSPF)

А) Router(config)**#router ospf 191**
Б) Router(config)**#network ospf 191**
В) Router(config-router)**#network ospf 191**
Г) Router(config-router)**#router ospf process-id 191**

B6 Каково назначение команды **show ip ospf interface**? (Источник: внедрение OSPF)

А) выводит сведения об интерфейсе, связанные с OSPF
Б) выводит общие сведения о процессах маршрутизации OSPF
В) отображает сведения о соседних узлах OSPF для интерфейсов
Г) отображает сведения о соседних узлах OSPF для типов интерфейсов

В7 Вывод какой команды включают сведения о длине пакета OSPF? (Источник: устранение неполадок OSPF)

А) debug ip ospf events
Б) **debug ip ospf packet**
В) **debug ip ospf packet size**
Г) **debug ip ospf mpls traffic-eng advertisements**

В8 Какой тип аутентификации обозначает код aut:1 в выводе команды **debug ip ospf packet**? (Источник: устранение неполадок OSPF)

А) аутентификация не используется
Б) нешифрованный пароль
В) MD5
Г) 3DES

В9 Какое состояние соседства OSPF указывает, что два маршрутизатора обменялись маршрутами? (Источник: устранение неполадок OSPF)

А) init
Б) two-way
В) loading
Г) full

Ответы на вопросы для самопроверки по модулю

В1	А, В
В2	Г
В3	Б
В4	А
В5	А
В6	А
В7	Б
В8	Б
В9	Г

