ICND1

Interconnecting Cisco Networking Devices Part 1

Том 1

Версия 1.0

Руководство для студента

Номер текста по каталогу: 97-2567-01

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

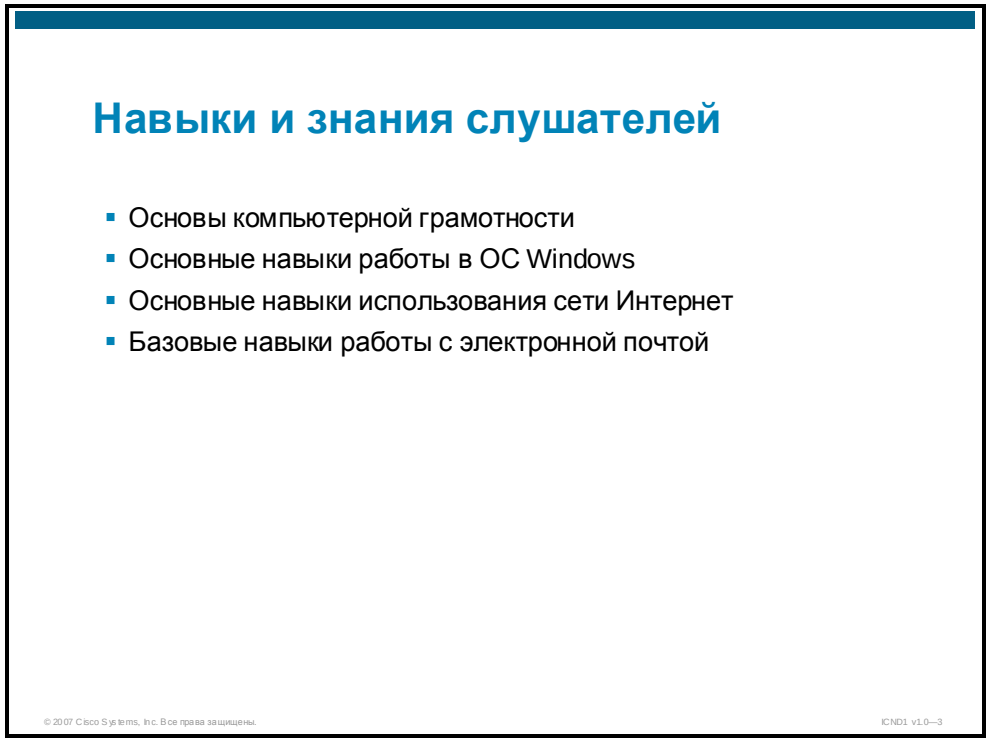
Введение в курс

Обзор

«Что необходимо знать для поддержания работоспособности сети?» Ответ на этот вопрос зависит от размера и уровня сложности вашей сети. К счастью, начальный этап обучения поддержке сети не зависит ни от ее размера, ни от степени сложности. Этот курс и должен стать этим начальным этапом. Он нацелен на выработку навыков и получение знаний, необходимых для внедрения небольших коммутируемых и маршрутизируемых сетей.

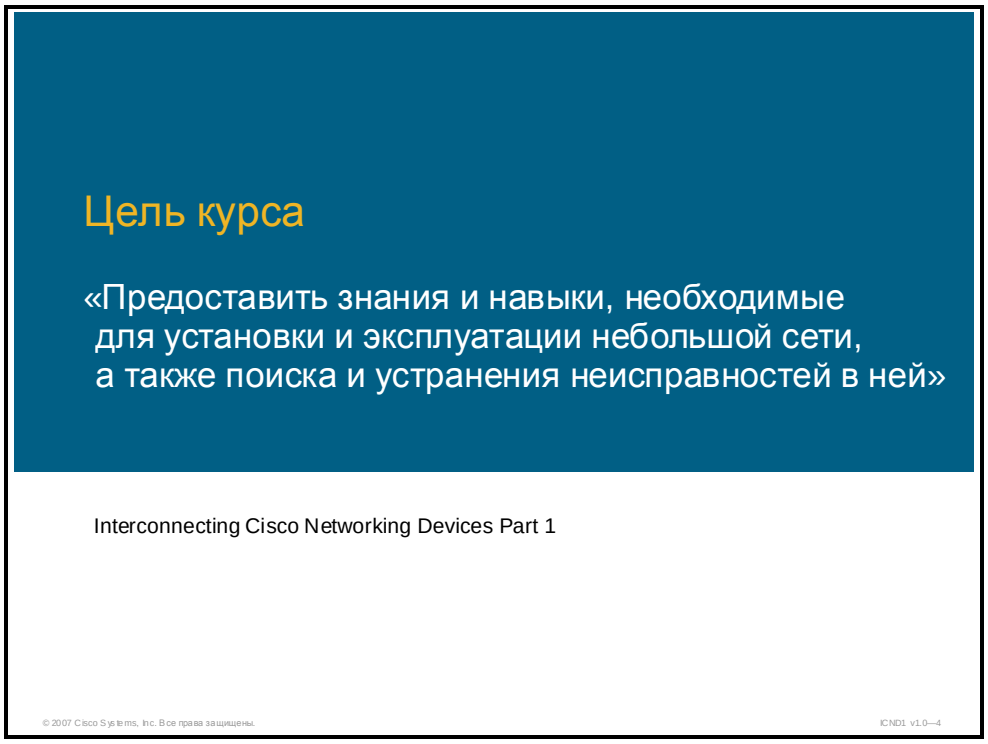
Навыки и знания слушателей

В этом разделе перечисляются навыки и знания, которыми слушатели должны обладать, чтобы извлечь максимальную пользу из этого курса. Кроме того, здесь приводятся рекомендуемые предложения Cisco по обучению, которые слушатели должны пройти, чтобы получить максимум от этого курса.



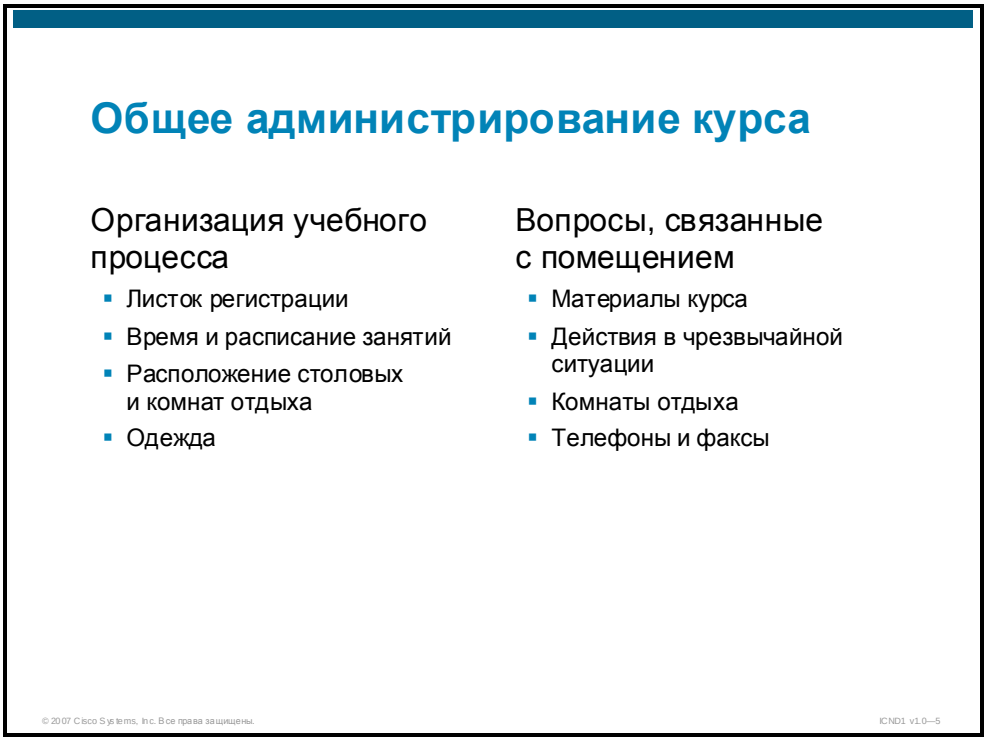
Цели и задачи курса

В этом разделе описываются цели и задачи курса.



По окончании этого курса вы будете способны выполнить следующие задачи:

- описывать работу сетей, выделять основные компоненты, функции компонентов сети и понимать эталонную модель OSI;
- используя процесс доставки пакетов данных между хостами, описывать проблемы, связанные с увеличением трафика в локальной сети Ethernet, и применять технологии коммутации для решения проблем сетей Ethernet;
- описывать причины, по которым необходимо расширение области функционирования локальных сетей, и объяснять конкретные способы, основанные на беспроводном РЧ-доступе;
- описывать причины, по которым необходимо соединение сетей с использованием маршрутизаторов, и методы передачи данных в маршрутизируемых сетях на основе протокола TCP/IP;
- описывать функции и основные устройства РВС (WAN), настраивать инкапсуляцию PPP, статическую и динамическую маршрутизацию, настраивать преобразование PAT и маршрутизацию RIP;
- использовать интерфейс командной строки (CLI) для обнаружения соседних узлов в сети, а также для управления запуском и настройки маршрутизатора.

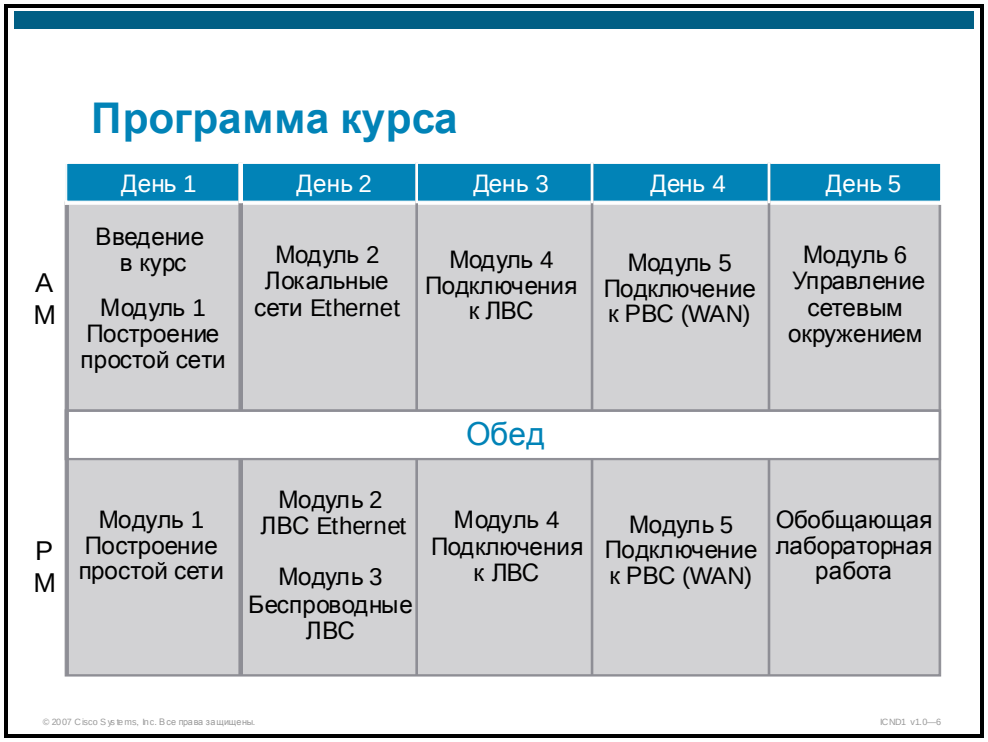


Инструктор обсудит эти организационные вопросы, чтобы дать слушателям представление о том, чего им следует ждать от курса:

- 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

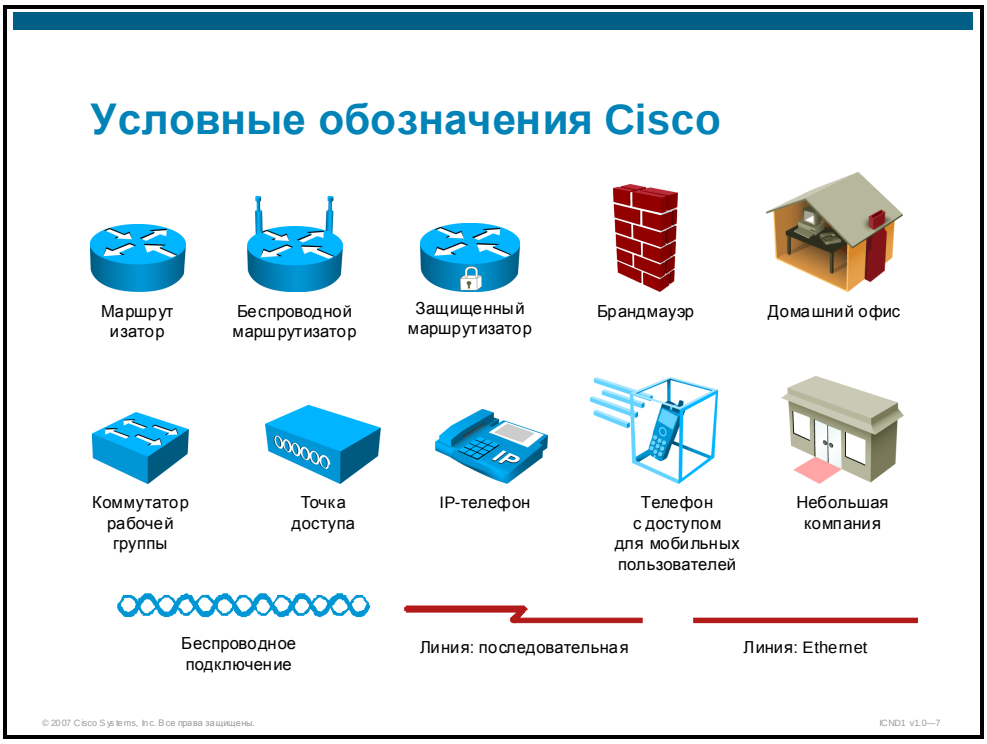
В этом разделе представлена рекомендуемая последовательность освоения материалов курса.



Этот график отражает рекомендуемую структуру курса. Эта структура дает достаточно времени, чтобы инструктор мог донести информацию курса до вас, и чтобы вы 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.

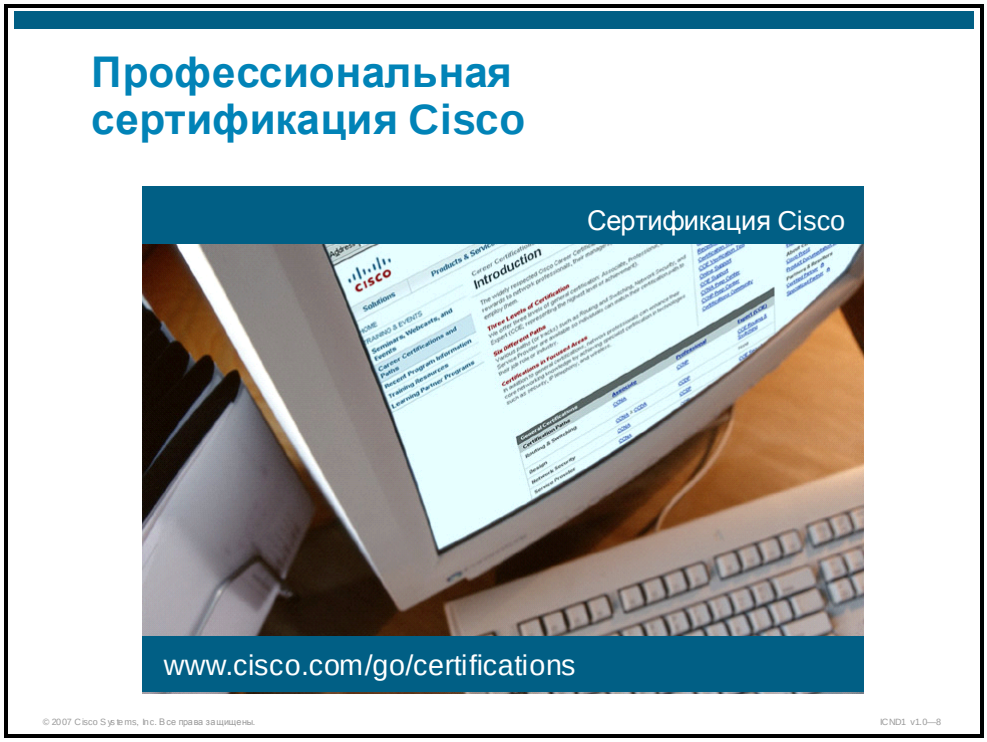


Глоссарий терминов Cisco

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.

План подготовки специалистов

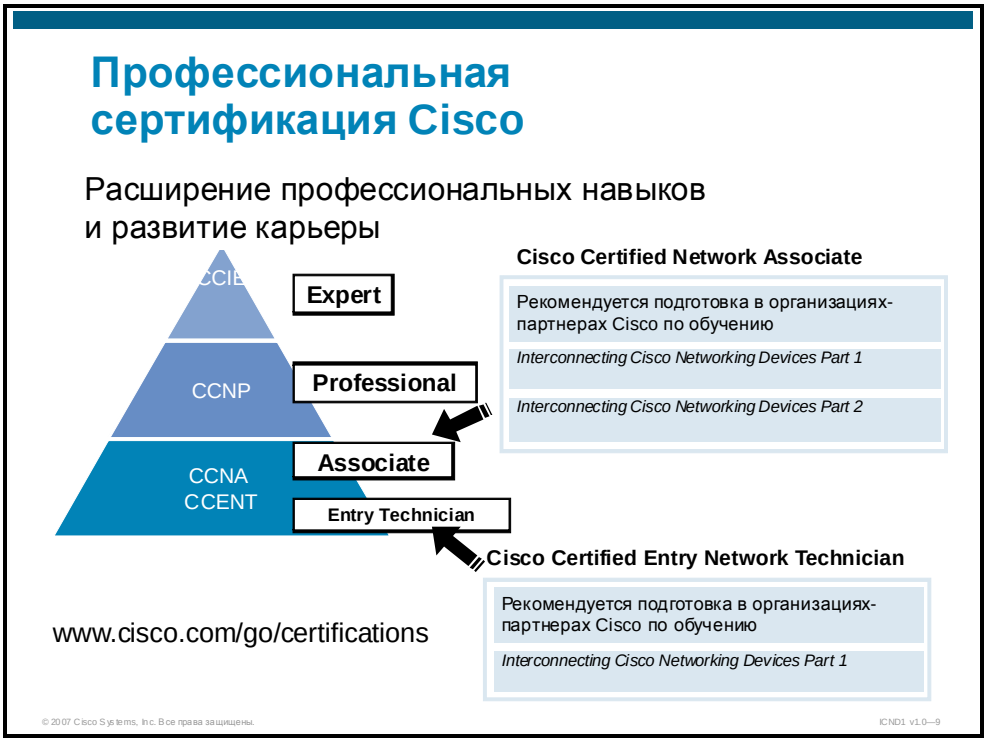
В этом разделе представлен учебный план курса.



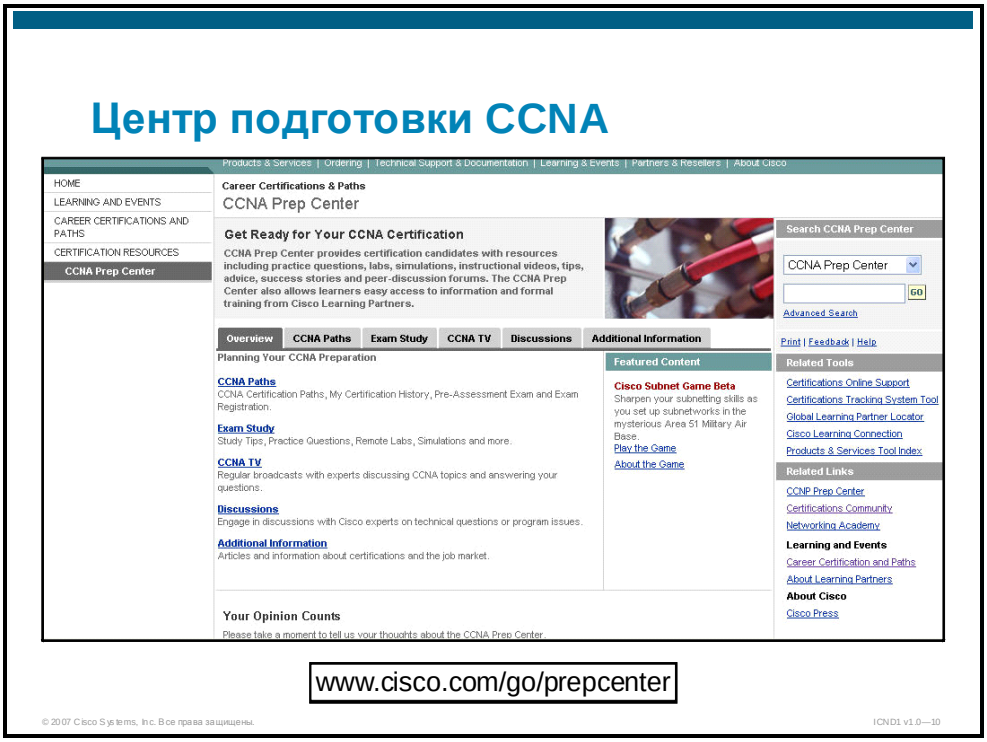
Мы предлагаем вам присоединиться к сообществу сертификации Cisco, форум открыт для всех владельцев профессиональных сертификатов Cisco (таких как Cisco CCIE®, CCNA®, CCDA®, CCNP®, CCDP®, CCIP®, CCVP™ или CCSP®). Форум представляет собой место встречи для сертифицированных профессионалов Cisco, где они 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.

План курсов для подготовки специалистов

В этом подразделе представлен учебный план для этого курса.



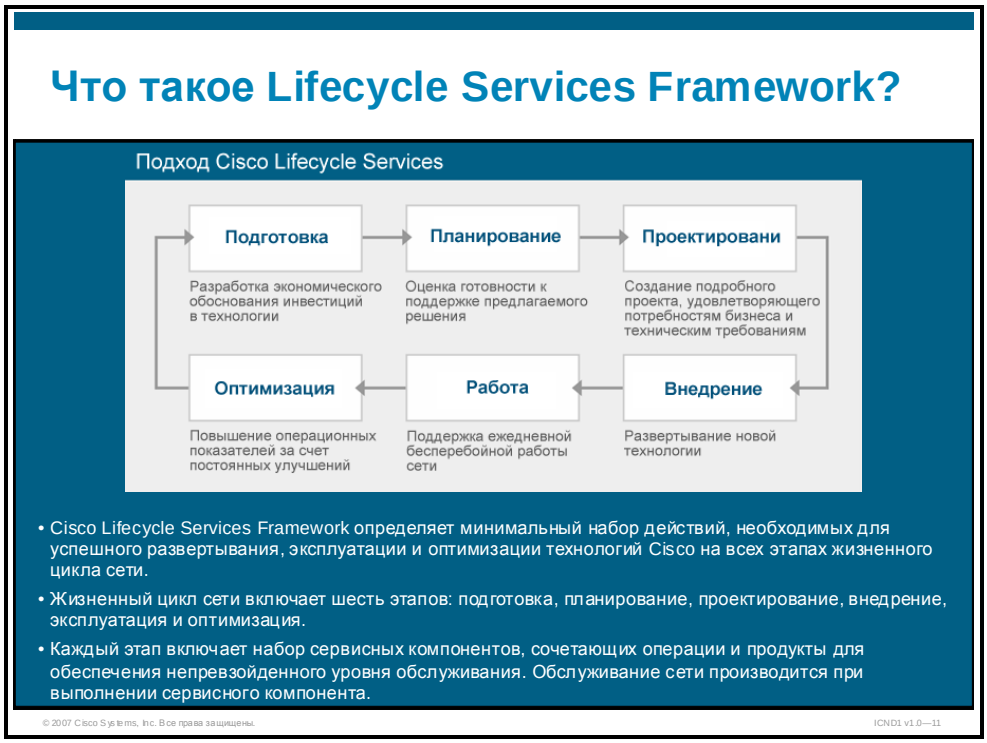
Дополнительные сведения о сертификации см. по адресу http://www.cisco.com/go/certifications.



См. дополнительные сведения по адресу http://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 развертывания 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 на основании бизнес-требований.
  - Уменьшение потребности в последующих изменениях за счет создания концептуальной архитектуры.
- **Планирование:** создание основы для своевременного и беспрепятственного внедрения.
  - Оценка сети и площадок.
  - Разработка плана управления проектом.
- **Проектирование:** снижение риска модификаций, быстрое и успешное внедрение.
  - Разработка всестороннего детального проекта, отвечающего как бизнес-, 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 связей между площадками. В современных условиях методы поиска и устранения отдельных уязвимостей и «точечных» проблем сети перестают быть приемлемыми, поскольку затраты, связанные с нарушениями и прерываниями работы систем безопасности высоки и могут принимать множество форм – простой сети, кража конфиденциальной информации, упущенная прибыль, потеря престижа фирмы и так далее.

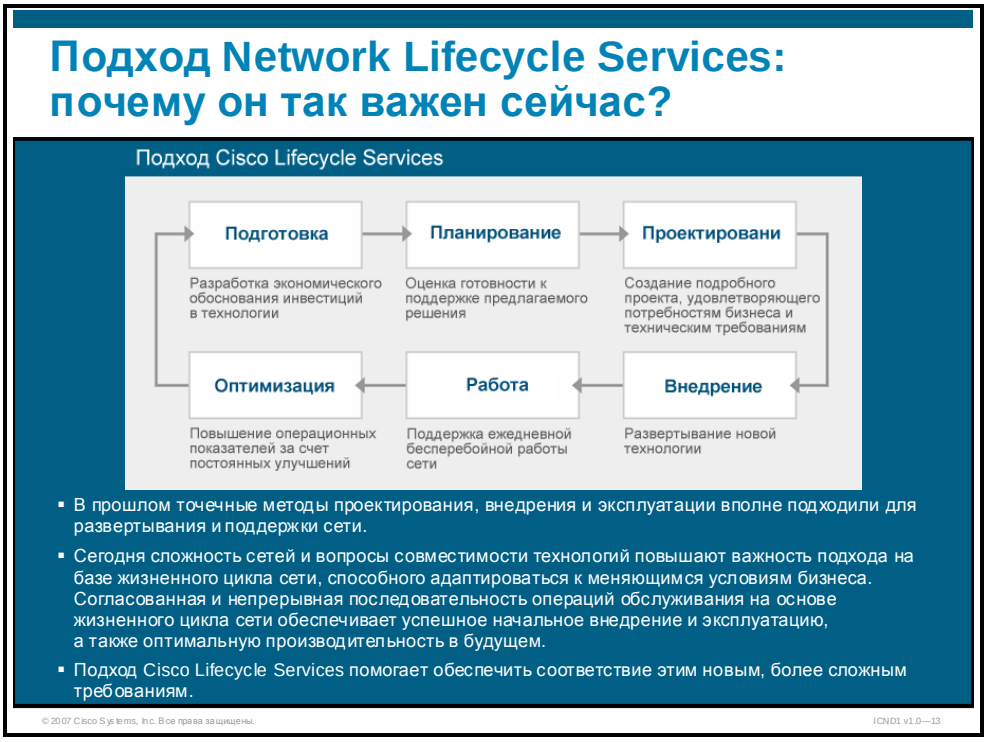
В настоящее время используется другой подход к решениям по безопасности:

- теперь безопасность требует системного подхода, подразумевающего защиту всей сети – периметра, ЦОД, локальных сетей комплексов зданий, беспроводных локальных сетей (WLAN) рабочих станций и конечных 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 с возможностями сети и техническими требованиями.

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.

Пожалуйста, представьтесь

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

ICND1 v1.0—14

Подготовьте следующие сведения о себе

- 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

Построение простой сети

Обзор

Для понимания работы сетей необходимо получить базовые знания об их основных компонентах. В этом модуле даются сведения об основных компонентах сети: перечисляются базовые компоненты компьютеров и сетей и их характеристики, функции, преимущества, достоинства и показатели, используемые для классификации функций и рабочих характеристик. Кроме того, в этом модуле описывается эталонная модель взаимодействия открытых систем (OSI), а также терминология и концепции, необходимые для описания процесса обмена данными. Наконец, в этом модуле объясняется создание сети хостов на базе локальной сети Ethernet.

Задачи модуля

По окончании этого модуля вы сможете создавать простые сети для соединения хостов, а также описывать компоненты сети и их функции. Это значит, что вы сможете выполнять следующие задачи:

- перечислять преимущества компьютерных сетей и их функции;
- выявлять общие угрозы для сетей и способы уменьшения воздействия этих угроз;
- понимать и сравнивать модели обмена данными, которые управляют связью между хостами;
- описывать классификацию IP-адресов и способы получения IP-адреса хостом;
- описывать процессы, используемые протоколом TCP для установления надежного соединения;
- описывать процессы передачи пакетов между хостами;
- описывать работу Ethernet на 1-ом и 2-ом уровнях модели OSI;
- определять методы подключения к локальной сети Ethernet.

Занятие 1

Обзор функций сети

Обзор

Для максимально эффективного использования каналов связи между конечными пользователями необходимо понимать преимущества и принцип работы компьютерных сетей. В этом занятии описывается концепция компьютерных сетей, перечисляются компоненты компьютерной сети и объясняются преимущества сетей для пользователей.

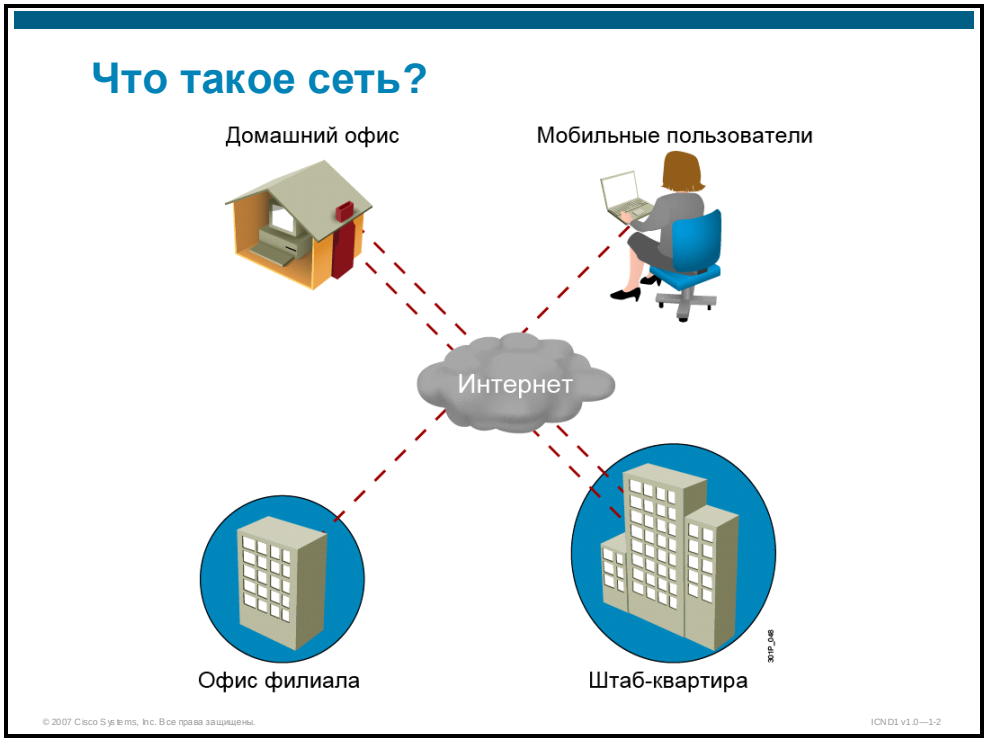
Задачи

По окончании этого занятия вы сможете перечислять стандартные компоненты сети, описывать ее назначение и функции. Это значит, что вы сможете выполнять следующие задачи:

- давать определение сети;
- перечислять стандартные компоненты сети;
- интерпретировать схемы сети;
- перечислять основные функции совместного использования ресурсов сети и их преимущества;
- называть четыре основных пользовательских приложения, требующих доступа к сети, и описывать их преимущества;
- описывать влияние пользовательских приложений на работу сети;
- перечислять категории характеристик, используемых для описания сетей различных типов;
- сравнивать и сопоставлять физические и логические топологии;
- перечислять характеристики шинной топологии;
- перечислять характеристики звездообразной и иерархической звездообразной топологии;
- перечислять характеристики кольцевой и двойной кольцевой топологии;
- перечислять характеристики полносвязной и частичносвязной топологии;
- описывать способы подключения к сети Интернет.

Что такое сеть?

В этом разделе описываются характеристики и среды сетей разных типов и приводятся примеры сетей.



Сеть – это набор устройств и конечных систем (например компьютеров и серверов), которые соединены между собой и могут обмениваться данными друг с другом. Сети служат для передачи данных в различных средах, включая жилые помещения, небольшие компании и крупные предприятия. Крупное предприятие может располагаться на нескольких площадках, которые должны поддерживать связь друг с другом. Эти площадки (то есть места, где находятся сотрудники компании) можно описать следующим образом.

- **Главный офис.** Главный офис – это площадка, в которой все сотрудники связаны через сеть, и где хранится значительная часть данных компании. В главном офисе могут работать сотни и даже тысячи людей, которые нуждаются в доступе к сети для выполнения своих обязанностей. В главном офисе могут использоваться несколько соединенных между собой сетей, охватывающих несколько этажей офисного здания или комплекс зданий (кампус).
- **Удаленные площадки.** Различные удаленные площадки, которые используют сети для связи с главным офисом или между собой.
  - **Филиалы.** В филиалах работают и взаимодействуют через сеть менее многочисленные группы сотрудников. Хотя в филиалах может храниться часть данных компании, более вероятно, что в филиале используются локальные сетевые ресурсы (например, принтеры), но большинство сотрудников получают доступ к информации непосредственно из главного офиса.

— **Домашний офис.** Если сотрудники работают на дому, их место работы называется домашним офисом. Часто сотрудникам, работающим на дому, необходимо подключение по требованию к главному офису или филиалу для доступа к информации или использования сетевых ресурсов (например файлового сервера).

— **Мобильные пользователи.** Мобильные пользователи подключаются к сети главного офиса, находясь в главном офисе, в филиале или в дороге. Требования мобильных пользователей к доступу зависят от того, где они находятся.

Можно использовать сеть в домашнем офисе для подключения к Интернету и поиска информации, размещения заказов на различные товары и обмена сообщениями с друзьями. Также можно организовать небольшой офис, снабженный сетью, соединяющей другие компьютеры и принтеры в офисе. Или можно работать на крупном предприятии, где для обмена данными и для хранения информации большого числа отделов, расположенных на обширных площадях, используется множество компьютеров, принтеров, систем хранения информации и серверов.

Стандартные физические компоненты сети

В этом разделе перечисляются типовые физические компоненты сети, включая ПК, соединительные устройства, коммутаторы и маршрутизаторы.

В компьютерную сеть входят физические компоненты, относящиеся к следующим четырем основным категориям.

- **Персональные компьютеры (ПК).** Компьютеры являются конечными устройствами сети, которые отправляют и получают данные.
- **Соединительные устройства.** Соединительные устройства – это компоненты, позволяющие передавать данные из одной точки сети в другую. В эту категорию входят следующие компоненты:
  - сетевые адаптеры (NIC), которые преобразуют данные компьютера в формат, который позволит передавать их по локальной сети;
  - сетевая среда передачи (например кабели или беспроводные среды), которые служат для передачи сигнала от одного сетевого устройства к другому;
  - разъемы, которые предоставляют точки подключения носителей.
- **Коммутаторы.** Коммутаторы – это устройства, обеспечивающие подключения сети к конечным системам и выполняющие интеллектуальную коммутацию данных внутри локальной сети.
- **Маршрутизаторы.** Маршрутизаторы служат для соединения сетей между собой и выбора наилучшего пути между ними.

Интерпретация схемы сети

В этом разделе описаны стандартные условные обозначения компонентов сети, включая ПК, коммутаторы и маршрутизаторы.

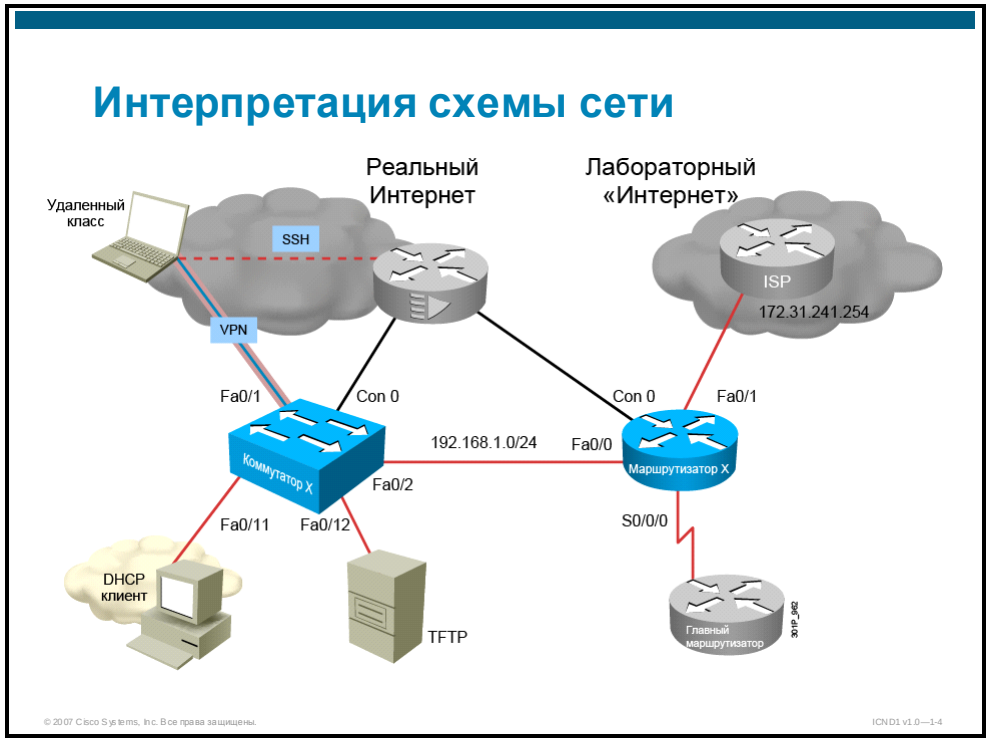


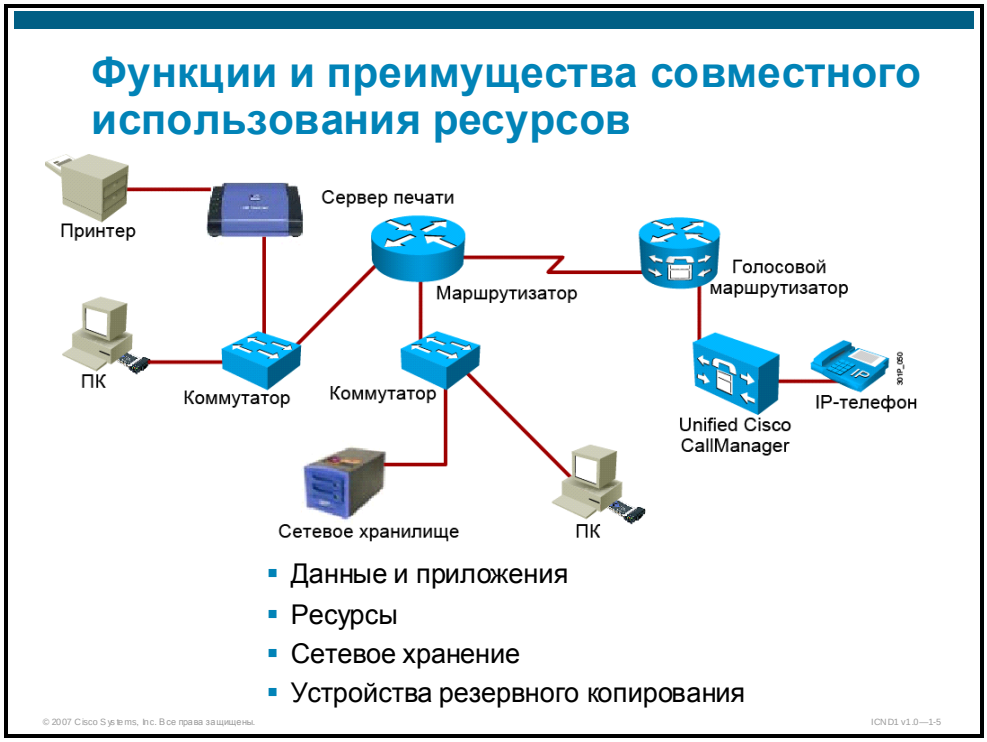
Схема сети используется для отображения информации о ней. Объем и детализация отображаемой информации варьируются в зависимости от организации. Топология сети, как правило, представляется с помощью линий и значков. На этой схеме

-  используется для обозначения сети Интернет.
-  используется для обозначения маршрутизатора.
-  используется для обозначения коммутатора рабочей группы.
-  используется для обозначения сервера.
-  используется для обозначения ПК.
- используется для обозначения канала Ethernet.
-  используется для обозначения последовательного канала.

При наличии свободного места могут быть включены другие сведения. Например, часто указывается интерфейс устройства в следующих форматах: s0/0/0 для последовательного интерфейса или fa0/0 для интерфейса Fast Ethernet. Также часто включают сетевые адреса сегмента в формате 10.1.1.0/24, где 10.1.1.0 обозначает сетевой адрес, а /24 – маску подсети.

Функции и преимущества совместного использования ресурсов

В этом разделе описаны основные функции совместного использования ресурсов в компьютерной сети, и преимущества этих функций для конечных пользователей.



Благодаря использованию сетей конечные пользователи могут совместно использовать как информационные, так и аппаратные ресурсы. Основные ресурсы, которые можно использовать совместно в компьютерной сети перечислены ниже.

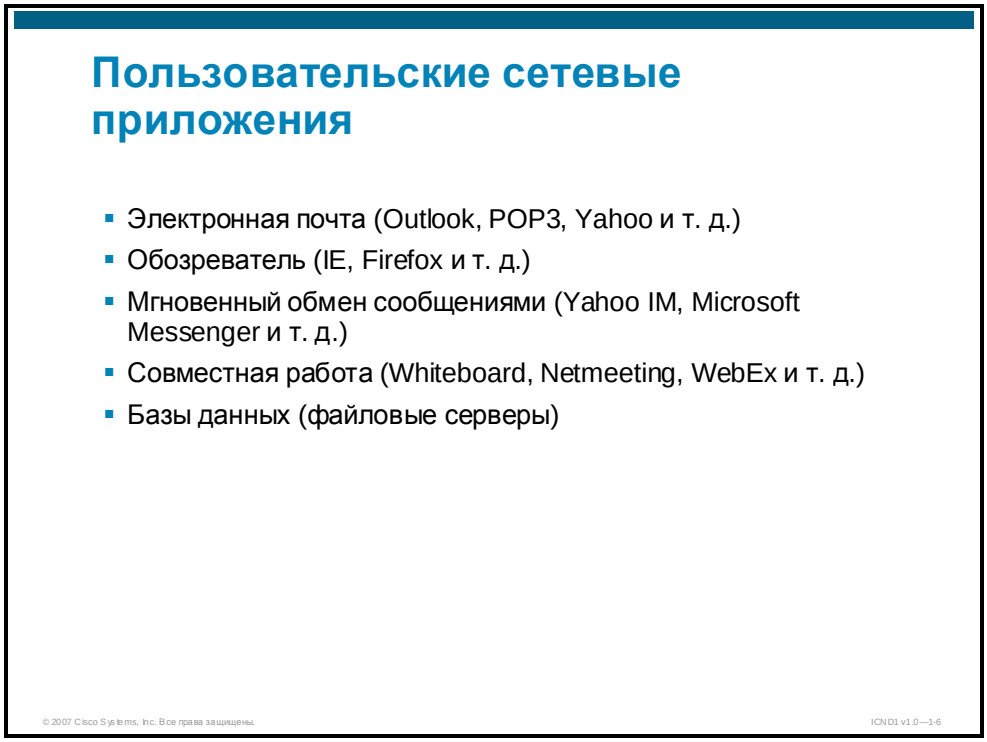
- **Данные и приложения.** Когда пользователи соединены через сеть, они могут совместно использовать файлы и даже приложения, что упрощает доступ к данным и повышает эффективность совместной работы над проектами.
- **Ресурсы.** Возможно совместное использование как устройств ввода (например, камер), так и устройств вывода информации (например, принтеров).
- **Сетевое хранение.** В настоящее время существует несколько способов хранения информации с использованием сети. Система хранения с прямым подключением (Direct Attached Storage - DAS) позволяет напрямую подключить физический носитель к ПК или общему серверу. Система сетевого хранения данных (Network Attached Storage - NAS) позволяет обеспечивает хранение данных с использованием специального сетевого оборудования. И, наконец, сети хранения данных (Storage Aria Networks - SAN) представляют собой сети устройств хранения.
- **Устройства резервного копирования.** Кроме того, в сеть могут входить устройства резервного копирования (например, накопители на магнитной ленте), позволяющие хранить файлы с нескольких компьютеров. Сетевые хранилища также используется для архивирования, обеспечения непрерывности бизнеса и аварийного восстановления.

Общее преимущество для пользователей, подключенных к сети, – это возможность эффективно использовать общие компоненты, необходимые для выполнения повседневных задач (обмена файлов, использования принтеров и хранения данных). Эта эффективность позволяет снизить издержки и повысить производительность.

В последние годы открытость, которая когда-то была доминирующей характеристикой сетей, сменилась необходимостью соблюдать осторожность. Было много хорошо известных случаев «кибервандализма», в ходе которых производилось вторжение как в конечные системы, так и в сетевые устройства. Таким образом, администратору следует найти компромисс между безопасностью сетей и потребностью в сетевых подключениях.

Пользовательские сетевые приложения

Для пользователей в сетевом окружения доступно множество приложений, а некоторые приложения используются практически всеми пользователями. В этом разделе описываются распространенные сетевые пользовательские приложения.



К самым распространенным сетевым пользовательским приложениями относятся:

- **Электронная почта.** Электронная почта – это очень важное приложение для большинства пользователей сети. Пользователи могут оперативно передавать информацию (сообщения и файлы) в электронном виде не только пользователям своей сети, но и пользователям за ее пределами (например поставщикам, на информационные ресурсы и клиентам). Примеры программ для работы с электронной почтой: Microsoft Outlook, Qualcomm Eudora.
- **Обозреватель.** Благодаря обозревателю пользователь может получать доступ в Интернет через общий интерфейс. В Интернете можно получить доступ к огромным объемам информации, и он стал совершенно необходим как для бытовых, так и для корпоративных пользователей. Обозреватели предоставляют общий интерфейс для общения с поставщиками и клиентами, обработки и выполнения заказов и поиска информации. Теперь эти операции, как правило, производятся в электронном виде через Интернет, что позволяет сэкономить время и повысить производительность. К наиболее популярным обозревателям относятся Microsoft Internet Explorer, Netscape Navigator, Mozilla и Firefox
- **Мгновенный обмен сообщениями.** Мгновенный обмен сообщениями появился как средство личного общения между пользователями, однако вскоре он принес значительные выгоды в корпоративный мир. Доступно множество приложений мгновенного обмена сообщениями (таких, как AOL и Yahoo), обеспечивающих функции шифрования и регистрации данных, в которых нуждаются компании.

- **Совместная работа.** Совместная работа групп или отдельных пользователей значительно упрощается при использовании сети. Например, сотрудники, создающие отдельные части ежегодного отчета или бизнес-плана, могут либо передавать свои файлы на центральный ресурс для составления единого документа, либо использовать приложения рабочей группы для создания и изменения всего документа без необходимости в обмене бумажными копиями. Одной из самых известных программ для совместной работы является Lotus Notes.
- **Базы данных.** Приложения этого типа позволяют пользователям в сети хранить информацию на централизованных узлах (например на файловых серверах), чтобы другие пользователи в сети могли легко загрузить выбранную информацию в тех форматах, которые для них наиболее удобны.

Влияние пользовательских приложений на работу сети

Приложения могут влиять на работу сети, а работа сети может влиять на работу приложений. В этом разделе описываются типовое взаимодействие между пользовательскими приложениями и сетью.

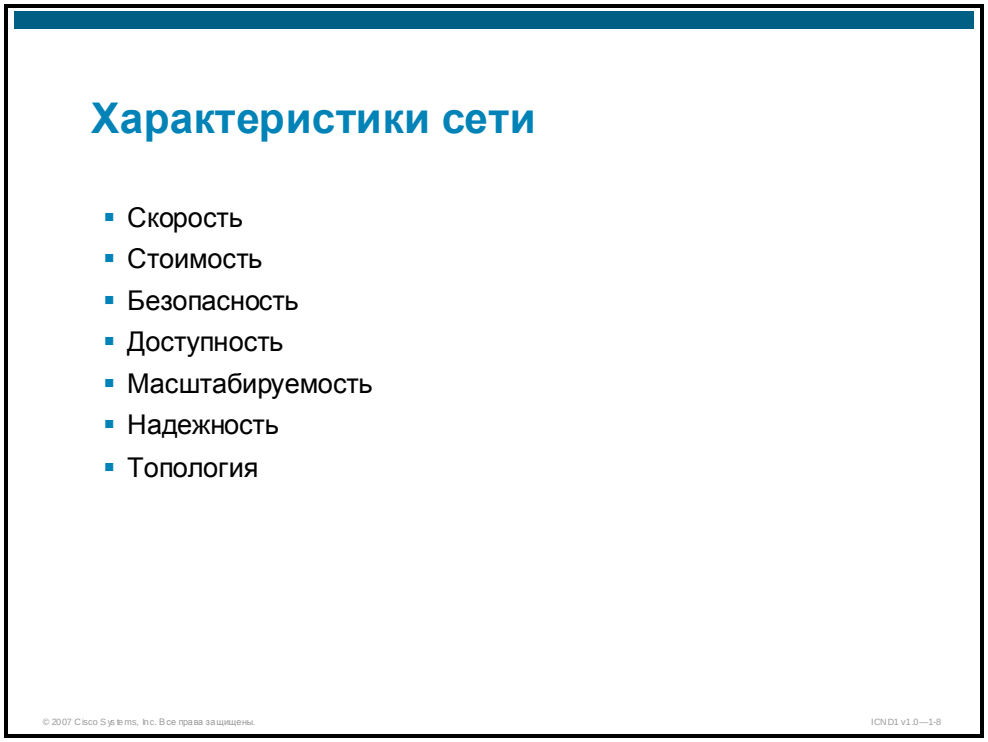
Традиционно при рассмотрении взаимодействия между сетью и приложениями, работающими в ней, основное внимание уделяется полосе пропускания. Такие пакетные приложения, как FTP, TFTP и обновление доступных ресурсов, запускаются пользователем, их работа и завершение управляется программно без прямого вмешательства со стороны пользователя. Поэтому полоса пропускания важна, но не играет решающей роли при условии, что для завершения приложения не требуется слишком много времени. Такие интерактивные приложения, как запросы о доступных ресурсах или обновления баз данных, требуют большего участия человека. Пользователь должен получить с сервера какие-то сведения, а потом ожидать ответа. Полоса пропускания в этом случае более важна, поскольку при сильной задержке ответа пользователи могут проявлять нетерпение. Однако ширина полосы пропускания снова не играет решающей роли, поскольку время ответа зависит не столько от сети, сколько от сервера. В большинстве случаев функции QoS могут преодолеть ограничения, накладываемые полосой пропускания, за счет предоставления интерактивным приложениям приоритета над пакетными приложениями.

Подобно интерактивным приложениям, приложения в реальном времени (например, VoIP и видео-приложения) подразумевают участие человека. Объемы передаваемой информации предъявляют серьезные требования к полосе пропускания. Кроме того, поскольку эти приложения предъявляют значительные требования к синхронизации, большую роль играет время запаздывания (задержка в сети). Даже колебания времени запаздывания могут оказывать влияние на сеть. При этом обязательным является не только приемлемое значение полосы пропускания, но и функции QoS. VoIP и видео-приложения должны получать максимальный приоритет.

Сейчас конечных пользователей атакуют рекламные объявления, указывающие, сколько они смогут сэкономить, перейдя на технологию VoIP, при этом подразумевается, что процесс установки очень несложен и ограничивается установкой в сети маршрутизатора VoIP. Это, как правило, справедливо для домашних сетей, но может привести к катастрофе в небольшой корпоративной сети. Простая установка маршрутизатора VoIP в сети не обеспечивает ни достаточной полосы пропускания для Интернета, ни приемлемой схемы QoS. В результате прежде работавшие приложения начинают выполняться так медленно, что их невозможно использовать, когда кто-нибудь говорит по телефону, и качество голоса значительно снижается. Обе проблемы можно решить путем правильного проектирования сети.

Характеристики сети

В этом разделе описывается набор характеристик, которые обычно используются для описания и сравнения сетей разных типов.



Сети можно описывать и сравнивать, используя следующие характеристики ее производительности и структуры:

- **Скорость.** Скорость определяет, насколько быстро данные передаются по сети. Более точным является термин «скорость передачи данных».
- **Стоимость.** Стоимость включает общую стоимость компонентов, установки и технического обслуживания сети.
- **Безопасность.** Безопасность описывает степень безопасности сети, включая безопасность данных, передаваемых по сети. Безопасность очень важна и постоянно развивается. При выполнении действий, влияющих на сеть, необходимо учитывать проблему безопасности.
- **Доступность.** Доступность описывает вероятность того, что сеть будет доступна для использования, когда это будет необходимо. Для сетей, которые предполагается использовать 24 часа в день, 7 дней в неделю, 365 дней в году, доступность вычисляют, разделив время, когда сеть фактически доступна, на общее время в году, а затем умножив результат на 100, чтобы выразить полученное значение в процентах.

  Например, если сеть недоступна в течение 15 минут в год из-за простоев сети, процент ее доступности можно вычислить следующим образом:

  ([количество минут в году – время простоя сети] / [количество минут в году]) * 100 = процентная доступность

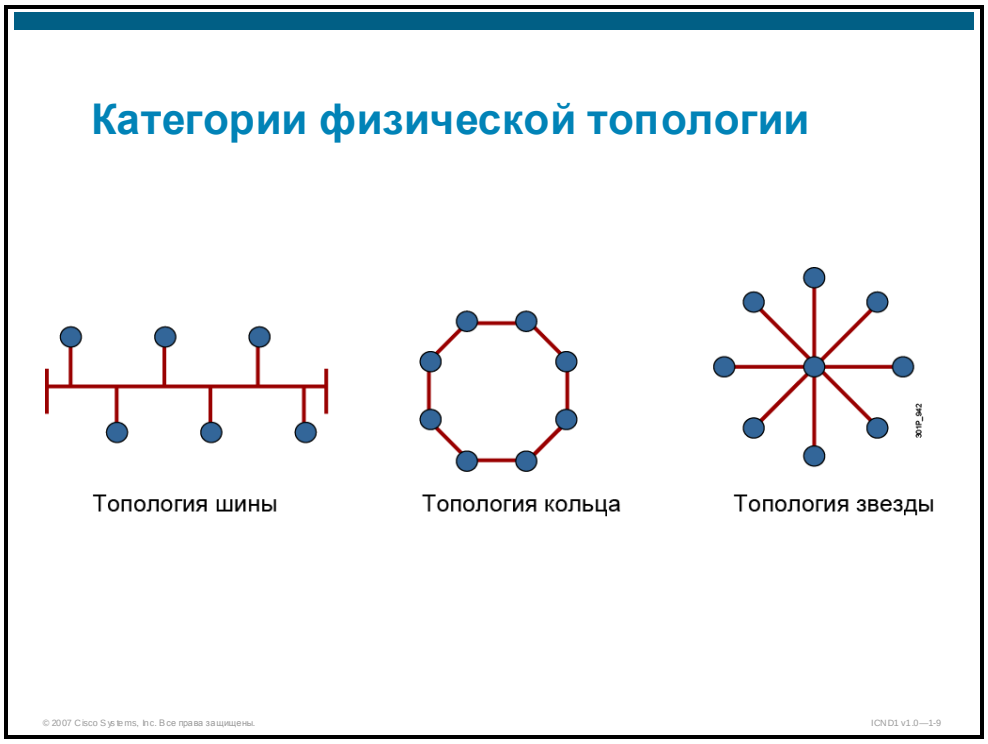
  ([525 600 – 15] / [525 600]) * 100 = 99,9971

- **Масштабируемость.** Масштабируемость обозначает, насколько хорошо сеть может удовлетворить потребности большего числа пользователей и требования к передаче большего объема данных. Если сеть спроектирована и оптимизирована только с учетом текущих требований, будет очень дорого и сложно обеспечивать соответствие новым требованиям, возникающим по мере роста сети.
- **Надежность.** Надежность означает безотказность компонентов (маршрутизаторов, коммутаторов, ПК и т. д.), составляющих сеть. Она часто измеряется как вероятность отказа или как среднее время между отказами (mean time between failures – MTBF).
- **Топология.** В сетях применяется два типа топологии: физическая топология (физическое расположение кабелей, сетевых устройств и конечных систем, таких как ПК и серверы) и логическая топология, которая описывает пути, по которым сигналы передаются через физическую топологию.

Эти характеристики и свойства позволяют сравнивать разные сетевые решения.

Сравнение физической и логической топологии

В этом разделе описаны физические и логические топологии сетей, включая расположение кабелей и устройств и пути передачи данных.

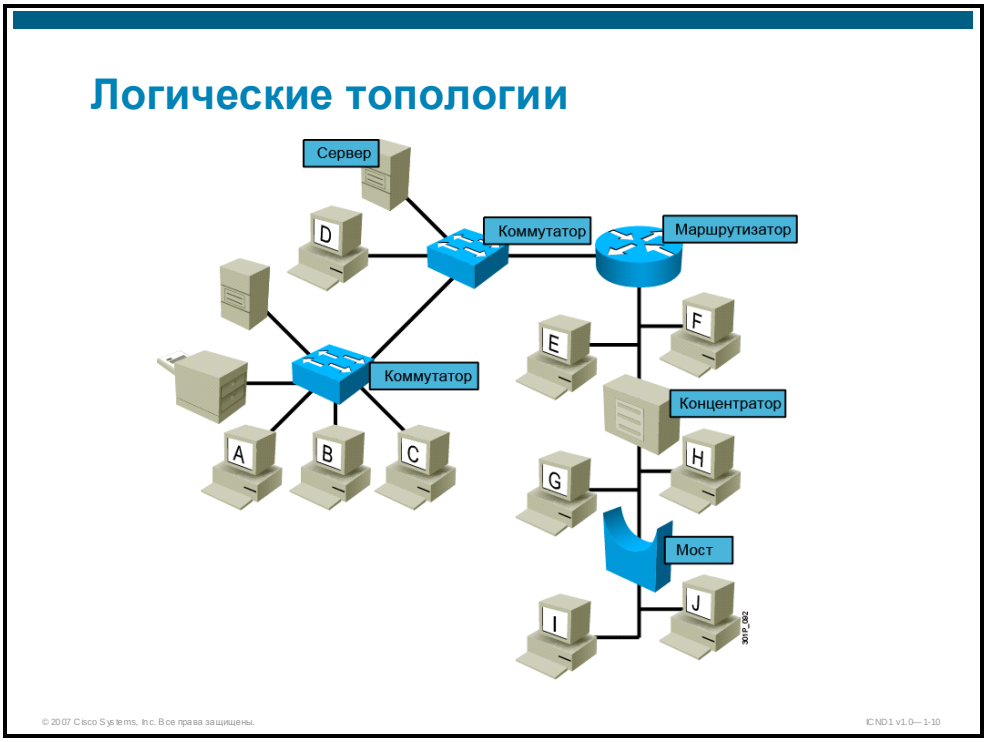


У каждой сети есть как физическая, так и логическая топология.

Физические топологии

Физическая топология сети описывает физическое расположение устройств и кабелей. Для каждого типа физической топологии необходимо подбирать соответствующий тип кабелей (витая пара, коаксиальный кабель, оптоволоконный кабель и т. д.). Следовательно, для понимании каждого типа физической топологии необходимо понять, какой тип кабеля в ней используется. Ниже приведены три основные категории физических топологий.

- **Шинная.** В первых шинных топологиях компьютеры и другие сетевые устройства соединялись последовательно с использованием коаксиального кабеля. В современных шинных топологиях шина реализована в виде отдельного устройства, хосты подсоединяются к шине с помощью витой пары.
- **Кольцевая.** Компьютеры и другие сетевые устройства соединяются кабелем, причем последнее устройство подсоединяется к первому с образованием окружности или кольца. К топологиям этого типа относятся кольцевые и двойные кольцевые топологии. Физическое подключение обеспечивается коаксиальным или оптоволоконным кабелем.
- **Звездообразная.** Компьютеры и другие сетевые устройства соединены через центральное кабельное устройство. К топологиям этого типа относятся звездообразные и иерархические звездообразные топологии. Физические подключения, как правило, реализуются с помощью витой пары.



Логические топологии

Логическая топология сети описывает логические пути, по которым сигналы передаются от одного узла сети на другой, т. е. способ доступа к сетевым носителям и передачи пакетов по ним.

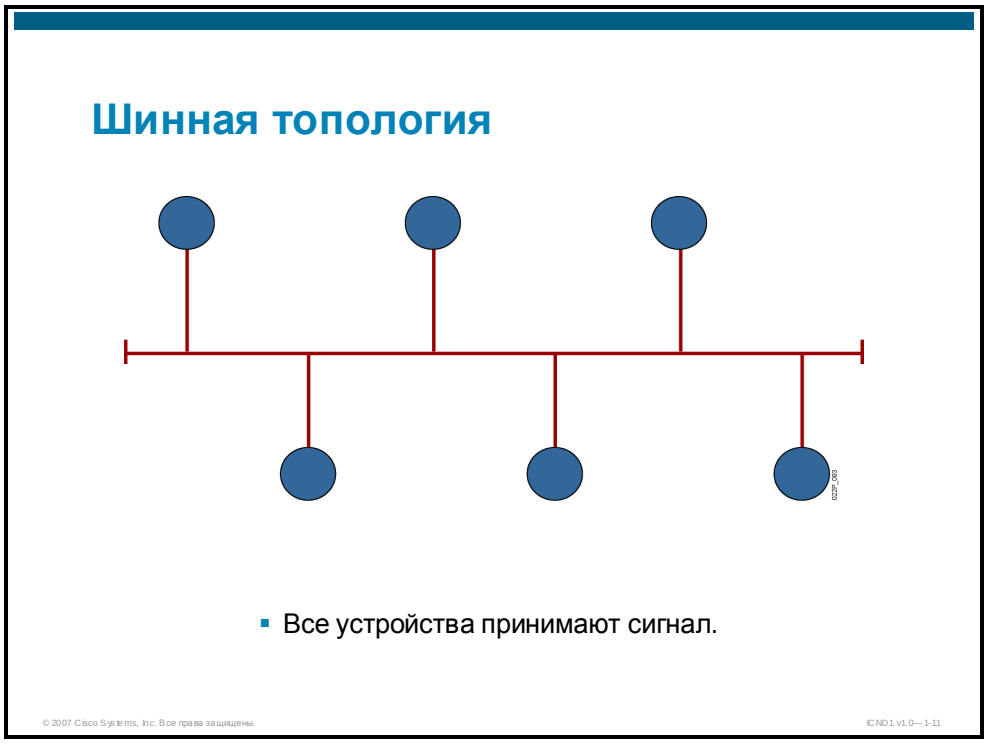
Физическая и логическая топология сети могут совпадать. Например, если сеть физически организована как линейная шина, данные перемещаются вдоль кабеля. Следовательно, эта сеть обладает физической шинной топологией и логической шинной топологией.

С другой стороны, сеть может обладать совершенно различными физической и логической топологиями. Например, физическая топология может иметь форму звезды, в которой все компьютеры подключены отрезками кабеля к центральному концентратору, но при этом обладать логической кольцевой топологией. В кольце данные передаются от компьютера к компьютеру, поэтому внутри концентратора используются соединения проводов, в которых сигнал передается по кольцу от одного порта к другому, создавая логическое кольцо. Следовательно физическая схема не всегда достаточна для прогноза перемещения данных по сети.

В настоящее время самой распространенной схемой реализации локальных сетей является звездообразная топология. Ethernet использует логическую шинную топология как в физической шинной, так и физической звездообразной топологии. Концентратор Ethernet – пример физической звездообразной топологии в сочетании с логической шинной топологией.

Шинная топология

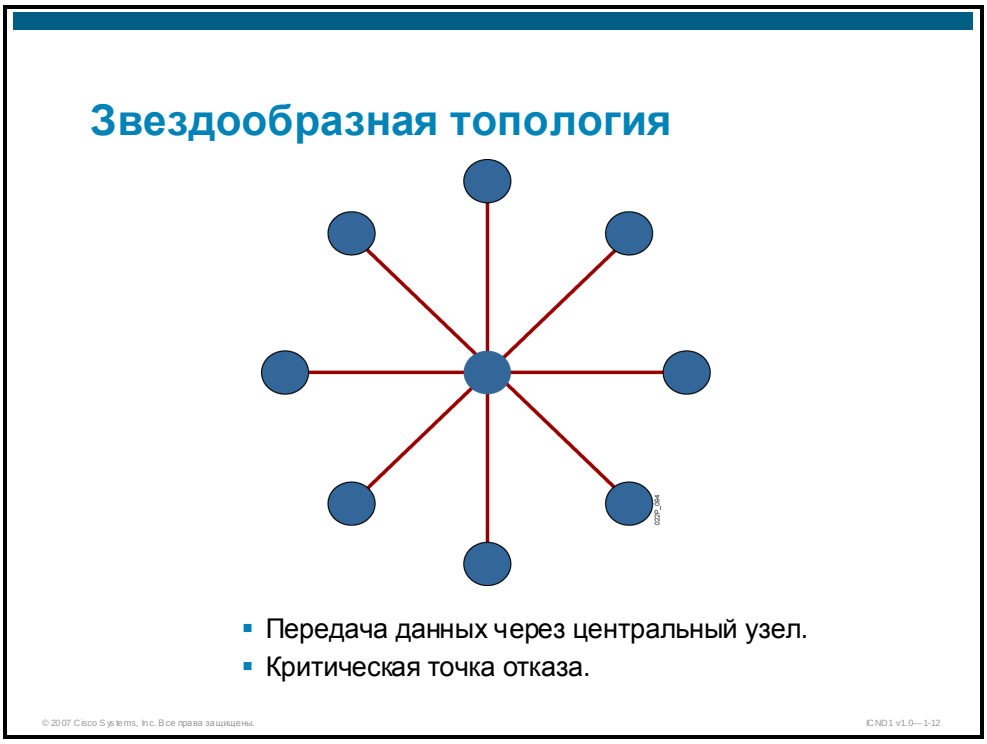
Часто называется линейной шиной. Все устройства в шинной топологии соединены с помощью одного кабеля. В этом разделе описывается шинная топология.



Как показано на рисунке, в шинной топологии кабель идет от одного компьютера к другому, подобно автобусной линии, проходящей через город. Основной участок кабеля должен заканчиваться терминатором, поглощающим сигнал, когда он достигает конца линии или провода. Если терминатор не установлен, электрический сигнал, соответствующий данным, отражается в конце кабеля, вызывая ошибки в сети.

Звездообразная и иерархическая звездообразная топологии

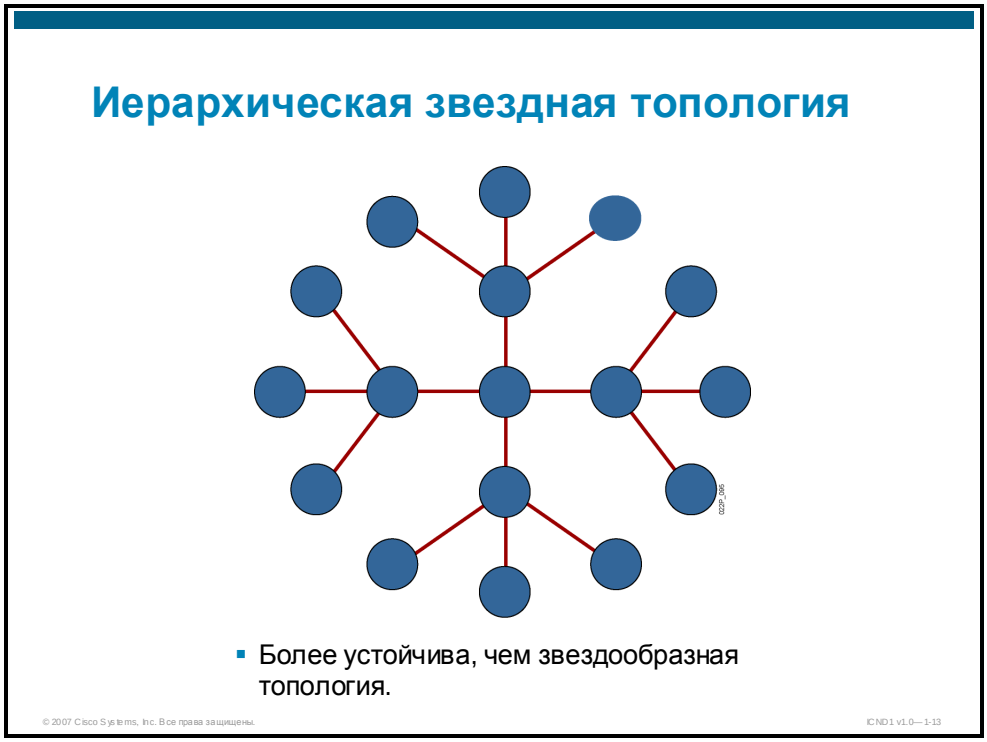
Звездообразная топология – наиболее часто встречающаяся топология в локальных сетях Ethernet. В этом разделе описываются звездообразные и иерархические звездообразные топологии.



При установке звездообразная топология напоминает спицы в велосипедном колесе. Она состоит из центральной точки подключения (концентратор, коммутатор или маршрутизатор), в которой соединяются все сегменты кабеля. Каждое устройство в сети подключено к центральному устройству с помощью отдельного кабеля.

Звездообразная топология

Хотя реализация физической звездообразной топологии стоит дороже, чем реализация физической шинной топологии, преимущества звездообразной топологии оправдывают дополнительные затраты. Каждое устройство подключено к центральному устройству с использованием отдельного кабеля, поэтому при неисправности этого кабеля затронуто только одно устройство, а остальная сеть остается в рабочем состоянии. Это преимущество крайне важно и является одной из причин, по которым почти все локальные сети Ethernet, спроектированные в последнее время, имеют физическую звездообразную топологию.



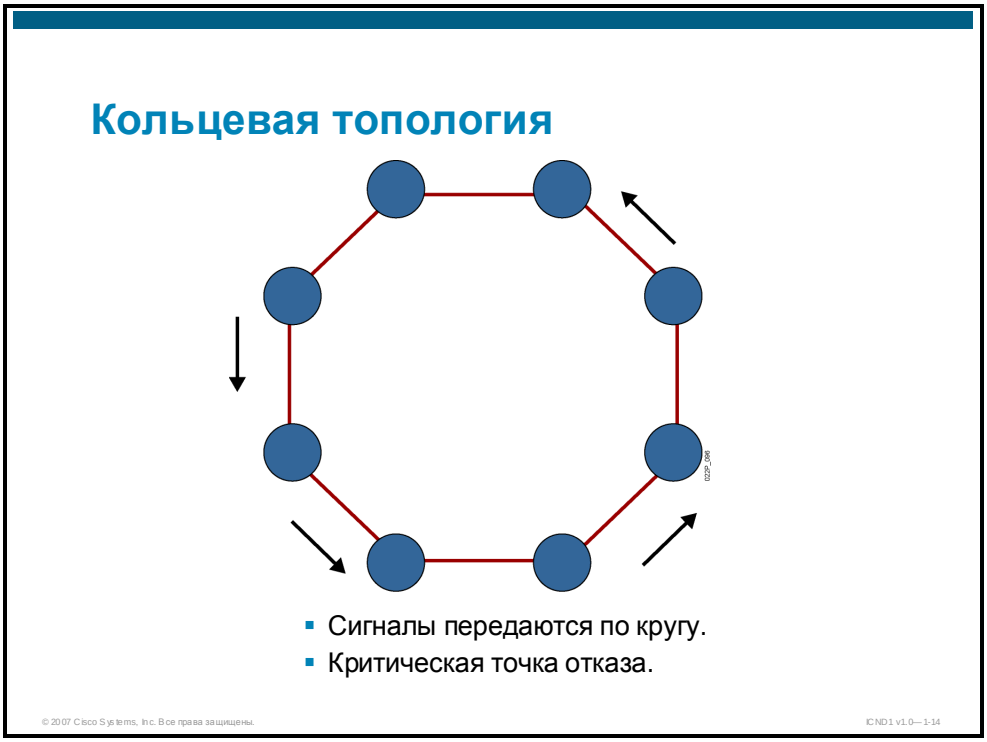
Иерархическая звездообразная топология

При расширении звездообразной топологии за счет добавления к сети дополнительных сетевых устройств, подключаемых к основным сетевым устройствам, топология называется «иерархической звездной топологией».

Но у чистой иерархической звездной топологии есть недостаток: при неисправности центрального узла большие фрагменты сети оказываются изолированными.

Кольцевые топологии

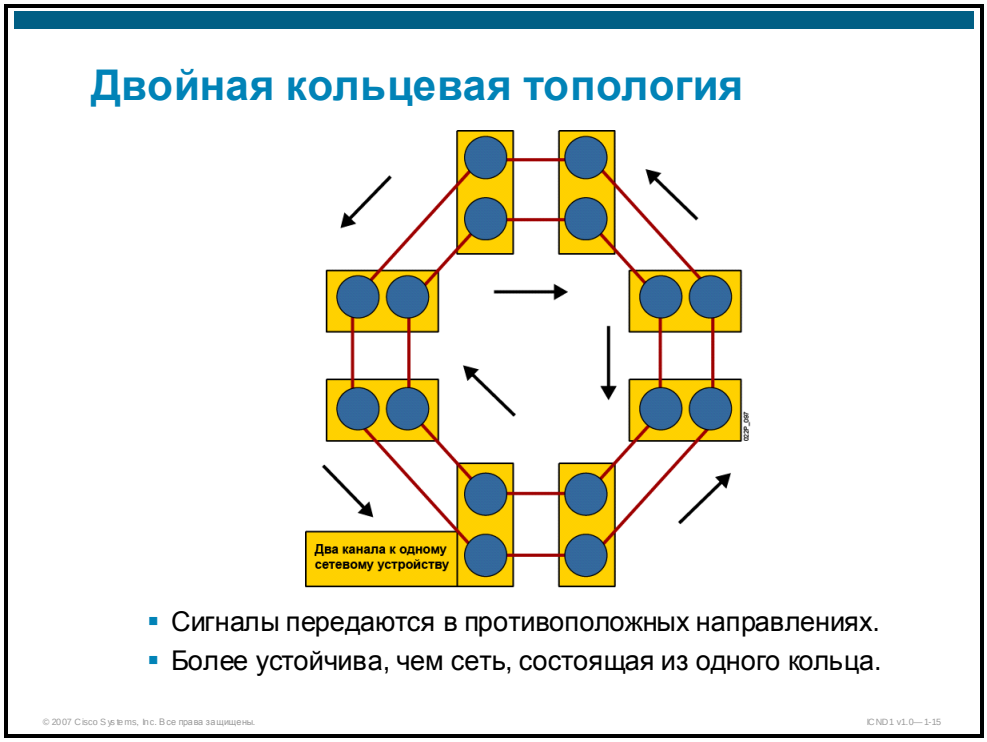
Как понятно из названия, в кольцевой топологии все устройства в сети соединены окружностью или кольцом. В этом разделе описывается кольцевая топология.



В отличие от физической шинной топологии в кольцевой топологии нет начальной и конечной точек, в которых необходимо подавлять сигнал. Данные передаются совершенно не так, как это происходит в логической шинной топологии. В одной из реализаций «маркер» перемещается вдоль кольца, останавливаясь на каждом устройстве. При передаче данных устройство добавляет данные и адрес назначения к маркеру. Далее маркер продолжает двигаться по окружности, пока не находит устройство назначения, которое извлекает данные из маркера. К преимуществам этого типа топологии относится отсутствие коллизий пакетов данных. Существуют два типа кольцевой типологии: одиночная кольцевая и двойная кольцевая.

Одиночная кольцевая топология

В одиночной кольцевой топологии все устройства сети расположены на одном кабеле, и данные передаются только в одном направлении. Каждое устройство ждет своей очереди для передачи данных по сети. Однако одиночное кольцо может пострадать от единственного отказа, в результате которого все кольцо прекращает функционировать.

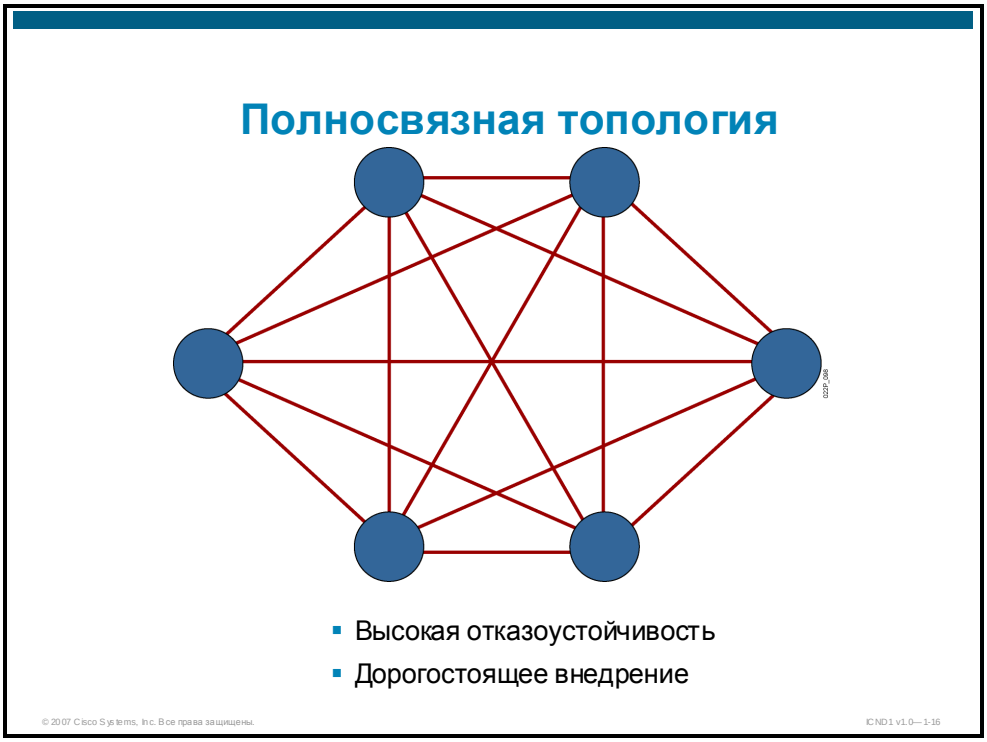


Двойная кольцевая топология

В двойной кольцевой топологии два кольца позволяют передавать данные в обоих направлениях. В такой конфигурации создается резервирование (отказоустойчивость). Это означает, что при неисправности в одном кольце данные можно передавать по другому.

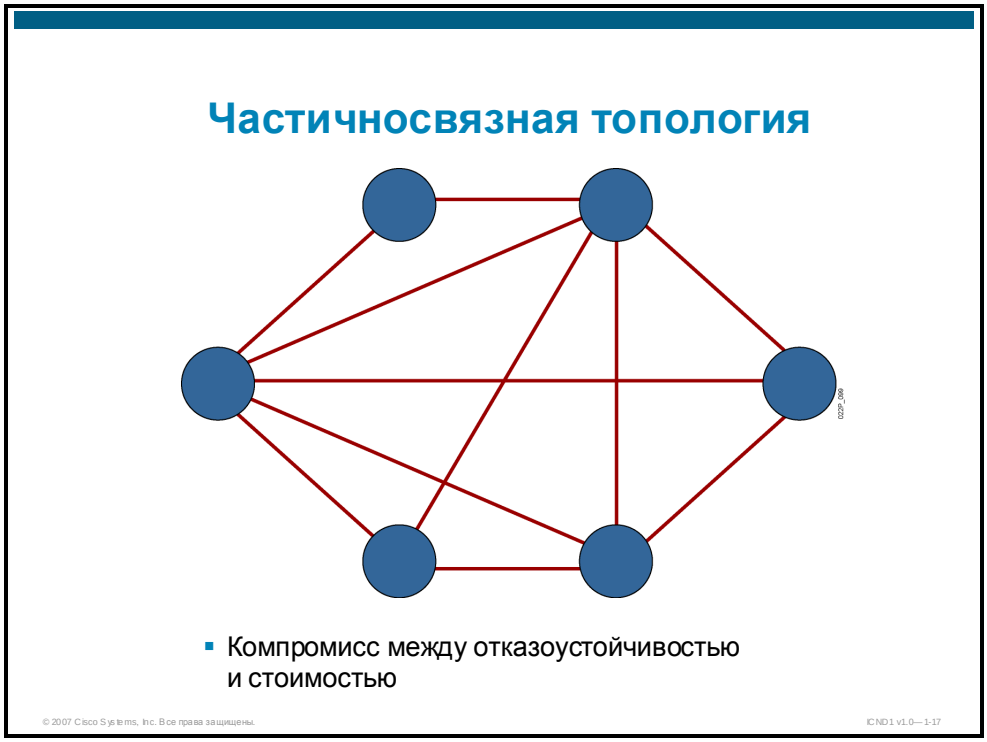
Полносвязная и частичносвязная топология

Такая топология схожа со звездообразной топологией. В этом разделе описаны полносвязная и частичносвязная топология.



Полносвязная топология

В полносвязной топологии все устройства (или узлы) соединены друг с другом, что обеспечивает резервирование и отказоустойчивость. Внедрение полносвязной топологии дорого и сложно. Этот вид топологии наиболее устойчив к сбоям, поскольку отказ одного канала не влияет на доступность сети.

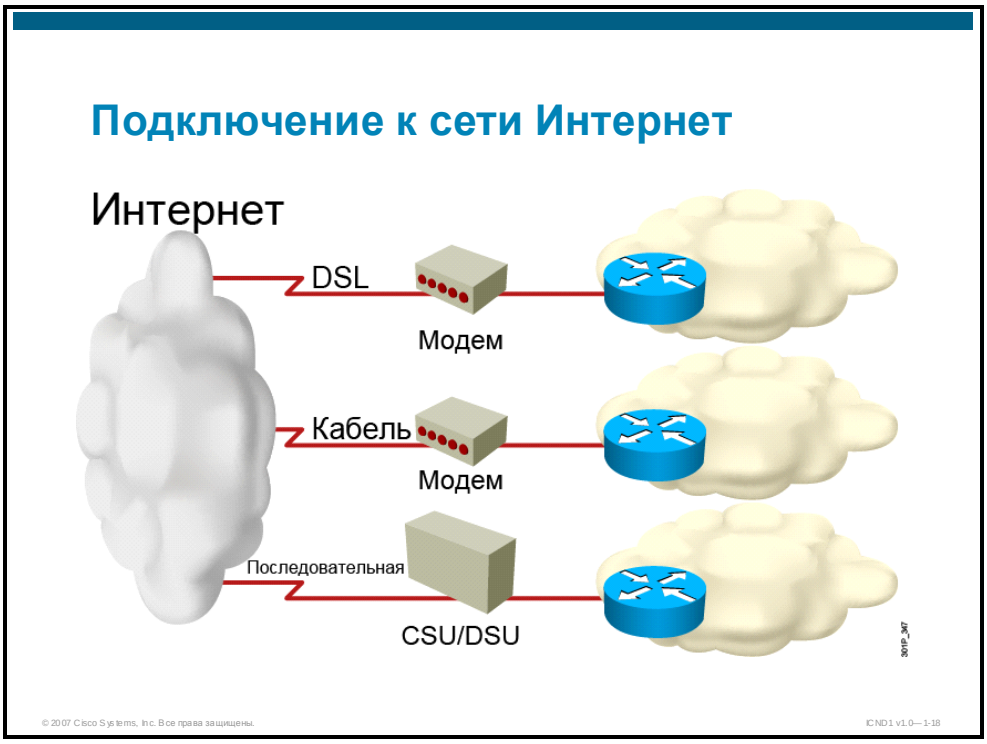


Частичносвязная топология

В частичной топологии, по крайней мере, одно устройство связано со всеми другими устройствами, но полносвязная сеть не формируется. При использовании такого способа соединения можно снизить стоимость за счет того, что не все устройства связаны со всеми остальными, и проектировщик сети получает возможность выбрать, какие узлы наиболее важны, и должным образом обеспечить их взаимное соединение.

Подключение к сети Интернет

В этом разделе описаны обычные методы подключения к сети Интернет.



Можно использовать три стандартных способа подключения небольшого офиса и сети Интернет. DSL (Digital Subscriber Line) использует существующие телефонные линии. При кабельном подключении используется инфраструктура кабельного телевидения. Последовательные каналы используют классические цифровые последние мили. При использовании DSL и кабеля входящие линии подключаются к модему, преобразующему входящий цифровой сигнал в формат Ethernet. При использовании последовательных каналов для этого используется каналообразующее оборудование CSU/DSU (Channel Service Unit/Data Service Unit). Во всех трех случаях (DSL, кабель и последовательный канал) выходной сигнал Ethernet передается на маршрутизатор, который входит в оборудование абонента (CPE-Customer Permises Equipment).

Резюме

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

Резюме

- Сеть – это комбинация соединенных устройств, которые могут обмениваться данными друг с другом. Сети служат для передачи данных в различных местах, включая дома, небольшие компании и крупные предприятия.
- В компьютерную сеть входят физические компоненты, относящиеся к четырем основным категориям: компьютеры, линии связи, коммутаторы и маршрутизаторы.
- Сети можно изображать графически с использованием набора условных обозначений.
- К основным ресурсам, которые могут совместно использоваться в сети, относятся данные и приложения, периферийное оборудование, устройства хранения и устройства резервного копирования.
- К наиболее распространенным сетевым пользовательским приложениям относится электронная почта, обозреватели, приложения мгновенного обмена сообщениями, совместной работы и базы данных.
- Пользовательские приложения влияют на работу сети, т. к. они используют сетевые ресурсы.

Резюме (прод.)

- Для описания сетей используются характеристики, отражающие их производительность и структуру: скорость, стоимость, безопасность, доступность, масштабируемость, надежность и топология.
- Термин «физическая топология» используется для описания способа соединения физических устройств, а термин «логическая топология» относится к потокам данных в сети.
- В физической шинной топологии все устройства фактически соединены одним кабелем.
- В физической звездообразной топологии каждое устройство в сети подключено к центральному устройству отдельным кабелем.
- При расширении звездообразной топологии к основным сетевым устройствам подключаются дополнительные сетевые устройства. Такая топология называется «иерархической звездообразной топологией».

Резюме (прод.)

- В кольцевой топологии все хосты соединены в форме кольца или окружности. В двойной кольцевой топологии формируются два кольца, которые обеспечивают резервирование.
- В полносвязной топологии все устройства попарно соединены, а в частичной топологии, по крайней мере, одно устройство соединено со всеми другими устройствами.
- Можно использовать три стандартных способа подключения небольшого офиса и сети Интернет: канал DSL на базе существующих телефонных линий, кабель на базе инфраструктуры кабельного телевидения и последовательные каналы на основе классических цифровых последних миль.

Занятие 3

Общие сведения о модели обмена данными между хостами

Обзор

Эталонная модель взаимодействия открытых систем (OSI) была создана, чтобы определить общий принцип работы сетевых процессов, включая различные компоненты сети и передачу данных. Для понимания обмена данными между хостами, необходимо представление о структуре и назначении модели OSI. В этом занятии представлена модель OSI и описаны все ее уровни.

Задачи

По окончании этого занятия вы сможете описывать уровни модели OSI и классифицировать устройства и их функции по уровням модели OSI. Это значит, что вы сможете выполнять следующие задачи:

- перечислять требования к модели обмена данными между хостами;
- определять назначение эталонной модели OSI;
- описывать характеристики, функции и назначение каждого уровня модели OSI;
- описывать процесс инкапсуляции и деинкапсуляции;
- описывать обмен данными между одноранговыми узлами;
- формулировать назначение и функции стека протоколов TCP/IP в процессе обмена данными.

Общие сведения об обмене данными между хостами

Для обмена данными между хостами необходима согласованная модель. Эта модель должна учитывать аппаратное и программное обеспечение, а также передачу данных. В этом разделе описано назначение этой модели.

На ранних этапах развитие сетей во многом шло хаотично. Первые модели обмена данными между хостами были собственностью поставщика, причем каждый поставщик контролировал свои собственные приложения и программное обеспечение для обмена данными. Приложение, созданное одним поставщиком, не функционировало в сети, разработанной другим.

Потребности бизнеса и развитие технологий подтолкнули к появлению решений с компонентами от разных поставщиков. Первым шагом было разграничение прикладного программного обеспечения и программного обеспечения для обмена данными. Это позволило внедрять новые технологии обмена данными, не создавая новые приложения, но все равно нужно было использовать программное обеспечение для обмена данными и аппаратное обеспечение от одного поставщика.

Стало очевидно, что для использования программного обеспечения обмена данными и аппаратного обеспечения от разных поставщиков необходим многоуровневый подход с четко определенными правилами взаимодействия между уровнями. В многоуровневой модели одни поставщики аппаратного обеспечения могут проектировать аппаратное и программное обеспечение для поддержки новых аппаратных технологий (например, Ethernet, Token Ring, Frame Relay и т. д.), а другие поставщики могут создавать программное обеспечение для сетевых операционных систем, управляющих обменом данными между хостами.

Эталонная модель OSI

Эталонная модель OSI описывает передачу данных по сети. Эта модель описывает аппаратное и программное обеспечение, а также передачу данных. В этом разделе описано назначение модели OSI.

На ранних этапах развитие сетей во многом шло хаотично. В начале 1980-х годов количество и размеры сетей значительно возросли. Как только компании поняли, что они могут сэкономить средства и увеличить производительность, используя сетевые технологии, они начали создавать новые сети и расширять уже существующие с такой скоростью, с какой новые сетевые технологии и продукты.

К середине 1980-х годов компании начали испытывать трудности в связи с этими расширениями. Обмен данными между сетями, имеющими разные технические характеристики и реализации, усложнился. Компании поняли, что им надо отказаться от проприетарных сетевых систем, то есть систем, разработанных внутри компании, используемых и управляемых этой компанией. В компьютерной промышленности возникла необходимость концепции «открытых» систем, противоположных «проприетарным». Проприетарность означает, что использование технологии контролируется одной компанией или маленькой группой. Открытость означает, что технология находится в свободном доступе.

Для решения проблемы несовместимости сетей и невозможности обмена между ними Международная организация по стандартам проанализировала несколько схем сетей. В результате этого исследования Международная организация по стандартам разработала модель, которая могла помочь поставщиками создавать сети, совместимые и способные взаимодействовать с другими сетями.

Эталонная модель OSI, предложенная в 1984 году, была описательной схемой, созданной Международной организацией по стандартам. Для поставщиков в ней предлагался набор стандартов, гарантировавших более высокую степень совместимости и возможности взаимодействия между сетевыми технологиями разных типов, производимыми компаниями во всем мире. Хотя это не единственная модель, большинство поставщиков сетевых технологий создают свою продукцию на основе эталонной модели OSI, особенно когда они хотят научить клиентов пользоваться своими продуктами. Считается, что модель OSI – лучшее средство для объяснения передачи и приема данных в сети.

В эталонной модели OSI сетевые функции делятся на семь категорий. Это разделение сетевых функций называется иерархическим представлением сети. Эталонная модель OSI состоит из семи нумерованных уровней, каждый из которых иллюстрирует определенную сетевую функцию. Эталонная модель OSI определяет функции сети, реализуемые на каждом уровне. Важнее то, что модель OSI облегчает понимание передачи данных по сети. Кроме того, модель OSI описывает, как данные приложений (например, электронных таблиц) передаются другому приложению, расположенному на другом компьютере через сетевую среду, даже если отправитель и получатель подключаются с помощью разных сетевых сред.

Эталонная модель OSI предлагает ряд преимуществ для понимания функций сети, так как она:

- **Снижает сложность.** Модель OSI разбивает каналы связи в сети на небольшие, более простые фрагменты.
- **Стандартизирует интерфейс.** Модель OSI стандартизирует сетевые компоненты, что обеспечивает разработку и поддержку решений с компонентами от разных поставщиков.
- **Облегчает модульное построение.** Модель OSI позволяет использовать аппаратное и программное обеспечение разных типов для обмена данными.
- **Гарантирует совместимость технологий.** При использовании модели OSI изменения на одном уровне не влияет на другие уровни. Это делает возможным более быстрое развитие.
- **Ускоряет эволюцию.** Модель OSI обеспечивает эффективное обновление и улучшение отдельных компонентов, которое не затрагивает другие компоненты и не требуют полной модификации протокола.
- **Упрощает преподавание и освоение.** В модели OSI обмен данными в сети разбит на небольшие составляющие, что упрощает обучение.

Уровни модели OSI и их функции

Каждый уровень модели OSI выполняет определенные функции и поддерживает соответствующее программное обеспечение и устройства. В этом разделе описываются все уровни и их функции.

Уровень 1: физический уровень

На физическом уровне определены электрические, механические, процедурные и функциональные характеристики активации, поддержания и отключения физического канала между конечными системами. Технические характеристики физического уровня определяют такие параметры, как уровни напряжения, синхронизацию изменений напряжения, физическую скорость передачи данных, максимальное расстояние передачи данных, физические подключения и другие аналогичные характеристики.

Уровень 2: канальный уровень

На канальном уровне определяется формат данных для передачи и методы контроля доступа к физическим средам. Этот уровень также включает функции обнаружения и коррекции ошибок для обеспечения надежной передачи данных.

Уровень 3: сетевой уровень

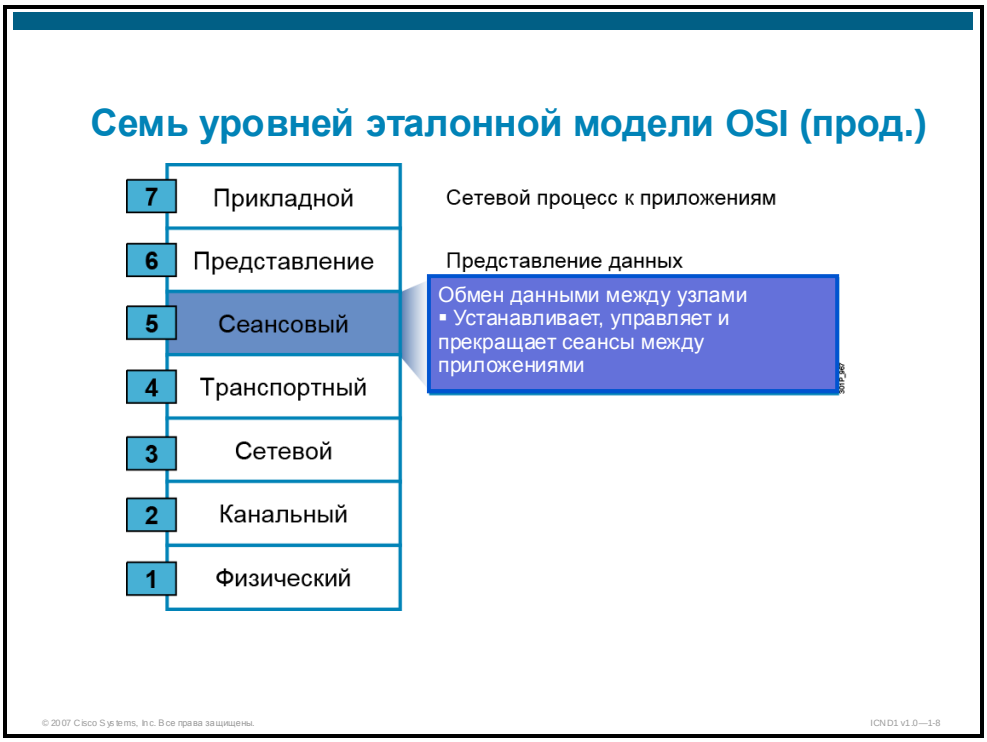
Сетевой уровень обеспечивает связь и выбор пути между двумя хостами, которые могут находиться в сетях, географически удаленных друг от друга. Развитие сети Интернет увеличило число пользователей, получающих доступ к информации на веб-сайтах, расположенных по всему свету, и именно на сетевом уровне реализуется управление связью.

Уровень 4: транспортный уровень

На транспортном уровне выполнятся сегментация данных от передающего хоста и реорганизация данных в поток данных в принимающем хосте. Например, бизнес-пользователи в крупных корпорациях часто передают большие файлы с периферийных объектов на корпоративную площадку. Необходима надежная доставка файлов, поэтому на транспортном уровне большие файлы разбиваются на более мелкие сегменты, которые с меньшей вероятностью могут столкнуться с проблемами при передаче.

Можно рассматривать границу между транспортным и сеансовым уровнем как границу между протоколами приложений и протоколами потока данных. В то время как на прикладном, сеансовом и представительском уровнях решаются задачи работы с приложениями, на четырех более низких уровнях решаются проблемы передачи данных.

Транспортный уровень скрывает детали передачи данных от верхних уровней. В частности, на транспортном уровне решаются задачи, связанные с надежностью передачи данных между двумя хостами. В рамках реализации службы обмена данными транспортный уровень создает, поддерживает и корректно завершает виртуальные каналы. Функции обнаружения и коррекции ошибок, а также управление потоками данных, обеспечивают надежность служб.



Уровень 5: сеансовый уровень

На сеансовом уровне выполняется создание, управление и завершение сеансов между двумя хостами, обменивающимися данными. Кроме того, на сеансовом уровне выполняется синхронизация диалога между представительскими уровнями двух хостов и управление обменом данными между ними. Например, веб-серверами пользуется большое число пользователей, и в каждый отдельно взятый момент времени выполняется много процессов обмена данными. Поэтому необходимо отслеживать, каким каналом пользуется тот или иной пользователь. Кроме управления сеансами, сеансовый уровень предлагает дополнительные средства для эффективной передачи данных – классы обслуживания (CoS) и событийная отчетность о проблемах сеансового, прикладного и представительского уровней.

Уровень 6: представительский уровень

Представительский уровень гарантирует, что сведения, передаваемые на прикладном уровне одной системы, могут быть распознаны на прикладном уровне другой системы. Например, программа на компьютере обменивается данными с другим компьютером, причем для представления одних и тех же символов на одном из компьютеров используется расширенный двоично-десятичный код обмена информацией (EBCDIC), а на другом используется американский стандартный код для обмена информацией (ASCII). При необходимости, на представительском уровне выполняется перевод из одного из многочисленных форматов данных в другой на основе общего формата.

Уровень 7: прикладной уровень

Прикладной уровень OSI находится ближе всего к пользователю. На этом уровне предоставляются сетевые услуги для таких пользовательских приложений, как электронная почта, пересылка файлов и эмуляция терминала. Прикладной уровень отличается от остальных уровней тем, что он не предоставляет услуг другим уровням OSI, а только приложениям вне модели OSI. Прикладной уровень обеспечивает доступность целевых партнеров по соединению, а также синхронизирует и формирует соглашения по процедурам коррекции ошибок и контроля целостности данных.

Инкапсуляция и деинкапсуляция

Данные, передаваемые по сети, должны пройти процесс преобразования как на передающей, так и на принимающей системе. Этот процесс преобразования называется инкапсуляцией и деинкапсуляцией данных. В этом разделе описываются процессы инкапсуляции и деинкапсуляции.

Инкапсуляция

Информация, передаваемая по сети, называется данными или пакетами данных. При передачи данных с одного компьютера на другой необходимо упаковать данные в пакеты. Этот процесс называется инкапсуляцией. Во время инкапсуляции данные разбиваются на пакеты с необходимыми данными протокола перед передачей через сеть. При перемещении данных через уровни модели OSI на каждом уровне к данным добавляется заголовок (и концевая метка, если необходимо), пока данные не доходят до самого низкого уровня. Заголовки и концевые метки содержат контрольную информацию для сетевых устройств и приемника, которая обеспечивает корректную доставку данных и их правильную интерпретацию на приемнике.

На рисунке описывается процесс инкапсуляции. На нем показано, как данные перемещаются между уровнями. Во время инкапсуляции данных выполняются следующие действия.

Шаг 1 Приложение передает пользовательские данные на прикладной уровень.

Шаг 2 На прикладном уровне к пользовательским данным добавляется заголовок прикладного уровня (заголовок уровня 7). Пользовательские данные вместе с заголовком уровня 7 передаются вниз на представительский уровень.

Шаг 3 На представительском уровне к данным добавляется заголовок представительского уровня (заголовок уровня 6). Получившиеся данные передаются на сеансовый уровень.

Шаг 4 На сеансовом уровне к данным добавляется заголовок сеансового уровня (заголовок уровня 5). Получившиеся данные передаются на транспортный уровень.

Шаг 5 На транспортном уровне к данным добавляется заголовок транспортного уровня (заголовок уровня 4). Получившиеся данные передаются на сетевой уровень.

Шаг 6 На сетевом уровне к данным добавляется заголовок сетевого уровня (заголовок уровня 3). Получившиеся данные передаются на канальный уровень.

Шаг 7 На канальном уровне к данным добавляется заголовок и концевая метка канального уровня (заголовок и концевая метка уровня 2). Концевая метка уровня 2 обычно представляет собой контрольную последовательность кадра, которая используется получателем для проверки целостности данных. Получившиеся данные передаются на физический уровень.

Шаг 8 С физического уровня биты данных передаются в среду передачи.

Пример: передача посылки по почте

Инкапсуляция очень похожа на процесс отправки посылки по почте. Сначала необходимо поместить содержимое посылки в упаковку. Затем на внешней стороне упаковки пишется адрес, по которому следует отправить посылку. После этого надписанная посылка помещается в почтовый ящик и начинает свое путешествие к месту назначения.

Деинкапсуляция

Когда удаленное устройство получает последовательность битов, его физический уровень передает биты данных на канальный уровень для обработки. На канальном уровне выполняются следующие действия.

Шаг 1 Канальный уровень проверяет концевую метку канального уровня (контрольную последовательность кадра), чтобы убедиться, что в данных нет ошибок.

Шаг 2 Если в данных есть ошибки, их можно забраковать, поэтому канальный уровень может запросить повторную передачу данных.

Шаг 3 Если в данных нет ошибок, канальный уровень считывает и интерпретирует контрольную информацию в своем заголовке.

Шаг 4 Канальный уровень удаляет заголовок и концевую метку канального уровня и передает оставшийся пакет данных вверх на сетевой уровень в зависимости от контрольной информации в заголовке канального уровня.

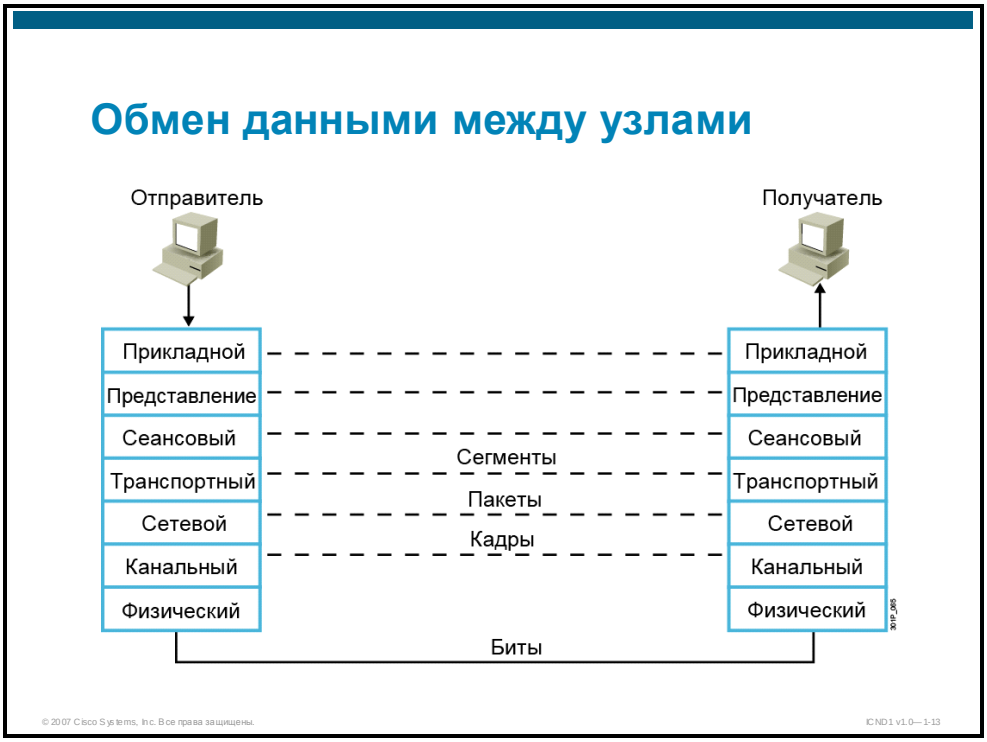
Этот процесс называется деинкапсуляцией. На каждом последующем уровне выполняется аналогичная процедура деинкапсуляции.

Пример: получение посылки

Процесс деинкапсуляции похож на чтение адреса на посылке, когда вы проверяете, кому она адресована. Если посылка адресована вам, вы извлекаете содержимое из упаковки.

Обмен данными между узлами

Чтобы пакеты данных могли передаваться от источника к месту назначения, каждый уровень модели OSI источника должен обмениваться данными с соответствующим уровнем получателя. В этом разделе описывается процесс обмена данными между узлами.



При обмене данными между узлами протоколы на каждом уровне обмениваются пакетами данных, которые называются «элементами информации протокола» (Packet Data Unit – PDU).

Эти пакеты данных создаются на источнике в сети, а затем передаются к месту назначения. Предоставление услуг на каждом уровне зависит от низлежащего уровня OSI. Для выполнения своих функций более низкий уровень использует инкапсуляцию для размещения элементов PDU верхнего уровня в поле данных нижнего уровня. После этого на каждом уровне добавляется заголовки, которые необходимы этому уровню для выполнения своих функций. По мере продвижения данных с уровня 7 до уровня 2 модели OSI добавляются дополнительные заголовки.

Сетевой уровень предоставляет услуги транспортному уровню, а транспортный уровень передает данные в сетевую подсистему. Сетевой уровень перемещает данные через Интернет, инкапсулируя их и добавляя заголовок для создания пакета (элемент PDU уровня 3). Заголовок содержит сведения, необходимые для передачи (например, логические адреса отправителя и получателя).

Канальный уровень предоставляет услуги сетевому уровню, инкапсулируя пакет сетевого уровня в кадр (элемент PDU уровня 2). Заголовок кадра содержит физические адреса, необходимые для выполнения функций канального уровня, а концевая метка кадра содержит контрольную последовательность кадра.

Физический уровень предоставляет услуги канальному уровню, кодируя кадр канального уровня в последовательность битов (1 и 0) для передачи по среде (обычно проводной) на уровне 1.

Семейство протоколов TCP/IP

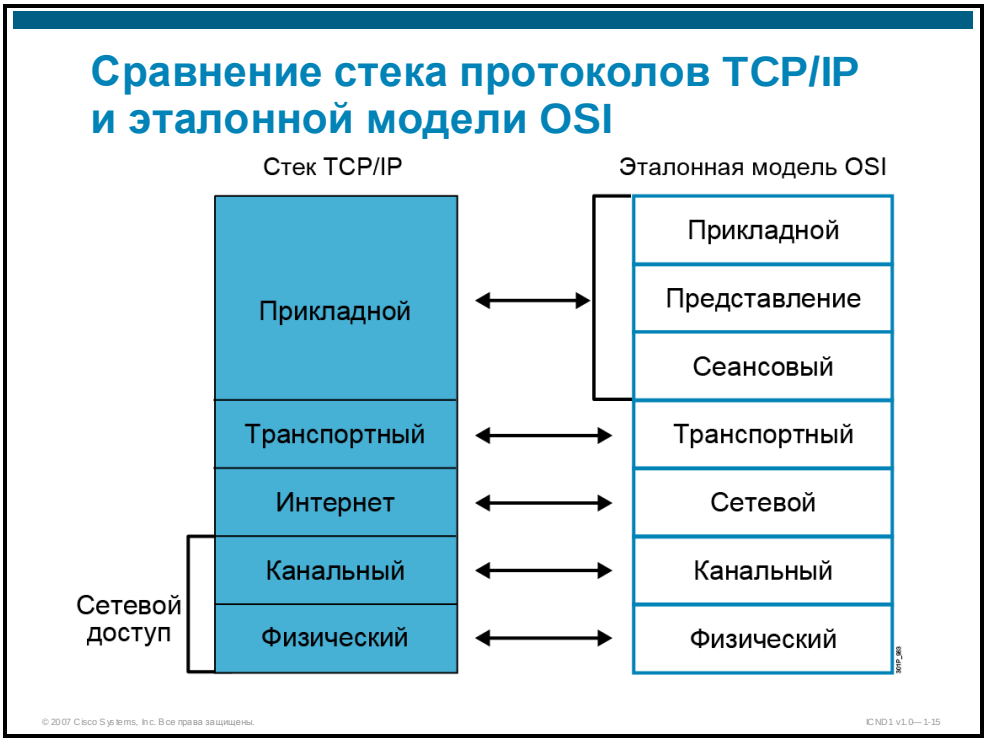
Семейство протоколов TCP/IP, название которого в действительности является комбинацией названий двух отдельных протоколов – протокола управления передачей данных (TCP) и протокола Интернета (IP), делится на уровни, каждый из которых выполняет определенные функции в процессе обмена данными. В этом разделе описано, как уровни TCP/IP организуются в стек.

Протоколы семейства TCP/IP были созданы примерно в то же время, что и модель OSI. Подобно модели OSI протоколы семейства TCP/IP предназначены для организации компонентов, при которой их расположение отражает функции протоколов в отношении друг друга. Стек протоколов TCP/IP состоит из следующих уровней.

- **Уровень сетевого доступа.** На этом уровне выполняются те же процессы, что на двух нижних уровнях OSI.
  - **Физический уровень.** На физическом уровне определены электрические, механические, процедурные и функциональные характеристики активации, поддержания и отключения физического канала между конечными системами. Технические характеристики физического уровня определяют такие параметры, как уровни напряжения, синхронизация изменения напряжения, физическую скорость передачи данных, максимальное расстояние передачи данных, физические подключения и другие аналогичные характеристики.
  - **Канальный уровень.** На канальном уровне определяется формат данных для передачи и методы контроля доступа к сети.

- **Уровень Интернета.** На этом уровне обеспечивается маршрутизация данных от источника к месту назначения. Для этого определяется формат пакета и схема адресации, данные перемещаются с канального уровня на транспортный, пакеты данных маршрутизируются на удаленный хост, выполняется фрагментация и восстановление пакетов данных.
- **Транспортный уровень.** Транспортный уровень является центральным в архитектуре TCP/IP. Он предоставляет услуги обмена данными приложениям, которые работают на хостах в сети.
- **Прикладной уровень.** На прикладном уровне выполняются приложения для передачи файлов, поиска и устранения неисправностей сети и работы с Интернетом. Этот уровень поддерживает прикладные программные интерфейсы (API), благодаря которым программы, написанные для определенной операционной системы, могут получать доступ к сети.

Примечание Хотя в этом учебном курсе используется термин «Стек протоколов TCP/IP», на практике этот термин часто сокращается до «Стек протоколов IP».



Модель OSI и стек протоколов TCP/IP были разработаны разными организациями примерно в одно и то же время в качестве методов организации и соединения компонентов, участвующих в передаче данных. Уровни стека протоколов TCP/IP соответствуют уровням модели OSI.

- Уровень сетевого доступа стека TCP/IP примерно соответствует физическому и канальному уровням модели OSI и, в основном, отвечает за взаимодействие с сетевым оборудованием и доступ к средам передачи данных.

Примечание Поскольку уровень сетевого доступа стека TCP/IP включает как канальный, так и физический уровни модели OSI, классическая четырехуровневая структура TCP/IP часто заменяется пятиуровневой структурой. В этом курсе используется пятиуровневая модель.

- Уровень Интернета в стеке TCP/IP почти в точности соответствует сетевому уровню модели OSI и отвечает за адресацию и маршрутизацию между сетевыми устройствами.
- Транспортный уровень TCP/IP, подобно транспортному уровню модели OSI, позволяет приложениям хоста получать доступ к сетевому уровню либо в режиме негарантированной доставки, либо в режиме надежной доставки.
- Прикладной уровень стека протоколов TCP/IP работает с приложениями, которые обмениваются данными с более низкими уровнями, и соответствует отдельным прикладному, сессионному уровнями и представительскому уровням в модели OSI. Дополнительные уровни модели OSI обеспечивают дополнительную организацию функций, связанных с приложениями.

Резюме

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

Резюме

- Эталонная модель OSI определяет функции сети, реализуемые на каждом уровне.
- На физическом уровне определены электрические, механические, процедурные и функциональные характеристики активации, поддержания и отключения физического канала между конечными системами.
- На канальном уровне определяется формат данных для передачи и методы контроля доступа к физическим средам.
- Сетевой уровень обеспечивает подключения и выбор пути между двумя хостами, которые могут находиться в сетях, географически удаленных друг от друга.

Резюме (прод.)

- На транспортном уровне выполнятся сегментация данных от передающего хоста и реорганизация данных в поток данных в принимающем хосте.
- На сеансовом уровне выполняется создание, управление и завершение сеансов между двумя хостами, которые обмениваются данными.
- Представительский уровень гарантирует, что сведения, передаваемые на прикладном уровне одной системы, могут быть прочитаны на прикладном уровне другой системы.
- На прикладном уровне предоставляются сетевые услуги для таких пользовательских приложений, как электронная почта, пересылка файлов и эмуляция терминала.

Резюме (прод.)

- Информация, передаваемая по сети, называется данными или пакетами данных. При передачи данных с одного компьютера на другой необходимо упаковать данные в пакеты. Этот процесс называется инкапсуляцией.
- Когда удаленное устройство получает последовательность битов, его физический уровень передает биты данных на канальный уровень для обработки. Этот процесс называется деинкапсуляцией.

Резюме (прод.)

- В настоящее время по ряду причин наиболее широко используется протокол TCP/IP. Его отличает гибкий метод адресации, совместимость с большинством операционных систем и платформ, большое число инструментов и утилит и необходимость в его использовании для подключения к Интернету.
- Стек TCP/IP состоит из уровня сетевого доступа, уровня Интернета, а также транспортного и прикладного уровней.
- Эталонная модель OSI и стек протоколов TCP/IP похожи по структуре и функциям и коррелируют на физическом, канальном, сетевом и транспортном уровнях. В эталонной модели OSI прикладной уровень стека протоколов TCP/IP делится на три отдельных уровня.

Занятие 4

Общие сведения об уровне Интернета стека протоколов TCP/IP

Обзор

IP-адресация включает различные аспекты, такие как расчеты для формирования IP-адреса, классы IP-адресов, выделенные для различных задач маршрутизации, общедоступные и частные IP-адреса. Существует два типа IP-адресов: IP версии 4 (IPv4) и IP версии 6 (IPv6). В настоящее время наибольшее распространение получили 32-битные адреса IPv4, однако 128-битные адреса IPv6 также используются и со временем, вероятно, станут основным типом IP-адресов. В этом занятии рассматривается 32-битная адресация IPv4, за исключением разделов, в которых явно указан IPv6.

Как конечные системы получают исходную информацию об IP-адресах? Информация об IP-адресе может быть назначена вручную, но этот способ затрудняет масштабирование и является препятствием при развертывании и обслуживании сетей. Поэтому в настоящее время разработаны протоколы для автоматического назначения IP-адресов, выполняющие эту важнейшую функцию без вмешательства конечного пользователя. В этом занятии описывается функционирование протоколов с помощью IP-адресов.

Задачи

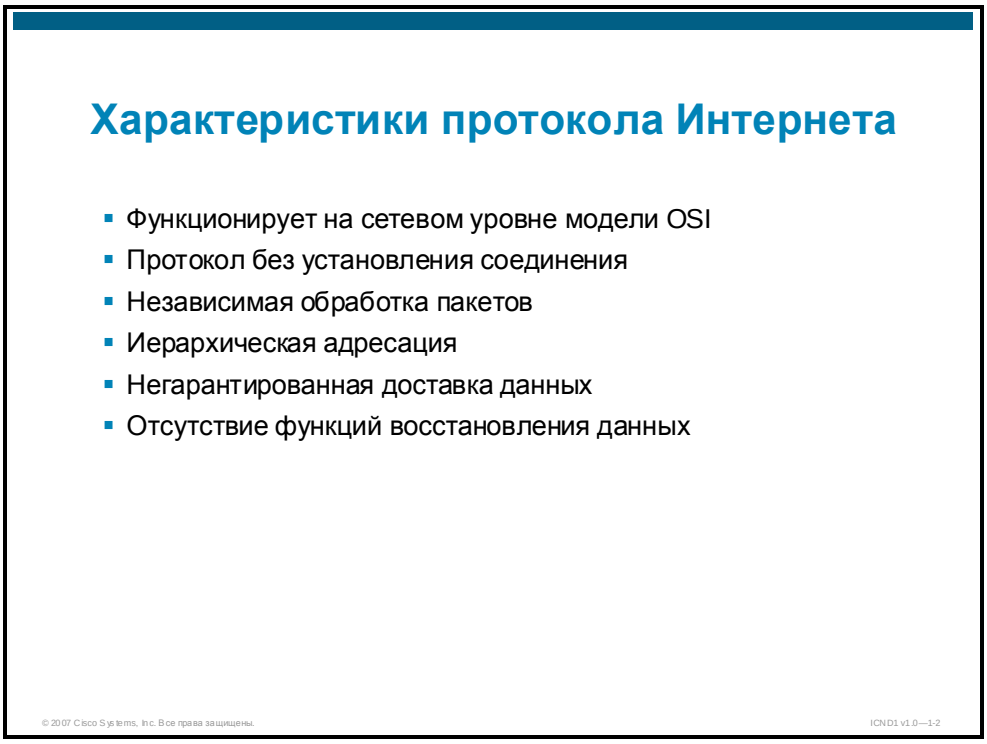
По окончании этого занятия вы сможете описывать последовательность действий управления IP-адресами и их привязки к MAC-адресам. Это значит, что вы сможете выполнять следующие задачи:

- перечислять характеристики протокола Интернета;
- описывать компоненты адреса IPv4;
- описывать структуру адреса IPv4;
- определять классы IP-адресов;
- описывать зарезервированные IP-адреса;
- сравнивать общедоступные и частные IP-адреса;
- определять функцию DHCP для IP-адресации;

- описывать роль DNS в IP-адресации;
- определять стандартные инструменты для определения IP-адреса хоста.

Протокол Интернета

Протокол Интернета (Internet Protocol – IP), входящий в стек протоколов TCP/IP, определяет механизм передачи пакетов на основании адресов назначения и имеет определенные характеристики, связанные с выполнением этой функции. В этом разделе описываются некоторые ключевые функции протокола Интернета.



Передача информации в сети по протоколу IP реализуется с помощью пакетов. Пакет представляет собой автономный независимый объект, который содержит данные и сведения, достаточные для маршрутизации пакета от источника к месту назначения, независимо от предшествующего обмена данными.

Протокол IP обладает следующими характеристиками:

- протокол IP действует на уровне 3 модели OSI (сетевой уровень) и уровне 3 стека протоколов TCP/IP (уровень Интернета);
- IP является протоколом без установления соединения, в котором адресату посылается односторонняя датаграмма без предварительного уведомления целевого устройства; целевое устройство получает данные и не возвращает устройству-отправителю сведения об их статусе;
- протокол IP использует иерархическую адресацию, в которой идентификатор сети можно рассмотреть как улицу, а идентификатор хоста – дом или строение на этой улице;
- протокол IP обеспечивает услуги по принципу "наименьших затрат" и не гарантирует доставку пакетов; на пути к месту назначения возможна отправка в неверном направлении, дублирование или потеря пакета;
- протокол IP не предоставляет никаких специальных возможностей для восстановления поврежденных пакетов; эти услуги обеспечиваются конечными системами сети.

При передаче голосовых или видеоданных в режиме реального времени допускается незначительная потеря пакетов; скорость имеет большее значение, чем восстановление пакета, поскольку восстановление пакетов вызвало бы задержку процесса, происходящего в реальном времени.

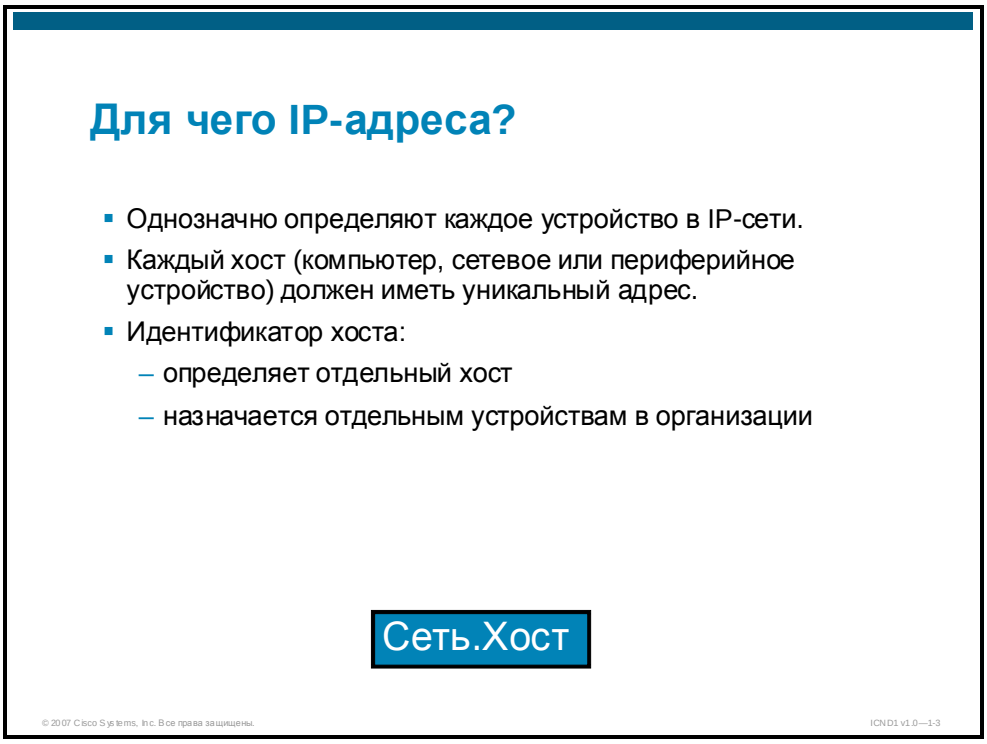
Пример: доставка письма по почте

Аналогом IP-сервисов может служить доставка корреспонденции по почте. В этом примере мы рассмотрим отправителя, живущего в Санкт-Петербурге, родственница которого проживает в Москве. Он посылает родственнице три отдельных письма. Каждое письмо вкладывается в отдельный конверт, на котором указывается адрес родственницы, а в верхнем левом углу – обратный адрес.

Эти три письма опускаются в щель ящика для писем в местном почтовом отделении. Почтовая служба сделает все возможное для доставки этих трех писем адресату в Москве. Однако она не гарантирует, что все три письма прибудут по назначению. Почта не гарантирует также, что все письма будут доставлены одним и тем же оператором или по одному маршруту. И, наконец, почта не гарантирует, что все письма будут доставлены в том порядке, в котором были отправлены.

IP-адресация

Для упрощения маршрутизации пакетов в сети, стек протоколов TCP/IP использует логический адрес, именуемый IP-адресом. В этом разделе описываются составляющие 32-битного адреса IPv4.



Так же как для определения расположения конкретных домов и предприятий необходимы физические адреса, которые позволяют эффективно доставлять почту на реальные объекты, для определения конкретных устройств в IP-сети используются логические IP-адреса, обеспечивающие доставку данных к этим сетевым объектам. Каждый хост, компьютер, сетевое или периферийное устройство, подключенное к сети Интернет, имеет уникальный идентификатор – 32-битный IP-адрес. Эффективная маршрутизация пакетов невозможна без структуры выделения IP-адресов. Изучение структуры IP-адресов и их роли в работе сети способствует пониманию процесса пересылки IP-пакетов по сети с помощью стека протоколов TCP/IP.

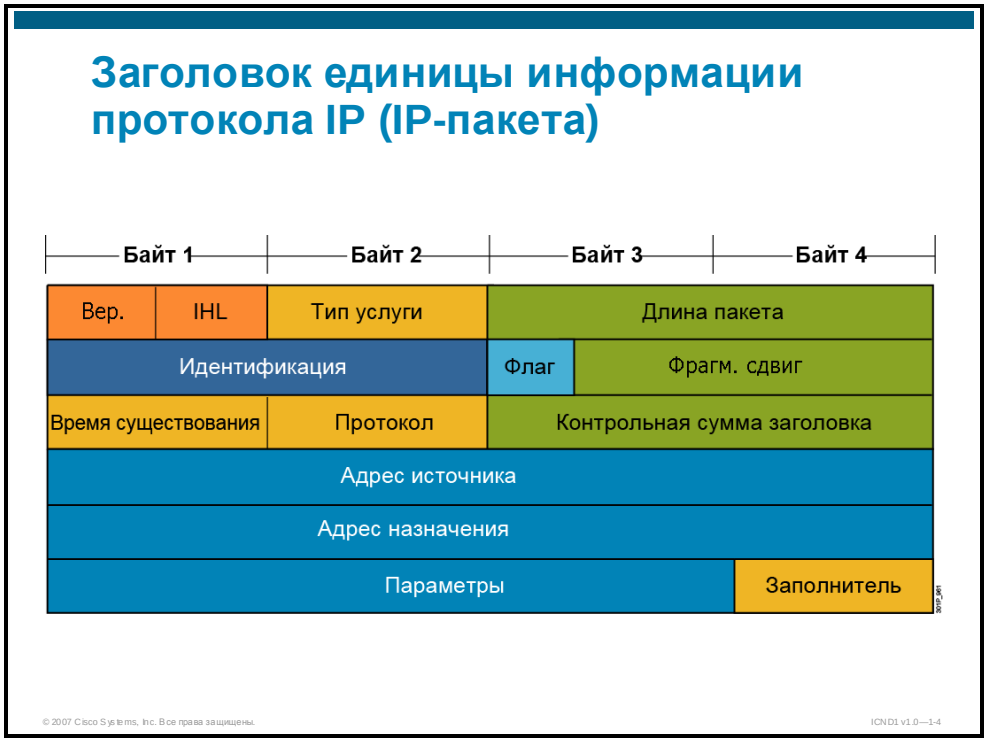
Адрес IPv4 является наиболее распространенным типом адресов, используемых в сети Интернет. Адреса IPv4 представляют собой 32-битные номера, описывающие местоположение сетевых устройств.

IP-адрес является иерархическим и состоит из следующих двух частей:

- Сетевой части (идентификатор сети) описывает сеть, компонентом которой является этот IP-адрес. Маршрутизатор хранит информацию о маршрутах к каждой сети.
- Хостовой части (идентификатор хоста) определяет конечную точку. Конечными точками служат серверы, компьютеры и другие устройства, подключенные к сети.

Поля протокола IP

В этом разделе описываются поля протокола IP в единице информации протокола IP (Protocol Data Unit – PDU).



Как было показано в занятии «Модель обмена данными между хостами», при прохождении через стек протоколов данные инкапсулируются. На уровне Интернета они инкапсулируются в элемент PDU (обычно именуемый «пакетом»). Заголовок этого пакета содержит несколько полей. В этом разделе подробно рассматриваются два поля:

- **Source Address (Адрес источника).** Определяет IP-адрес узла-отправителя.
- **Destination Address (Адрес назначения).** Определяет IP-адрес узла-получателя.

Формат IP-адреса: десятичный формат с точками

	Пример			
IP-адрес представляет собой 32-битное двоичное число	10101100	00010000	10000000	00010001
Для лучшей читаемости 32-битные двоичные числа могут разделяться на четыре 8-битных октета	10101100	00010000	10000000	00010001
Каждый октет (или байт) может быть преобразован в десятичное число	172	16	128	17
Адрес может быть записан в разделенной точками десятичной записи	172.	16.	128.	17

30ip_311

Преобразование двоичного формата адреса в десятичный и наоборот подробно будут рассматривается в курсе позже.

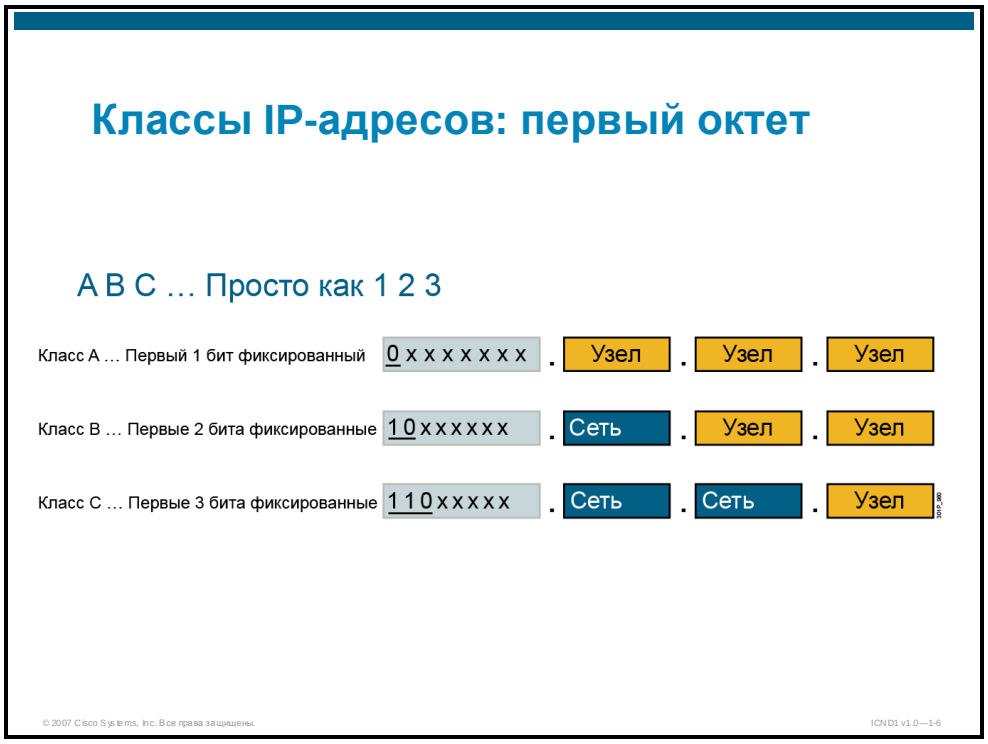
В любом IP-адресе одна часть 32-битного номера представляет сеть, а другая – хост. В то время как сетевые адреса нескольких компьютеров могут совпадать, комбинация сетевого адреса с адресом хоста уникально идентифицирует любое устройство, подключенное к сети.

На рисунке показан двоичный IP-адрес 10101100000100001000000000010001.

Для удобства эти 32-битные номера разбиваются на 4 группы цифр, именуемые октетами (1 октет равен 8 битам). Каждый октет затем представляется в виде десятичного числа от 0 до 255, которые разделяются точкой. Эта схема известна как «десятичное представление с разделительными точками». Показанный выше IP-адрес может быть записан как 172.16.128.17 и читается как «172 точка 16 точка 128 точка 17».

Классы IP-адресов

Чтобы упростить классификацию различных сетей с учетом их размера, IP-адреса подразделяются на категории, именуемые классами. В этом разделе описываются классы и структура IP-адресов в рамках этих классов.



Назначение IP-адресов классам называется классовой (classful) адресацией. Определение классов было дано на ранних этапах развития сети Интернет организацией IANA (Internet Assigned Numbers Authority).

Каждый IP-адрес делится на идентификатор сети и хоста. Кроме того, бит или последовательность битов в начале каждого адреса определяет класс данного адреса. На приведенном ниже рисунке показаны три из пяти классов IP-адресов.

Класс A

В адресах класса A для обозначения сетевого адреса используется только первый октет (8 бит) 32-битного числа. Остальные три октета 32-битного числа используются для адресации хостов. В адресах класса A первый бит всегда имеет значение «0». Поскольку первый бит всегда имеет значение 0, наименьший номер может быть представлен, как 00000000 (десятичный 0), а высший – как 01111111 (десятичное число 127). Однако эти два числа, 0 и 127, зарезервированы и не могут использоваться в качестве сетевых адресов. Любой адрес, который начинается со значения от 1 до 126 в первом октете 32-битного номера, является адресом класса A.

Класс B

В адресах класса B для задания сетевого адреса используется два из четырех октетов (16 бит). Остальные два октета определяют адреса хостов. Первые 2 бита первого октета в адресах класса B всегда равны двоичному числу 10. Двоичное число 10 в начале первого октета гарантирует, что пространство класса B не накладывается на верхние уровни пространства класса A. Остальные 6 битов первого октета могут быть заполнены значениями 1 или 0. Следовательно, наименьший номер, который может представлять адрес класса B, равен 10000000 (десятичное число 128), а наибольший – 10111111 (десятичное число 191). Любой адрес, который начинается со значения в диапазоне от 128 до 191 в первом октете, является адресом класса B.

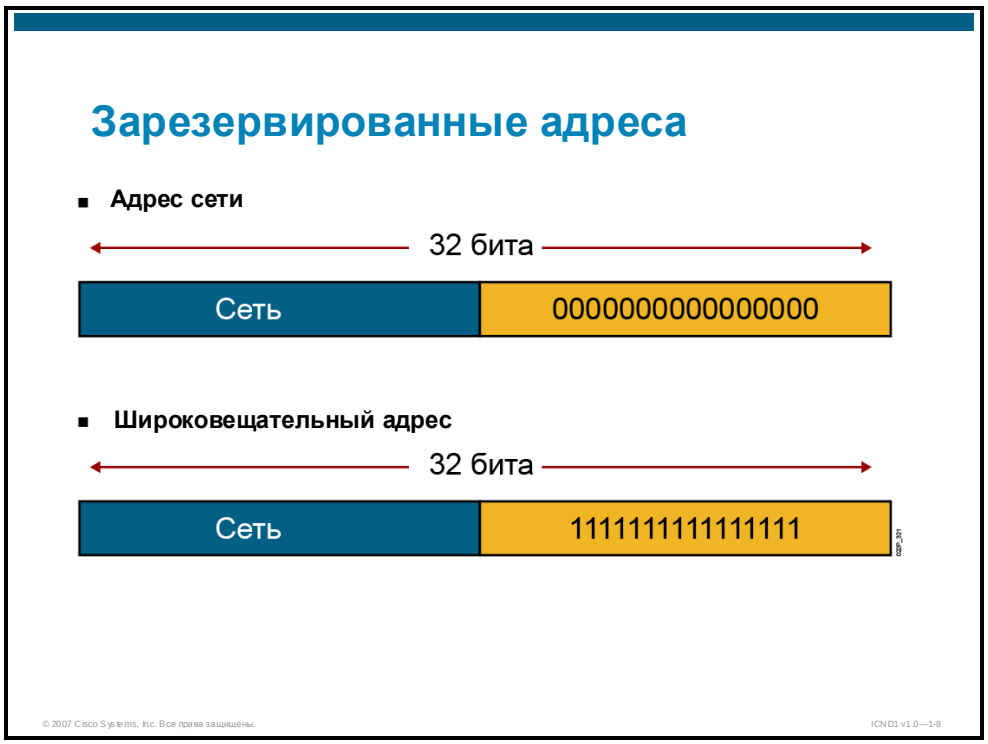
Класс C

В адресах класса C первые три октета (24 бита) IP-адреса определяют сетевую часть, а оставшийся октет резервируется для хостов. Адреса класса C начинаются с двоичного числа 110. Следовательно, наименьший номер, который может представлять адрес класса C, равен 11000000 (десятичное число 192), а наибольший – 11011111 (десятичное число 223). Если адрес содержит в первом октете значение в пределах 192 до 223, он относится к классу C.

На рисунке представлен диапазон IP-адресов первого октетов (в десятичном и двоичном представлении) для классов IP-адресов A–C, а также число доступных хостовых адресов для каждого класса.

Зарезервированные IP-адреса

Некоторые IP-адреса зарезервированы и не могут быть присвоены отдельным устройствам в сети. Эти зарезервированные адреса включают адрес сети, который служит для идентификации самой сети, и широковещательный адрес, используемый для широковещательной рассылки пакетов на все устройства сети. В этом разделе описываются типы зарезервированных IP-адресов и приводятся соответствующие примеры.



Адрес сети

IP-адрес с двоичными нулями во всех хостовых битах зарезервирован для адресации сети. Следовательно, для сети класса A IP-адрес 10.0.0.0 является адресом сети, в которой находится хост 10.1.2.3. IP-адрес 172.16.0.0 является примером адреса сети класса B, тогда как 192.16.1.0 относится к сети класса C. IP-адрес используется маршрутизатором для поиска в таблице IP-маршрутов расположения сети назначения.

Назначаются десятичные числа, заполняющие первые два октета в сетевых адресах класса B. Последние два октета содержат нули, поскольку эти 16 бит предназначены для адресации хостов и используются для конечных устройств, подключенных к сети. В IP-адресе 172.16.0.0 первые два октета зарезервированы для адреса сети; эти октеты никогда не используются для адресации адреса подключенных устройств. Например, устройство в сети 172.16.0.0 может иметь IP-адрес 172.16.16.1. В этом примере 172.16 является сетевой частью адреса, а 16.1 – хостовой.

Направленный широковещательный адрес

Для передачи данных на все устройства в определенной сети используется широковещательный адрес (Directed Broadcast Address). Все хостовые биты в широковещательном IP-адресе заполняются двоичными единицами.

В сети из предыдущего примера (172.16.0.0), в которой 16 бит – хостовые, для широковещательной рассылки по всем устройствам данной сети используется адрес назначения 172.16.255.255.

Направленная широковещательная рассылка может маршрутизироваться. Однако в некоторых версиях операционной системы Cisco IOS маршрутизация широковещательной рассылки по умолчанию не поддерживается.

Локальный широковещательный адрес

При передачи данных с IP-устройства на все устройства локальной сети, во всех битах адреса назначения пакета указываются двоичные единицы (255.255.255.255). Например, этот адрес могут использовать хосты, не имеющие информации о своей сети и апрашивающие этот адрес у сервера. Локальная широковещательная рассылка не подлежит маршрутизации.

Локальный адрес обратной связи

Локальный адрес обратной связи позволяет системе передать сообщение самой себе для тестирования. Типичным локальным IP-адресом обратной связи является 127.0.0.1.

Автоконфигурация IP-адресов

Если при загрузке не было обнаружено ни статически заданных, ни динамически заданных IP-адресов, на хостах с поддержкой локальных для линка IPv4-адресов (RFC 3927) будет создан адрес в диапазоне префиксов 169.254/16. Этот адрес может использоваться только для соединений в собственной локальной сети и имеет множество ограничений, одно из которых состоит в отсутствии поддержки маршрутизации. Как правило, этот адрес используется в случае отказа, если компьютер не может получить адрес через DHCP.

Идентификатор сети

Сетевая часть IP-адреса называется также идентификатором сети и имеет большое значение, поскольку большинство хостов сети может непосредственно взаимодействовать только с устройствами в этой сети. Если хосты должны обмениваться данными с устройствами, интерфейсы которых имеют другой сетевой идентификатор, требуется сетевое оборудование, способное осуществлять маршрутизацию данных между сетями. Это справедливо даже в том случае, если устройства используют один и тот же сегмент среды передачи.

Сетевой идентификатор позволяет маршрутизатору передавать пакет в нужный сегмент сети. Идентификатор хоста помогает маршрутизатору доставлять кадр 2-го уровня с инкапсулированным пакетом указанному хосту в сети. В результате IP-адрес сопоставляется с конкретным MAC-адресом, который требуется процессу маршрутизатора на 2-м уровне для адресации кадра.

Идентификатор хоста

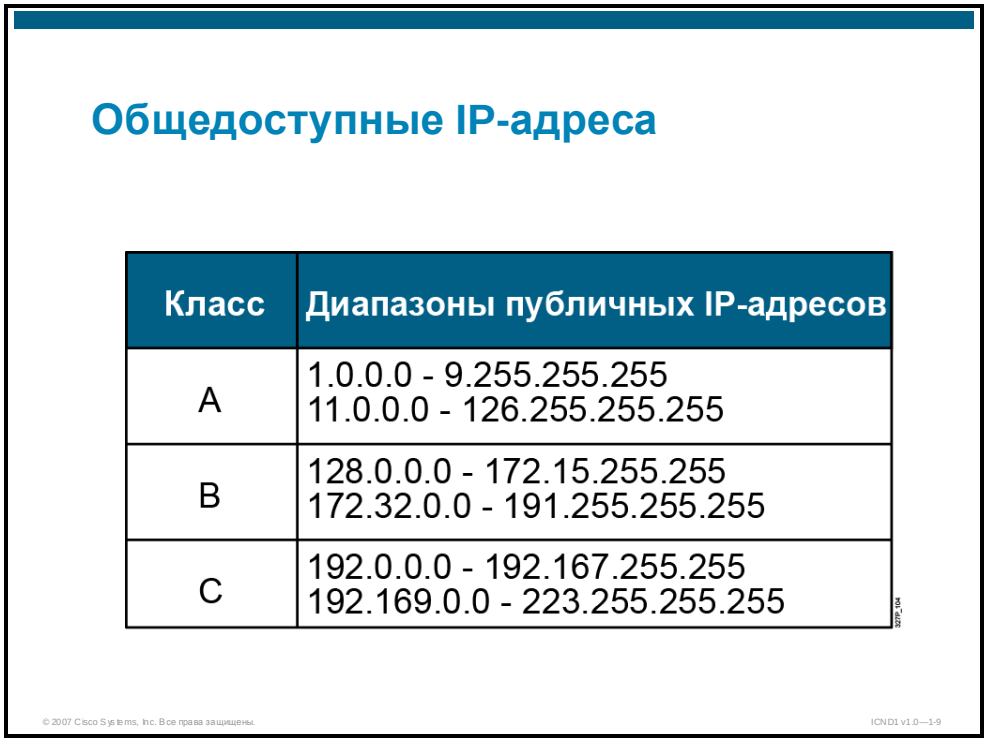
Для каждого класса сетей допускается фиксированное число хостов. В сетях класса A первый октет назначается сети, а три последних октета – хостам. Первый адрес хоста в каждой сети (все нули) зарезервирован для фактического адреса сети, а последний (все единицы) – для широковещательной рассылки. Максимальное число хостов в сети класса A составляет $2^{24} – 2$ (за вычетом зарезервированных сетевого и широковещательного адресов), или 16 777 214.

В сетях класса B первые два октета назначаются сети, а два последних октета – хостам. Максимальное число хостов в сети класса B равно $2^{16} – 2$, или 65 534.

В сетях класса C сети назначаются три первых октета. Хостам присваивается последний октет, следовательно, максимальное число хостов составляет $2^{8} – 2$, или 254.

Общедоступные и частные IP-адреса

Одни сети соединяются между собой через Интернет, тогда как другие являются частными. Так, адреса, используемые в примерах этого курса, являются частными, то есть они не предназначены для общего пользования. Для всех типов сетей необходимы как общедоступные (Public), так и частные (Private) IP-адреса. В этом разделе описываются задачи и источники общих и частных IP-адресов.



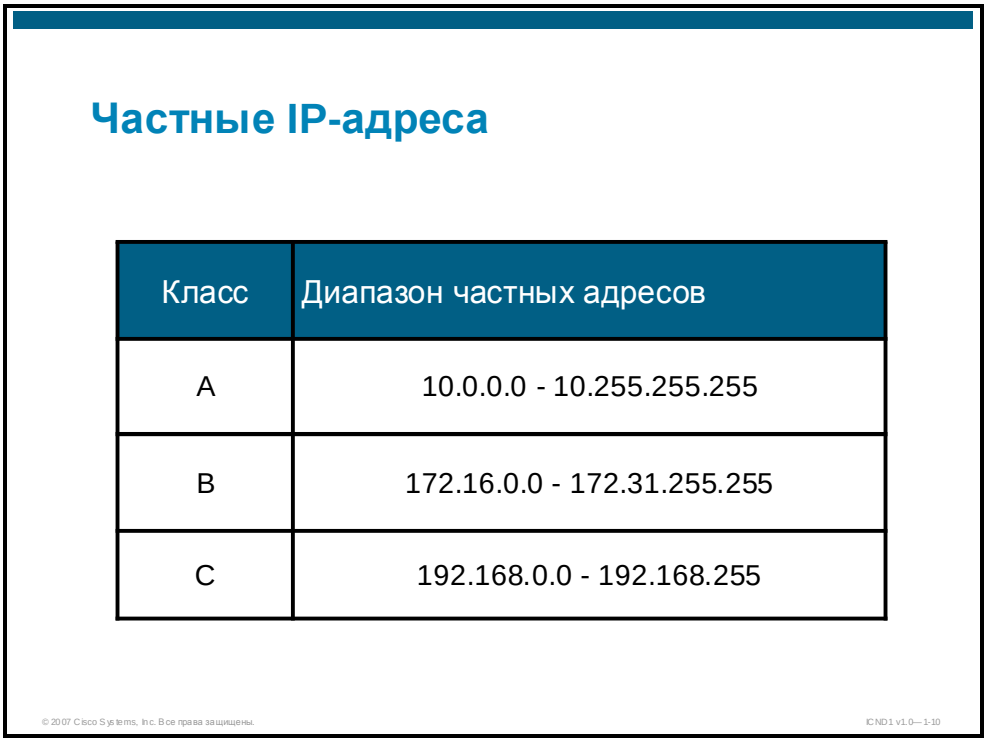
Общедоступные IP-адреса

Стабильность сети Интернет непосредственно зависит от уникальности сетевых адресов общего пользования. Поэтому требуется механизм, гарантирующий эту уникальность. Эти полномочия первоначально были возложены на организацию InterNIC- Internet Network Information Center (Информационный центр сети Internet). Преемником InterNIC стала IANA (Internet Assigned Numbers Autority -Администрация адресного пространства Internet). IANA осуществляет строгий контроль за присвоением IP-адресов, гарантируя отсутствие дублирования адресов общего пользования. Подобное дублирование могут вызвать нестабильность сети Интернет и сделать невозможной доставку датаграмм в сетях, использующих такие адреса.

Для получения IP-адреса или блока адресов необходимо обратиться к поставщику услуг Интернета (ISP). Затем поставщик услуг Интернета связывается с вышестоящей или региональной регистрирующей организацией:

- APNIC (Asia Pacific Network Information Center)
- ARIN (American Registry for Internet Numbers)
- RIPE NCC (Réseaux IP Européens Network Coordination Centre)

Стремительный рост сети Интернет привел к истощению запаса общедоступных IP-адресов, для решения этой проблемы были разработаны новые схемы адресации, такие как преобразование сетевых адресов NAT – Network Address Translation, бесклассовая междоменная маршрутизация (CIDR – Classless Interdomain Routing) и IPv6.



Частные IP-адреса

В отличие от глобальных хостов Интернета, требующих уникальных IP-адресов, для частных хостов, не подключенных к сети Интернет, можно использовать любые адреса при условии их уникальности в рамках частной сети. Однако поскольку множество частных сетей существует параллельно с публичными сетями, захват «первых попавшихся» адресов категорически не рекомендуется.

В 1994 году сообщество IETF опубликовало документ RFC 1597, в котором утверждалось, что многие организации, использующие TCP/IP и IP-адресацию, не подключены к Интернету. Вслед за RFC 1597 был опубликован документ RFC 1918, в котором предлагалось выделить блок доступного пространства IP-адресов для частных сетей. Частные сети, в которых протокол IP необходим для поддержки приложений, но нет необходимости в подключении к Интернету, могут просто использовать адреса из выделенного диапазона для частного применения.

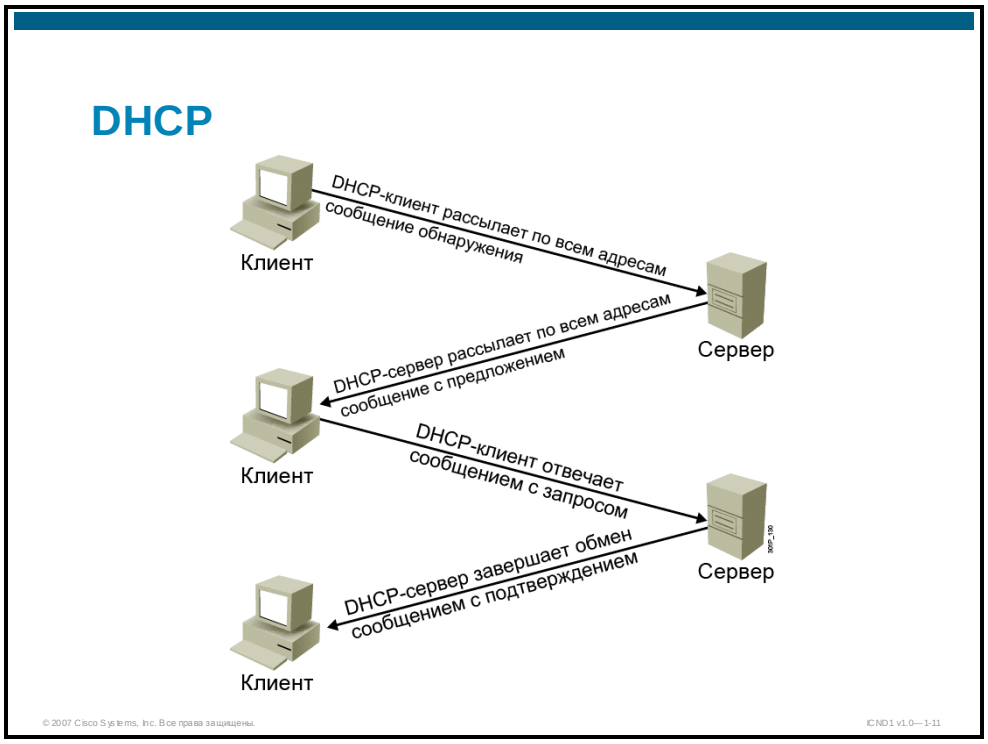
Для частного, внутреннего использования было выделено три блока IP-адресов (одна сеть класса A, 16 сетей класса B и 256 сетей класса C). Адреса из этого диапазона не подлежат маршрутизации в магистральной сети Интернет (см. рисунок). Маршрутизаторы Интернета настроены на отбрасывание частных адресов.

При адресации во внутренней, не публичной сети эти частные адреса могут использоваться вместо общедоступных адресов.

Если сеть, использующая частные адреса, должна подключаться к Интернету, необходимо преобразовать частные адреса в адреса общего пользования. Таким процессом преобразования является NAT. Сетевым устройством, осуществляющим преобразование NAT, как правило, служит маршрутизатор.

Протокол DHCP (Dynamic Host Configuration Protocol)

Существует несколько автоматизированных методов присвоения IP-адресов на основе протоколов. В этом разделе рассматривается метод получения IP-адреса с помощью протокола DHCP.

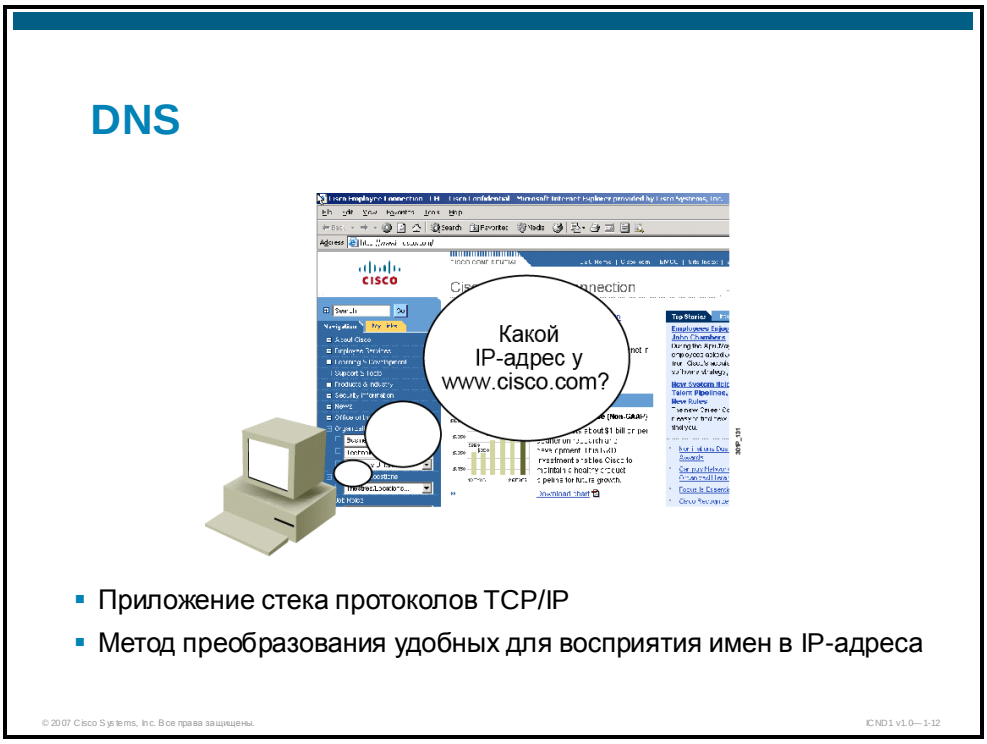


DHCP используется для автоматического присвоения IP-адресов и задания параметров конфигурации стека протоколов TCP/IP, таких как маска подсети, маршрутизатор по умолчанию и DNS-серверы. Протокол DHCP применяется также для задания других базовых параметров конфигурации, включая время, на которое адрес выделяется хосту. DHCP состоит из двух компонентов: протокол для доставки параметров конфигурации конкретного хоста с DHCP-сервера и механизм выделения сетевых адресов хостам.

Протокол DHCP обеспечивает быстрое и динамическое выделение IP-адреса хосту. Для этого требуется только заданный диапазон IP-адресов на сервере DHCP. При подключении к сети хосты обращаются к DHCP-серверу и запрашивают сведения об адресе. DHCP-сервер выбирает адрес и выделяет его хосту. Хост только «арендует» этот адрес и периодически обращается к DHCP-серверу для продления аренды. Этот механизм позволяет аннулировать выделение адресов отсутствующим или отключенным в течение длительного времени хостам. Адреса возвращаются в пул адресов DHCP-сервера и могут быть выделены повторно при необходимости.

Система доменных имен (DNS)

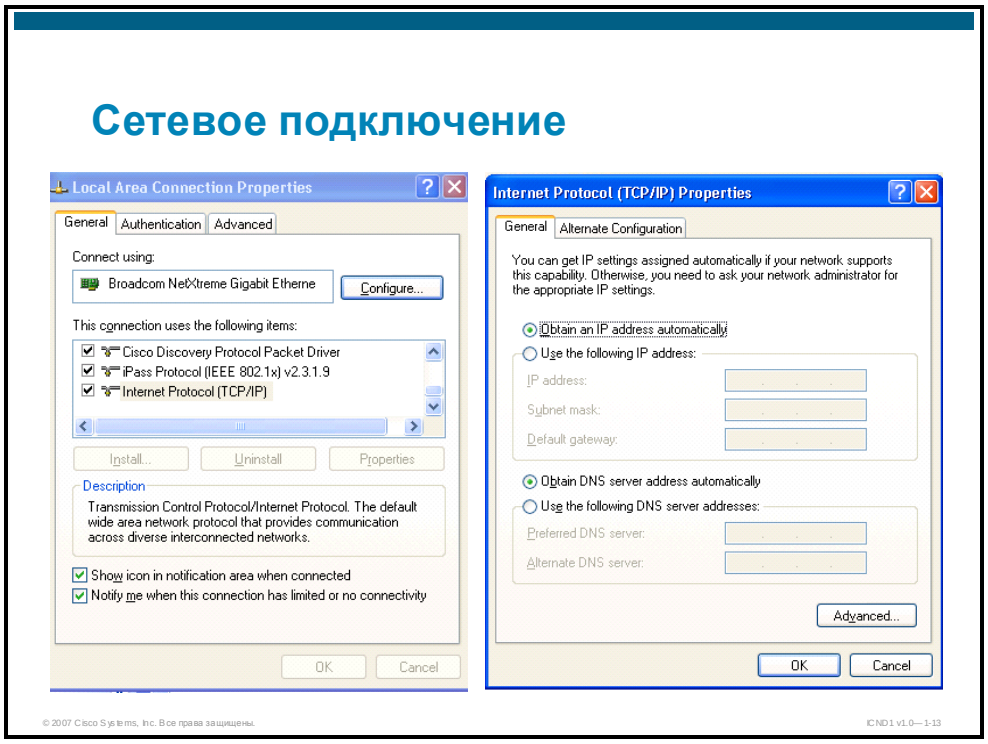
Система доменных имен (DNS) обеспечивает эффективный способ преобразования удобных для восприятия имен конечных IP-систем в понятные оборудованию IP-адреса, необходимые для маршрутизации. В этом разделе описывается действие DNS.



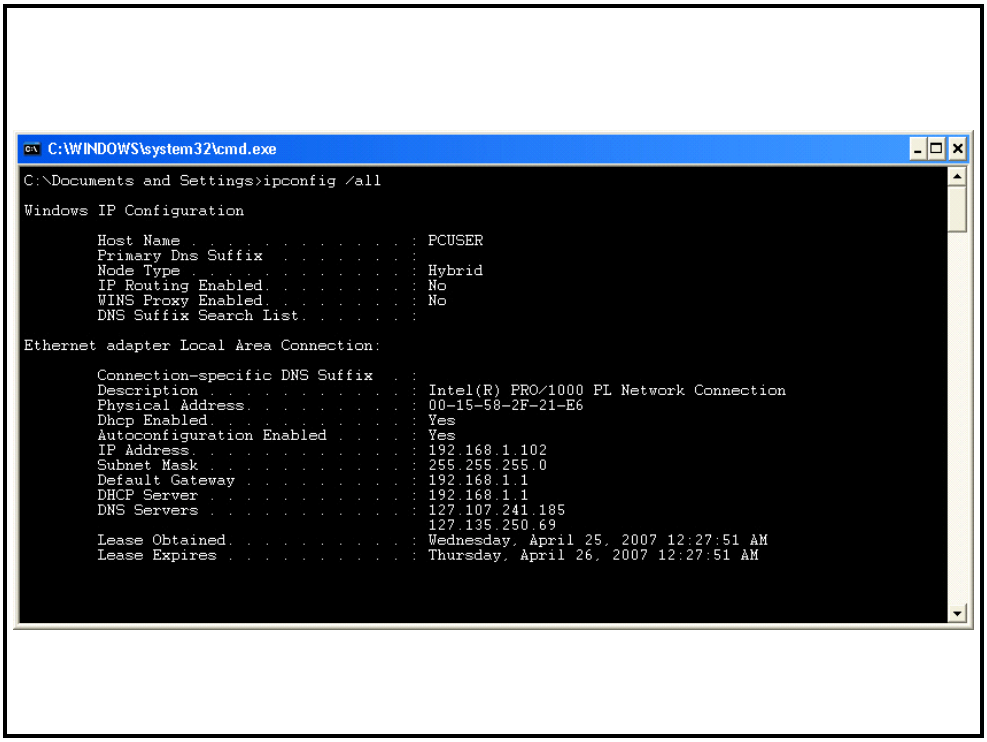
DNS – это механизм преобразования символьных имен в IP-адреса. Приложение DNS избавляет пользователей IP-сетей от необходимости запоминать IP-адреса. Без этого Интернет *не был бы* популярным и распространенным, каким является сейчас.

Использование стандартных инструментов для определения IP-адреса хоста

В большинстве операционных систем предусмотрен набор инструментов для проверки адресации хоста. В этом разделе рассматриваются инструменты, доступные на большинстве персональных компьютеров.



Пункт **Сетевые подключения** в разделе «Панель управления» позволяет устанавливать и просматривать IP-адрес, настроенный на персональном компьютере. В рассматриваемом примере на персональном компьютере выбрано получение адреса с DHCP-сервера.



Для отображения всех текущих значений конфигурации сети TCP/IP и обновления параметров протокола DHCP и службы DNS можно использовать команду IPCONFIG. Команда **ipconfig** без параметров позволяет отобразить IP-адрес, маску подсети и шлюз по умолчанию для всех адаптеров.

Синтаксис

ipconfig [**/all**] [**/renew** [*Adapter*]] [**/release** [*Adapter*]] [**/flushdns**] [**/displaydns**] [**/registerdns**] [**/showclassid** *Adapter*] [**/setclassid** *Adapter* [*ClassID*]]

Параметры

/all: отображает полную конфигурацию TCP/IP для всех адаптеров. Команда **ipconfig** без данного параметра отображает только значения IP-адреса, маски подсети и шлюза по умолчанию для каждого адаптера. Адаптеры могут представлять физические интерфейсы, например установленные сетевые адаптеры, или логические, такие как коммутируемые подключения.

/renew [*Adapter*]**:** обновляет конфигурацию DHCP для всех адаптеров (если не указан конкретный адаптер) или для заданного адаптера, если включен параметр *Adapter*. Этот параметр доступен только на компьютерах с адаптерами, для которых настроено автоматическое получение IP-адреса. Чтобы указать имя адаптера, введите имя адаптера, отображаемое при использовании команды **ipconfig** без параметров.

/release [*Adapter*]**:** отправляет сообщение DHCPRELEASE DHCP-серверу для освобождения текущей конфигурации DHCP и сброса параметров IP-адреса для всех адаптеров (если адаптер не указан) или для заданного адаптера, если параметр *Adapter* включен. Этот параметр отключает TCP/IP для адаптеров, настроенных на автоматическое получение IP-адреса. Чтобы указать имя адаптера, введите имя адаптера, отображаемое при использовании команды **ipconfig** без параметров.

/flushdns: очищает и сбрасывает содержание кэша DNS-клиента. При поиске неполадок DNS можно использовать эту процедуру для удаления из кэша устаревших, а также других динамически добавленных записей.

/displaydns: отображает содержимое кэша DNS-клиента, включая записи, предварительно загруженные из локального файла Hosts, а также любые полученные за последнее время записи запросов распознавания имен. Эта информация используется службой DNS-клиента для быстрого определения адресов для часто запрашиваемых имен без обращения к указанным в конфигурации DNS-серверам.

/registerdns: инициирует ручное динамическое обновление регистрации имен DNS и IP-адресов, заданных в конфигурации компьютера. Этот параметр полезен при устранении неполадок в случае отказа в регистрации имени DNS или при выяснении причин неполадок динамического обновления, связанных с взаимодействием DNS-клиента и сервера, без перезапуска клиента. Параметры конфигурации DNS в дополнительных свойствах протокола TCP/IP определяют имена, зарегистрированные в DNS.

/showclassid *Adapter***:** отображает идентификатор класса DHCP для заданного адаптера. Для просмотра идентификатора класса DHCP всех адаптеров необходимо использовать вместо параметра *Adapter* шаблонный символ звездочки (*****). Этот параметр доступен только на компьютерах с адаптерами, для которых задано автоматическое получение IP-адреса.

/setclassid *Adapter* [*ClassID*]**:** настраивает идентификатор класса DHCP для заданного адаптера. Для задания идентификатора класса DHCP для всех адаптеров необходимо использовать вместо параметра *Adapter* шаблонный символ звездочки (*****). Этот параметр доступен только на компьютерах с адаптерами, для которых задано автоматическое получение IP-адреса. Если идентификатор класса DHCP не указан, текущий идентификатор класса удаляется.

/?: отображает справку в командной строке.

Резюме

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

Резюме

- Сетевые IP-адреса состоят из двух частей: идентификатор сети и идентификатор хоста.
- Адреса IPv4 содержат 32 бита, разделенных на октеты, и обычно отображаются в десятичном формате с точками (например, 192.168.54.18).
- При записи в двоичном формате первый бит в адресе класса A всегда имеет значение 0, первые 2 бита в адресе класса B всегда имеют значение 10, и первые 3 бита в адресе класса C всегда 110.

Резюме (прод.)

- Некоторые IP-адреса (сетевые и широковещательные) зарезервированы и не могут быть присвоены отдельным устройствам в сети.
- Хосты Интернета должны иметь уникальный общий IP-адрес, тогда как частные хосты могут иметь любой действительный частный адрес, уникальный внутри данной сети.
- Протокол DHCP используется для автоматического присвоения IP-адресов и задания параметров конфигурации стека протоколов TCP/IP, таких как маска подсети, маршрутизатор по умолчанию и DNS-серверы.
- DNS представляет собой приложение, определенное в стеке протоколов TCP/IP и обеспечивающее преобразование удобных для восприятия имен в IP-адреса.

Резюме (прод.)

- На хостах предусмотрены инструменты для проверки IP-адреса хоста:
  - Пункт «Сетевые подключения» в Панели управления
  - IPCONFIG

Занятие 5

Общие сведения о транспортном уровне стека протоколов TCP/IP

Обзор

Для взаимодействия компьютеры нуждаются в определенных правилах, или протоколах, позволяющих упорядочить обмен данными между ними. Самым распространенным стеком протоколов во всем мире является TCP/IP. Представление о работе TCP/IP необходимо для понимания способа передачи данных в сетевых средах.

Способ доставки пакета данных по сети протоколом IP является основополагающей концепцией в архитектуре TCP/IP, используемой в крупных сетях. Четкое понимание процесса передачи данных по протоколу IP необходимо для формирования представления о принципе работы стека протоколов TCP/IP в целом. Это, в свою очередь, позволяет осмыслить приоритизацию, отсеивание, защиту, оптимизацию и обслуживание передаваемых по сетям данных. В этом занятии описывается последовательность действий по доставке IP-пакетов, а также связанные с этим процессом концепции и структуры, такие как пакеты, датаграммы и поля протоколов. Это позволит понять, как происходит передача данных в крупных сетях.

Для правильной работы Интернета и частных сетей требуется надежная доставка данных. Обеспечить такую безотказную доставку данных позволяет развертывание прикладного уровня и использование услуг, предоставляемых сетевым протоколом. В моделях OSI и TCP/TP управление процессом надежной передачи данных отдано транспортному уровню. Транспортный уровень скрывает подробные сведения о сети от верхних уровней, обеспечивая прозрачную передачу данных. Протоколы UDP и TCP стека TCP/IP функционируют между транспортным уровнем и прикладным уровнем, скрывая подробные сведения о сети от прикладного уровня. Кроме того, изучение принципов работы протоколов UDP и TCP между сетевым и транспортным уровнями способствует более глубокому пониманию процесса передачи данных в сетевых средах TCP/IP. В этом занятии описывается функция транспортного уровня и принцип работы протоколов UDP и TCP.

Задачи

По окончании этого занятия вы сможете сравнивать и сопоставлять стек TCP/IP с моделью OSI. Это значит, что вы сможете выполнять следующие задачи:

- объяснять задачи и функции транспортного уровня;
- сравнивать протоколы транспортного уровня с установлением и без установления соединения;
- знать характеристики UDP;
- знать характеристики TCP;
- перечислять стандартные приложения TCP/IP;
- описывать взаимодействие уровня 3 с уровнем 4 стека протоколов;
- описывать взаимодействие уровня 4 с уровнем приложений стека протоколов;
- определять порядок действий по инициализации TCP-соединения;
- описывать механизм управления потоками и причины, по которым оно необходимо;
- определять принцип подтверждения последовательности данных;
- определять функцию оконирования;
- определять номера последовательности и номера подтверждений.

Функции транспортного протокола

Функционируя между прикладным и сетевым уровнями, транспортный уровень является фундаментальной частью многоуровневой сетевой архитектуры TCP/IP. В этом разделе описываются функции транспортного уровня.

Сетевой уровень направляет данные к получателю, но он не может обеспечить доставку данных в правильном порядке, отсутствие ошибок и потерь. Транспортный уровень использует два протокола, UDP и TCP, предоставляющие услуги обмена данными непосредственно для прикладных процессов, выполняемых на хостах. «Базовой» услугой, предоставляемой транспортным уровнем, является мультиплексирование сеансов, выполняемое протоколами UDP и TCP. Услуга «Премиум» транспортного уровня – обеспечение надежной доставки, осуществляется только протоколом TCP.

Главной обязанностью транспортного уровня является передача сеансов приложений на сетевой уровень, которая обеспечивается протоколами UDP и TCP. При использовании TCP транспортный уровень выполняет дополнительные функции по обеспечению операций полного цикла обмена, сегментации, управлению потоками и применению механизмов обеспечения надежности.

Пример: UDP – отправка обычной почты

Услуги UDP можно сравнить с обычной услугой по отправке платежей по счетам, оказываемой почтовым отделением. Каждый платеж по счету запечатывается в конверт, на котором указывается адрес конкретной компании и обратный адрес. Почтовая служба гарантирует, что приложит все усилия, чтобы доставить каждый платеж. Однако почта не гарантирует доставку и не обязана уведомлять отправителя о том, было ли доставлено отправление. Так же как и обычная

почтовая служба, UDP является очень простым протоколом, обеспечивающим только базовые услуги по передаче данных.

Пример: TCP – отправка по почте с уведомлением

Услуги TCP можно сравнить с отправкой почтового сообщения с уведомлением о вручении. Предположим, что вам необходимо переслать книгу из Санкт-Петербурга вашей родственнице в Москву. Но оказывается, почта обрабатывает только письма. Вы вырываете страницы из книги и упаковываете их в отдельные конверты. Чтобы быть уверенным, что книга будет собрана правильно, каждый конверт нумеруется. Затем вы надписываете адреса на конвертах и отправляете первый из них как почтовое отправление с уведомлением о вручении. Почтовая служба доставляет его любым доступным ей способом, но, поскольку это письмо с уведомлением, при доставке перевозчик обязан получить у вашей родственницы расписку и вернуть вам уведомление о доставке.

Отправка каждой страницы по отдельности весьма утомительна, поэтому вы отправляете несколько конвертов вместе. Почтовая служба опять доставляет каждый конверт любым доступным ей способом и маршрутом. Ваша родственница расписывается в отдельной квитанции о получении за каждый конверт в пакете при их получении. Если один конверт потеряется при пересылке, вы не получите уведомление о доставке этого пронумерованного конверта и вам придется повторно послать эту страницу. После получения всех конвертов ваша родственница соберет страницы в нужном порядке и склеит книгу. Подобно почтовому отправлению с уведомлением о вручении TCP является сложным протоколом, предлагающим услуги по точной и отслеживаемой передаче данных.

Мультиплексирование сеансов

Мультиплексирование сеансов представляет собой операцию, в которой отдельный компьютер с одним IP-адресом может работать с несколькими сеансами одновременно. Сеанс создается, когда требуется передать данные с исходного компьютера на целевой компьютер. Обычно эта процедура предусматривает ответ, хотя это не является обязательным. Создание сеанса и управление им осуществляется в сетевом IP-приложении, которое содержит уровни модели OSI с 5-ого по 7-ой.

Сеанс с негарантированной доставкой (best-effort) очень прост. Параметры сеанса передаются протоколу UDP. Сеанс с негарантированной доставкой отправляет данные по указанному IP-адресу с использованием заданных номеров портов. Каждая передача является отдельным событием, и никаких записей или связей между передачами не сохраняется.

При использовании надежной службы TCP перед передачей необходимо установить соединение между отправителем и получателем. TCP открывает соединение и согласует его параметры с получателем. Во время передачи потока данных протокол TCP поддерживает надежную доставку данных и после ее завершения закрывает соединение.

Например, при вводе ссылки на Yahoo в адресной строке окна Internet Explorer появится веб-сайт Yahoo, соответствующий заданному URL-адресу. Оставив открытым сайт Yahoo, можно снова открыть обозреватель в другом окне и ввести другой URL-адрес (например, Google). Можно открыть еще одно окно обозревателя и ввести URL-адрес Cisco.com. Таким образом, с использованием одного IP-подключения будут открыты три веб-сайта, поскольку сеансовый уровень разделяет отдельные запросы по номеру порта.

Сегментация

Протокол TCP берет блоки данных с прикладных уровней и готовит их к отправке по сети. Каждый блок разбивается на более мелкие сегменты, соответствующие максимальному размеру блока (MTU – Maximum Transmission Unit) нижнего уровня модели. Более простой протокол UDP не выполняет проверку или согласование, он работает с данными, полученными от прикладного процесса.

Управление потоком

Если отправитель передает данные быстрее, чем получатель может их принять, получатель отбрасывает данные, требуя их повторной передачи. Повторная передача может потребовать дополнительное время и ресурсы сети, поэтому большая часть методов управления потоком стремится максимально увеличить скорость передачи данных при одновременном сокращении потребностей в повторной передаче.

В протоколе TCP основная часть управления потоком реализуется за счет подтверждения приема данных получателем; перед отправкой следующего блока отправитель ждет этого подтверждения. Однако, если время на передачу и подтверждение приема (RTT – Round-Trip Time) слишком велико, общая скорость передачи данных может снизиться до недопустимого уровня. Механизм определения размера окна в сочетании с подтверждением приема позволяет повысить производительность сети. Размер окна позволяет компьютеру-получателю сообщать о том, сколько данных он может получить, до передачи подтверждения компьютеру-отправителю.

Транспортный протокол с установлением соединения

В рамках транспортного уровня протокол с установлением соединения, например TCP, устанавливает сеансовое соединение и поддерживает его на протяжении всего процесса передачи. После завершения передачи сеанс прекращается. Этот принцип более подробно рассматривается в разделе «Сравнение режимов надежной и негарантированной доставки».

Надежность (гарантия доставки)

Функция надежности протокола TCP выполняет три основные задачи:

- распознавание и восстановление потерянных данных;
- выявление и устранение продублированных и некорректных данных;
- предотвращение перегрузок.

Надежность не всегда необходима. Например, при потере пакета из потока видеоданных и последующей повторной передаче их изображение будет искажено. Это может привести к недовольству и замешательству аудитории и сделает данные бесполезными. В приложениях реального времени, например, при передаче голосовых и видеоданных, отбрасывание пакетов допустимо до тех пор, пока общий процент отброшенных пакетов мал.

Сравнение режимов надежной и негарантированной доставки

Термины «режим надежной доставки» и «режим негарантированной доставки» (best-effort) описывают два различных типа соединений между компьютерами. Каждый тип имеет свои преимущества и недостатки. В этом разделе рассматриваются и сравниваются оба типа соединений.

Режим надежной доставки (с установлением соединения)

TCP является надежным протоколом транспортного уровня. Для поддержки надежности доставки протокол TCP устанавливает соединение между компьютерами. В начале процесса происходит обмен информацией о возможностях получателя и согласование исходных параметров. Эти параметры затем используются для отслеживания передачи данных, в процессе активности соединения.

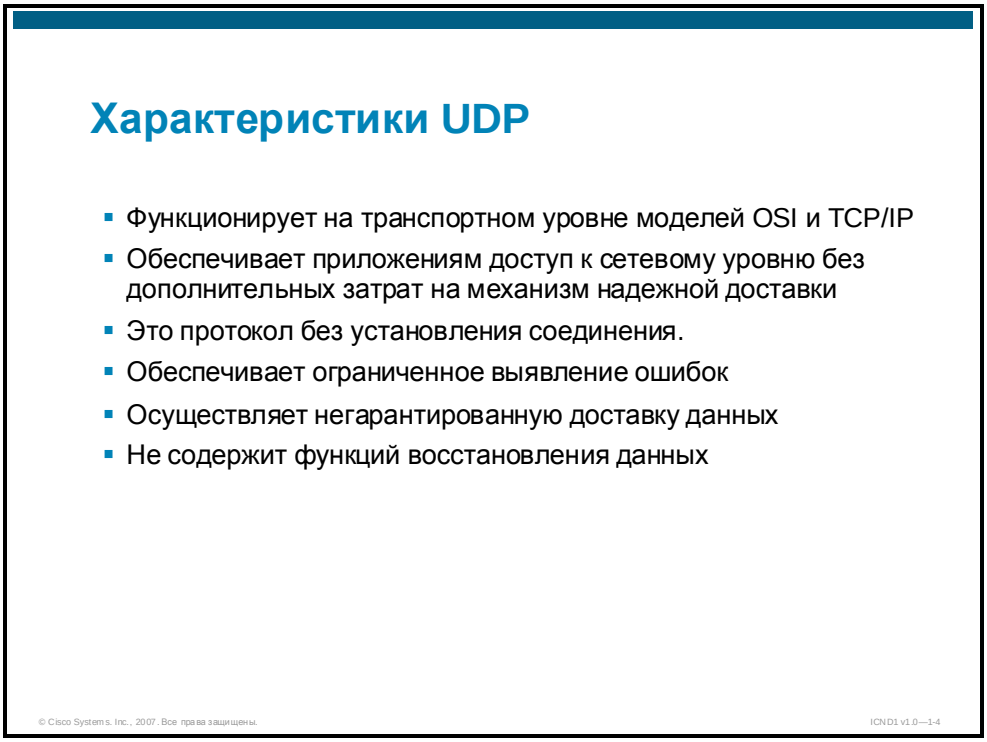
Когда компьютер-отправитель передает данные, он присваивает им номер последовательности. Затем получатель посылает ответ с подтверждением, содержащим следующий ожидаемый номер последовательности. Этот обмен номерами последовательности и номерами подтверждения позволяет протоколу обнаруживать потери, дублирование или ошибочность данных. TCP является сложным протоколом транспортного уровня. В данном модуле обсуждаются только самые общие сведения о работе протокола TCP.

Режим негарантированной доставки (без установления соединения)

Протокол UDP является протоколом негарантированной доставки. Он не требует и не предполагает сохранение информации о ранее отправленных данных. Поэтому протокол UDP не требует установления соединения с получателем и называется протоколом «без установления соединения». Существует множество ситуаций, в которых этот тип соединения является более удобным, чем режим гарантированной доставки. Передача данных без установления виртуального соединения предпочтительна для приложений, для которых требуется более высокая скорость обмена данными без контроля доставки.

Протокол UDP

Транспортный уровень стека TCP/IP содержит протоколы, которые обеспечивают адресацию для передачи данных по сети. Протокол UDP является расширением первоначального стека протоколов TCP/IP и является одним из таких протоколов. В данном разделе описываются некоторые из основных функций протокола UDP.

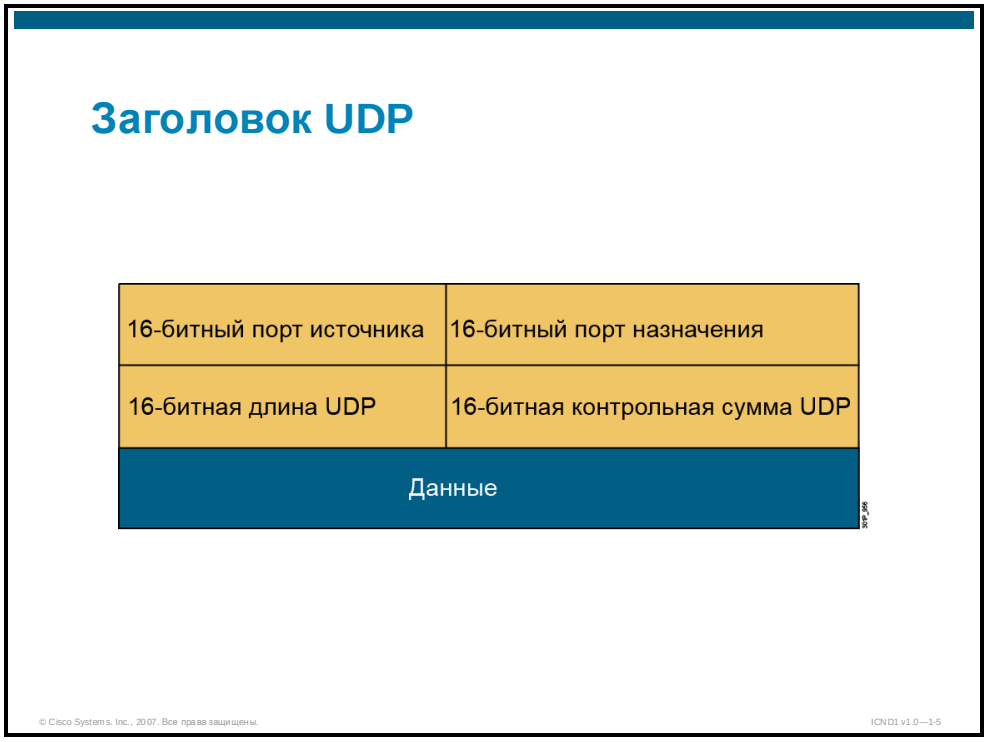


Протокол UDP обладает следующими характеристиками.

- Протокол UDP функционирует на уровне 4 (транспортном) модели OSI и стека протоколов TCP/IP.
- Протокол UDP обеспечивает приложениям доступ к сетевому уровню без дополнительных затрат на механизм надежной доставки.
- UDP, как и IP, является протоколом без установления соединения, адресату пересылаются датаграммы в одностороннем порядке без предварительного уведомления устройства назначения.
- Протокол UDP выполняет выявление ошибок в очень ограниченной форме. Датаграмма UDP содержит необязательное поле контрольной суммы, которое может использоваться получающим устройством для проверки целостности данных. Кроме того, датаграмма UDP содержит псевдозаголовок, в котором имеется порт получателя. Если получающее устройство обнаруживает, что датаграмма направлена на неактивный порт, оно отвечает сообщением, что порт недоступен.
- Протокол UDP обеспечивает услуги по принципу «наименьших затрат» и не гарантирует доставку пакетов, поскольку на пути к получателю пакеты могут быть направлены в неверном направлении, продублированы или потеряны.
- Протокол UDP не предоставляет никаких специальных возможностей по восстановлению потерянных или поврежденных пакетов. При необходимости эти услуги выполняются вышестоящими уровнями.

Пример: рассылка рекламных листков

Услуги протокола UDP можно сравнить с рассылкой по почте рекламных листков, уведомляющих соседей о распродаже домашней утвари. В этом примере продавец печатает рекламные листки с указанием даты, времени и месте распродажи. Продавец указывает на каждом листке имя и адрес соседей, проживающих в радиусе двух километров. Почтовая служба доставляет каждый рекламный листок любым доступным ей способом и маршрутом. Однако продавец не использует почтовые отправления с уведомлением о доставке, поскольку для него не имеет особого значения, будет ли рекламный листок потерян в пути или сосед подтвердит его получение.



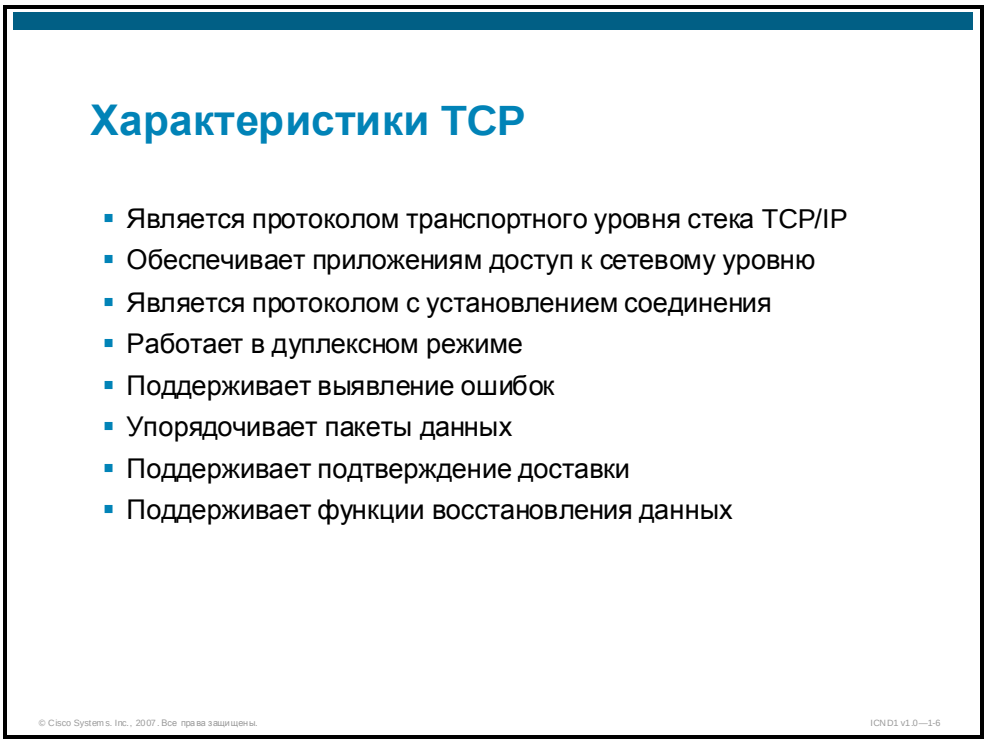
Размер заголовка UDP составляет 64 бита. Заголовок UDP (см. рисунок) содержит следующие поля:

- **Source port (Порт источника).** Номер порта источника (16 битов).
- **Destination port (Порт назначения).** Номер порта назначения (16 битов).
- **Length (Длина).** Длина заголовка UDP и данных UDP (16 битов).
- **Checksum (Контрольная сумма).** Рассчитанная контрольная сумма заголовка и данных (16 битов).
- **Data (Данные).** Данные протокола верхнего уровня (Upper-layer protocol – ULP) (размер нефиксирован).

Протокол UDP используется протоколами TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), NFS (Network File System) и системой DNS (Domain Name System).

Протокол TCP

TCP расшифровывается как Transmission Control Protocol (протокол управления передачей). Это протокол с установлением соединения, обеспечивающий надежную доставку данных между хостами. Протокол TCP имеет ряд уникальных характеристик, связанных с таким методом доставки. В этом разделе обсуждаются основные характеристики протокола TCP.



Протокол TCP также является протоколом транспортного уровня стека TCP/IP. Он выполняет функции адресации для обеспечения передачи данных по сети.

Протокол TCP имеет следующие характеристики.

- Протокол TCP, так же как протокол UDP, функционирует на уровне 4 (транспортном) модели OSI и стека протоколов TCP/IP.
- Подобно протоколу UDP, протокол TCP предоставляет приложениям доступ к сетевому уровню.
- TCP является протоколом с установлением соединения между двумя сетевыми устройствами для обмена данными. Конечные устройства синхронизируют параметры передачи данных между собой для управления скоростью передачи и предотвращения перегрузки в сети.
- Соединение TCP представляет собой пару виртуальных каналов, по одному в каждом направлении, то есть функционирует в дуплексном режиме.
- Протокол TCP выполняет обнаружение ошибок, помещая в датаграмму контрольную сумму, которая позволяет удостовериться, что информация заголовка TCP не повреждена.
- Сегменты TCP последовательно нумеруются, так что получатель может выполнить сортировку сегментов и определить потерю информации.

- После получения одного или нескольких сегментов TCP получатель отвечает отправителю подтверждением их получения. Если получение сегментов не подтверждается, отправитель может повторно передать сегмент или прекратить соединение, если обнаружит, что соединение с получателем прервано.
- Протокол TCP предоставляет услуги по восстановлению информации, в соответствии с которыми получатель может запросить повторную передачу сегмента. Если получение сегмента не подтверждено, отправитель повторно передает сегмент.

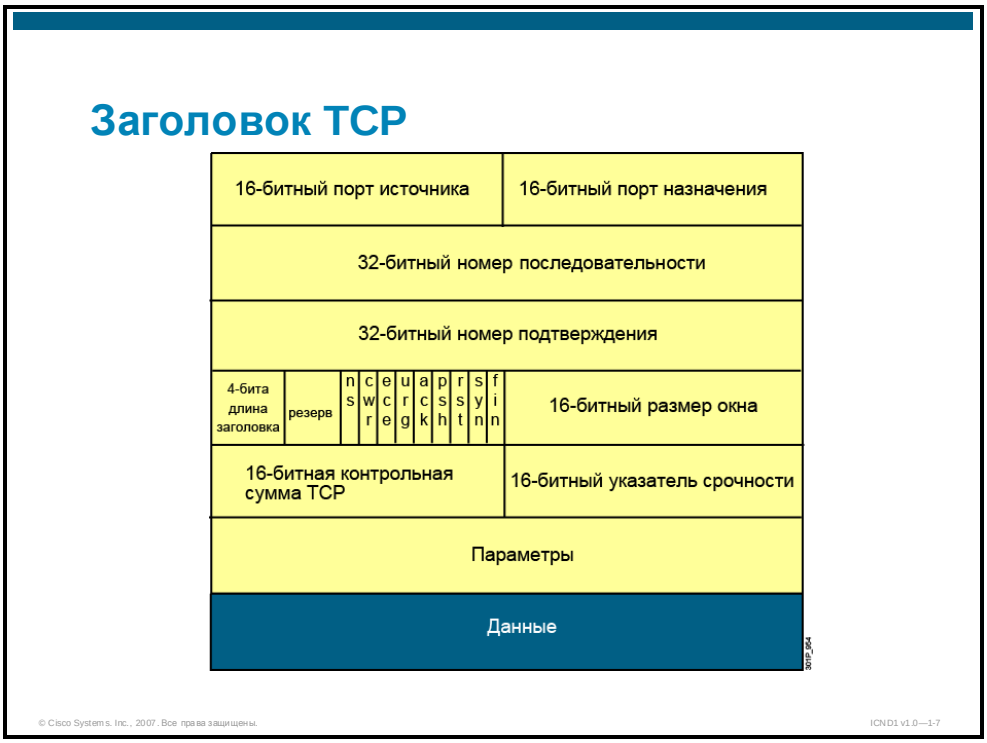
Услуги надежной доставки информации имеют огромное значение для приложений, связанных с передачей файлов, службами баз данных, обработкой транзакций, и другими критически важными приложениями, требующими гарантированную доставку каждого пакета. Протокол TCP обеспечивает такую надежность, иногда в ущерб скорости, тогда как UDP предоставляет скорость в ущерб надежности.

Пример: отправка по почте с уведомлением о получении

Услуги протокола TCP можно сравнить с отправкой почтового сообщения с уведомлением о вручении. Предположим, что вам необходимо переслать книгу из Санкт-Петербурга вашей родственнице в Москву, но почта обрабатывает только письма. Вы вырываете страницы из книги и упаковываете их по нескольку штук в отдельные конверты. Чтобы быть уверенным, что книга будет собрана получателем правильно, каждый конверт нумеруется с указанием номера последней страницы в группе. Затем вы надписываете адрес на конвертах и отправляете первый из них как почтовое отправление с уведомлением о вручении. Почтовая служба доставляет первый конверт любым доступным ей способом и маршрутом. Но при доставке этого конверта перевозчик обязан получить у вашей родственницы расписку и вернуть вам уведомление о доставке. Отправка каждой группы страниц по отдельности весьма утомительна, поэтому вы отправляете несколько конвертов вместе. Почтовая служба опять доставляет каждый конверт любым доступным ей способом и маршрутом. Ваша родственница расписывается в отдельной квитанции за каждый конверт при получении. Если один конверт потеряется при пересылке, вы не получите уведомление о его доставке и вам придется повторно послать все страницы этой группы. После получения всех конвертов ваша родственница соберет страницы в нужном порядке и склеит книгу.

Заголовок TCP сегмента

Заголовок TCP содержит информацию TCP протокола. В этом разделе описываются поля заголовка TCP.

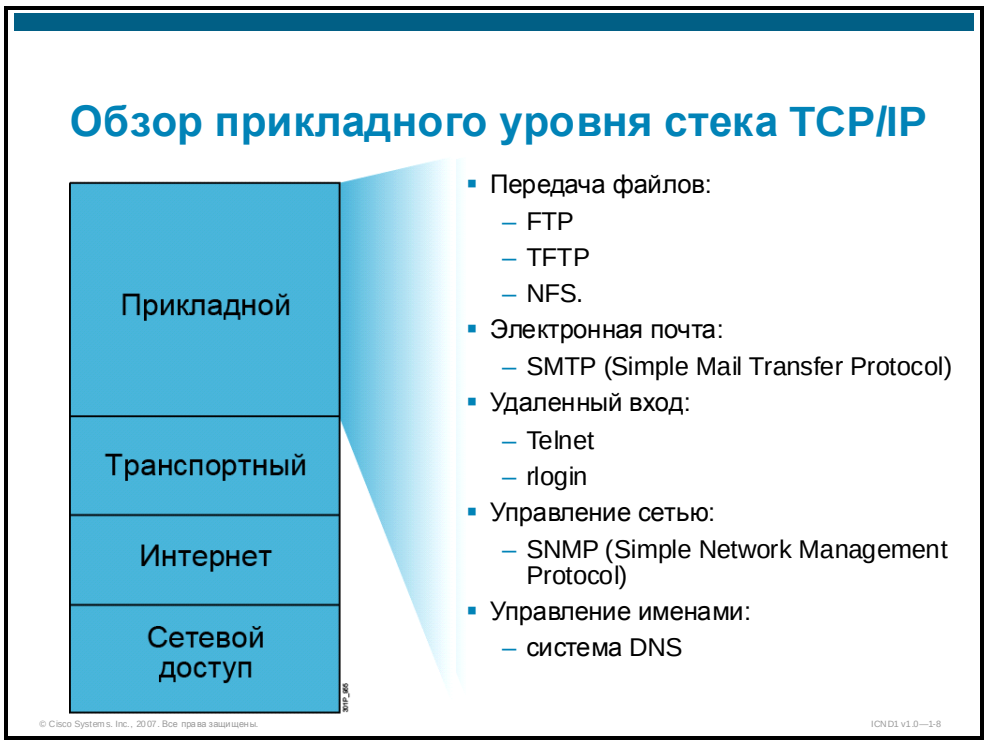


Для отправки сегментов TCP используются IP пакеты. Заголовок TCP располагается вслед за заголовком IP и содержит информацию, относящуюся к протоколу TCP. Такое разделение позволяет хосту обрабатывать и другие протоколы, отличные от TCP. Заголовок TCP содержит следующие поля:

- **Source port (Порт источника).** Номер порта источника (16 битов).
- **Destination port (Порт назначения).** Номер порта назначения (16 битов).
- **Sequence number (Номер последовательноти).** Номер последовательноти первого байта в сегменте, обеспечивает правильную последовательность поступающих данных (32 бита).
- **Acknowledgment number (Номер подтверждения).** Следующий ожидаемый байт по протоколу TCP (32 бита)
- **Header length (Длина заголовка).** Количество 32-битных слов в заголовке (4 бита).
- **Reserved (Резервное поле).** Имеет значение 0 (3 бита).
- **Control bits (Биты управления).** Управляют функциями настройки, контролем перегрузки в сети и прекращением сеанса (9 битов). (Отдельный бит, имеющий определенное назначение, часто называется флагом.)
- **Window (Окно).** Число байтов данных, которые устройство ожидает принять (16 битов).
- **Checksum (Контрольная сумма).** Рассчитанная контрольная сумма заголовка и данных (16 битов).
- **Urgent (Срочность).** Это поле указывает на конец срочных данных (16 битов).
- **Options (Параметры).** В настоящее время определен один параметр – максимальный размер сегмента TCP (0 или 32 бита, при наличии)
- **Data (Данные).** Данные протокола верхнего уровня (размер нефиксирован).

Приложения TCP/IP

Кроме протоколов IP, TCP и UDP стек протоколов TCP/IP включает приложения, поддерживающие услуги передачи файлов, электронной почты и удаленного доступа к системе. В этом разделе рассматриваются три основных приложения стека протоколов TCP/IP.

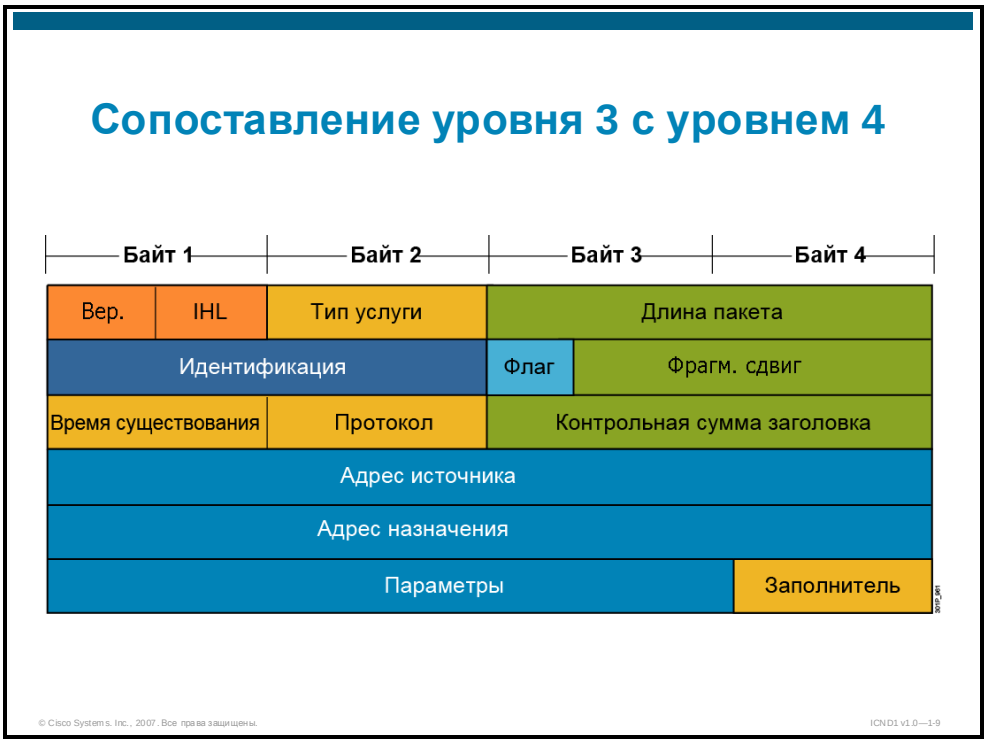


Стек протоколов TCP/IP поддерживает следующие приложения.

- **Протокол FTP (File Transfer Protoco).** Протокол FTP предоставляет надежную службу с установлением соединения, использующую протокол TCP для передачи файлов между системами, которые поддерживают FTP. FTP поддерживает двунаправленную передачу двоичных файлов и файлов ASCII.
- **Протокол TFTP (Trivial File Transfer Protocol).** Протокол TFTP предоставляет службу без установления соединения, использующую протокол UDP. Протокол TFTP используется маршрутизаторами для передачи файлов конфигураций и ПО Cisco IOS, а также для передачу файлов между системами, которые поддерживают TFTP.
- **Telnet.** Telnet обеспечивает удаленный доступ к другому компьютеру. Telnet позволяет пользователю входить в удаленную систему и выполнять команды.

Сопоставление уровня 3 с уровнем 4

Протокол IP передает данные в виде пакетов, также известных как датаграммы. В этом разделе рассматривается сопоставление уровня 3 с уровнем 4 стека протоколов.



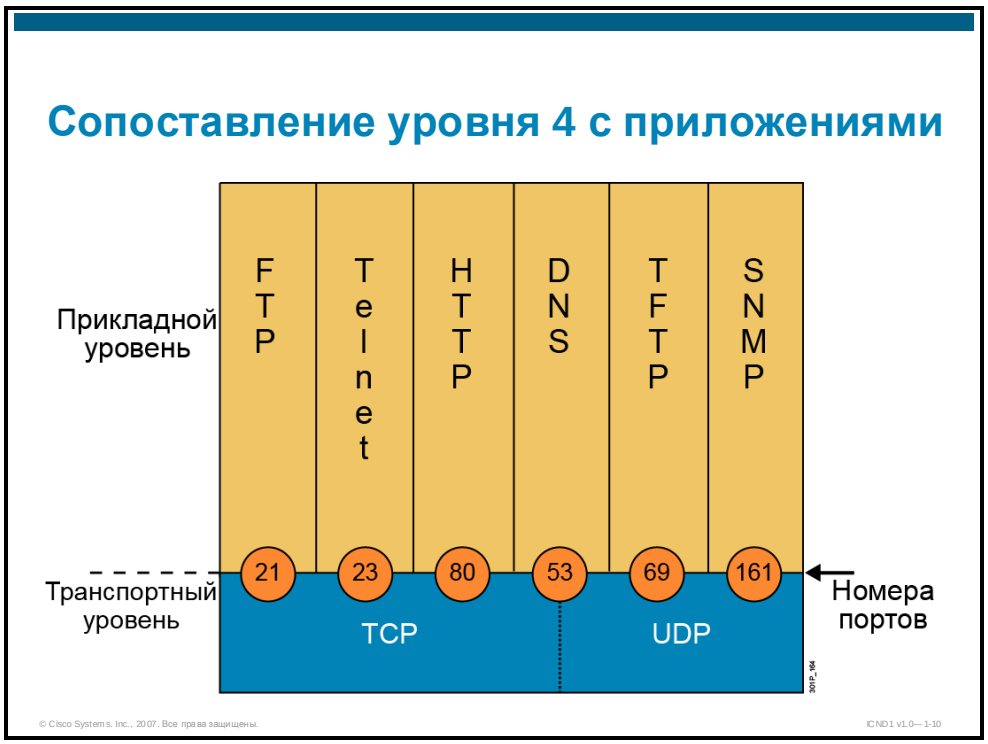
В этом разделе рассматривается поле протокола, одно из полей заголовка IP-пакета. Протокол IP использует номер протокола в заголовке датаграммы для определения протокола верхнего уровня, которому будут переданы данные, причем каждый протокол имеет свой номер. В этом разделе описывается структура поля протокола.

Хост или маршрутизатор считывает номер из заголовка датаграммы, сравнивает его с записями в таблице транспортных протоколов и передает данные датаграммы соответствующему протоколу. Например, если протокол имеет номер 6, IP передает данные протоколу TCP. Если протокол имеет номер 17, IP передает данные протоколу UDP.

Хотя большая часть трафика использует протоколы TCP или UDP, применяющие протокол IP в качестве транспорта, существуют и другие протоколы, которые могут использовать напрямую протокол IP для транспорта. Около 100 различных протоколов транспортного уровня имеют зарегистрированные номера протоколов, которые позволяют им использовать протокол IP для транспорта.

Сопоставление уровня 4 с приложениями

Для поддержки одновременного обмена данными между различными сетевыми устройствами протоколы UDP и TCP используют внутренние программные порты. В этом разделе описываются различные номера портов, используемые протоколами UDP и TCP.



На одном устройстве может выполняться одновременно несколько сеансов связи с одним или несколькими компьютерами. Каждый сеанс должен отличаться от других, что достигается с помощью номеров портов. Все эти сеансы мультиплексируется через один сетевой интерфейс и канал передачи. Сегменты этих сеансов чередуются при передаче через сетевой интерфейс. Порт можно рассматривать как очередь сообщений, через которую проходят сегменты конкретного сеанса связи.

Номера портов контролируются организацией Internet Assigned Numbers Authority (IANA). Некоторым часто используемым приложениям назначены постоянные номера портов. Эти номера портов иногда называют «хорошо известными». Например, Telnet всегда использует порт 23. Другие приложения могут использовать динамические номера портов, но они должны принадлежать соответствующему диапазону.

Кроме того, хорошо известные или зарегистрированные номера портов позволяют конечным системам выбирать нужное приложение-получатель. Хост-отправитель, который создает сеанс верхнего уровня, при использовании транспортного протокола динамически назначает порты из диапазона 49152–65535.

Приложения протокола UDP

Среди прочих, протокол UDP используется следующими приложениями.

- **Протокол TFTP (Trivial File Transfer Protocol).** TFTP является простейшим протоколом передачи файлов. Чаще всего он используется для копирования и установки операционной системы компьютера из файлов, расположенных на TFTP-сервере. Приложение TFTP меньше, чем FTP, и обычно применяется в сетях для простой передачи файлов. В приложении TFTP предусмотрена собственная проверка ошибок и нумерация, поэтому ему не требуются эти функции на транспортном уровне.
- **Протокол SNMP (Simple Network Management Protocol).** Протокол SNMP служит для мониторинга сетей, подключенных к ним устройств и данных о производительности сети, а также для управления этими устройствами. SNMP отправляет сообщения единицы информации протокола (PDU – Protocol Data Unit), позволяющие программному обеспечению контролировать устройства в сети.

Приложения протокола TCP

Среди прочих, протокол TCP поддерживается следующими приложениями.

- **FTP.** FTP является полнофункциональным приложением для копирования файлов. На компьютере запускается клиентское приложение, которое обращается к серверному приложению FTP на удаленном компьютере. С помощью этого приложения выполняется выгрузка и загрузка файлов.
- **Telnet.** Telnet обеспечивает эмуляцию терминала на удаленном устройстве, например хосте UNIX, маршрутизаторе или коммутаторе. Эмуляция терминала позволяет управлять сетевым устройством так же, как при непосредственном подключении через последовательный интерфейс. Telnet применяется только для систем, использующих синтаксис команд в символьном режиме. Telnet не поддерживает среды графичесих пользовательских интерфейсов (GUI). Поскольку приложение Telnet посылает свои сообщения в виде незашифрованного открытого текста, большинство организаций в настоящее время пользуется протоколом SSH для удаленной связи.

На рисунке показаны некоторые номера портов для каждого протокола и соответствующие им приложения.

Хорошо известные порты

Хорошо известные порты назначаются организацией IANA и имеют значения от 0 до 1023. Эти номера присваиваются основным приложениям Интернета.

Зарегистрированные порты

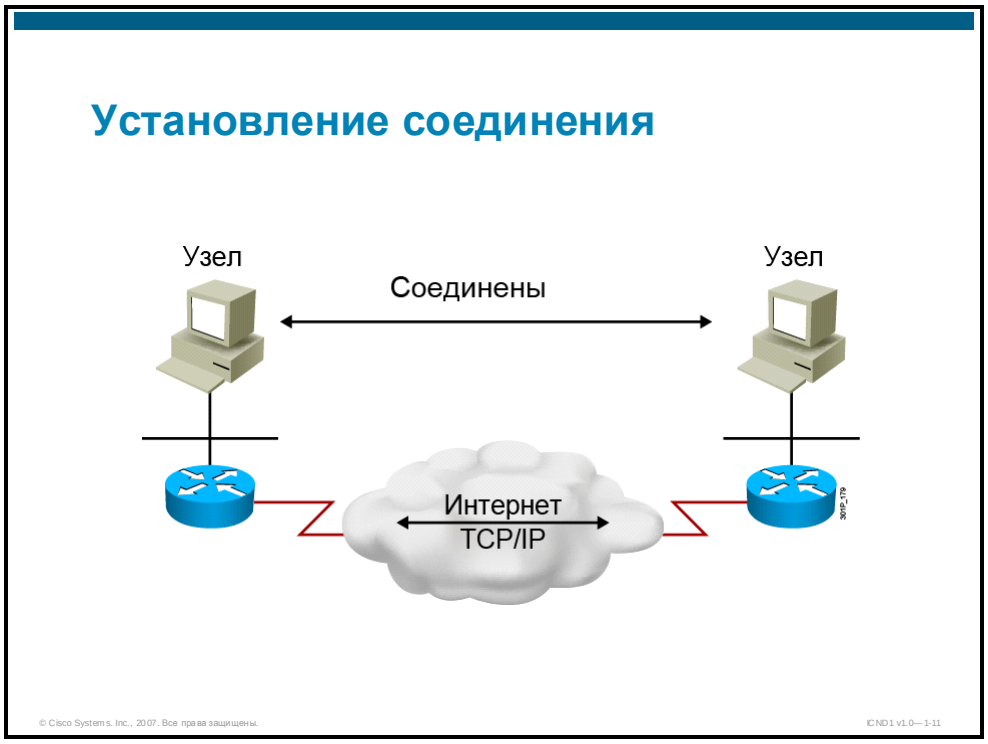
Номера с 1024 до 49151 представляют зарегистрированный диапазон портов, также контролируемый IANA. Эти порты используются для проприетарных приложений, например Lotus Mail.

Динамические порты

Динамические порты представляют собой номера из диапазона от 49152 до 65535. Эти порты динамически выделяются на время конкретного сеанса.

Установление соединения с удаленной системой

Пользователь услуги транспортного уровня с надежной доставкой должен организовать сеанс с установлением соединения с удаленной системой. В этом разделе обсуждается основной принцип сеанса с установлением соединения.

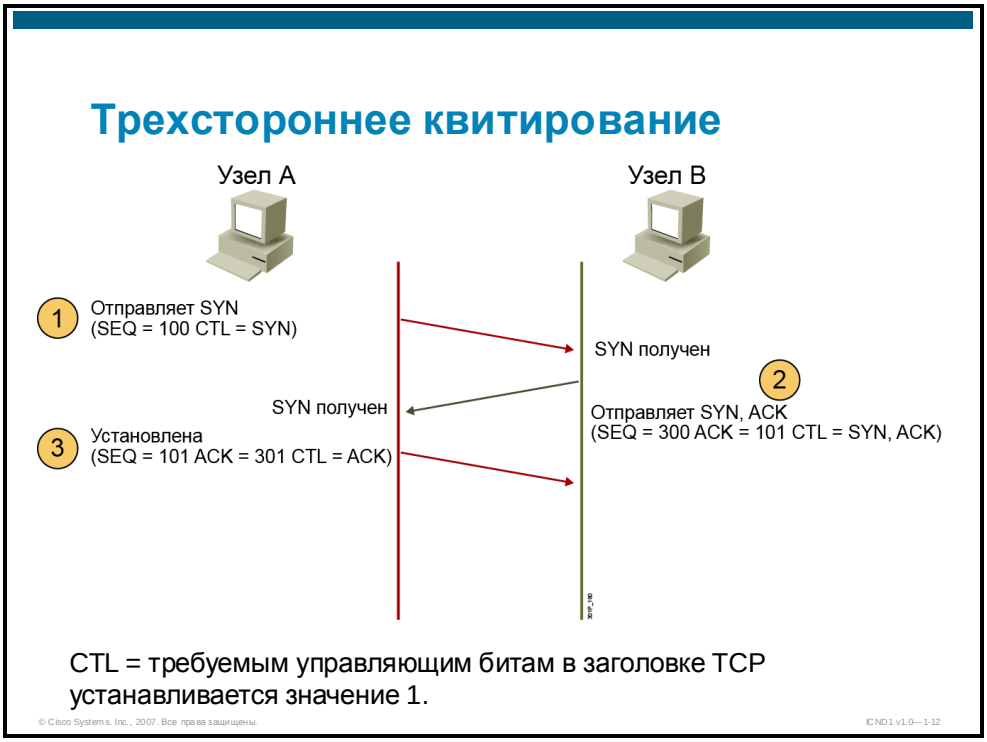


Чтобы начать передачу данных, передающее и получающее приложения информируют свои операционные системы о том, что соединение будет инициировано. Одна из машин инициирует соединение, которое должно быть принято другой. Программные модули двух операционных систем, реализующие функции сетевых протоколов взаимодействуют между собой, обмениваясь сообщениями по сети, которые позволяют удостовериться, что передача разрешена и обе стороны готовы для выполнения нужных функций.

После успешной синхронизации между двумя конечными системами устанавливается соединение, и передача данных может быть начата. Во время передачи обе машины проверяют корректность соединения.

Трехстороннее квитирование

Протокол TCP перед началом передачи данных требует установить соединение между двумя конечными системами.



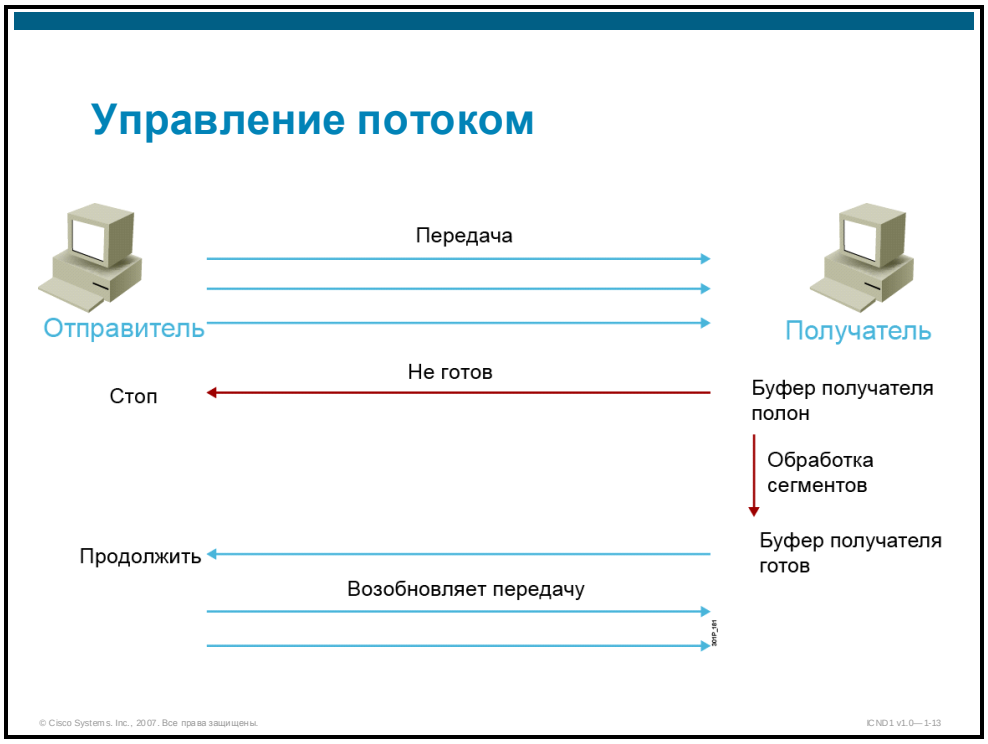
Протокол TCP устанавливает соединение с помощью процесса, известного под названием «трехстороннее квитирование». Этот процесс предусматривает установку в сегментах бита синхронизации (SYN) и бита подтверждения (ACK) в процессе обмена сообщениями между двумя устройствами. Другой важной функцией, выполняемой при установлении соединения, является уведомление первым устройством второму начального номера последовательности (ISN – Initial Sequence Number), который позволяет отслеживать байты данных в этом соединении. Таблица содержит упрощенное разъяснение процесса трехстороннего квитирования.

Процедура установления соединения TCP

№	Действие	Примечания
1.	**Устройство, запрашивающее соединение, посылает получающему устройству сегмент синхронизации (устанавливает бит SYN), начиная процесс квитирования.**	**Сегмент синхронизации указывает номер порта, к которому хочет подключиться отправитель. Сегмент синхронизации содержит также значение ISN, используемое в процессе подтверждения.**
2.	**Получающее устройство посылает в ответ сегмент с набором битов SYN и ACK, чтобы согласовать соединение и подтвердить получение сегмента синхронизации от отправителя.**	**Получающее устройство посылает в ответ номер последовательности следующего байта данных, который оно ожидает от отправителя. Следующий номер последовательности равен ISN плюс 1.**
3.	**Инициирующее устройство подтверждает сегмент синхронизации получателя.**	**Бит SYN в заголовке TCP сбрасывается, подтверждая завершение трехстороннего квитирования.**

Управление потоком

Управление потоком позволяет предотвратить проблему переполнения отправителем буферов получателя. В этом разделе рассматривается управление потоком.



При передаче данных может возникнуть перегрузка среды. Компьютер-отправитель может оказаться высокоскоростным устройством, генерирующим трафик быстрее, чем сеть может передать его. Кроме того, если несколько компьютеров одновременно отправляют датаграммы одному получателю, на конечном устройстве может возникнуть перегрузка при их получении. Если датаграммы прибывают настолько быстро, что получающее устройство не успевает их обрабатывать, они будут временно сохранены в памяти. Эта область в памяти (буфер) не безгранична, поэтому, если датаграммы продолжают поступать, а память переполнена, датаграммы будут отброшены.

Поскольку потеря данных недопустима, управление потоком является обязательной функцией системы. Транспортная функция может организовать передачу отправителю индикатора «не готов». Этот индикатор фактически означает, что компьютер-получатель сообщает о новом размере окна, равном 0. Индикатор неготовности дает отправителю сигнал прекратить отправку данных и ожидать индикатора «готов». После обработки компьютером-получателем достаточного количества датаграмм для освобождения пространства, транспортная функция посылает отправителю индикатор «готов». Получив этот индикатор, отправитель возобновляет отправку датаграмм.

Подтверждение

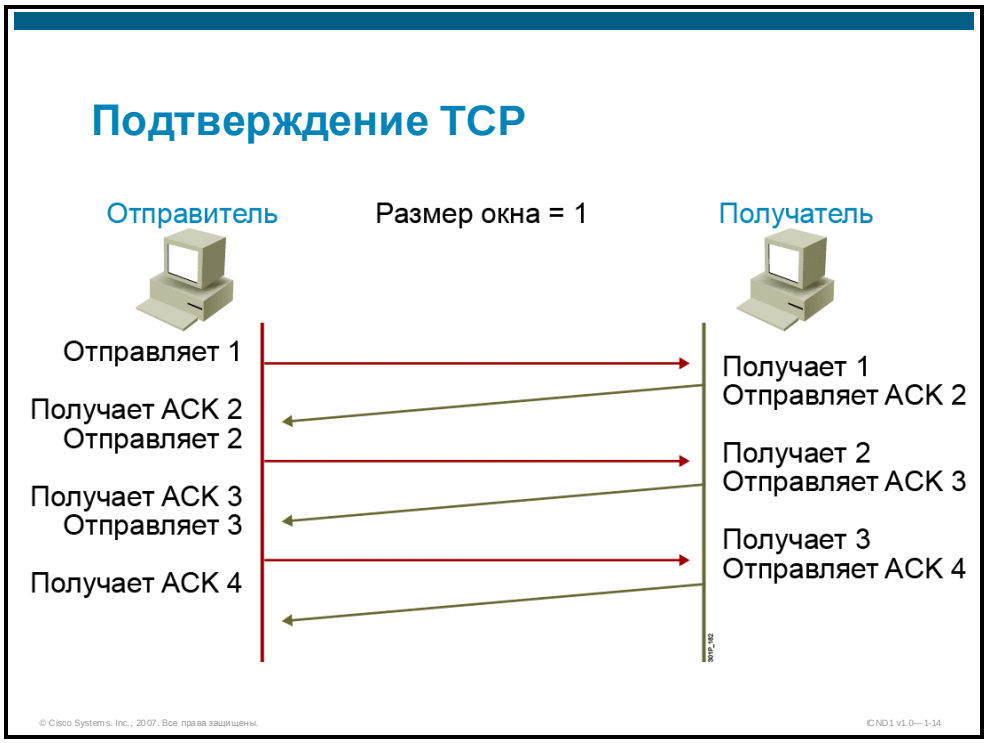
Соединение TCP является надежным, поэтому отправляющий и получающий компьютеры используют сигналы подтверждения, гарантирующие, что отправленные данные получены без ошибок и в правильном порядке.

Концепция размера окна

Размер окна позволяет компьютеру-отправителю посылать группу пакетов без получения подтверждения для каждого пакета. Это помогает поддерживать скорость и надежность соединения.

Подтверждение TCP

Протокол TCP выполняет последовательную нумерацию сегментов и предоставление прямых подтверждений. Прямое подтверждение приходит с принимающего устройства и сообщает отправителю, какой сегмент должен быть передан следующим. В этом разделе описывается получение подтверджений сегментов по протоколу TCP.



Для большей понятности, мы упростили описание работы протокола TCP. В качестве номеров последовательности и номеров подтверждения используются просто возрастающие номера, хотя в реальности номера последовательности отражают число полученных байт. При простом подтверждении TCP компьютер-отправитель передает сегмент, запускает таймер и ожидает подтверждения до передачи следующего сегмента. Если таймер истекает до подтверждения получения сегмента, компьютер-отправитель повторно передает сегмент и снова запускает таймер.

Предположим, что каждый сегмент нумеруется перед передачей (следует помнить, что на самом деле отслеживается число передаваемых байт). На получающей станции TCP собирает сегменты в полное сообщение. Если в серии отсутствует какой-то номер последовательности, этот сегмент и все последующие сегменты могут быть отправлены повторно.

Процесс подтверждения

№	Действие	Примечания
1.	Отправитель и получатель договариваются, что перед отправкой следующего сегмента требуется подтверждение предыдущего.	Это происходит во время процедуры установления соединения путем установки для размера окна 1.
2.	Отправитель передает получателю сегмент 1.	Отправитель запускает таймер и ожидает подтверждения от получателя.
3.	Получатель принимает сегмент 1 и возвращает ACK = 2.	Получатель подтверждает успешное получение предыдущего сегмента, заявляя ожидаемый номер следующего сегмента.
4.	Отправитель получает ACK = 2 и передает получателю сегмент 2.	Отправитель запускает таймер и ожидает подтверждения от получателя.
5.	Получатель принимает сегмент 2 и возвращает ACK = 3.	Получатель подтверждает успешное получение предыдущего сегмента.
6.	Отправитель получает ACK = 3 и передает получателю сегмент 3.	Этот процесс продолжается, пока не будут отосланы все данные.

Концепция размера окна

Окно TCP позволяет поддерживать скорость передачи на уровне, который не вызовет перегрузку и потерю данных. В этом разделе описан процесс передачи с использованием механизма размера окна.

Фиксированный размер окна

Большинство форм надежной передачи данных с установлением соединения не учитывают перегрузку сети, они предусматривают подтверждение получателем приема каждого сегмента данных, для гарантии целостности передачи. Однако если отправитель должен ожидать подтверждения после отправки каждого сегмента, скорость пересылки окажется низкой и будет зависеть от времени прохождения сегмента (RTT – Round-Trip Time) между отправкой данных и получением подтверждения.

Большинство надежных протоколов с установлением соединения допускают ожидание подтверждения доставки сразу нескольких сегментов. Это возможно, поскольку между передачей сегмента отправителем и обработкой им подтверждения получения проходит определенный промежуток времени. В течение этого интервала отправитель может передать дополнительные данные, при условии, что размер окна получателя достаточно велик для обработки сразу нескольких сегментов. Окно представляет собой число сегментов данных, разрешенное для передачи отправителем без получения подтверждения от получателя (см. рисунок).

Концепция размера окна позволяет посылать получателю определенное число сегментов, сокращая тем самым время ожидания. Время ожидания в этом случае относится к суммарному времени, необходимому на отправку данных и получение подтверждения.

Пример: бросок мяча

Представьте себе двух человек, стоящих на расстоянии 15 метров друг от друга. Один из них бросает другому футбольный мяч, который преодолевает это расстояние за 3 секунды. Второй принимает мяч и бросает его обратно, что также занимает три 3 секунды. Путь мяча туда и обратно занимает 6 секунд. Трехкратное повторение этого процесса займет 18 секунд. А теперь представим, что у первого игрока есть три мяча и он бросает их один за другим. Эта часть пути по прежнему преодолевается мячом за три секунды. Второй игрок бросает обратно один мяч, чтобы подтвердить получение третьего мяча, что также занимает три 3 секунды. Путь мяча туда и обратно занимает в итоге 6 секунд. (Разумеется, здесь не учитывается время на обработку и т. п.)

Эта процедура объясняет процесс использования окна в подключении по протоколу TCP.

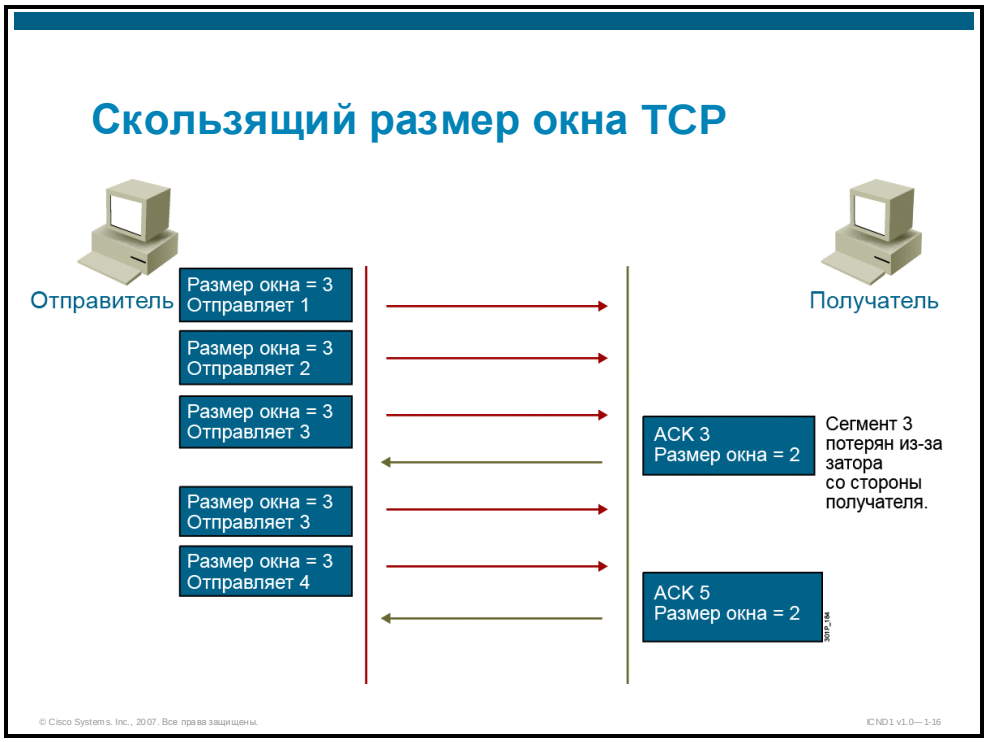
Простая процедура, размер окна = 3

№	Действие	Примечания
1.	Перед отправкой подтверждения отправитель и получатель обмениваются информацией о начальном размере окна, равном трем сегментам.	Это происходит во время процедуры установления соединения.
2.	Отправитель передает получателю сегменты 1, 2 и 3.	Отправитель передает сегменты, запускает таймер и ожидает подтверждения от получателя.
3.	Получатель принимает сегмент 1, 2 и 3 и возвращает ACK = 4.	Получатель подтверждает успешное получение предыдущих сегментов.
4.	Отправитель получает ACK = 4 и передает получателю сегмент 4, 5 и 6.	Отправитель передает сегменты, запускает таймер и ожидает подтверждения от получателя.
5.	Получатель принимает сегмент 4, 5 и 6 и возвращает ACK = 7.	Получатель подтверждает успешное получение предыдущих сегментов.

В данном примере для лучшего понимания использована упрощенная нумерация сегментов. На самом деле эти номера представляют октеты (байты) и их приращение имеет гораздо большее значение, содержащееся в сегментах TCP, а не сами сегменты.

Скользящий размер окна в протоколе TCP

В протоколе TCP для определения числа сегментов используется принцип скользящего окна, начинающийся с номера подтверждения, с которым получатель может согласиться. В этом разделе рассматривается механизм скользящего окна TCP.



В механизме фиксированного окна заданный размер окна не меняется. В механизме скользящего окна размер окна устанавливается в начале соединения в результате согласования и может динамически меняться в течение сеанса TCP. Скользящее окно обеспечивает более эффективное использование полосы пропускания, поскольку больший размер окна позволяет передавать большее количество данных с отсрочкой подтверждения. Кроме того, если получатель уменьшает заявленный размер окна до 0, это фактически прекращает дальнейшую передачу данных, пока не будет отправлено новое, более высокое значение окна.

На рисунке размер окна равен 3. Отправитель может передать получателю три сегмента. Затем он должен ждать подтверждения от получателя. После того как получатель подтверждает получение трех сегментов, отправитель может передать еще три сегмента. Однако если на стороне получателя возникает нехватка ресурсов, он может уменьшить размер окна, чтобы избежать переполнения и отбрасывания сегментов данных.

Каждое подтверждение, переданное получателем, содержит объявление о размере окна с указанием числа байтов, которые может принять получатель. Это позволяет увеличивать или уменьшать размер окна по мере необходимости для управления размером буфера и обработки.

Протокол TCP поддерживает отдельный параметр размера окна перегрузки (CWS – Congestion Window Size), который обычно совпадает с размером

окна получателя, но уменьшается наполовину при потере сегментов. Потеря сегмента воспринимается как перегрузка сети. Протокол TCP вызывает сложные алгоритмы отката и перезапуска, поэтому он не приводит к перегрузке сети.

Принцип работы скользящего окна

№	Действие	Примечания
1.	Отправитель и получатель обмениваются исходными значениями окон. В данном примере размер окна равен 3 сегментам до обязательного получения подтверждения.	Это происходит во время процедуры установления соединения.
2.	Отправитель передает получателю сегменты 1, 2 и 3.	После передачи сегмента 3 отправитель будет ожидать подтверждения от получателя.
3.	Получатель принимает сегменты 1 и 2, но может теперь обработать только размер окна, равный 2. ACK = 3 WS = 2	Скорость обработки сегментов на получателе может снизиться по ряду причин, например, из-за того, что ЦП занят поиском по базе данных или загрузкой большого графического файла.
4.	Отправитель передает сегменты 3 и 4.	После передачи сегмента 5 отправитель будет ожидать подтверждения от получателя, поскольку у него осталось два неподтвержденных сегмента.
5.	Получатель подтверждает получение сегментов 3 и 4, но по-прежнему поддерживает размер окна, равный 2. ACK = 5 WS = 2	Получатель подтверждает успешное получение сегментов 3 и 4, запрашивая передачу сегмента 5.

Увеличение пропускной способности

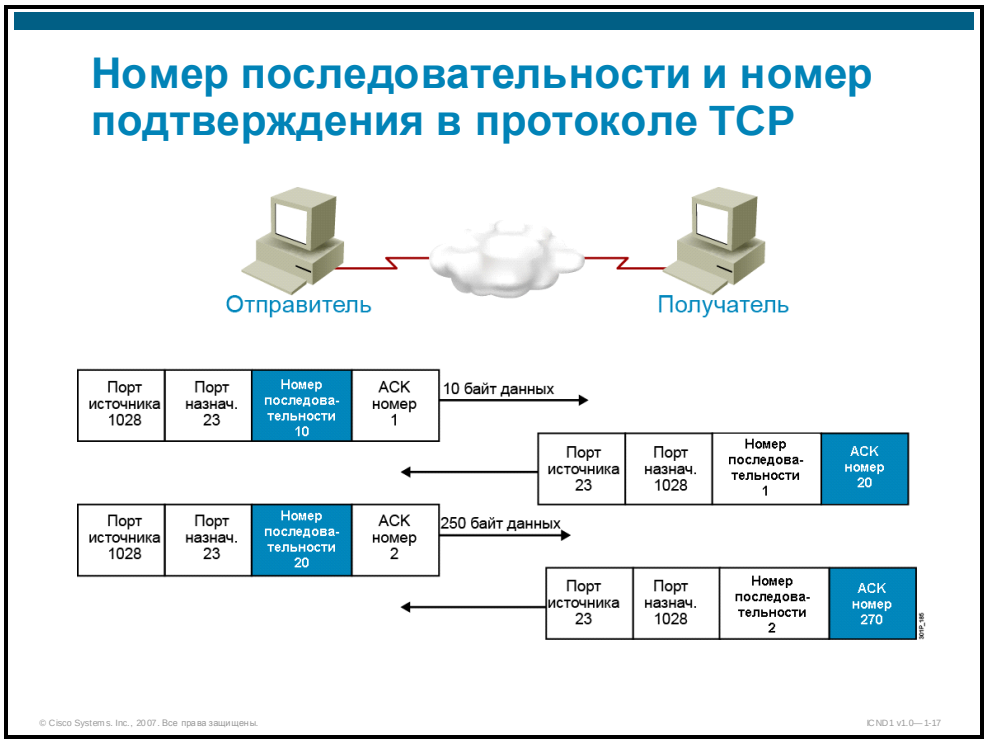
Алгоритм размера окна перегрузки управляет скоростью передачи данных. Он позволяет свести к минимуму отбрасывание данных и время их восстановления, следовательно, повышает эффективность.

Глобальная синхронизация

Хотя алгоритм размера окна перегрузки, в общем, повышает эффективность передачи данных, он может также оказать на нее крайне негативное влияние, вызывая глобальную синхронизацию процесса TCP. Глобальная синхронизация означает, что все отправители используют одинаковый алгоритм и их работа синхронизирована. Все отправители одновременно испытывают одинаковую перегрузку и снижение скорости. Затем, поскольку все отправители используют один и тот же алгоритм, они одновременно наращивают скорость передачи, создавая волны перегрузки.

Номер последовательности и номер подтверждения в протоколе TCP

TCP упорядочивает сегменты, используя номера последовательности и номера подтверждений в заголовках TCP. В этом разделе рассматриваются номера последовательности и номера подтверждений в протоколе TCP.



Каждый сегмент содержит порт отправителя (порт источника), порт получателя (порт назначения), номер последовательности и номер подтверждения. Номера портов устанавливаются во время начального этапа соединения TCP и остаются постоянными на протяжении этого соединения. Отправитель генерирует номера последовательности перед передачей сегментов. Каждый сегмент передается с прямым номером подтверждения ACK. Протокол TCP восстанавливает правильный порядок сегментов на конечном устройстве-получателе. Следует отметить, что на рисунке показаны более реалистичные последовательные номера, отражающие байты данных, передаваемые в каждом сегменте.

Резюме

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

Резюме

- Транспортный уровень скрывает требования сети от прикладного уровня.
- Протокол с установлением соединения обеспечивает надежную доставку данных; протокол без установления соединения осуществляет негарантированную доставку.
- Протокол UDP функционирует на транспортном уровне и обеспечивает приложениям доступ к сетевому уровню без дополнительных затрат на механизмы надежной доставки, как это делает TCP. UDP является протоколом без установления соединения, осуществляющим негарантированную доставку данных.
- Протокол TCP функционирует на транспортном уровне и обеспечивает приложениям доступ к сетевому уровню. TCP является протоколом с установлением соединения, обеспечивает контроль ошибок и гарантированную доставку данных, функционирует в дуплексном режиме и обеспечивает некоторые функции восстановления данных.

Резюме (прод.)

- Протокол TCP/IP поддерживает ряд приложений, включая FTP (выполняет двунаправленную передачу двоичных и ASCII-файлов), TFTP (передача файлов конфигураций и образов Cisco IOS) и Telnet (обеспечивает удаленный доступ к другому компьютеру).
- Протокол IP использует номер протокола в заголовке датаграммы, чтобы определить, какой протокол вышестоящего уровня следует использовать для данной датаграммы.
- Номера портов служат для сопоставления уровня 4 с приложением.

Резюме (прод.)

- Управление потоком позволяет предотвратить проблему переполнения буферов на принимающем хосте и снижения производительности сети.
- Протокол TCP выполняет упорядочение сегментов с помощью механизма прямого подтверждения. После отправки сегмента подтверждается его получение, и только затем посылается следующий сегмент.

Резюме (прод.)

- Окно TCP позволяет поддерживать скорость передачи на уровне, который не вызовет перегрузку сети и потерю данных. Размер окна TCP позволяет посылать получателю заданное число сегментов без подтверждения доставки.
- Фиксированное окно — это окно постоянного размера, которое позволяет передать заданный поток сегментов.
- Скользящее окно TCP — это окно, размер которого может динамически изменяться в процессе передачи сегментов.
- TCP упорядочивает сегменты, используя номера последовательности и номера подтверждений в заголовках TCP.

Занятие 6

Изучение процесса доставки пакетов

Обзор

В предыдущих занятиях рассматривались элементы, управляющие обменом данными между хостами. Важно понимать, как эти элементы взаимодействуют между собой. В этом занятии дается графическое представление обмена данными между хостами.

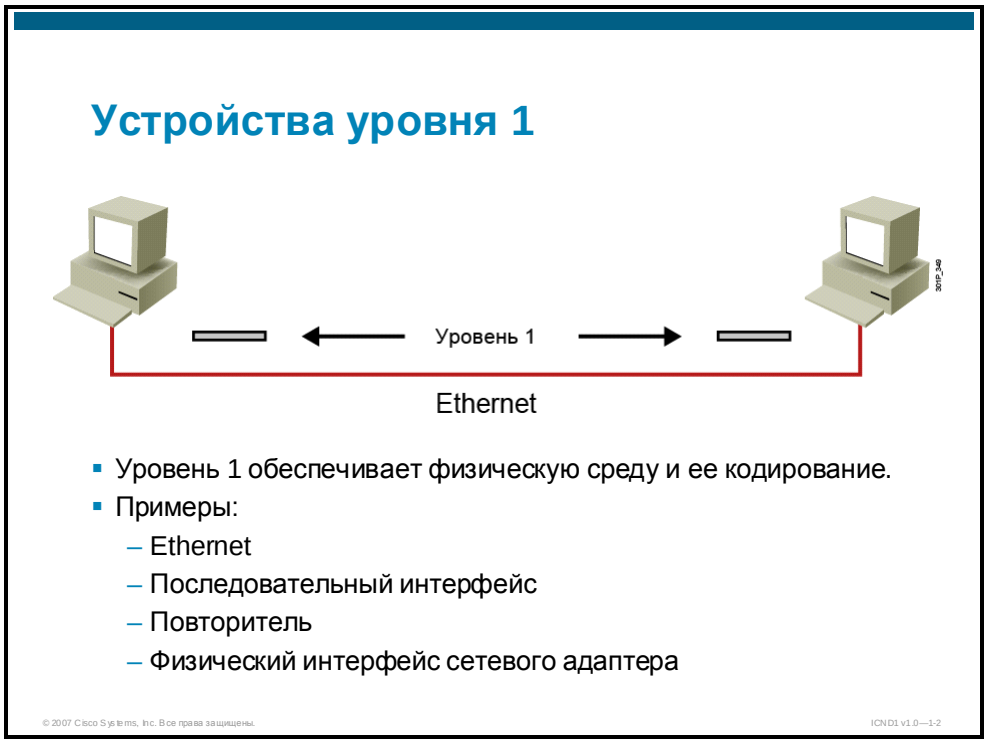
Задачи

По окончании этого занятия вы сможете описывать создание и поддержку обмена данными между хостами. Это значит, что вы сможете выполнить следующие задачи:

- описывать устройства уровня 1 и их функцию;
- описывать устройства уровня 2 и их функцию;
- описывать адресацию на уровне 2;
- описывать устройства уровня 3 и их функцию;
- описывать адресацию на уровне 3;
- описывать сопоставление адресации уровня 2 и уровня 3;
- описывать таблицу ARP;
- описывать передачу пакетов данных между хостами;
- описывать работу шлюза по умолчанию;
- использовать стандартные средства хоста для определения пути между двумя хостами в сети.

Устройства уровня 1 и их функция

В этом разделе описываются устройства уровня 1 и их функция.



На уровне 1 определены электрические, механические, процедурные и функциональные характеристики активации, поддержания и отключения физического канала между конечными системами. Распространенными примерами могут служить сегменты Ethernet и последовательные каналы, подобные Frame Relay и T1. К устройствам уровня 1 также относятся повторители, которые обеспечивают усиление сигнала.

Компонентом уровня 1 можно считать и физический интерфейс сетевого адаптера (NIC – Network Interface Card).

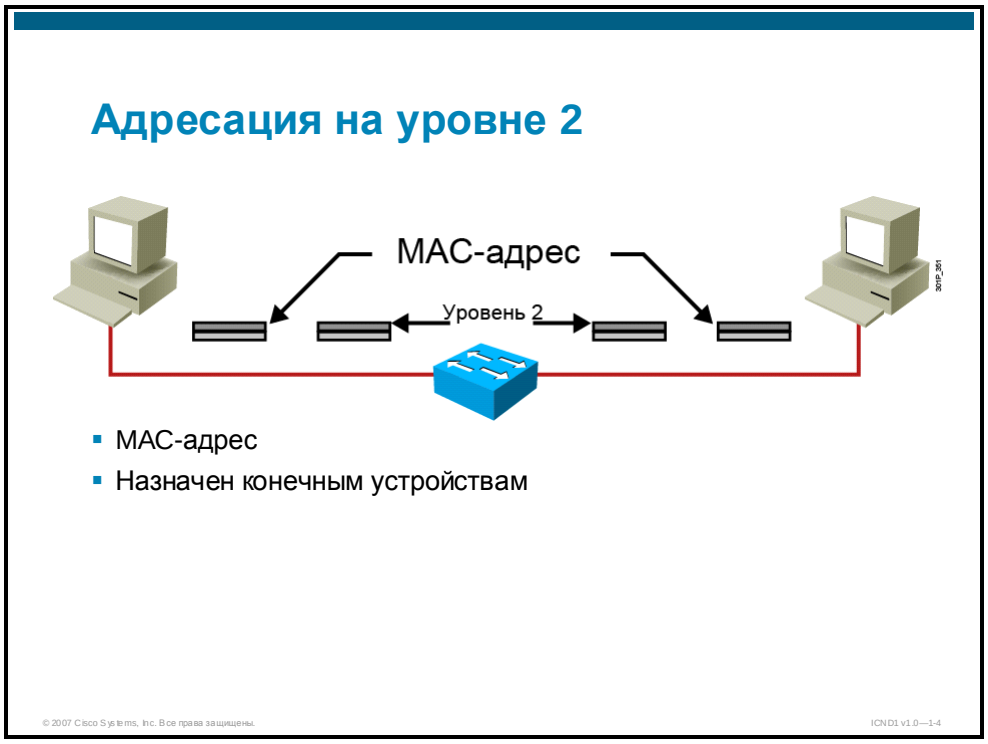
Устройства уровня 2 и их функция

В этом разделе описываются устройства уровня 2 и их функция.

На уровне 2 определяется формат данных для передачи и методы контроля доступа к физическим средам. Кроме того, эти устройства обеспечивают интерфейс для связи с физическими средами. В качестве примера можно привести сетевой адаптер (NIC – Network Interface Card), установленный на хосте, мосте или коммутаторе.

Адресация на уровне 2

Для обмена данными между хостами требуется адрес 2-го уровня. В этом разделе рассматривается роль адреса 2-го уровня в модели обмена данными между хостами.

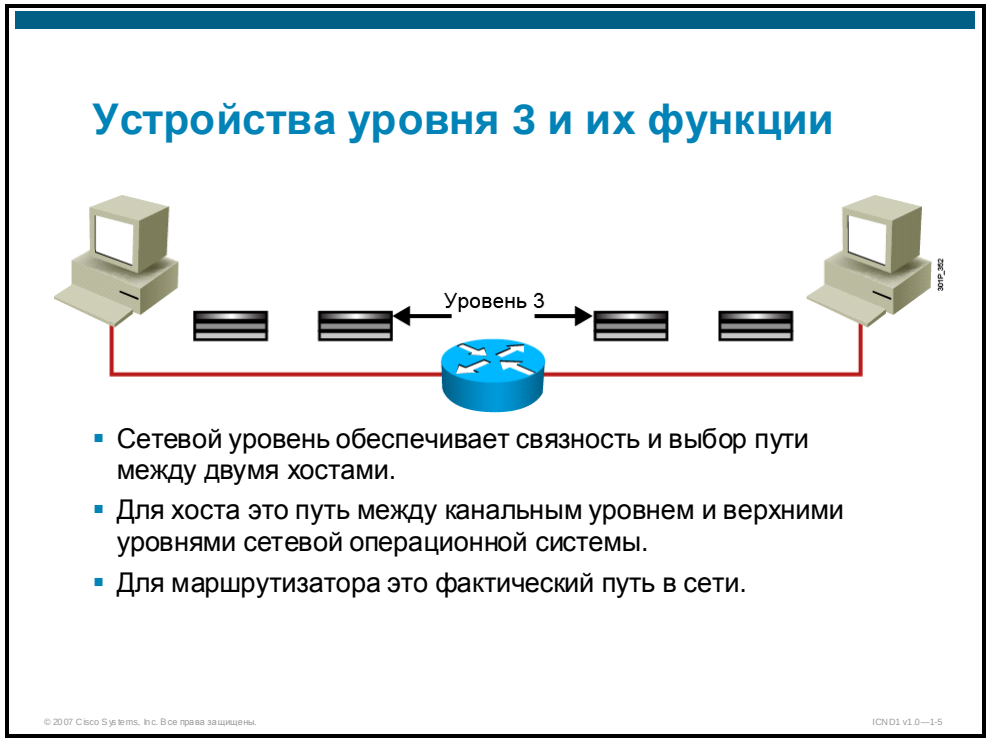


На начальных этапах развития обмена данными между хостами существовало несколько протоколов сетевого уровня, именуемых сетевыми операционными системами (NOS – Network Operating System). К первым сетевым операционным системам можно отнести Netware, IP, Open Systems Interconnection (OSI) и Banyan-Vines. Со временем стало очевидным, что существует необходимость в адресах уровня 2, независимых от NOS, что привело к созданию адреса Media Access Control (MAC).

MAC-адреса присваиваются таким конечным устройствам, как хосты. В большинстве случаев сетевым устройствам уровня 2, например мостам и коммутаторам, MAC-адреса не назначаются. Однако в некоторых особых случаях допускается назначение адреса коммутаторам. Эти случаи будут рассмотрены в данном курсе позднее.

Устройства уровня 3 и их функция

В этом разделе рассматривается роль устройств уровня 3 в модели обмена данными между хостами.



Сетевой уровень обеспечивает связность и выбор пути между двумя хостами, которые могут находиться в сетях, географически удаленных друг от друга. В случае хоста это путь между канальным уровнем и верхними уровнями NOS. Для маршрутизатора это фактический путь в сети.

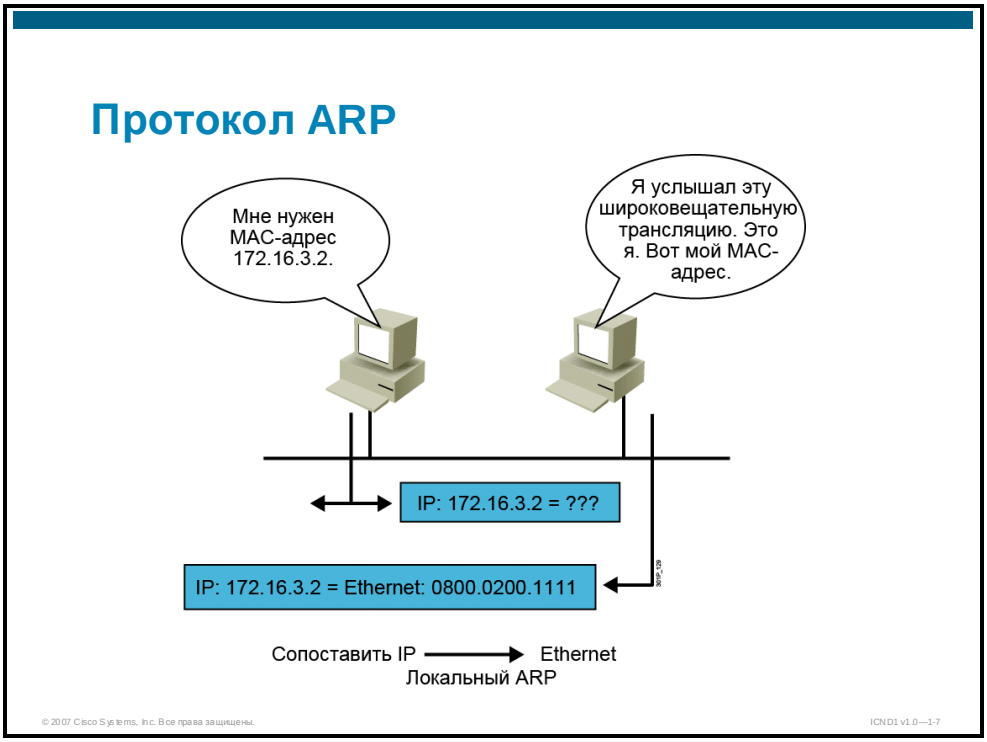
Адресация на уровне 3

В этом разделе рассматривается роль адресации уровня 3 в модели обмена данными между хостами.

Каждая сетевая операционная система имеет собственный формат адреса уровня 3. Например, в стеке протоколов модели OSI используется точка доступа к сетевому сервису (NSAP), а в стеке протоколов TCP/IP – IP-адрес. В этом курсе мы остановимся на стеке протоколов TCP/IP.

Сопоставление адресации уровня 2 и уровня 3

Для обмена данными протокола IP в сетях Ethernet логический (IP) адрес должен быть связан с физическим (MAC) адресом места назначения. Этот процесс реализуется с помощью протокола Address Resolution Protocol (ARP). В этом разделе описывается работа протокола ARP.



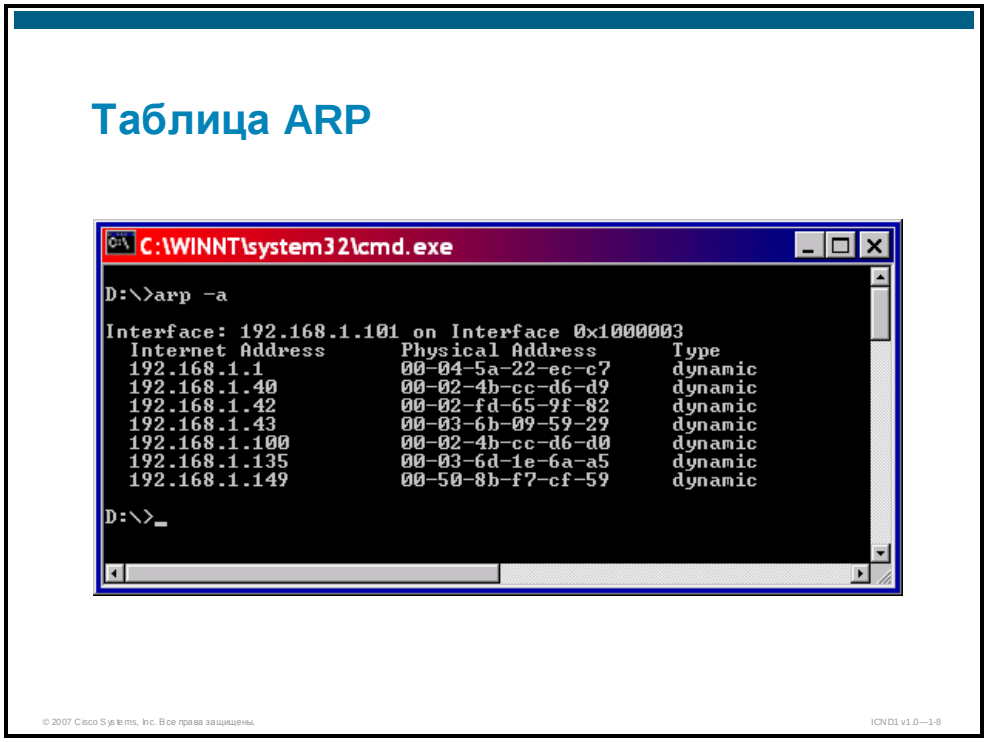
Для отправки данных получателю, хосту в сети Ethernet, необходимо знать его физический (MAC) адрес. Протокол ARP предоставляет важную услугу, заключающуюся в сопоставлении IP-адресов с физическими адресами в сети.

Термин «разрешение адреса» подразумевает связывание IP-адреса сетеого уровня удаленного хоста с его локально доступным MAC-адресом канального уровня. Адрес «разрешается» (или сопоставляется), когда протокол ARP выполняет широковещательную рассылку известной информации (IP-адрес места назначения и его собственный IP-адрес). Широковещательная рассылка принимается всеми устройствами сегмента сети Ethernet. Когда конечное устройство распознает себя, считывая содержимое пакета запроса ARP, оно посылает ARP ответ с запрашиваемым MAC-адресом. Процедура разрешения адреса завершается, когда источник получает от конечного устройства ответный пакет (с запрашиваемым MAC-адресом) и обновляет таблицу, которая содержит все текущие связи. (Как правило, эта таблица называется ARP или ARP-таблицей.) Таблица ARP позволяет поддерживать связь между всеми IP-адресами и соответствующими MAC-адресами.

Актуальность привязок в таблице поддерживается процессом устаревания записей при неактивности. Время устаревания по умолчанию обычно составляет 300 секунд (5 минут), что обеспечивает отсутствие в таблице информации, относящейся к отключенным или перемещенным системам.

Таблица ARP

В таблице или кэше ARP, хранятся последние записи привязки IP-адресов к MAC-адресам. В этом разделе описывается функция таблицы ARP.



Каждое IP-устройство в сегменте сети хранит в своей памяти таблицу или кэш ARP. В этой таблице IP-адреса других устройств сопоставляются с их физическими (MAC) адресами. Когда хосту требуется передать данные другому хосту в этой же сети, он ищет соответствующую запись в таблице ARP. Если такая запись присутствует, хост использует ее; если же нет, он получает нужную запись с помощью протокола ARP.

Таблица ARP создается и обновляется динамически, путем добавления и изменения отношений между адресами по мере их использования на локальном хосте. Срок действия записей в таблице ARP истекает спустя определенный период времени, по умолчанию через 300 секунд; однако при необходимости в повторной передаче данных с локального хоста запись в таблице ARP восстанавливается с помощью процесса ARP.

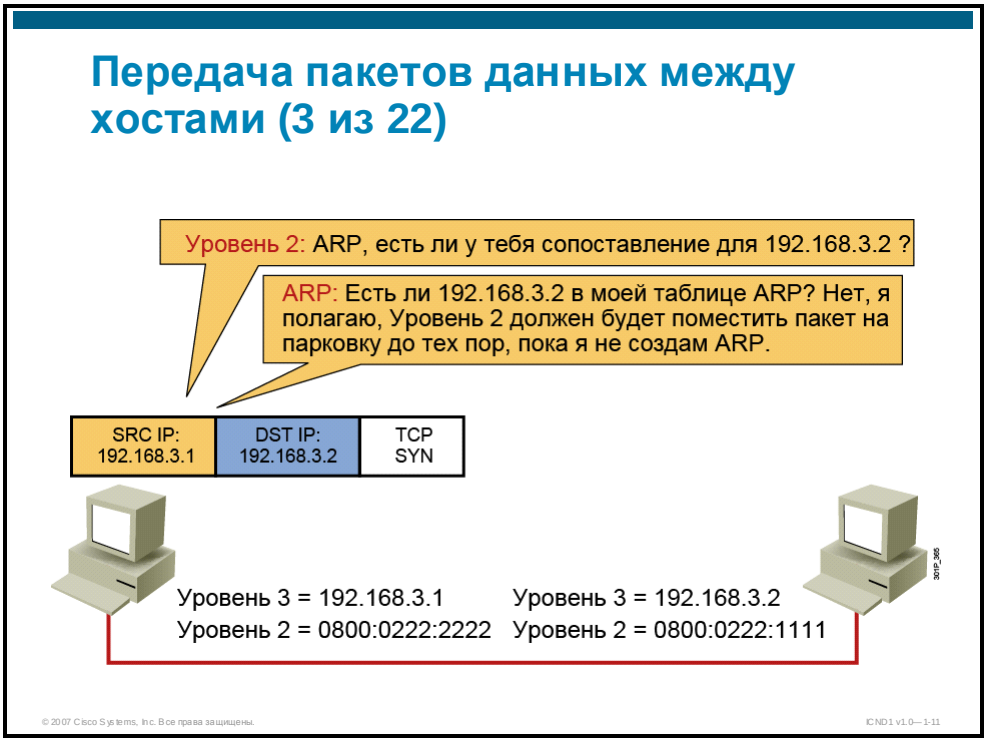
Передача пакетов данных между хостами

В этом разделе описывается обычный обмен данными между хостами.

В этом примере приложению, выполняемому на хосте с адресом 3-его уровня 192.168.3.1, необходимо отправить данные хосту с адресом 3-его уровня 192.168.3.2. При этом требуется использовать надежное соединение. Приложение запрашивает эту услугу на транспортном уровне.

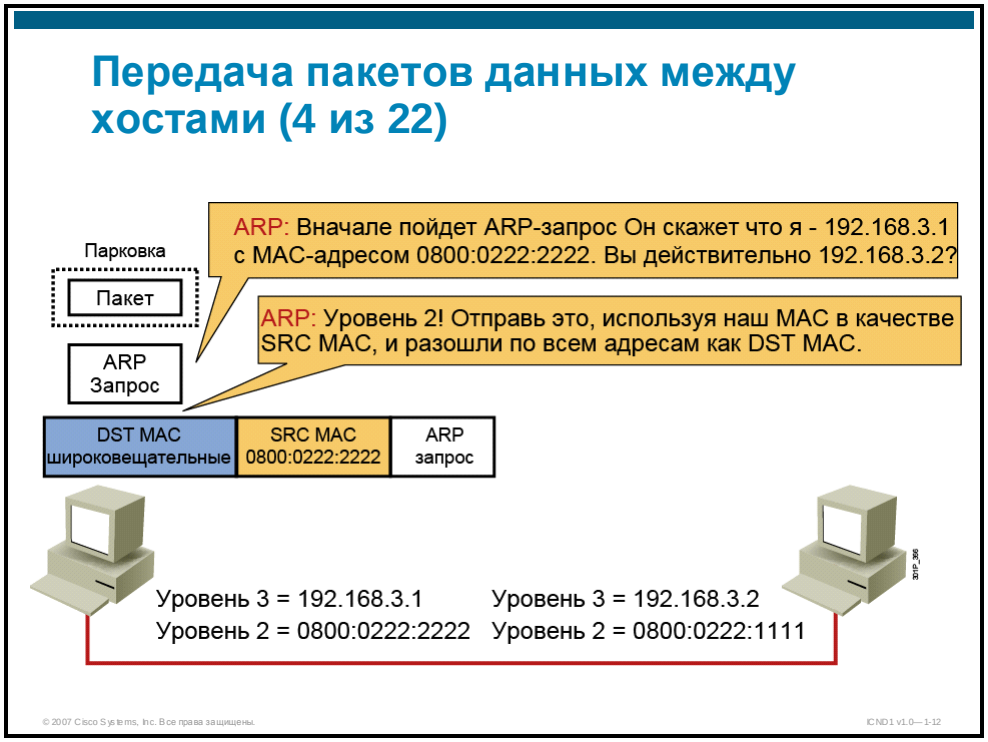
Транспортный уровень выбирает для установления сеанса протокол TCP. Протокол TCP инициирует сеанс, передавая заголовок TCP с набором битов SYN и адресом 3-его уровня (192.168.3.2) на уровень IP.

На уровне IP элемент SYN протокола TCP инкапсулируется в пакет уровня 2 с добавлением собственного адреса уровня 3 и адресом уровня 3, полученным протоколом IP от протокола TCP. После этого IP передает пакет уровню 2.



На уровне 2 пакет уровня 3 должен быть инкапсулирован в кадр уровня 2. Для этого уровень 2 должен привязать адрес назначения пакета уровня 3 к его MAC-адресу. Эта привязка запрашивается у программы ARP.

Протокол ARP проверяет свою таблицу. В этом примере предполагается, что рассматриваемый хост не обменивался данными со вторым хостом, поэтому запись в таблице ARP отсутствует. В результате пакет хранится на уровне 2, пока протокол ARP не найдет привязку.

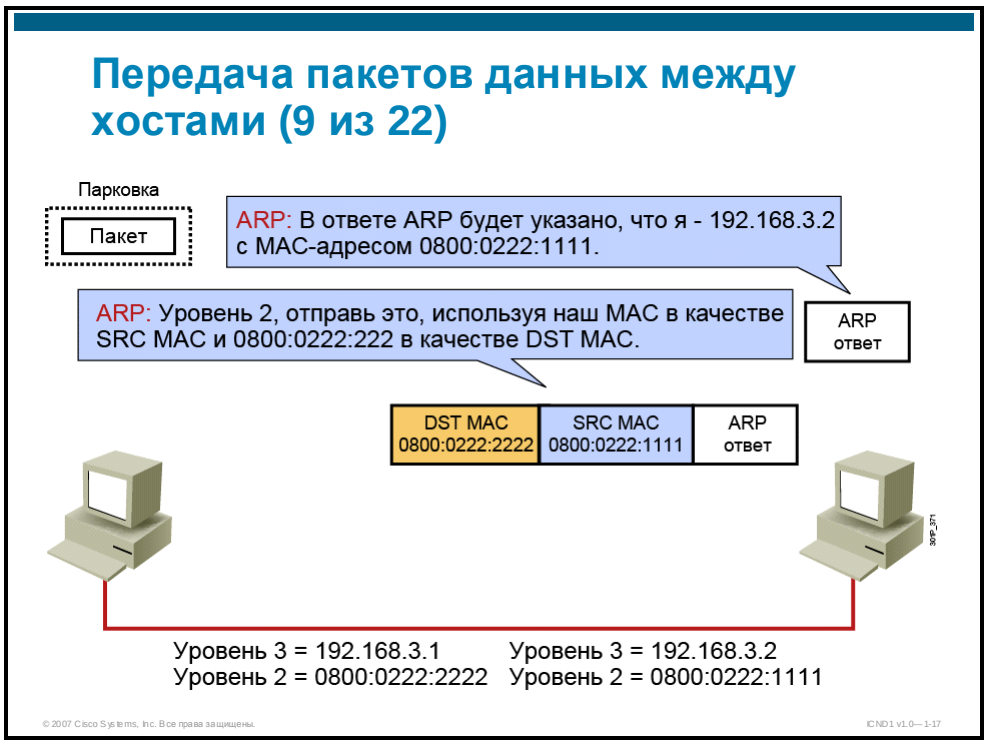


Программа ARP создает ARP-запрос и передает на уровень 2 для отправки по широковещательному адресу (F во всех позициях). На уровне 2 запрос ARP инкапсулируется в кадр уровня 2, в качестве MAC-адреса назначения используется широковещательный адрес, в качестве адреса источника – локальный MAC-адрес.

Когда хост с адресом 192.168.3.2 получает кадр, он распознает широковещательный адрес и удаляет инкапсуляцию уровня 2.

Оставшийся запрос ARP передается программе ARP.

Протокол ARP обновляет свою таблицу, используя информацию из запроса ARP.



ARP создает ответ и передает на уровень 2 для отправки по MAC-адресу 0800:0222:2222 (хост 192.168.3.1).

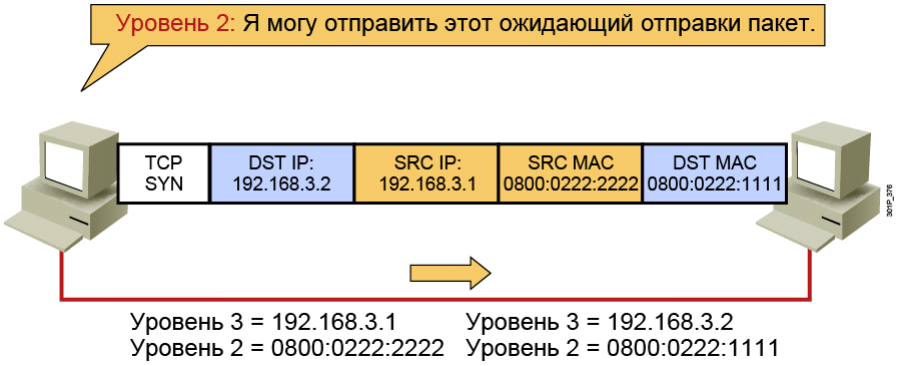
На уровне 2 ответ ARP инкапсулируется в кадр уровня 2 с использованием MAC-адреса назначения, предоставленного протоколом ARP, и локального MAC-адреса источника.

Когда хост 192.168.3.1 получает этот кадр, он определяет, что MAC-адрес совпадает с его собственным адресом, и снимает инкапсуляцию уровня 2.

Оставшийся ответ ARP передается программе ARP.

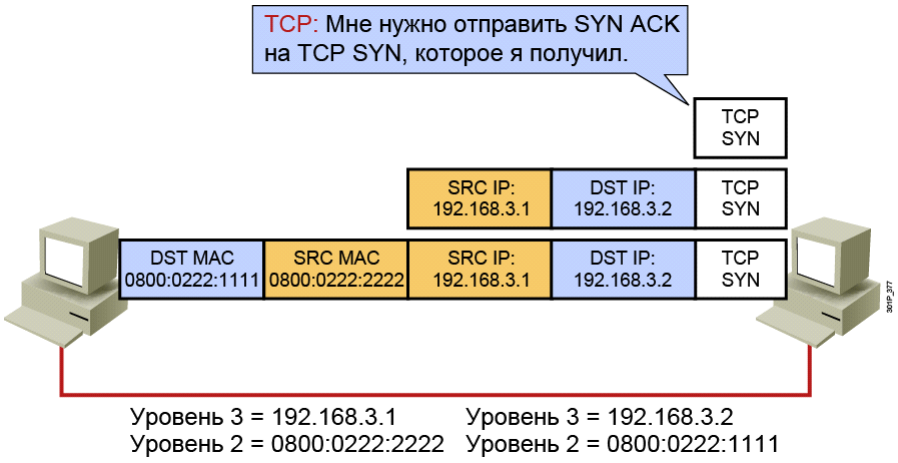
Протокол ARP обновляет свою таблицу и передает сопоставление на уровень 2.

Передача пакетов данных между хостами (14 из 22)



После этого уровень 2 может отправить отложенный пакет уровня 2.

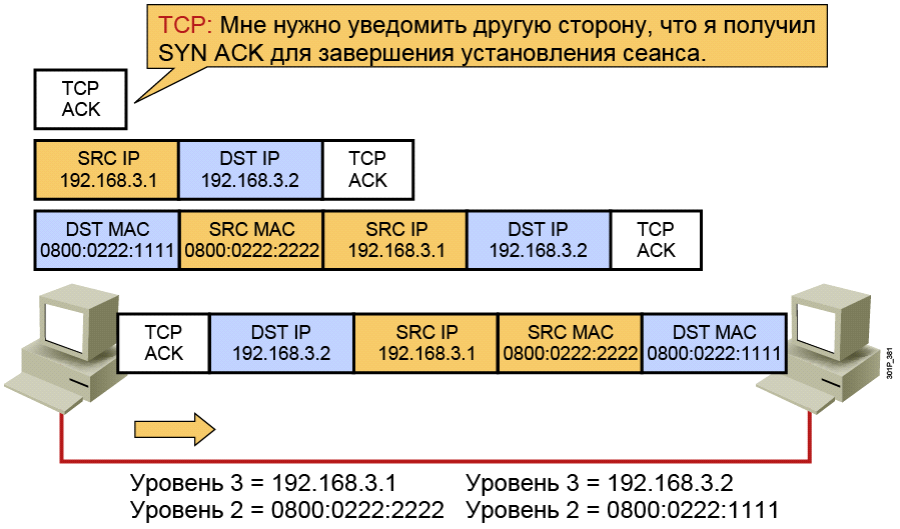
Передача пакетов данных между хостами (15 из 22)



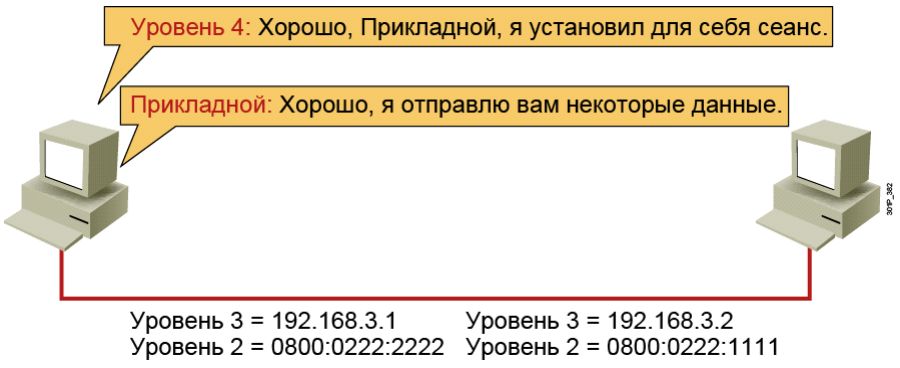
На хосте 192.168.3.2 кадр проходит через стек, где инкапсуляция удаляется. Оставшийся элемент информации протокола (PDU) передается протоколу TCP.

В ответ на элемент SYN протокол TCP передает в стек подтверждение SYN ACK для инкапсуляции.

Передача пакетов данных между хостами (18 из 22)

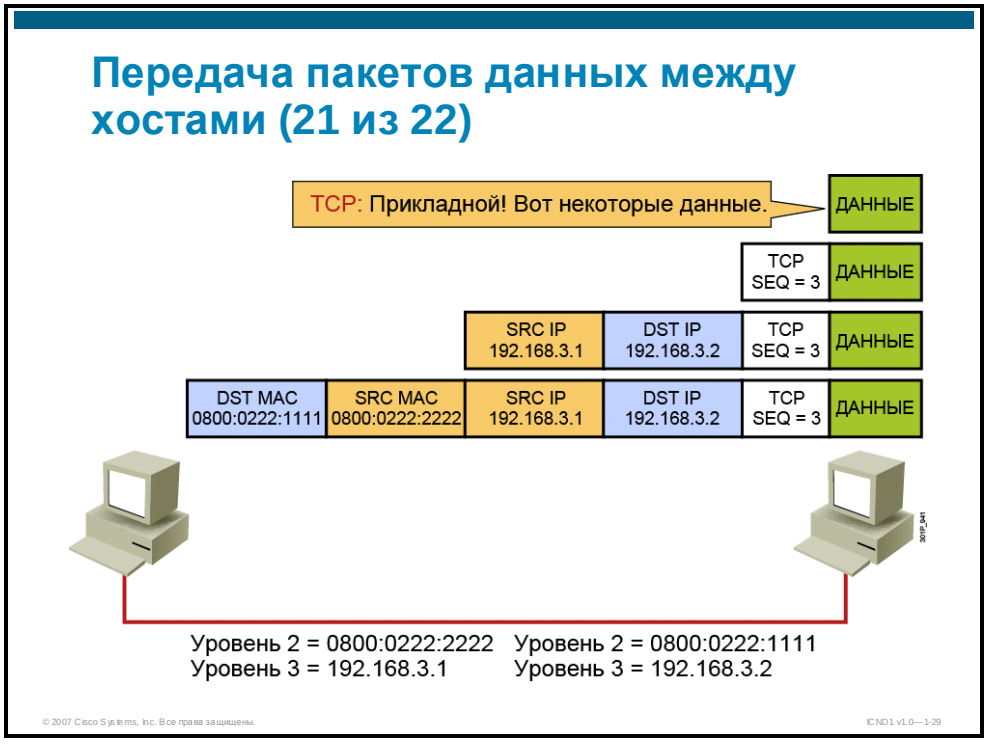


Передача пакетов данных между хостами (19 из 22)



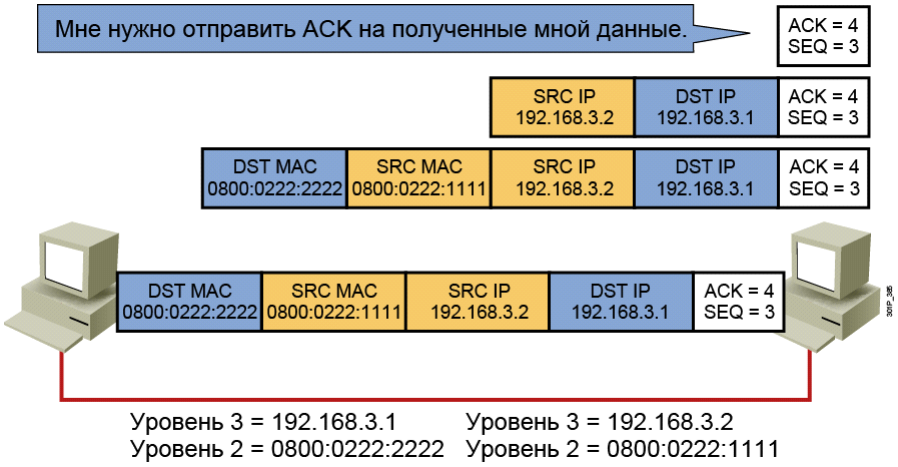
После завершения трехстороннего квитирования протокол TCP может информировать приложение о том, что сеанс установлен.

Теперь приложение может использовать сеанс для передачи данных, возлагая на протокол TCP обнаружение ошибок.



Обмен данными будет продолжаться до тех пор, пока приложение не прекратит отправку данных.

Передача пакетов данных между хостами (22 из 22)



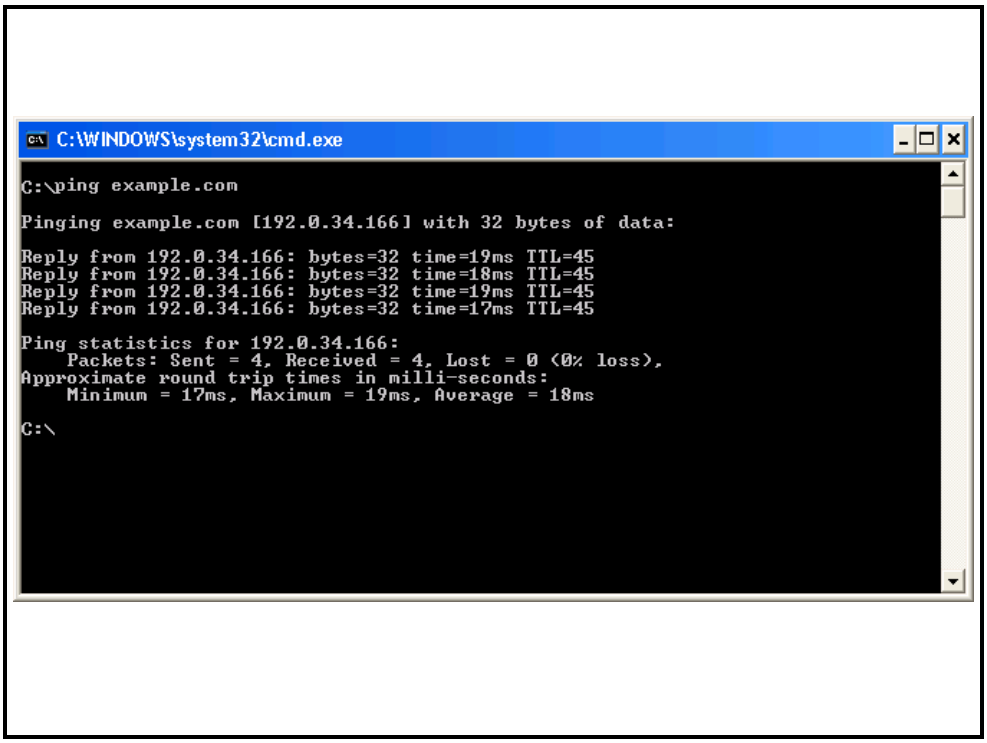
Назначение шлюза по умолчанию

В этом разделе описывается функция шлюза по умолчанию.

В предыдущем примере для сопоставления MAC- и IP-адресов назначения на хосте использовался протокол ARP. Однако этот вариант доступен только для хостов, расположенных в одной сети. Если хосты принадлежат разным сетям, хост-отправитель должен передать данные в шлюз по умолчанию, который пересылает данные к месту назначения.

Использование стандартных средств хоста для определения пути между двумя хостами в сети

В этом разделе рассматриваются стандартные средства тестирования хостов.



Ping является стандартным инструментом компьютерной сети, используемым для проверки достижимости конкретного хоста в IP-сети. На конечный хост посылаются пакеты эхо-запросов ICMP («Ping?»), затем выполняется прослушивание «эхо-ответов» ICMP. Измеряя интервал времени и скорость ответа, эхо-запрос оценивает время прохождения сигнала в прямом и обратном направлении (RTT – Round-Trip Time) (обычно в миллисекундах) и коэффициент потерь пакетов между хостами.

Синтаксис

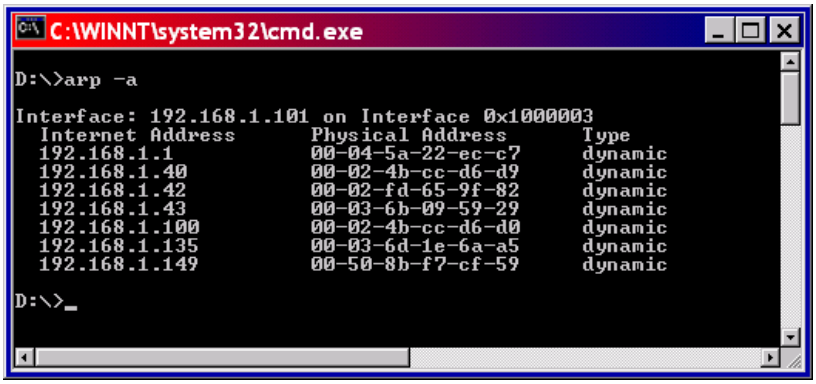
```
ping [-t] [-a] [-n Count] [-l Size] [-f] [-i TTL] [-v TOS]
[-r Count] [-s Count] [{-j HostList | -k HostList}] [-w
Timeout] [TargetName]
```

Параметры

- **-t.** Означает отправку эхо-запроса на указанный адрес до тех пор, пока не будет выполнено ручное прерывание. Для прерывания и вывода статистики нажмите **Ctrl-Break**. Для прерывания и выхода из программы эхо-запроса нажмите **Ctrl-C**.
- **-a.** Определяет обратное разрешение имен выполнется на IP-адресе назначения. Если разрешение выполнено успешно, программа отображает соответствующее имя хоста.
- **-n Count.** Число отправляемых эхо-запросов. По умолчанию равно 4.

- **-l Size.** Длина поля данных отправляемых эхо-запросов (в байтах). По умолчанию равна 32. Максимальный размер составляет 65 527.
- **-f.** Означает, что флаг запрета фрагментации в сообщениях эхо-запроса в IP-заголовке имеет значение 1, т. е. фрагментация эхо-запросов на пути к получателю запрещена. Этот параметр используется при поиске неполадок максимального размера блока в пути (PMTU – Path MTU).
- **-i TTL.** Задает значение поля времени жизни пакета (TTL) в IP-заголовке для посылаемых сообщений эхо-запроса. По умолчанию используется значение TTL для хоста. Для хостов под управлением Windows XP обычно составляет 128. Максимальное время жизни составляет 255.
- **-v TOS.** Задает значение поля TOS в IP-заголовке для посылаемых сообщений эхо-запроса. По умолчанию равняется 0. TOS задается в виде десятичного значения от 0 до 255.
- **-r Count.** Активирует использование параметра Record Route в IP-заголовке для записи пути эхо-запроса и соответствующего эхо-ответа. Каждый участок пути использует запись в параметре записи маршрута. По возможности это число не должно быть меньше числа переходов между источником и местом назначения. Минимальное число равно 1, а максимальное – 9.
- **-s Count.** Активирует использование параметра Internet Timestamp в IP-заголовке для записи времени прибытия эхо-запроса и соответствующего эхо-ответа на каждом переходе. Минимальное значение равно 1, а максимальное – 4.
- **-j HostList.** Активирует использование параметра Loose Source Route в IP-заголовке сообщениями эхо-запроса с набором промежуточных переходов, перечисленных в списке хостов. Свободная маршрутизация от источника позволяет разделять последовательные промежуточные переходы одним или несколькими маршрутизаторами. Максимальное число адресов или имен в списке хостов равно девяти. Список хостов представляет собой набор IP-адресов (в десятичном формате с точками), разделенных пробелами.
- **-k HostList.** Активирует использование параметра Strict Source Route в IP-заголовке сообщениями эхо-запроса с набором промежуточных переходов, перечисленных в списке хостов. При использовании строгой маршрутизации от источника каждый последующий промежуточный переход должен быть доступен напрямую (он должен быть соседним узлом или интерфейсом маршрутизатора). Максимальное число адресов или имен в списке хостов равно девяти. Список хостов представляет собой набор IP-адресов (в десятичном формате с точками), разделенных пробелами.
- **-w Timeout.** Задает время ожидания эхо-ответа в миллисекундах для данного эхо-запроса. Если в пределах этого временного интервала эхо-ответ не получен, отображается сообщение об ошибке «Request timed out». По умолчанию время ожидания составляет 4000 (четыре секунды).
- **TargetName.** Указывает место назначения, которое определяется IP-адресом или именем хоста.
- **/?:** Отображает справку в командной строке.

Таблица ARP



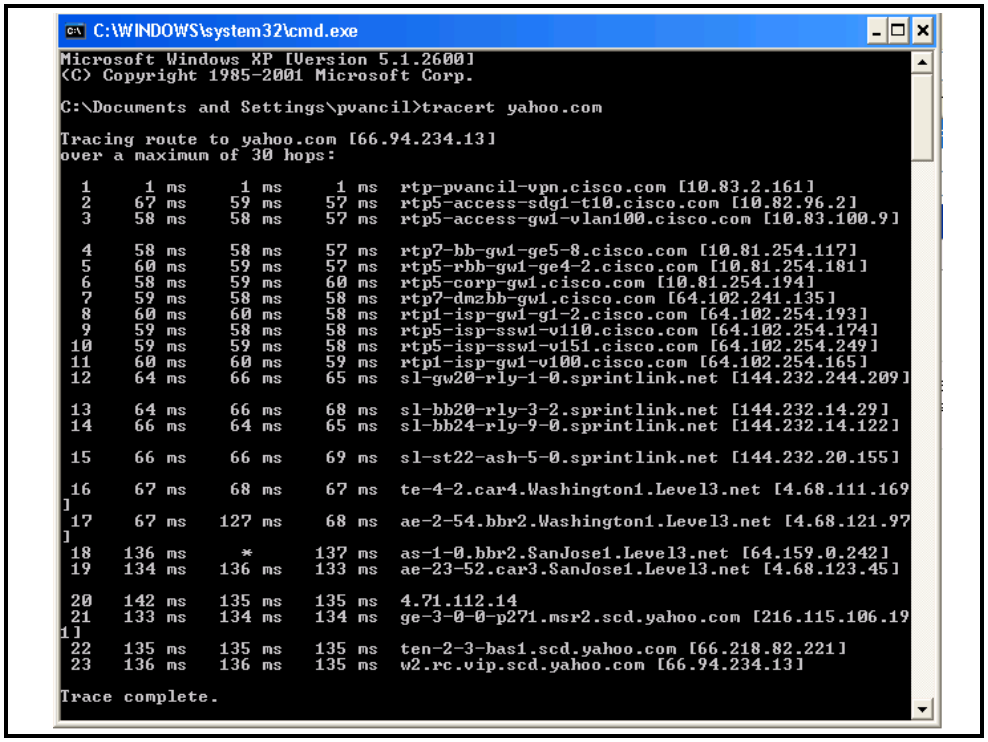
Команда **arp** выводит и изменяет записи в кэше ARP, который содержит одну или несколько таблиц, используемых для хранения IP-адресов и соответствующих им физических адресов Ethernet. Для каждого сетевого адаптера Ethernet или Token Ring, установленного на компьютере, задается отдельная таблица. При использовании команды **arp** без параметров отображается справка.

Синтаксис

```
arp [-a [InetAddr] [-N IfaceAddr]] [-g [InetAddr] [-N
IfaceAddr]] [-d InetAddr [IfaceAddr]] [-s InetAddr
EtherAddr [IfaceAddr]]
```

Параметры

- **-a** [**InetAddr**] [**-N IfaceAddr**]**.** Отображает текущие таблицы кэша ARP для всех интерфейсов. Чтобы отобразить запись кэша ARP для конкретного IP-адреса, следует использовать команду **arp -a** с параметром InetAddr, где InetAddr представляет IP-адрес. Чтобы отобразить запись кэша ARP для конкретного интерфейса, используйте параметр -N IfaceAddr, где IfaceAddr представляет IP-адрес, назначенный интерфейсу. Параметр -N чувствителен к регистру символов.
- **-g** [**InetAddr**] [**-N IfaceAddr**]**.** Идентичен параметру **-a**.
- **-d InetAddr** [**IfaceAddr**]**.** Удаляет запись с указанным IP-адресом, где InetAddr представляет IP-адрес. Чтобы удалить запись из таблицы конкретного интерфейса, используйте параметр IfaceAddr, где IfaceAddr представляет IP-адрес, назначенный интерфейсу. Для удаления всех записей следует использовать вместо InetAddr шаблонный символ астериска (*****).
- **-s InetAddr EtherAddr** [**IfaceAddr**]**.** Добавляет в кэш ARP статическую запись, сопоставляющую IP-адрес InetAddr с физическим адресом EtherAddr. Чтобы добавить статическую запись кэша ARP в таблицу для конкретного интерфейса, используйте параметр IfaceAddr, где IfaceAddr представляет IP-адрес, назначенный интерфейсу.
- **/?:** Отображает справку в командной строке.



Диагностическая утилита TRACERT определяет маршрут к конечному хосту, отправляя адресату эхо-пакеты протокола ICMP. Для этих пакетов утилита TRACERT использует различные значения времени жизни пакета (IP TTL). Поскольку каждый маршрутизатор на пути перед пересылкой пакета уменьшает значение TTL пакета на 1, TTL является эффективным счетчиком переходов. Когда TTL пакета достигает значения (0), маршрутизатор отправляет на исходный компьютер сообщение ICMP «Time Exceeded».

Программа TRACERT отправляет первый эхо-пакет с TTL, равным 1, и при каждой следующей отправке увеличивает TTL на 1, пока не будет получен ответ адресата или не достигнуто максимальное значение времени жизни. Сообщения ICMP «Time Exceeded», возвращаемые маршрутизаторами, указывают маршрут. Однако следует отметить, что некоторые маршрутизаторы отбрасывают пакеты с истекшими значениями TTL без сообщений, и эти пакеты невидимы для программы TRACERT.

Программа TRACERT выводит упорядоченный список промежуточных маршрутизаторов, которые возвращают сообщения ICMP «Time Exceeded». Использование команды **tracert** с параметром **-d** дает программе TRACERT инструкции не выполнять разрешение имени DNS каждого IP-адреса, поэтому TRACERT сообщает IP-адрес ближайшего интерфейса маршрутизатора.

Синтаксис

`tracert -d -h` *`maximum_hops`* `-j` *`host-list`* `-w` *`timeout target_host`*

Параметры

- **-d.** Отменяет сопоставление адресов с именами хостов.
- **-h maximum_hops.** Определяет максимальное число переходов для поиска адресата.
- **-j host-list.** Задает свободную маршрутизацию от источника по списку хостов.
- **-w timeout.** Задает время ожидания (в миллисекундах) для каждого отклика.
- **target_host.** Определяет имя или IP-адрес конечного хоста.

Резюме

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

Резюме

- Уровень 1 обеспечивает физическую среду и ее кодирование.
- Устройства уровня 2 обеспечивают интерфейс с физическими средами.
- Уровень 2 использует MAC-адреса.
- Сетевой уровень обеспечивает связность и выбор пути между двумя хостами.
- Уровень 3 использует IP-адреса.

Резюме (прод.)

- Для отправки данных хосту необходимо знать MAC-адрес этого хоста.
- Если MAC-адрес неизвестен, для сопоставления адресов уровня 2 и уровня 3 используется протокол ARP.
- Для надежного обмена данными необходим сеанс TCP.
- Требуется подтверждение отправленных данных.
- Для хостов, находящихся в разных сегментах сети, необходим шлюз по умолчанию.
- Для проверки подключения между хостами существует несколько средств:
  - **ping**
  - **tracert**
  - **arp**

Занятие 7

Общие сведения об Ethernet

Обзор

Локальная сеть представляет собой стандартный тип сети, используемый в домашних офисах, малых и крупных предприятиях. Понимание принципа работы локальной сети, включая сетевые компоненты, кадры, адреса Ethernet и эксплуатационные характеристики, необходимо для формирования общего представления о сетевых технологиях.

В этом занятии рассматриваются локальные сети и приводятся общие сведения о их характеристиках, компонентах и функциях. Кроме того, здесь представлено описание основных операций локальной сети Ethernet и способов передачи кадров внутри этой сети.

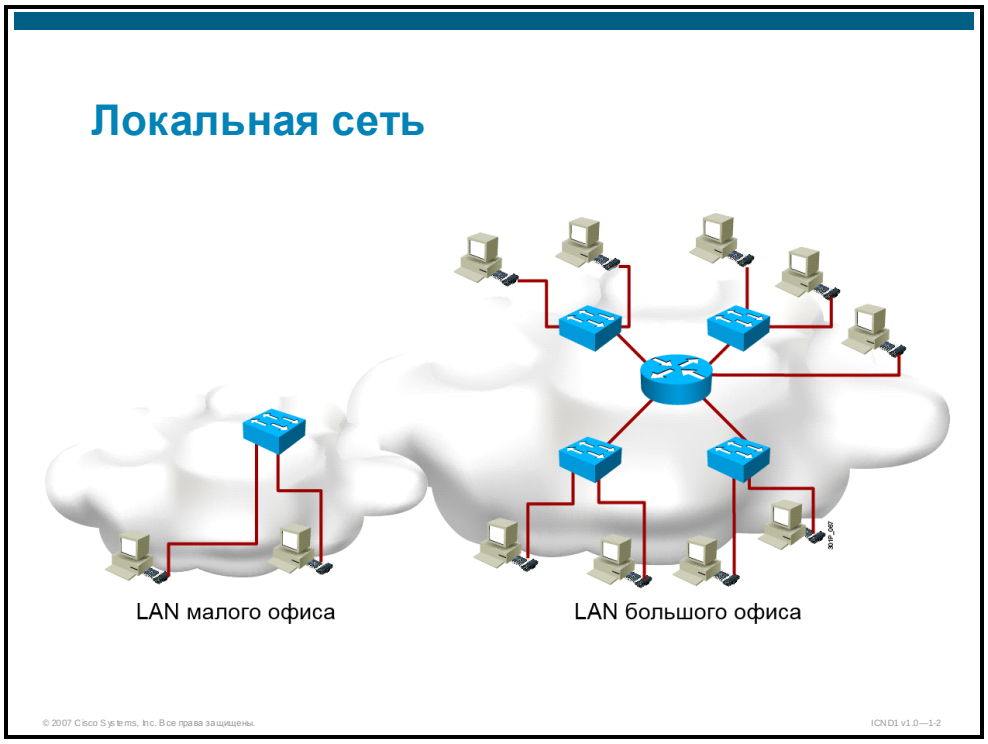
Задачи

По окончании этого занятия вы сможете перечислять характеристики и преимущества локальной сети, ее компонентов и связанных с ними функций. Это значит, что вы сможете выполнять следующие задачи:

- давать определение локальной сети;
- определять компоненты локальной сети;
- перечислять функции локальной сети;
- определять размеры локальной сети;
- описывать развитие стандарта Ethernet (IEEE 802.3);
- описывать регулирующие стандарты Ethernet;
- определять принцип действия CSMA/CD;
- идентифицировать поля кадра Ethernet и объяснять их функции;
- перечислять характеристики всех типов адресации кадра Ethernet;
- определять цель и компоненты адреса Ethernet;
- определять шестнадцатеричную структуру и функцию MAC-адреса в локальной сети Ethernet.

Определение локальной сети

В этом разделе представлено определение локальной сети.



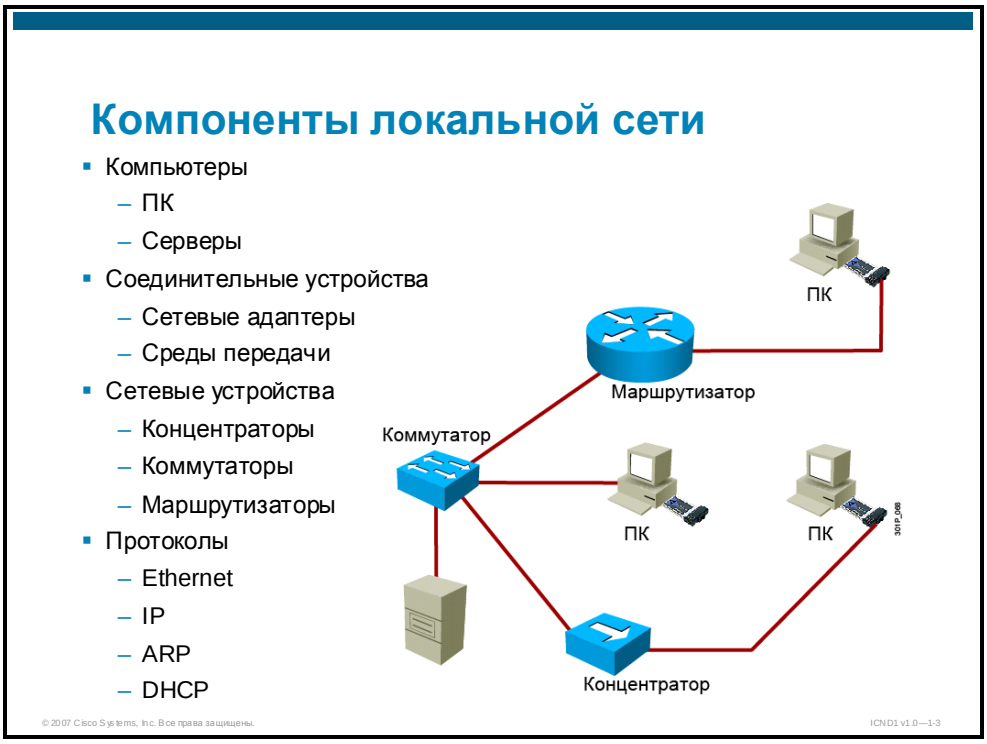
Локальная сеть представляет собой совокупность соединенных между собой компьютеров и других компонентов, расположенных относительно недалеко друг от друга на ограниченной площади. Размеры локальных сетей могут сильно различаться. Локальная сеть может состоять всего из двух компьютеров в домашнем офисе или на малом предприятии, или включать сотни компьютеров в крупном корпоративном офисе или комплексе зданий.

Примеры: локальные сети малого офиса и крупного предприятия

В среде домашнего бизнеса или небольшого офиса может использоваться небольшая локальная сеть, соединяющая несколько компьютеров и общих периферийных устройств, например принтеров. В офисе крупной корпорации в финансовых или производственных отделах, расположенных на нескольких этажах здания, могут использоваться несколько локальных сетей, охватывающих сотни компьютеров и общих периферийных устройств.

Компоненты локальной сети

Каждая локальная сеть включает определенные компоненты, в том числе оборудование, соединительные устройства и программное обеспечение. В этом разделе рассматриваются компоненты локальной сети.



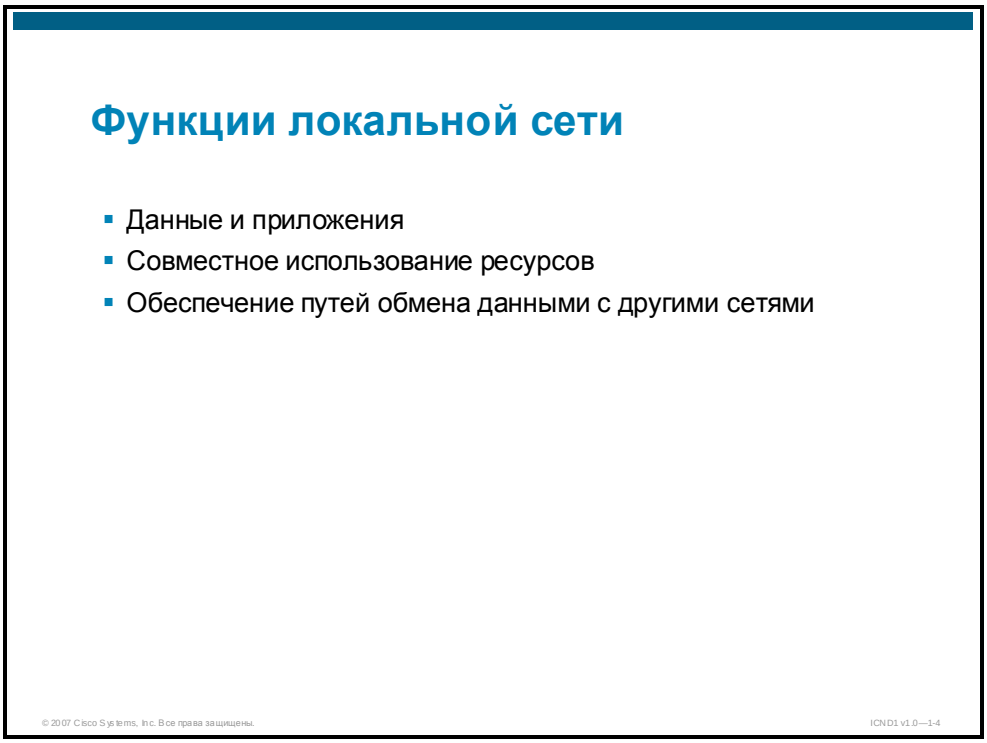
Независимо от размера локальной сети для ее работы необходимы следующие базовые компоненты.

- **Компьютеры.** Компьютеры служат конечными устройствами сети, которые отправляют и получают данные.
- **Соединительные устройства.** Соединительные устройства позволяют передавать данные из одной точки сети в другую. Соединительные устройства включают следующие компоненты:
  - **Сетевые адаптеры (NIC).** Сетевые адаптеры преобразуют данные компьютера в формат, пригодный для передачи по локальной сети.
  - **Сетевые среды.** Сетевые среды (например, кабели или беспроводные устройства), через которые происходит передача сигнала от одного устройства локальной сети к другому.

- **Сетевые устройства.** Для локальной сети необходимы следующие сетевые устройства:
  - **Концентраторы.** Концентраторы — это устройства агрегирования, действующие на уровне 1 эталонной модели OSI. Однако в настоящее время функцию концентраторов выполняют коммутаторы.
  - **Коммутаторы Ethernet.** Коммутаторы Ethernet образуют точки агрегирования для локальных сетей. Коммутаторы Ethernet действуют на уровне 2 модели OSI и обеспечивают интеллектуальную передачу кадров внутри локальной сети.
  - **Маршрутизаторы.** Маршрутизаторы, которые иногда называются шлюзами, обеспечивают соединение сегментов локальной сети. Маршрутизаторы действуют на 3-м уровне модели OSI.
- **Протоколы.** Протоколы представляют собой наборы правил, управляющие передачей данных по локальной сети, включая следующие:
  - протоколы Ethernet;
  - протокол Интернета (IP);
  - протоколы ARP (Address Resolution Protocol) и RARP (Reverse ARP);
  - DHCP (Dynamic Host Configuration Protocol).

Функции локальной сети

В этом разделе описываются стандартные функции локальных сетей.

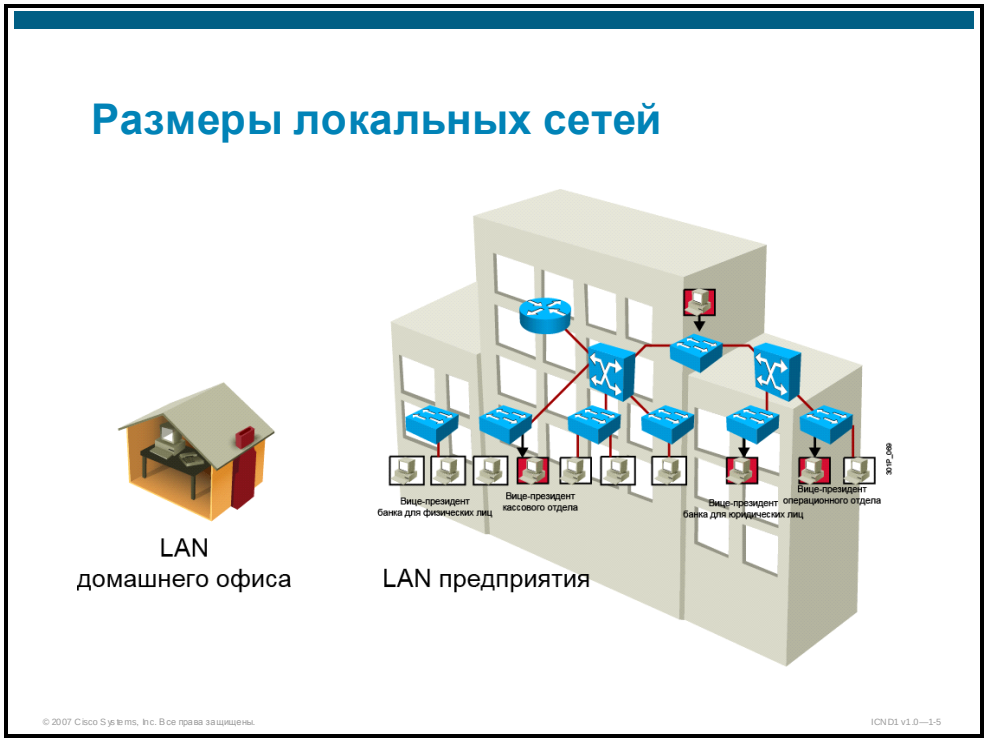


Локальные сети предоставляют пользователям функции обмена данными и совместного использования ресурсов.

- **Данные и приложения.** Пользователи с подключением к сети могут совместно использовать файлы и даже программные приложения. Это увеличивает доступность данных и повышает эффективность совместной работы над проектами.
- **Ресурсы.** Возможно совместное использование как устройств ввода (например, фотоаппаратов), так и устройств вывода информации (например, принтеров).
- **Пути обмена данными с другими сетями.** Если ресурс недоступен внутри локальной сети, сеть может обеспечить соединение с другими ресурсами, например, доступ к Интернету.

Каков размер локальной сети?

Размер локальной сети может меняться в зависимости от требований среды. В этом разделе рассматриваются размеры локальной сети.

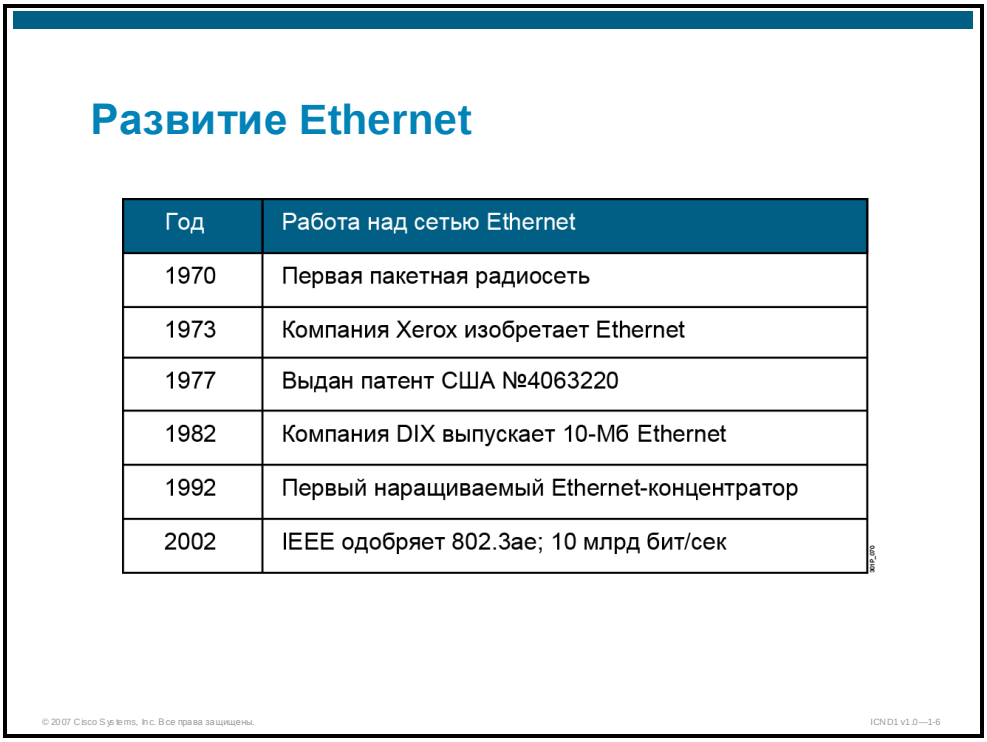


Локальные сети могут иметь разный размер в зависимости от эксплуатационных требований, включая следующие:

- **Малые и домашние офисы.** Среда малых и домашних офисов имеет всего несколько компьютеров и периферийных устройств, например, принтеров.
- **Крупное предприятие.** Среда крупного предприятия может включать множество отдельных локальных сетей в большом офисном здании или в корпоративном комплексе зданий. Каждая из локальных сетей среды предприятия может объединять сотни компьютеров и периферийных устройств.

Ethernet

Самый распространенный тип локальных сетей – это Ethernet. В этом разделе описывается история и уникальные характеристики Ethernet.

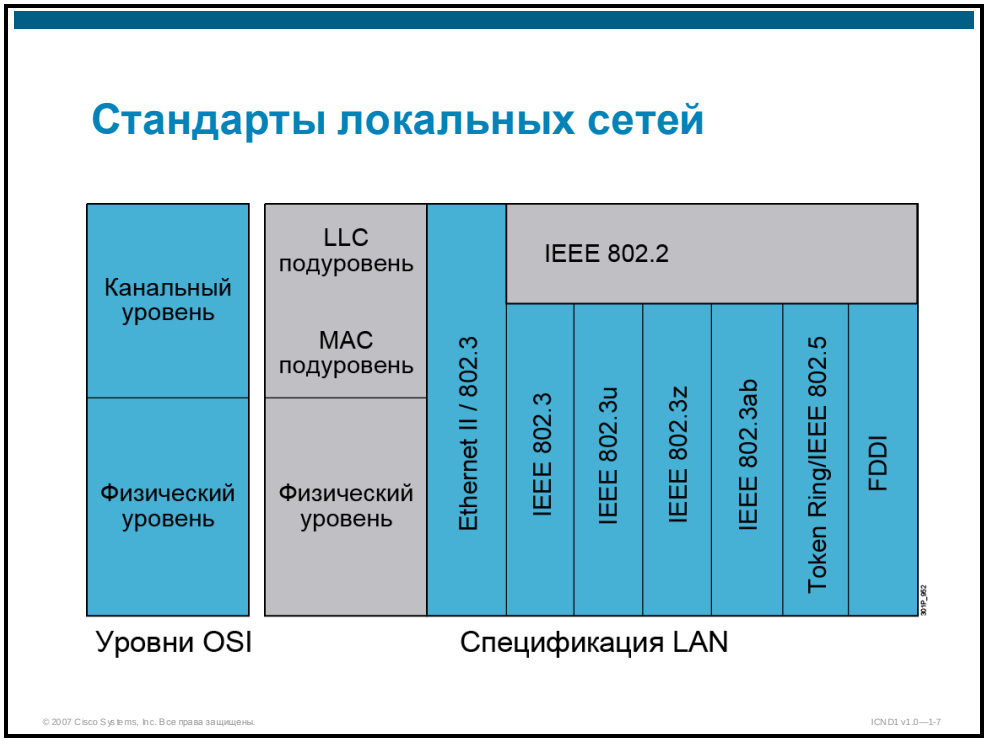


Стандарт Ethernet был разработан в 1970-ых годах корпорациями Digital Equipment Corporation (DEC), Intel и Xerox и получил название DIX Ethernet. Позже он был назван «толстым» Ethernet (из-за толщины кабеля, используемого в сетях этого типа), а скорость передачи данных составляла 10 мегабит в секунду (Мбит/с). В 1980-ых годах стандарт Ethernet был обновлен, его возможности расширены. Новая версия Ethernet получила название Ethernet версии 2 (или Ethernet II).

Разработкой сетевых стандартов занимается профессиональная организация Институт инженеров по электротехнике и радиоэлектронике (IEEE). Стандарты IEEE являются доминирующими стандартами локальных сетей в современном мире. В середине 1980-х годов рабочей группой IEEE были определены новые стандарты для сетей, подобных Ethernet. Созданный ими набор стандартов получил название Ethernet 802.3 и был основан на принципе множественного доступа с контролем несущей и обнаружением коллизий (CSMA/CD). Ethernet 802.3 определил физический уровень (уровень 1) и подуровень управления доступом к среде (MAC) канального уровня (уровень 2). В настоящее время этот набор стандартов чаще всего называют просто Ethernet.

Стандарты локальной сети Ethernet

Стандарты локальной сети Ethernet определяют соединительные кабели и передачу сигналов на физическом и канальном уровнях модели OSI. В этом разделе рассматриваются стандарты локальной сети Ethernet на канальном уровне.



На рисунке приводится сопоставление протоколов локальной сети с базовой моделью OSI.

Согласно определению IEEE канальный уровень OSI делится на два отдельных подуровня:

- **Управление логическим каналом – Logical Link Control (LLC) –** взаимодействие с верхним, сетевым уровнем
- **Управление доступом к среде – Media Access Control (MAC) –** взаимодействие с нижним, физическим уровнем

Подуровень LLC

Подуровень LLC был создан IEEE, чтобы обеспечить независимость канального уровня от существующих технологий. Этот уровень обеспечивает универсальные услуги для сетевых протоколов верхнего уровня и эффективное взаимодействие с разнообразными технологиями подуровня MAC и уровня 1, которые располагаются ниже. Подуровень LLC участвует в процессе инкапсуляции.

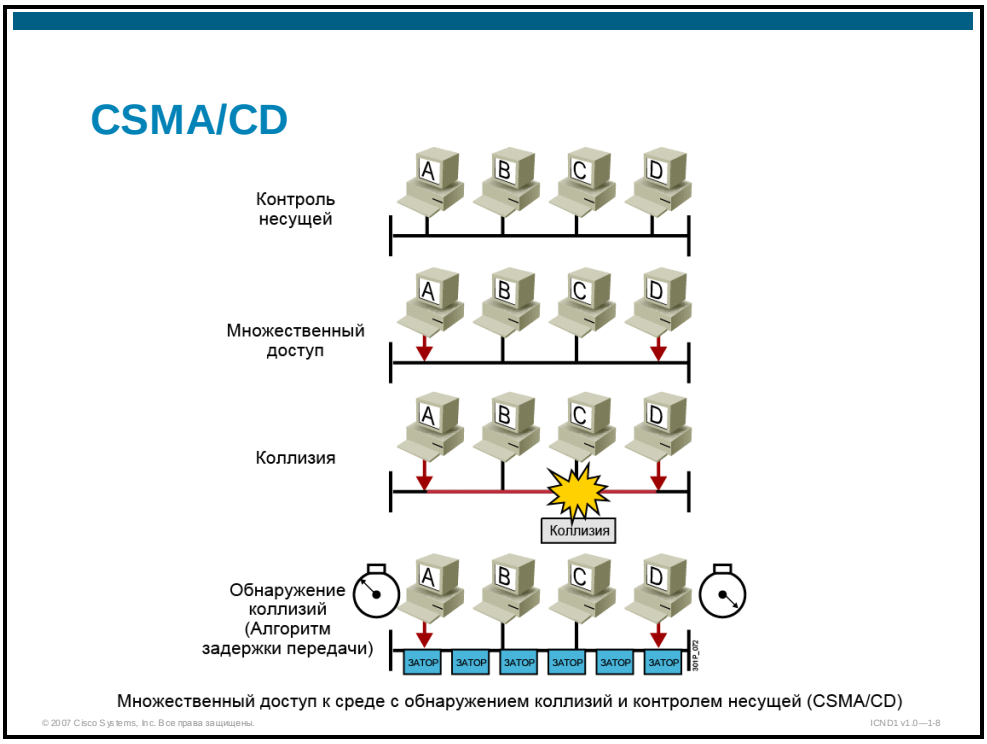
Заголовок LLC сообщает канальному уровню, как следует поступить с пакетом при получении кадра. Например, при получении кадра хост может определить, что пакет предназначен для протокола IP на сетевом уровне, используя его заголовок.

Подуровень MAC

Подуровень MAC отвечает за управление доступом к физической среде. Спецификация IEEE 802.3 MAC определяет MAC-адреса, уникально идентифицирующие множество устройств на канальном уровне. Подуровень MAC поддерживает таблицы MAC-адресов (физических адресов) устройств. Каждое устройство в сети должно иметь уникальный MAC-адрес.

Роль CSMA/CD в Ethernet

Сигналы Ethernet передаются всем хостам, подключенным к локальной сети, с помощью специального набора правил, который позволяет определить, какая станция может передавать данные в каждый момент времени. В данном разделе описывается этот набор правил.



В локальных сетях Ethernet управление сигналами в сети осуществляется с помощью метода множественного доступа с контролем несущей и обнаружением коллизий (CSMA/CD), который является важнейшим аспектом Ethernet. На рисунке показан процесс CSMA/CD.

В локальной сети Ethernet до передачи данных компьютер сначала «прослушивает» сетевую среду. Если она не занята, компьютер отправляет данные. После отправки данных компьютеры сети соревнуются между собой на предмет отправки другого кадра в следующий свободный промежуток. Это соревнование за свободное время означает, что станции в сети равноценны и не имеют преимуществ друг перед другом.

Станции в локальной сети CSMA/CD могут получить доступ к сети в любой момент времени. Перед отправкой данных станции CSMA/CD «прослушивают» сеть, чтобы определить, занята ли она. Если да, станции CSMA/CD ждут ее освобождения. Если сеть свободна, станции начинают передачу. Коллизия происходит, если две станции, прослушивающие сетевой трафик, обнаруживают его отсутствие и одновременно осуществляют передачу данных (см. рисунок). В этом случае будут повреждены обе передачи и станции должны повторить их через какой-то промежуток времени. Станции CSMA/CD должны уметь распознавать коллизии, чтобы определить необходимость повторной передачи данных.

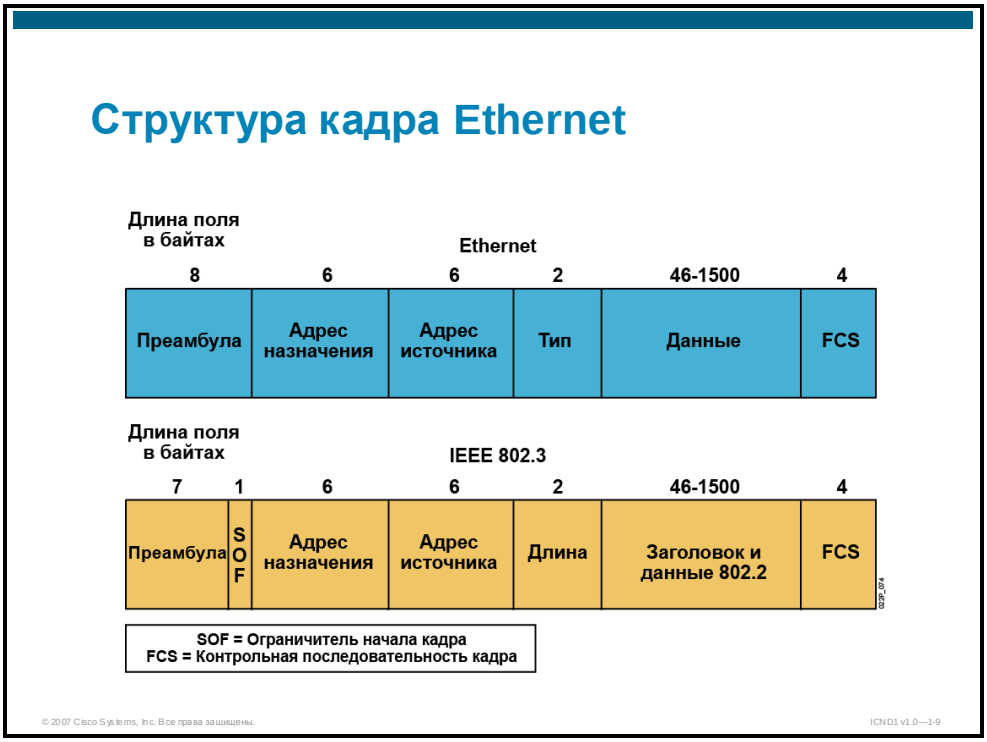
Сигнал, передаваемый станцией, называется несущей. Сетевой адаптер распознает несущую и поэтому воздерживается от широковещательной передачи сигнала. Если несущая отсутствует, ожидающая станция может начать передачу. Эта часть протокола называется контролем несущей.

Сетевой сегмент, в котором происходят коллизии, называется доменом коллизий. Размер домена коллизий влияет на эффективность, а, следовательно, и на полосу пропускания.

В процессе CSMA/CD отдельным станциям не назначается приоритет, поэтому все станции в сети имеют равные права. Эта часть протокола отражается в названии «множественный доступ». Коллизия возникает, когда две или более станции одновременно начинают передавать свои кадры. Станции оповещаются о коллизии и выполняют алгоритм отката, который назначает случайное время для повторной отправки кадра. Этот сценарий предотвращает повторную одновременную передачу двумя компьютерами. Обычное время устранения коллизий составляет микросекунды. Эта часть протокола называется обнаружением коллизий.

Кадры Ethernet

Биты, передаваемые по локальной сети Ethernet, организуются в кадры. В этом разделе рассматривается структура кадра Ethernet.



В терминологии Ethernet под кадром понимается контейнер, в который помещаются данные для передачи. Кадр содержит данные заголовка, конца передачи и фактические передаваемые данные.

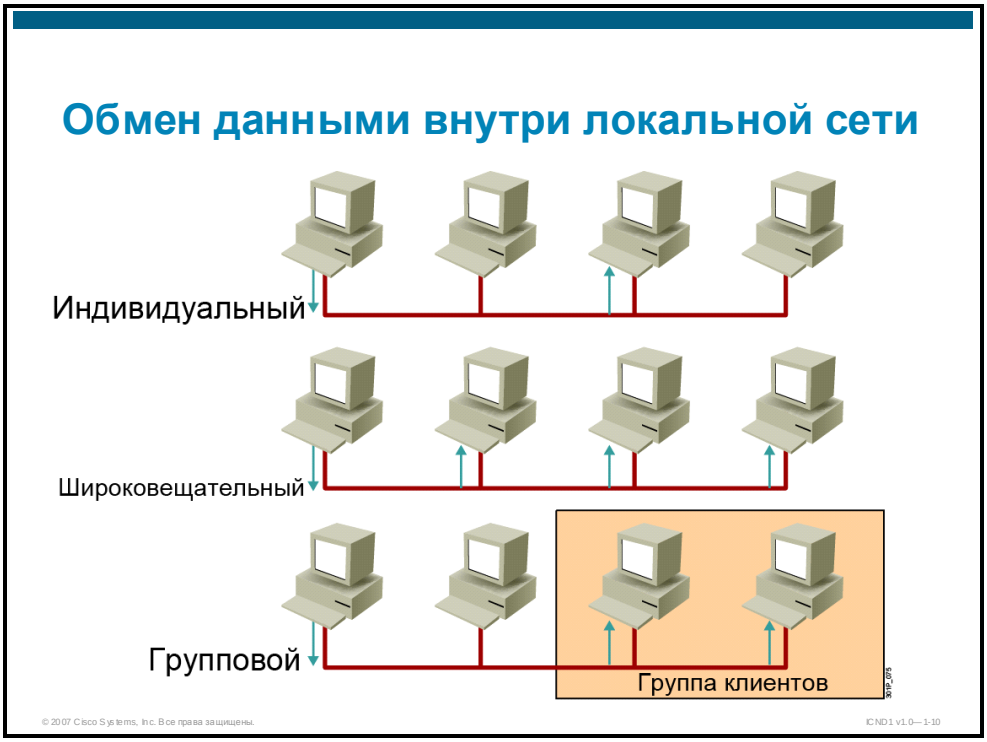
На рисунке показаны поля MAC-уровня кадра Ethernet, в том числе:

- **Preamble (Преамбула).** Это поле состоит из семи байтов, заполненных чередующимися единицами и нулями, которые используются для синхронизации сигналов компьютеров, обменивающихся данными.
- **Start-of-frame (SOF) delimiter (Разделитель начала кадра) (только 802.3).** Это поле содержит бит, оповещающий компьютер-получатель о начале передачи фактического кадра и о том, что все следующие данные являются частью пакета.
- **Destination Address (Адрес назначения).** Это поле содержит адрес сетевого адаптера в локальной сети, которому направляется пакет.
- **Source Address (Адрес источника).** Это поле содержит адрес сетевого адаптера компьютера-отправителя.
- **Type/length (Тип/длина).** В стандарте Ethernet II это поле содержит код, который идентифицирует протокол сетевого уровня. В стандарте 802.3 это поле определяет длину поля данных. Таким образом, все сведения о протоколе содержатся в полях 802.2, которые на уровне LLC содержатся в заголовке 802.2 и поле данных.

- **Data and pad (Данные и заполнитель).** Это поле содержит данные, полученные с сетевого уровня передающего компьютера. Затем эти данные передаются в тот же протокол компьютера-получателя. Если длина данных недостаточна, строка случайных битов используется для заполнения поля до минимальной длины, равной 46 байтам.
- **Frame check sequence (FCS) (Контрольная последовательность кадра).** Это поле включает механизм проверки, позволяющий гарантировать передачу пакета данных без повреждения.

Адресация кадров Ethernet

Передача данных в сети осуществляется тремя способами: индивидуальная, групповая и широковещательная рассылка. Адресация кадров Ethernet выполняется соответствующим образом. В этом разделе описывается отношение кадров Ethernet к методам сетевого взаимодействия.

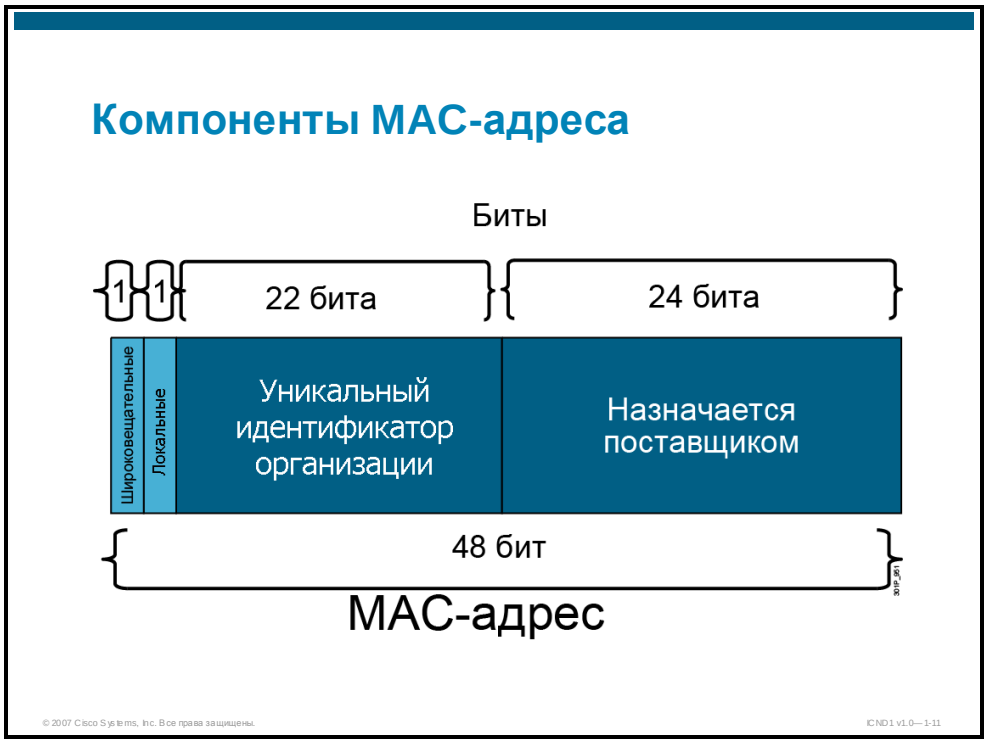


Существует три основных типа сетевого обмена данными.

- **Индивидуальная пересылка.** Обмен данными, при котором кадр отправляется с одного хоста и адресуется одному конкретному получателю. В одноадресной передаче участвует только один отправитель и один получатель. Индивидуальная пересылка является преобладающей формой передачи в локальных сетях и в Интернете.
- **Широковещательная рассылка.** Обмен данными, при котором кадр отправляется с одного адреса всем остальным адресам. В этом случае отправитель один, но информация посылается всем подключенным получателям. Широковещательная рассылка необходима при отправке одного сообщения всем устройствам в локальной сети.
- **Групповая рассылка.** Обмен данными, при котором информация передается конкретной группе устройств или клиентов. В отличие от широковещательной передачи в групповой рассылке для получения информации клиенты должны быть членами многоадресной группы.

Адреса Ethernet

Адрес, используемый в локальной сети Ethernet и связанный с сетевым адаптером позволяет направить данные соответствующему получателю. В этом разделе описываются характеристики адреса Ethernet.

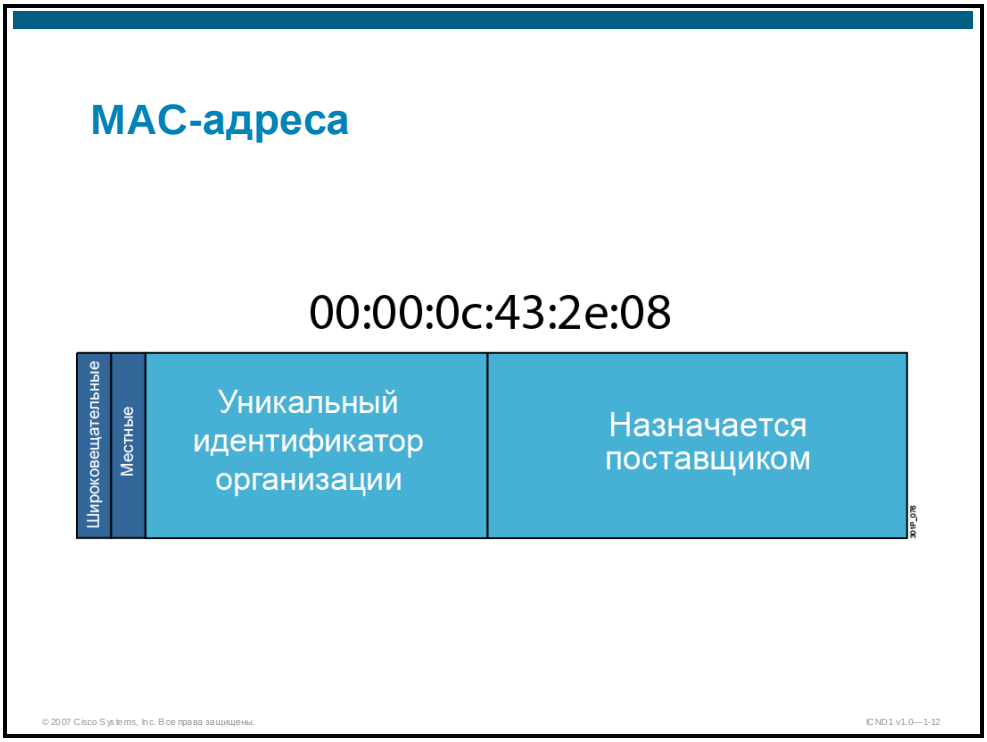


В качестве адреса сетевого адаптера используется MAC-адрес, часто именуемым BIA-адресом (Base Interface Address); некоторые поставщики допускают изменение этого адреса в соответствие с локальными требованиями. 48-битный MAC-адрес Ethernet состоит из двух компонентов.

- **24-битный уникальный идентификатор организации (OUI).** OUI определяет производителя интерфейсного адаптера. Назначение номеров OUI регулируется IEEE. В MAC адресе 2 бита из номера OUI имеют специальное назначение:
  - **Бит широковещательной или групповой рассылки.** Сообщает принимающему интерфейсу, что кадр предназначен для всех или для группы конечных станций в сегменте локальной сети.
  - **Бит локально-администрируемого адреса.** Обычно комбинация OUI и 24-битного адреса станции является уникальной, однако при локальном изменении адреса этот бит должен быть установлен в 1.
- **24-битный адрес конечной станции, назначенный поставщиком.** Этот адрес уникально идентифицирует оборудование Ethernet.

MAC-адреса и двоичные и шестнадцатеричные числа

MAC-адрес играет особую роль в работе локальной сети Ethernet. В этом разделе описываются MAC-адреса и их функция.



Подуровень MAC канального уровня OSI имеет дело с физической адресацией, а физический адрес представляет собой число 48-битное число, записанное в шестнадцатеричном формате, фактически, адрес «прошит» на сетевом адаптере. Этот номер называется MAC-адресом и отображается в виде шестнадцатеричных цифр, сгруппированных по две или четыре:

00:00:0c:43:2e:08 или 0000:0c43:2e08

Каждое устройство в ЛВС должно иметь уникальный MAC-адрес, чтобы участвовать в сети. MAC-адрес определяет местоположение конкретного компьютера в локальной сети. В отличие от других адресов, используемых в сети, изменение MAC-адреса без особой необходимости *не* рекомендуется.

Резюме

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

Резюме

- Локальная сеть представляет собой совокупность соединенных между собой компьютеров и других компонентов, расположенных относительно недалеко друг от друга на ограниченной площади.
- Независимо от размера локальной сети для ее работы необходимы такие основные компоненты, как компьютеры, соединительные устройства, сетевые устройства и протоколы.
- Локальные сети предоставляют пользователям функции обмена данными и совместного использования ресурсов.
- Размеры локальных сетей могут варьироваться от домашних офисов до крупных предприятий в зависимости от требований окружения.

Резюме (прод.)

- Стандарт Ethernet был разработан в 1970-е годы корпорациями DEC, Intel и Xerox и получил название DIX Ethernet. В середине 1980-х рабочей группой организации IEEE 802.3 были определены новые стандарты для сетей общего доступа, аналогичные Ethernet, Ethernet 802.3 и 802.2.
- Стандарты локальной сети Ethernet определяют соединительные кабели и передачу сигналов на физическом и канальном уровнях модели OSI
- Станции в локальной сети CSMA/CD могут получить доступ к сети в любой момент времени. Перед отправкой данных станции CSMA/CD "прослушивают" сеть, чтобы определить, занята ли она. Если сеть занята, они ожидают ее освобождения. Если сеть не занята, станции начинают передачу. Коллизия происходит, если две станции, прослушивающие сетевой трафик, обнаруживают его отсутствие и одновременно осуществляют передачу данных.

Резюме (прод.)

- Кадр Ethernet состоит из нескольких полей, включая поля преамбулы, разделителя начала кадра, адреса источника и назначения, типа/длины, данных, а также контрольной последовательности кадра.
- Существует три основных типа обмена данными в сетях: индивидуальная передача, при которой кадр отправляется с одного хоста и адресуется одному конкретному получателю; широковещательная рассылка при которой кадр отправляется с одного адреса на все остальные адреса; и групповая рассылка, при которой информация передается конкретной группе устройств.
- Адрес, используемый в локальной сети Ethernet, служит для направления данных нужному получателю.

Резюме (прод.)

- Подуровень MAC обрабатывает физическую адресацию, физический адрес представляет собой 48-битное число, записанное в шестнадцатеричном формате.

Занятие 8

Подключение к локальной сети Ethernet

Обзор

Помимо компонентов локальной сети Ethernet и стандартов, управляющих ее архитектурой, необходимо знать соединительные компоненты локальной сети Ethernet. На этом уроке рассматриваются соединительные компоненты локальной сети Ethernet, в том числе сетевые адаптеры (NIC) и кабели.

Задачи

По окончании этого занятия вы сможете перечислять типы и функции соединительных компонентов локальной сети Ethernet. Это значит, что вы сможете выполнять следующие задачи:

- перечислять функции сетевого адаптера в локальной сети Ethernet;
- знать требования к соединению для локальной сети Ethernet;
- определять типы соединительной среды локальной сети Ethernet;
- перечислять характеристики кабеля на основе неэкранированной витой пары;
- определять различия между прямым (straight-through) и перекрестным (crossover) кабелями.

Сетевые адаптеры Ethernet

Сетевой адаптер (NIC – Network Interface Card) представляет собой печатную плату, которая обеспечивает двунаправленное соединение персонального компьютера в сети. В этом разделе описывается сетевой адаптер и его функции.

Сетевой адаптер, также известный как адаптер ЛВС, устанавливается в материнскую плату и предоставляет порт для подключения к сети. Сетевой адаптер формирует компьютерный интерфейс для связи с локальной сетью.

Сетевой адаптер взаимодействует с сетью посредством последовательного соединения, а с компьютером – через параллельное соединение. При установке сетевого адаптера в компьютер требуется номер прерывания (IRQ) и адресный диапазон ввода-вывода, область памяти внутри операционной системы (например, DOS или Windows) и драйверы (программное обеспечение), позволяющие ему выполнять свою функцию. Прерывание – это сигнал, информирующий ЦП о событии, требующем внимания. Он посылается микропроцессору по аппаратной линии. Примером отправки сигнала IRQ может служить нажатие клавиши на клавиатуре, в результате которого ЦП должен передать символ с клавиатуры в ОЗУ. Адрес ввода-вывода представляет собой область памяти, используемый вспомогательным устройством для ввода данных в компьютер и извлечения данных из компьютера.

MAC-адрес присваивается каждому сетевому адаптеру производителем и представляет уникальный физический сетевой адрес.

Среда передачи Ethernet и требования к соединению

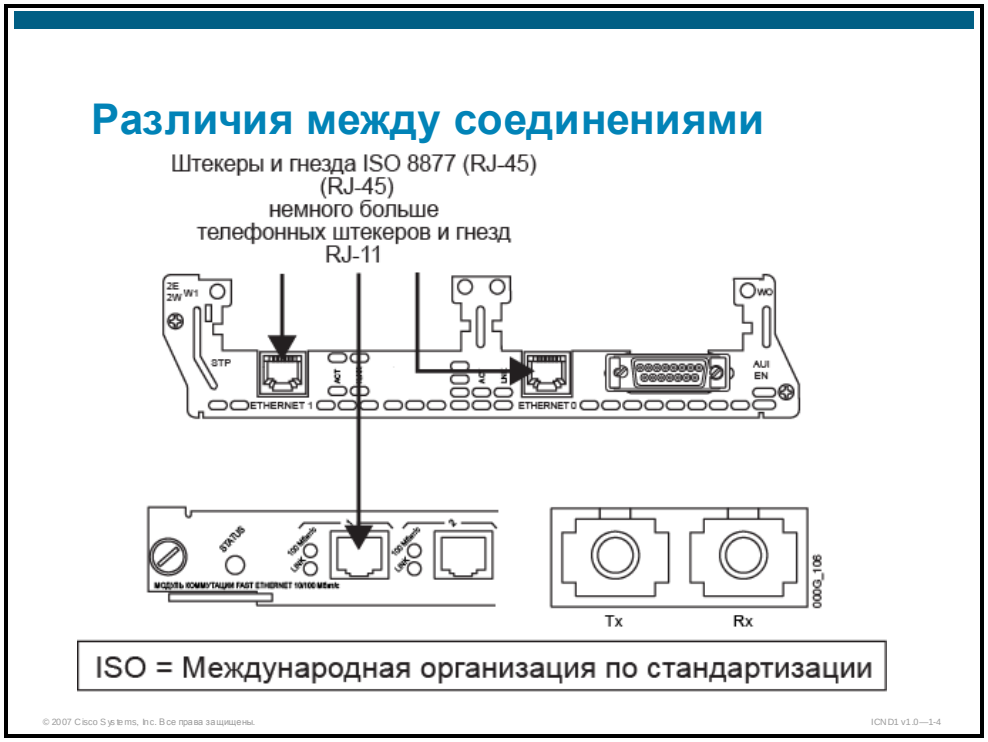
Необходимый тип соединения Ethernet определяется расстоянием и временем. В этом разделе описываются спецификации кабелей и разъемов, используемых для поддержки сред Ethernet.

Спецификации кабелей и разъемов, используемых для поддержки среды Ethernet, основываются на стандартах EIA/TIA. Категории кабелей, определенные для Ethernet, основываются на стандартах прокладки телекоммуникационных каналов коммерческих зданий EIA/TIA-568 (SP-2840). Согласно EIA/TIA для неэкранированной витой пары (UTP) используется разъем RJ-45.

На рисунке сравниваются спецификации кабелей и разъемов для наиболее популярных сред Ethernet. Важно отметить существенное различие носителей, используемых для Ethernet 10-Мбит/с, и носителей Ethernet 100-Мбит/с. В современных сетях со смешанными требованиями 10- и 100-Мбит/с, необходимо быть готовым к переходу на витую пару 5-ой категории для поддержки стандарта Fast Ethernet.

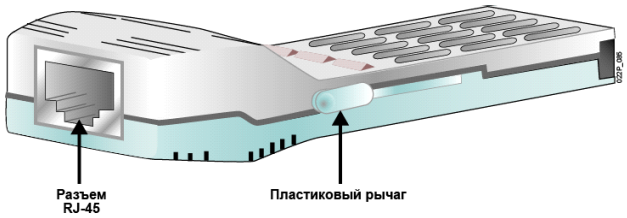
Соединители

В локальных сетях Ethernet используется несколько типов соединительной среды. В этом разделе рассматриваются различные типы соединений.



Наиболее распространенным типом соединительных устройств являются штекер и гнездо RJ-45 (см. рисунок). Буквы «RJ» означают «стандартный разъем» (registred jack), а цифры «45» относится к конкретному физическому разъему с восемью проводами.

Преобразователь 1000BASE-T GBIC



Преобразователь интерфейса Gigabit (GBIC) является устройством ввода-вывода с поддержкой «горячей» замены, которое подключается к порту Gigabit Ethernet маршрутизатора или коммутатора. Ключевым преимуществом преобразователя GBIC является его взаимозаменяемость, обеспечивающая гибкость для развертывания других технологий 1000BASE-X без замены физического интерфейса или модели маршрутизатора или коммутатора. Преобразователи GBIC поддерживают медную витую пару и оптоволоконные носители для передачи данных по стандарту Gigabit Ethernet.

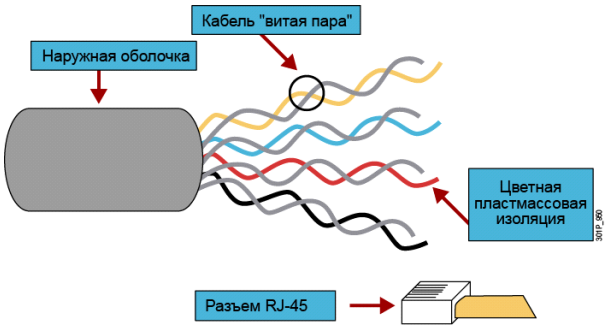
Обычно преобразователи GBIC используются в локальных сетях для восходящих каналов, а также в магистральных каналах. Кроме того, преобразователи GBIC применяются в удаленных сетях.

Оптоволоконный преобразователь GBIC – это трансивер, преобразующий последовательные электрические сигналы в оптические, а оптические сигналы в цифровые электрические сигналы. Существуют следующие типы оптических преобразователей GBIC:

- коротковолновые (1000BASE-SX);
- длинноволновые/для протяженных сетей (1000BASE-LX/LH);
- для больших расстояний (1000BASE-ZX);
- неэкранированная витая пара.

Витая пара представляет собой кабель с медными жилами, который может быть экранированным или неэкранированным. В локальных сетях часто используется кабель на основе неэкранированной витой пары (UTP). В этом разделе описываются характеристики и варианты использования неэкранированной витой пары.

Кабель на основе неэкранированной витой пары



- Скорость и полоса пропускания: от 10 до 1000 Мбит/с
- Средняя стоимость узла: минимальная
- Разъем носителя и разъема: компактный
- Максимальная длина кабеля: переменная

В кабеле UTP используется четыре пары проводников. Каждый из восьми медных проводников в кабеле изолирован. Кроме того, проводники в каждой паре скручены между собой. Преимущество кабеля на основе неэкранированной витой пары состоит в ограничении затухания сигнала из-за электромагнитных и радиочастотных помех. Для дополнительного сокращения перекрестных помех между парами кабеля UTP используется различное количество витков в парах. Существуют строгие спецификации, определяющие количество витков и оплетки на метр кабеля на основе неэкранированной (UTP) и экранированной (STP) витой пары.

Кабель UTP используется в сетях различных типов. В качестве сетевой среды обычно используются неэкранированные кабели из четырех пар медных проводников диаметром 22 или 24 AWG, что соответствует 0,64 или 0,51 мм. Сетевой кабель на основе неэкранированной витой пары имеет сопротивление 100 Ом. Это его отличие от других типов витых пар, например, используемых в телефонии. Поскольку внешний диаметр кабеля UTP составляет около 0,43 см (0,17 дюймов), его небольшой размер может оказаться преимуществом при установке. Кроме того, поскольку кабель UTP может применяться в большинстве сетевых архитектур, его популярность продолжает расти.

Выделяют несколько категорий кабеля на основе неэкранированной витой пары:

- **Категория 1.** Кабель этой категории предназначен для телефонных коммуникаций и не пригоден для передачи данных.
- **Категория 2.** Подходит для передачи данных со скоростями до 4 Мбит/с.
- **Категория 3.** Применяется в сетях 10BASE-T и предназначен для передачи данных со скоростями до 10 Мбит/с.
- **Категория 4.** Используется в сетях Token Ring (скорость передачи до 16 Мбит/с).
- **Категория 5.** Предназначен для передачи данных со скоростями до 100 Мбит/с.
- **Категория 5e.** Применяется в сетях, работающих со скоростями до 1000 Мбит/с (1 Гбит/с).
- **Категория 6.** Состоит из четырех пар медных жил диаметром 24 AWG (0,51 мм), способных обеспечивать передачу данных со скоростями до 1000 Мбит/с.

В современных локальных сетях наибольшее распространение получили категории 1 (используется, в основном, для телефонии), 5, 5e и 6.

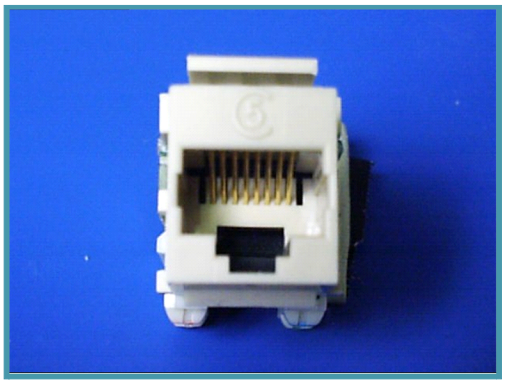
Внедрение кабеля UTP

Для внедрения кабеля UTP в локальной сети необходимо определить тип кабеля по стандартам EIA/TIA и выбрать между прямым и перекрестным кабелем. В этом разделе описываются характеристики и варианты использования прямого и перекрестного кабелей, а также типы разъемов, применяемых при внедрении кабеля UTP в локальной сети.

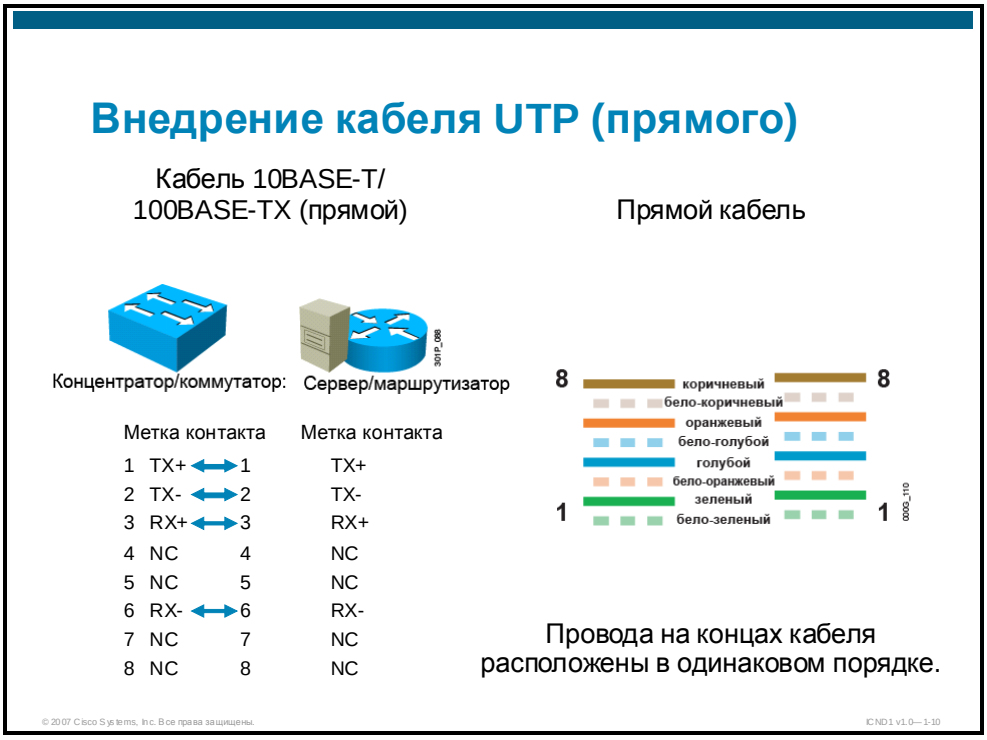
Если внимательно посмотреть на прозрачный разъем RJ-45, можно увидеть восемь цветных проводов, скрученных в четыре пары. Четыре провода (две пары) переносят положительное напряжение (true) и называются «tip» (T1 – T4); остальные четыре переносят обратное базовое напряжение (false) и называются «ring» (R1 – R4). Термины «tip» и «ring» пришли из телефонии. В настоящее время они относятся к положительному и отрицательному проводникам в паре. Провода первой пары кабеля или разъема обозначаются T1 и R1, второй пары – T2 и R2 и т. д.

Штекер RJ-45 («папа») крепится к концу кабеля методом обжима. Если смотреть на этот разъем спереди, как показано на рисунке, его контакты нумеруются слева направо с 8 до 1.

Гнездо RJ-45



Гнездо («мама») располагается на сетевом устройстве, стене, выводе перегородки или коммутационной панели. Если смотреть на гнездо спереди, как показано на рисунке, его контакты нумеруются слева направо с 1 до 8.



Помимо определения нужной категории кабеля, используемого для соединительного устройства, согласно стандарту EIA/TIA (в зависимости от стандарта штекера сетевого устройства) необходимо определить тип кабеля:

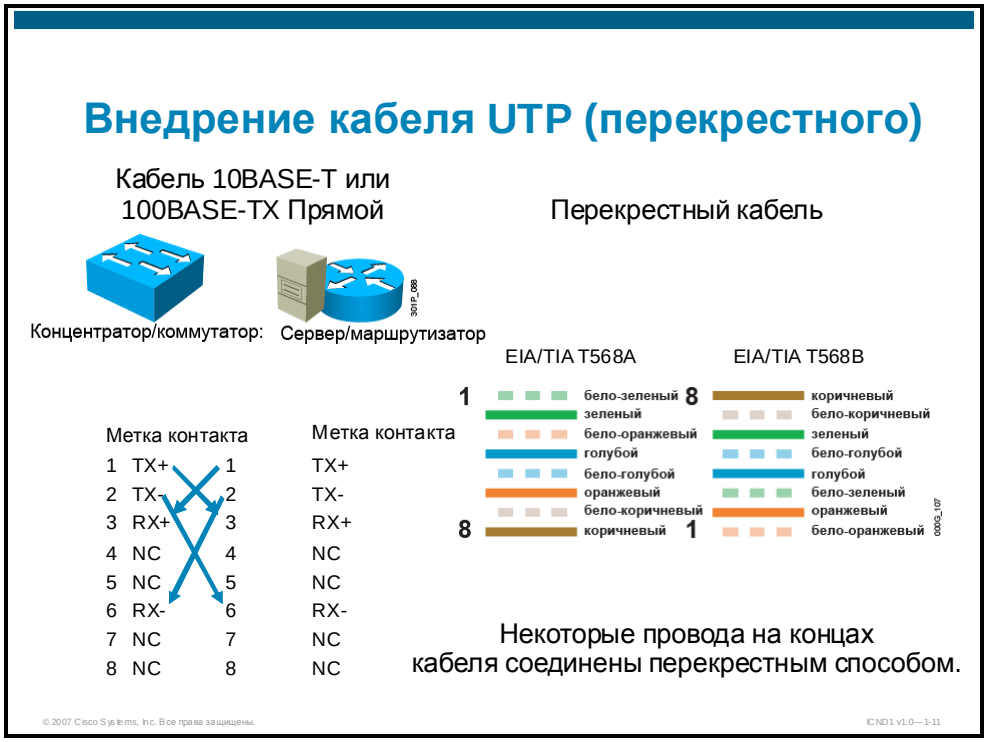
- прямой кабель;
- перекрестный кабель.

В прямом кабеле все провода разъемов RJ-45 на обоих концах расположены в одинаковом порядке. Если поместить два разъема RJ-45 кабеля рядом и с одинаковой ориентацией, на каждом разъеме будут видны цветные провода (полоски или контакты). Если порядок цветных проводов на каждом конце совпадает, это прямой тип кабеля (см. рисунок).

Прямой кабель

Концентратор или сервер **Сервер или хост**

Номер контакта	Цвет	Функция	Номер контакта	Цвет	Функция
1	Белый/зеленый	TX+	1	Белый/зеленый	TX+
2	Зеленый	TX-	2	Зеленый	TX-
3	Белый/оранжевый	RX+	3	Белый/оранжевый	RX+
6	Оранжевый	RX-	6	Оранжевый	RX-

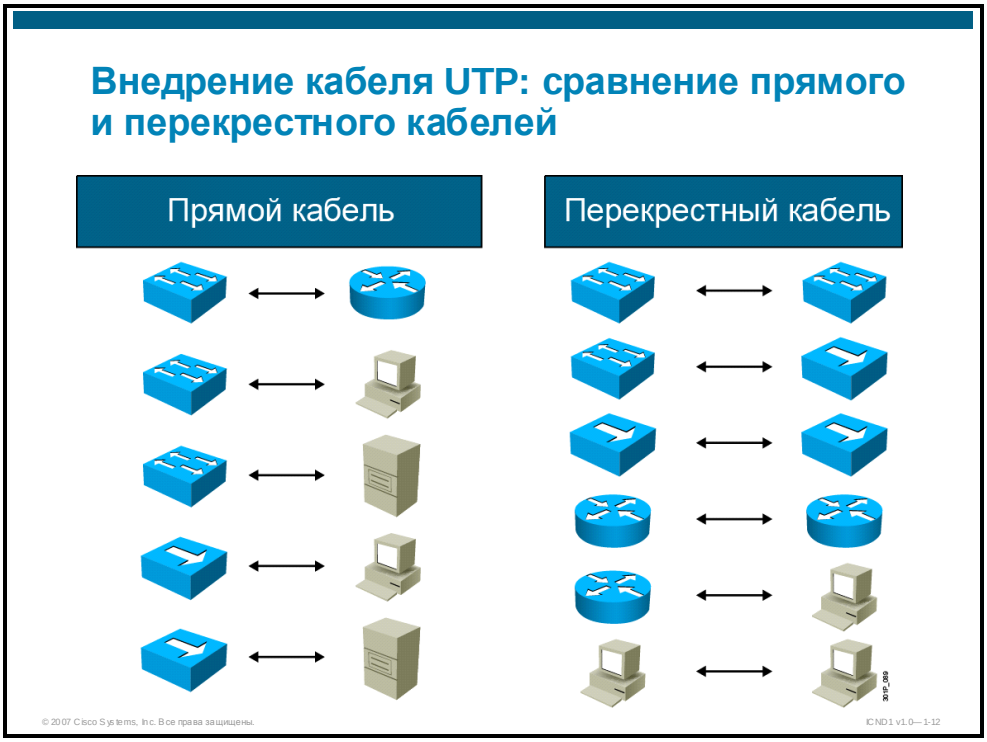


В перекрестных кабелях провода разъемов RJ-45 на разных концах кабеля располагаются в другом порядке. В частности, для Ethernet, контакт 1 на одном конце RJ-45 должен быть соединен с контактом 3 на другом. Контакт 2 на одном конце должен быть соединен с контактом 6 на другом, как показано на рисунке.

Перекрестный

Концентратор или сервер **Сервер или хост**

Номер контакта	Цвет	Функция	Номер контакта	Цвет	Функция
1	Белый/зеленый	TX+	3	Оранжевый	RX+
2	Зеленый	TX-	6	Белый/оранжевый	RX-
3	Белый/оранжевый	RX+	1	Зеленый	TX+
6	Оранжевый	RX-	2	Белый/зеленый	TX-



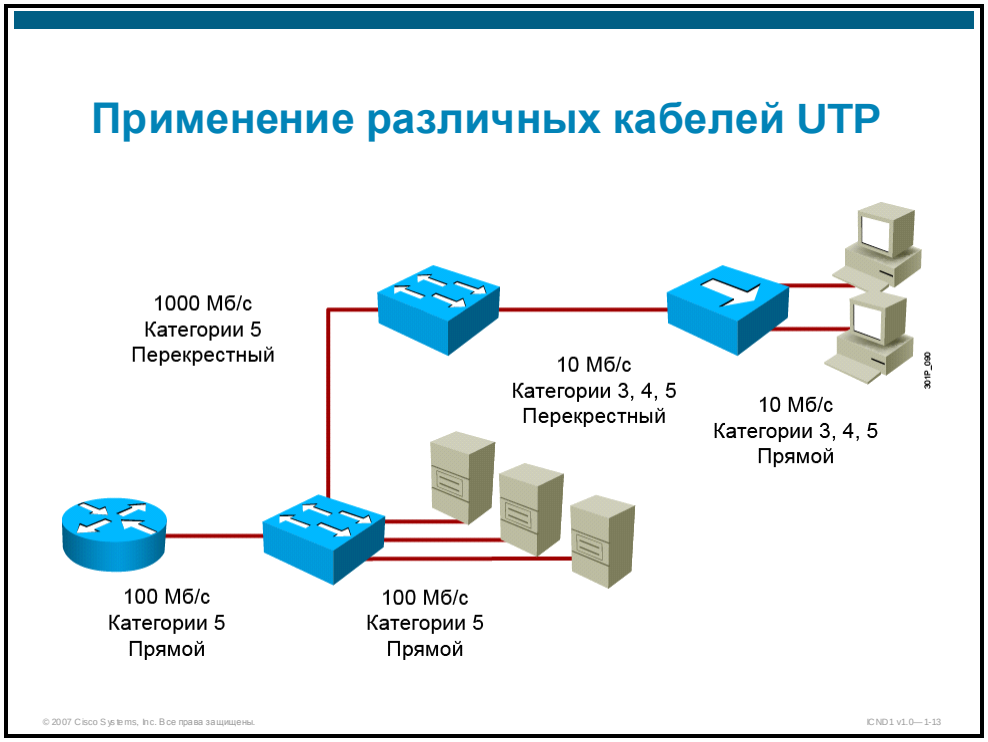
На этом рисунке показаны инструкции по выбору типа кабеля, используемого для соединения устройств Cisco. В дополнение к проверке категории кабеля необходимо определить тип используемого кабеля: прямой или перекрестный.

Прямые кабели используются при следующих кабельных соединениях:

- коммутатор – маршрутизатор;
- коммутатор – ПК (или сервер);
- концентратор – ПК (или сервер).

Перекрестные кабели используются при следующих кабельных соединениях:

- коммутатор – коммутатор;
- коммутатор – концентратор;
- концентратор – концентратор;
- маршрутизатор – маршрутизатор;
- порт Ethernet маршрутизатора – сетевой адаптер ПК
- ПК – ПК.



На рисунке показаны разные типы кабелей UTP, которые могут использоваться в сети. Следует отметить, что категория UTP зависит от типа Ethernet, который вы внедряете.

Резюме

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

Резюме

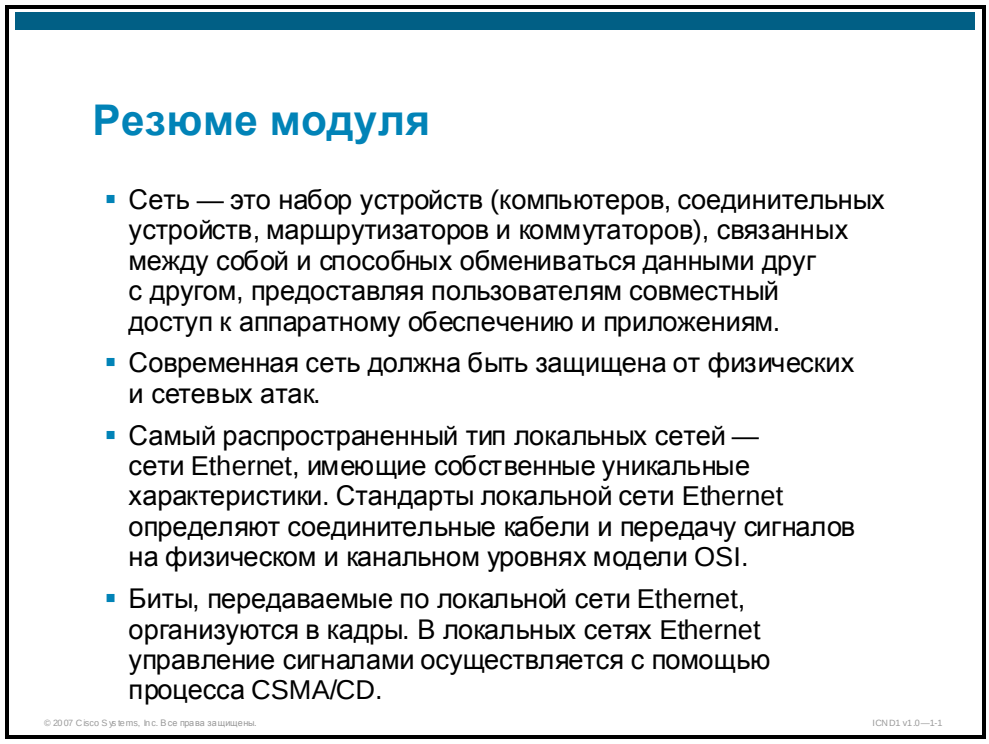
- Сетевой адаптер, также известный как адаптер ЛВС, устанавливается в материнскую плату и предоставляет порт для подключения к сети.
- MAC-адрес присваивается каждому сетевому адаптеру производителем и представляет уникальный физический сетевой адрес, позволяющий устройству участвовать в обмене данными в сети.
- Спецификации кабелей и разъемов, используемых для поддержки сред Ethernet, основываются на стандартах EIA/TIA.
- Категории кабелей, определенные для Ethernet, основываются на стандартах прокладки телекоммуникационных каналов коммерческих зданий EIA/TIA-568 (SP-2840).

Резюме (прод.)

- В кабеле UTP используется четыре пары проводников. Все восемь отдельных медных проводов в кабеле изолированы и попарно скручены между собой.
- Перекрестный кабель используется для соединения аналогичных устройств (например, коммутатора с коммутатором, маршрутизатора с маршрутизатором, ПК с ПК или концентратора с концентратором).
- Прямой кабель используется для соединения разнородных устройств (например, коммутатора с маршрутизатором, коммутатора с ПК, концентратора с маршрутизатором или концентратора с ПК).

Резюме модуля

В этом разделе приводится резюме вопросов, рассмотренных в модуле.



Резюме модуля (прод.)

- Обмен данными между хостами определяется моделью OSI и TCP/IP.
- Эталонная модель OSI определяет функции сети, реализуемые на каждом уровне, и облегчает понимание передачи данных в сети.
- Протокол TCP/IP определяет 32-битный адрес, состоящий из 4 октетов, разделенных точками.
- Адрес хоста может настраиваться вручную или получаться с DHCP-сервера.

Справочные материалы

См. дополнительные сведения в следующем источнике.

- Большая часть материалов занятия взята из легко доступных документов, предоставляемыми многими правительственными агентствами. Форум по техническому обеспечению доступности, целостности и безопасности информации (IATFF) – это пропагандистская инициатива, финансируемая Агентством национальной безопасности и созданная для диалога, нацеленного на поиск решения проблем доступности, целостности и безопасности информации. Веб-сайт форума IATFF находится по адресу http://www.iatf.net.

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 Какие три утверждения о сетях наиболее соответствуют действительности? (Выберите три варианта.) (Источник: обзор функций сети)

А) Сети служат для передачи данных в различных окружениях, включая домашние офисы, небольшие компании и крупные предприятия.
Б) В главном офисе могут работать сотни и даже тысячи людей, которые нуждаются в доступе к сети для своей работы.
В) Сеть – это комбинация устройств, связанных между собой и способных обмениваться данными друг с другом.
Г) В главном офисе для соединения всех пользователей обычно используется одна большая сеть.
Д) Предназначение сети состоит в предоставлении средств доступа ко всей информации и компонентам сети всем работникам.
Е) Подключение удаленных площадок к главному офису через сеть невозможно.

В2 Каково назначение маршрутизатора? (Источник: обзор функций сети)

А) соединение сетей между собой и выбор наилучшего пути между ними
Б) обеспечение точек подключения к среде передачи
В) они служат конечными устройствами сети, которые отправляют и получают данные
Г) обеспечение средств передачи сигнала от одного сетевого устройства к другому

В3 Каково назначение коммутатора? (Источник: обзор функций сети)

А) соединение отдельных сетей и фильтрация трафика для передачи данных по наиболее эффективному маршруту
Б) выбор пути, по которому данные отправляются получателю
В) они служат конечными устройствами сети, которые отправляют и получают данные
Г) подключение сети к конечным системам и интеллектуальная коммутация данных внутри локальной сети

В4 Каково назначение соединительных устройств? (Источник: обзор функций сети)

А) соединение отдельных сетей и фильтрация трафика для передачи данных по наиболее эффективному маршруту
Б) выбор пути, по которому данные отправляются получателю
В) обеспечение средств передачи данных из одной точки сети в другую
Г) подключение сети к конечным системам и интеллектуальная коммутация данных внутри локальной сети

В5 Для какого ресурса невозможно совместное использование в сети? (Источник: обзор функций сети)

А) память
Б) приложения
В) периферийные устройства
Г) устройства хранения

В6 Какие из перечисленных ниже приложений являются общими сетевыми приложениями? (Выберите три варианта.) (Источник: обзор функций сети)

А) электронная почта
Б) совместная работа
В) создание графики
Г) базы данных
Д) текстовые редакторы
Е) электронные таблицы

В7 Сопоставьте каждую характеристику сети с ее определением. (Источник: обзор функций сети)

_____ 1. Скорость

_____ 2. Стоимость

_____ 3. Безопасность

_____ 4. Доступность

_____ 5. Масштабируемость

_____ 6. Надежность

_____ 7. Топология

А) определяет, насколько легко пользователи могут получить доступ к сети
Б) определяет степень надежности сети
В) характеризует уровень защиты самой сети и передаваемых ею данных
Г) определяет скорость передачи данных по сети
Д) определяет, насколько хорошо сеть может удовлетворить потребности большего числа пользователей и требованиям к передаче большего объема данных
Е) определяет структуру сети
Ж) обозначает общую стоимость компонентов, установки и технического обслуживания сети

В8 Какое утверждение относительно физических топологий сети является верным? (Источник: обзор функций сети)

А) Физическая топология определяет способ соединения компьютеров, принтеров, сетевых и прочих устройств.
Б) Существует две основные категории физических топологий: шинные и звездообразные.
В) Физическая топология описывает пути, по которым сигналы передаются из одной точки сети в другую.
Г) Выбор физической топологии в значительной степени определяется типом передаваемых данных.

В9 Какое утверждение относительно логических топологий сети является верным? (Источник: обзор функций сети)

А) Логическая топология определяет способ соединения компьютеров, принтеров, сетевых и прочих устройств.
Б) Логическая топология определяется исключительно типом компьютеров, которые должны быть включены в сеть.
В) Логическая топология описывает пути, по которым сигналы передаются из одной точки сети в другую.
Г) Физическая и логическая топология сети должны совпадать.

В10 Сопоставьте каждый тип топологии с его описанием. (Источник: обзор функций сети)

_____ 1. Все сетевые устройства непосредственно соединены между собой посредством одной линии.

_____ 2. Все сетевые устройства непосредственно соединены с одной центральной точкой и не имеют других соединений между собой.

_____ 3. Все устройства в сети соединены по кругу.

_____ 4. Каждое устройство соединено со всеми остальными устройствами.

_____ 5. По крайней мере одно устройство соединено со всеми другими устройствами.

_____ 6. Эта структура обеспечивает резервирование сети.

А) Звездообразная.
Б) Шинная
В) полносвязная ячеистая
Г) кольцевая
Д) частичносвязная ячеистая
Е) двойная кольцевая

В11 Какие три утверждения о беспроводных сетях наиболее соответствуют действительности? (Выберите два варианта.) (Источник: обзор функций сети)

А) Вместо кабелей в беспроводных соединениях передачи данных используются радиочастотные или инфракрасные волны.
Б) Для получения сигнала от точки доступа на компьютере должна быть установлена беспроводная интерфейсная плата или беспроводной адаптер.
В) Ключевым компонентом беспроводных локальных сетей является маршрутизатор, который служит для распространения сигнала.
Г) Беспроводные сети мало распространены и используются только в крупных корпорациях.

В12 Какова главная опасность в закрытой сети? (Источник: обеспечение безопасности сети)

А) намеренная внешняя атака;
Б) намеренная или случайная внутренняя атака
В) злонамеренное использование со стороны клиентов
Г) злонамеренное использование со стороны сотрудников

В13 Какие два фактора за последнее время вызвали увеличение угроз со стороны хакеров? (Выберите два варианта.) (Источник: обеспечение безопасности сети)

А) Использование инструментов хакеров требует более глубоких технических знаний.
Б) Инструменты хакеров стали более сложными.
В) Число заявленных угроз безопасности остается постоянным из года в год.
Г) Использование инструментов хакеров требует меньших технических знаний.

В14 Какая из следующих четырех атак классифицируется как атака получения доступа? (Источник: обеспечение безопасности сети)

А) атаки посредством подбора пароля;
Б) атаки DDoS;
В) «троянский конь»;
Г) вирус Love Bug

В15 Какие два утверждения о цели модели OSI являются верными? (Выберите два варианта.) (Источник: общие сведения о модели обмена данными между хостами)

А) Эталонная модель OSI определяет функции сети, реализуемые на каждом уровне.
Б) Модель OSI облегчает понимание передачи данных по сети.
В) Многоуровневый подход, используемый в модели OSI, гарантирует надежную доставку данных.
Г) Модель OSI позволяет изменениям на одном уровне влиять на другие уровни.

В16 Сопоставьте каждый уровень OSI с его функцией. (Источник: общие сведения о модели обмена данными между хостами)

_____ 1. Физический

_____ 2. Канальный

_____ 3. Сетевой

_____ 4. Транспортный

_____ 5. Сеансовый

_____ 6. Представительский

_____ 7. Прикладной

А) Обеспечивает связь и выбор пути между двумя хостами, которые могут находиться в сетях, географически удаленных друг от друга.
Б) гарантирует, что сведения, передаваемые на прикладном уровне одной системы, могут быть прочитаны на прикладном уровне другой системы.
В) Определяет формат данных для передачи и способы контроля доступа к сети
Г) Выполняет сегментацию данных от передающего хоста и реорганизацию данных в поток данных на принимающем хосте.
Д) Определяет электрические, механические, процедурные и функциональные характеристики активации, поддержки и отключения физического канала между конечными системами.
Е) Предоставляет сетевые услуги для таких пользовательских приложений, как электронная почта, пересылка файлов и эмуляция терминала.
Ж) Устанавливает и прекращает сеансы между двумя взаимодействующими хостами и осуществляет управление ими, а также синхронизирует диалог между представительскими уровнями двух хостов и управляет обменом данными между ними.

B17 Расположите этапы процесса инкапсуляции данных в правильном порядке. (Источник: общие сведения о модели обмена данными между хостами)

_____ 1. Этап 1.
_____ 2. Этап 2.
_____ 3. Этап 3.
_____ 4. Этап 4.
_____ 5. Этап 5.
_____ 6. Этап 6.
_____ 7. Этап 7.
_____ 8. Этап 8.

А) На представительском уровне к данным добавляется заголовок представительского уровня (заголовок уровня 6). Получившиеся данные передаются на сеансовый уровень.
Б) На сеансовом уровне к данным добавляется заголовок сеансового уровня (заголовок уровня 5). Получившиеся данные передаются на транспортный уровень.
В) На прикладном уровне к пользовательским данным добавляется заголовок прикладного уровня (заголовок уровня 7). Пользовательские данные вместе с заголовком уровня 7 передаются вниз на представительский уровень.
Г) На сетевом уровне к данным добавляется заголовок сетевого уровня (заголовок уровня 3). Получившиеся данные передаются на канальный уровень.
Д) На транспортном уровне к данным добавляется заголовок транспортного уровня (заголовок уровня 4). Получившиеся данные передаются на сетевой уровень.
Е) Приложение передает пользовательские данные на прикладной уровень.
Ж) На канальном уровне к данным добавляется заголовок и метка окончания канального уровня (заголовок и концевая метка уровня 2). Метка окончания уровня 2 обычно представляет собой контрольную последовательность кадра, которая используется получателем для проверки правильности данных. Получившиеся данные передаются на физический уровень.
З) С физического уровня биты данных передаются в среду передачи.

B18 На каком уровне впервые выполняется деинкапсуляция? (Источник: общие сведения о модели обмена данными между хостами)

А) Прикладной
Б) Канальный
В) Сетевой
Г) Транспортный

B19 Сопоставьте каждый уровень и его функцию в обмене данными между равноправными уровнями.
(Источник: общие сведения о модели обмена данными между хостами)

_____ 1. Сетевой уровень
_____ 2. Канальный уровень
_____ 3. Физический уровень

А) Инкапсулирует пакет сетевого уровня в кадр.
Б) Перемещает данные между сетями, инкапсулируя их и добавляя заголовок для создания пакета.
В) Кодирует кадр канального уровня в последовательность битов (1 и 0) для передачи в среде передачи (обычно проводам).

В20 Каково назначение сетевого протокола? (Источник: общие сведения о модели обмена данными между хостами)

А) Использует набор правил, которые сообщают сетевым службам, что необходимо сделать.
Б) Обеспечивает надежную доставку данных.
В) Направляет данные получателю наиболее эффективным способом.
Г) Представляет собой набор функций для идентификации определения данных.

В21 Сопоставьте каждый уровень стека протоколов TCP/IP с его функцией. (Источник: общие сведения о модели обмена данными между хостами)

_____ 1. Предлагает приложения для передачи файлов, поиска и устранения неисправностей сети и работы с Интернетом. Поддерживает сеть.

_____ 2. Определяет форматирование данных для передачи и способы контроля доступа к сети

_____ 3. Определяет электрические, механические, процедурные и функциональные характеристики активации, поддержки и отключения физического канала между конечными системами.

_____ 4. Обеспечивает маршрутизацию данных от источника к месту назначения. Для этого определяется формат пакета и схема адресации, данные перемещаются с канального уровня на транспортный, пакеты данных маршрутизируются на удаленный хост, выполняется фрагментация и восстановление пакетов данных.

_____ 5. Предоставляет услуги обмена данными напрямую приложениям, запущенным на различных хостах в сети.

А) Физический уровень
Б) Канальный уровень
В) Уровень Интернета
Г) Транспортный уровень
Д) Прикладной уровень

В22 Какие компоненты модели OSI и стека протоколов TCP/IP расходятся сильнее всего? (Источник: общие сведения о модели обмена данными между хостами)

А) Сетевой уровень
Б) Транспортный уровень
В) Прикладной уровень
Г) Канальный уровень

В23 Сколько бит содержит IPv4-адрес? (Источник: Общие сведения об уровне Интернета стека протоколов TCP/IP)

А) 16
Б) 32
В) 48
Г) 64
Д) 128

B24 Какие октеты относятся к хостовой части и назначаются локально в адресе класса B? (Источник: общие сведения об уровне Интернета стека протоколов TCP/IP)

А) Локально назначается первый октет.
Б) Локально назначаются первый и второй октеты.
В) Локально назначается второй и третий октеты.
Г) Локально назначается третий и четвертый октеты.

B25 К какому классу относится адрес 172.16.128.17? (Источник: общие сведения об уровне Интернета стека протоколов TCP/IP)

А) Класс A
Б) Класс B
В) Класс C
Г) Класс D

B26 Какое из следующих утверждений о направленном широковещательном адресе верно? (Источник: общие сведения об уровне Интернета стека протоколов TCP/IP)

А) Широковещательный адрес – это адрес, в котором в хостовой части представлены только нули.
Б) Любой IP-адрес в сети может использоваться как широковещательный.
В) Направленный широковещательный адрес – это адрес, в котором в хостовой части представлены только единицы.
Г) Все утверждения неверны.

B27 Какие два из перечисленных ниже адреса являются частными IP-адресами? (Выберите два варианта.) (Источник: общие сведения об уровне Интернета стека протоколов TCP/IP)

А) 10.215.34.124
Б) 127.16.71.43
В) 172.17.10.10
Г) 225.200.15.10

B28 Какие три утверждения относительно протокола IP являются верными? (Выберите три варианта.) (Источник: общие сведения об уровне Интернета стека протоколов TCP/IP)

А) IP является протоколом без установления соединения.
Б) Протокол IP использует относительную адресацию.
В) Протокол IP обеспечивает надежную доставку данных.
Г) Протокол IP функционирует на уровне 2 стека протоколов TCP/IP и модели OSI.
Д) Протокол IP не предлагает функции восстановления.
Е) Протокол IP осуществляет негарантированную доставку данных.

B29 Какие три утверждения о протоколе TCP являются верными? (Выберите три варианта.) (Источник: общие сведения о транспортном уровне стека протоколов TCP/IP)

А) Протокол TCP функционирует на уровне 3 стека протоколов TCP/IP.
Б) TCP является протоколом с установлением соединения.
В) Протокол TCP не обеспечивает проверку ошибок.
Г) Нумерация и упорядочение пакетов TCP позволяет получателю восстановить их порядок и обнаружить отсутствующий пакет.
Д) Протокол TCP не предоставляет услугу по восстановлению информации.
Е) После получения одного или нескольких пакетов TCP получатель отвечает отправителю подтверждением их получения.

В30 Какие характеристики являются общими для протоколов TCP и UDP? (Источник: общие сведения о транспортном уровне стека протоколов TCP/IP)

А) Функционирует на уровне 4 (транспортном) модели OSI и стека протоколов TCP/IP.
Б) Использует выявление ошибок в очень ограниченной форме.
В) Обеспечивает услуги по принципу «наименьших затрат» и не гарантирует доставку пакетов.
Г) Не предоставляет никаких специальных возможностей для восстановления потерянных или поврежденных пакетов.

В31 Если на компьютере с одним IP-адресом одновременно открыто несколько веб-сайтов, это называется _____. (Источник: общие сведения о транспортном уровне стека протоколов TCP/IP)

А) Определение размера окна
Б) Мультиплексирование сеансов
В) Сегментация
Г) Протокол с установлением соединения

В32 Для каких двух из перечисленных ниже приложений оптимален протокол TCP? (Выберите два варианта.) общие сведения о транспортном уровне стека протоколов TCP/IP)

А) Электронная почта
Б) Передача голосовых данных
В) Загрузка файлов
Г) Потоковое видео

В33 Какие три из перечисленных ниже характеристик относятся к протоколу UDP? (Выберите три варианта.) (Источник: общие сведения о транспортном уровне стека протоколов TCP/IP)

А) Пакеты обрабатываются независимо.
Б) Доставка пакетов гарантирована.
В) Доставка пакетов не гарантирована.
Г) Потерянные или поврежденные пакеты данных не посылаются повторно.

В34 Какие две из перечисленных ниже характеристик относятся к протоколу TCP? (Выберите два варианта.) (Источник: общие сведения о транспортном уровне стека протоколов TCP/IP)

А) Доставка пакетов не гарантирована.
Б) Потерянные или поврежденные пакеты данных не посылаются повторно.
В) Потерянные или поврежденные пакеты данных посылаются повторно.
Г) Сегмент TCP содержит последовательный номер и номер подтверждения.

В35 Какой вид портов используется проприетарными приложениями? (Источник: общие сведения о транспортном уровне стека протоколов TCP/IP)

А) Динамические порты
Б) Известные порты
В) Зарегистрированные порты

В36 Порты, используемые только в течение определенного сеанса, – это _____. (Источник: общие сведения о транспортном уровне стека протоколов TCP/IP)

А) Динамические порты
Б) Известные порты
В) Зарегистрированные порты

В37 Порт источника в заголовках UDP и TCP – это _____. (Источник: общие сведения о транспортном уровне стека протоколов TCP/IP)

А) 16-битный номер вызываемого порта
Б) 16-битная длина заголовка
В) 16-битная сумма заголовка и полей данных
Г) 16-битный номер вызывающего порта

В38 Какое поле в заголовке TCP обеспечивает правильный порядок поступления данных? (Источник: общие сведения о транспортном уровне стека протоколов TCP/IP)

А) Номер подтверждения
Б) Номер последовательности
В) Резервное поле
Г) Параметры

В39 Какое сообщение отправляет инициирующее устройство при установлении соединения TCP? (Источник: общие сведения о транспортном уровне стека протоколов TCP/IP)

А) ACK
Б) получает SYN
В) отправляет SYN

В40 Функции подтверждения и определения размера окна являются двумя формами _____. (Источник: общие сведения о транспортном уровне стека протоколов TCP/IP)

А) Управления потоком
Б) Соединения TCP
В) Упорядочения сегментов TCP
Г) Надежных соединений

В41 Какая из следующих услуг обеспечивается функцией определения размера окна? (Источник: общие сведения о транспортном уровне стека протоколов TCP/IP)

А) Отправитель может выполнять мультиплексирование.
Б) Получатель может иметь незавершенные подтверждения.
В) Получатель может выполнять мультиплексирование.
Г) Отправитель может передавать заданное число сегментов без подтверждения.

В42 Где содержатся номер последовательности и номер подтверждения? (Источник: общие сведения о транспортном уровне стека протоколов TCP/IP)

А) Заголовок протокола UDP
Б) Заголовок протокола TCP
В) Начальный последовательный номер
Г) Прикладной уровень

В43 Какая организация отвечает за стандарты Ethernet? (Источник: общие сведения об Ethernet)

А) ISO
Б) IEEE
В) EIA
Г) IEC

В44 Какие три из указанных характеристик относятся к Ethernet 802.3? (Выберите три варианта.) (Источник: общие сведения об Ethernet)

А) Основан на процессе CSMA/CD.
Б) Является стандартом, который был заменен стандартом Ethernet II.
В) Определяет физический уровень (уровень 1).
Г) Разработан в середине 1970-х годов.
Д) Определяет подуровень MAC канального уровня (уровня 2).
Е) Известен также как «толстый» Ethernet.

В45 Какое утверждение об адресе Ethernet является верным? (Источник: общие сведения об Ethernet)

А) Адрес, используемый в локальной сети Ethernet, направляет данные нужному получателю.
Б) Адрес источника – 4-байтовый шестнадцатеричный адрес сетевого адаптера компьютера, создавшего пакет данных.
В) Адрес назначения – 8-байтовый шестнадцатеричный адрес сетевого адаптера в локальной сети, в которую передается пакет данных.
Г) Адреса источника и назначения состоят из 6-байтового шестнадцатеричного номера.

В46 Какое утверждение о MAC-адресе является точным? (Источник: общие сведения об Ethernet)

А) MAC-адрес представляет собой число в шестнадцатеричном формате, физически записанное на сетевом адаптере.
Б) MAC-адрес отображается в виде шестнадцатеричных цифр, сгруппированных попарно.
В) Устройство в локальной сети не обязательно должно иметь уникальный MAC-адрес, чтобы работать в сети.
Г) Изменение MAC-адреса невозможно.

В47 Какое утверждение о сетевых адаптерах является верным? (Источник: подключение к локальной сети Ethernet)

А) Сетевой адаптер вставляется в порт USB и предоставляет порт для подключения к сети.
Б) Сетевой адаптер взаимодействует с сетью через последовательное подключение, а с компьютером – через параллельное подключение.
В) Сетевой адаптер взаимодействует с сетью через параллельное подключение, а с компьютером – через последовательное подключение.
Г) Сетевой адаптер также называется адаптером коммутатора.

B48 Какова минимальная категория UTP для Ethernet 1000BASE-T? (Источник: подключение к локальной сети Ethernet)

А) Категория 3
Б) Категория 4
В) Категория 5
Г) Категория 5e

B49 Сопоставьте категории UTP и среды, в которых они получили наибольшее распространение. (Источник: подключение к локальной сети Ethernet)

_____ 1. Категория 1

_____ 2. Категория 2

_____ 3. Категория 3

_____ 4. Категория 4

_____ 5. Категория 5

_____ 6. Категория 5e

_____ 7. Категория 6

А) Предназначена для передачи данных со скоростями до 100 Мбит/с.
Б) Применяется в сетях, работающих со скоростями до 1000 Мбит/с (1 Гбит/с).
В) Состоит из четырех пар медных жил диаметром 24 AWG (0,51 мм), способных обеспечивать передачу данных со скоростями до 1000 Мбит/с.
Г) Предназначена для телефонных коммуникаций и непригодна для передачи данных.
Д) Используется в сетях Token Ring (скорость передачи до 16 Мбит/с).
Е) Предназначена для передачи данных со скоростями до 4 Мбит/с.
Ж) Применяется в сетях 10BASE-T и предназначена для передачи данных со скоростями до 10 Мбит/с.

B50 Какие три характеристики относятся к UTP? (Выберите три варианта.) (Источник: подключение к локальной сети Ethernet)

А) Кабель UTP представляет собой восемь пар проводников.
Б) Каждый отдельный медный провод в кабеле UTP изолирован.
В) Проводники в каждой паре скручены между собой.
Г) Затухание сигнала в результате электромагнитных и радиочастотных помех ограничено.
Д) Существует семь категорий кабеля UTP.

Ответы на вопросы для самопроверки по модулю

В1	А, Б, В
В2	А
В3	Г
В4	В
В5	А
В6	А, Б, Г
В7	1 = Г, 2 = Ж, 3 = В, 4 = А, 5 = Д, 6 = Б, 7 = Е
В8	А
В9	В
В10	1 = Б , 2 = А , 3 = Г, 4 = В, 5 = Д , 6 = Е
В11	А, Б
В12	Б
В13	Б, Г
В14	А
В15	А, Б
В16	1 = Д, 2 = В, 3 = А, 4 = Г, 5 = Ж, 6 = Б, 7 = Е
В17	1 = Е, 2 = В, 3 = А, 4 = Б, 5 = Д, 7 = Г, 7 = Ж, 8 = З
В18	Б
В19	1 = Б, 2 = А, 3 = В
В20	А
В21	1 = Д, 2 = Б, 3 = А, 4 = В, 5 = Г
В22	Г
В23	Б
В24	Г
В25	Б
В26	В
В27	Б, В
В28	А, Д, Е
В29	Б, Г, Е
В30	А
В31	Б
В32	А, В
В33	А, В, Г
В34	В, Г
В35	В

B36	А
B37	Г
B38	Б
B39	В
B40	А
B41	Г
B42	Б
B43	Б
B44	А, Г, Д
B45	Г
B46	А
B47	Б
B48	Г
B49	1 = Г, 2 = Е, 3 = Ж, 4 = Д, 5 = А, 6 = Б, 7 = В
B50	Б, В, Д

Модуль 2

ЛВС Ethernet

Обзор

В этом модуле описываются различные виды топологий локальных сетей, проблемы, связанные с разделяемыми локальными сетями, методы решения этих проблем с помощью технологии коммутируемых локальных сетей, а также способы оптимизации локальных сетей.

Задачи модуля

По окончании этого модуля вы научитесь расширять сеть Ethernet посредством концентратора. Это значит, что вы сможете выполнять следующие задачи:

- описывать проблемы, связанные с увеличением трафика в локальной сети Ethernet;
- определять решения проблем сетей Ethernet на основе технологии коммутируемых локальных сетей;
- описывать процессы передачи пакетов данных между хостами через коммутатор;
- описывать функции и возможности интерфейса командной строки ПО Cisco IOS;
- запускать коммутатор уровня доступа и использовать интерфейс командной строки для настройки и проверки работы коммутатора;
- активировать функции безопасности на физическом уровне, уровне доступа и на уровне порта;
- перечислять способы оптимизации локальной сети Ethernet;
- описывать способы решения проблем, связанных с коммутатором.

Занятие 1

Общие сведения о проблемах разделяемых локальных сетей

Обзор

Локальные вычислительные сети (ЛВС) – это относительно дешевое средство, обеспечивающее общий доступ к дорогим ресурсам. ЛВС позволяют нескольким пользователям в относительно небольшом географическом районе обмениваться файлами и сообщениями, а также получать доступ к общим ресурсам, например файловым серверам. ЛВС быстро развились в системы поддержки, которые играют важнейшую роль в обмене информацией в пределах организации. В этом занятии описываются проблемы, с которыми сталкиваются ЛВС при увеличении роста требований к полосе пропускания и скорости передачи для удовлетворения потребностей большого количества пользователей.

Задачи

По окончании этого занятия вы сможете выявлять проблемы, связанные с увеличением трафика в ЛВС Ethernet. Это значит, что вы сможете выполнять следующие задачи:

- определять сегменты ЛВС Ethernet и их ограничения по расстоянию;
- перечислять характеристики и функции концентратора в ЛВС Ethernet;
- определять коллизии в ЛВС и условия, при которых они возникают;
- определять домены коллизий в ЛВС Ethernet.

Сегменты ЛВС Ethernet

Длина сегмента – это важная характеристика при использовании технологии Ethernet в ЛВС. В этом разделе описываются сегменты и их ограничения.

Сегмент – это сетевое соединение по отдельному непрерывному сетевому кабелю. Кабели и сегменты Ethernet могут действовать на ограниченном расстоянии, за пределами которого передача данных ухудшается из-за шумов в линии, ослабления уровня сигнала и несоответствия требованиям множественного доступа с контролем несущей и обнаружением коллизий (CSMA/CD) для обнаружения коллизий. Тип кабеля, скорость передачи данных и метод модуляции влияют на максимальную длину сегмента.

Любое устройство, которое работает на уровне 1 модели взаимодействия открытых систем (OSI), не ограничивает сегмент Ethernet ЛВС, так как устройства уровня 1 только повторяют электрические сигналы.

Для каждой спецификации Ethernet определен необходимый тип кабеля, скорость передачи данных и метод модуляции, которые в свою очередь определяют максимальную длину сегмента, как указано в таблице.

Ниже приведены правила для стандарта 10BASE-T (Ethernet по витой паре):

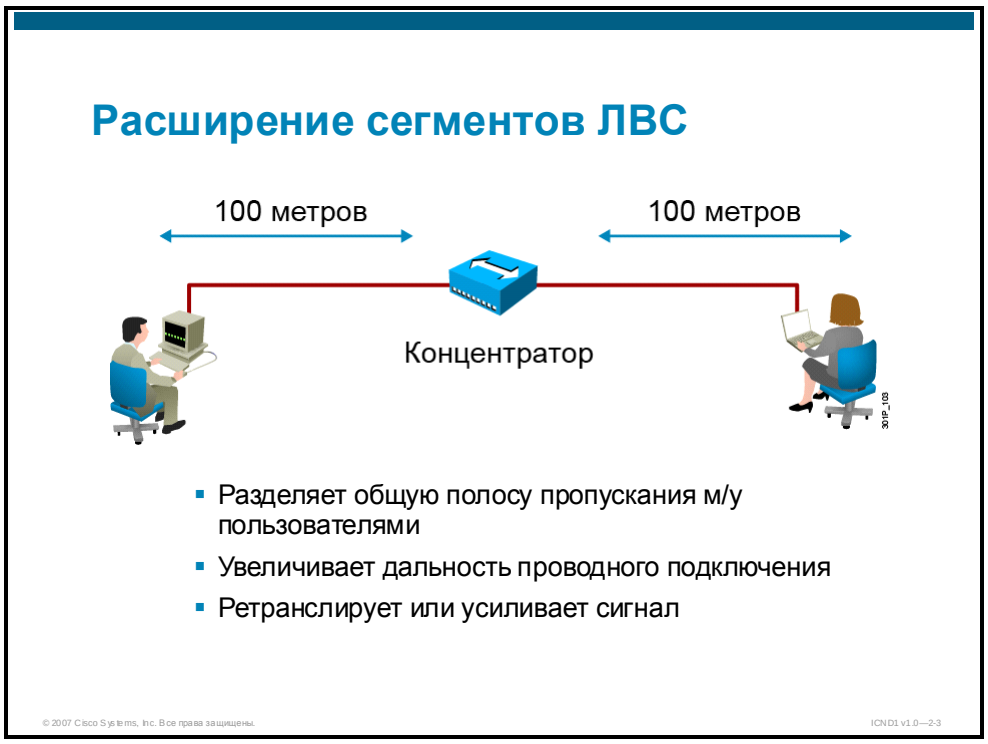
- число 10 обозначает поддерживаемую скорость, в данном случае 10 Мбит/с.
- Слово BASE (ОСНОВНОЙ) означает, что Ethernet работает по основной полосе частот.
- Буква «T» означает витую пару.
- FL означает использование волоконно-оптического кабеля.

Ограничения сегментов Ethernet по расстоянию

Спецификация Ethernet	Описание	Длина сегмента
10BASE-T	Ethernet, 10 Мбит/с, по витой паре	100 м
10BASE-FL	Ethernet, 10 Мбит/с, по волоконно-оптическому кабелю	2 000 м
100BASE-TX	Ethernet, 100 Мбит/с, по витой паре	100 м
100BASE-FX	Fast Ethernet, по волоконно-оптическому кабелю.	400 м
1000BASE-T	Gigabit Ethernet, по витой паре	100 м
1000BASE-LX	Gigabit Ethernet, по волоконно-оптическому кабелю.	550 м для носителя толщиной 62,5 микрона (с многомодовым волоконно-оптическим кабелем µ или 50-µ; 10 км с одномодовым волоконно-оптическим кабелем 10-µ)
1000BASE-SX	Gigabit Ethernet, по волоконно-оптическому кабелю.	250 м по многомодовому волоконно-оптическому кабелю 62,5-µ; 550 м по многомодовому волоконно-оптическому кабелю 50-µ
1000BASE-CX	Gigabit Ethernet по медному кабелю	25 м

Увеличение длины сегмента ЛВС

К ЛВС Ethernet можно добавлять устройства для увеличения длины сегмента. В этом разделе описывается решение проблемы ограничения по расстоянию в ЛВС Ethernet путем добавления повторителей и концентраторов.



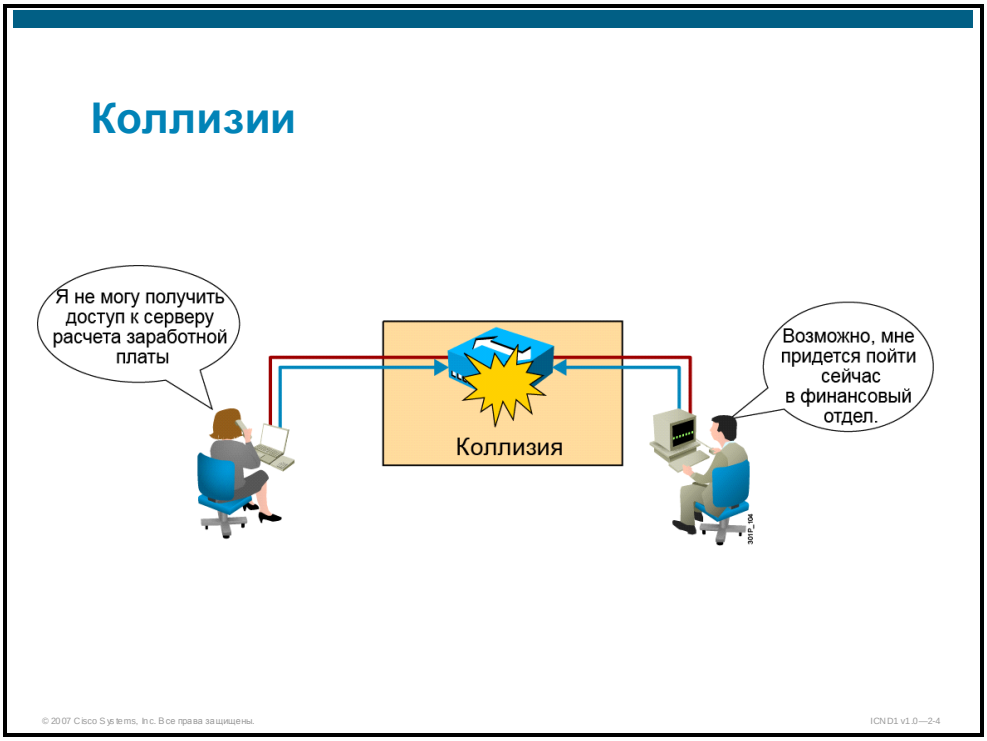
Повторитель – это устройство физического уровня, которое принимает сигнал от устройства в сети и действует как усилитель. Добавление повторителей в сеть увеличивает длину сегментов и позволяет передавать данные на большее расстояние. Однако существует ограничение по количеству повторителей, которые можно добавить в сеть.

Концентратор, который также работает на физическом уровне, аналогичен повторителю. Когда концентратор получает сигнал, он усиливает сигнал и ретранслирует его. Однако в отличие от повторителя концентратор может иметь несколько портов для подключения нескольких сетевых устройств. Поэтому концентратор ретранслирует сигнал на каждый порт, к которому подключена рабочая станция или сервер. Концентраторы не анализируют проходящие через них данные и не знают об источнике или получателе кадра. По существу концентратор просто получает входящие биты, усиливает электрический сигнал и передает эти биты через все свои порты на другие устройства в сети.

Концентратор удлиняет, но не ограничивает ЛВС Ethernet. Ограничение технологии общего доступа по полосе пропускания остается. Хотя у каждого устройства есть собственный кабель, который подключается к концентратору, все пользователи того или иного сегмента Ethernet конкурируют за одну и ту же полосу пропускания.

Коллизии

Коллизии – это часть рабочего процесса Ethernet, которые возникают, когда две станции пытаются передать данные одновременно. В этом занятии описывается возникновение коллизий в ЛВС.



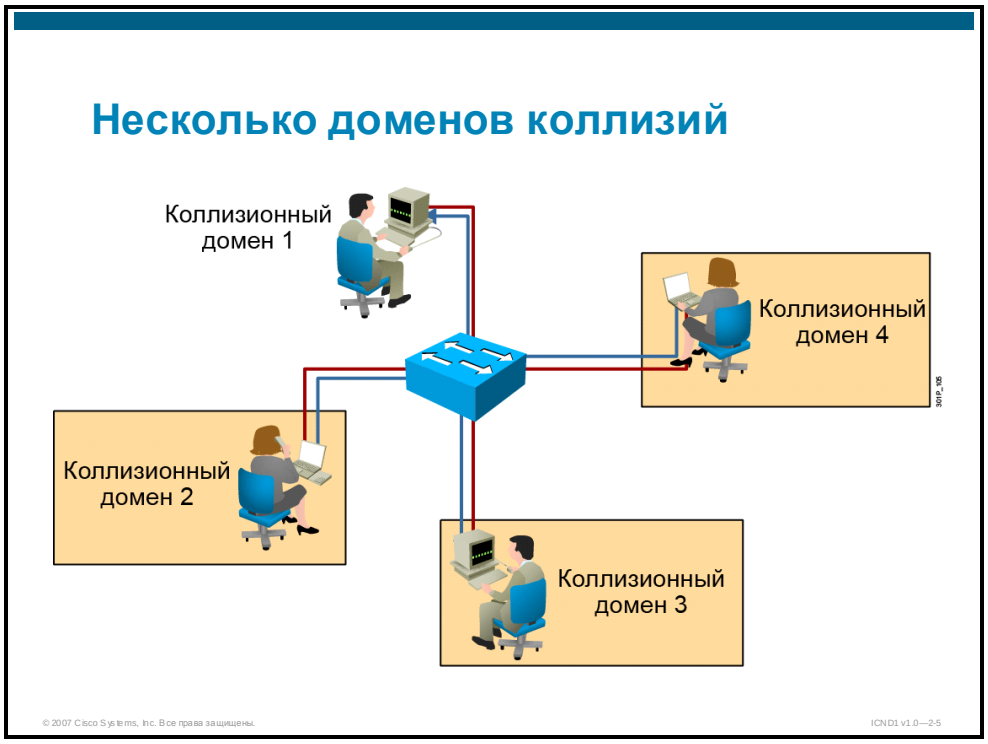
Коллизии – это побочное явление метода CSMA/CD, используемого в Ethernet. В сети Ethernet несколько устройств совместно используют один сегмент. Несмотря на то что станции прослушивают, свободен ли канал передачи, они могут пытаться передавать данные одновременно. Если две или более станций одновременно передают данные по общему каналу, происходит коллизия, и кадры разрушаются. Когда передающие станции выявляют коллизию, они передают специальный сигнал «jam» в течение определенного промежутка времени, в результате чего устройства в сегменте узнают, что кадр был поврежден, и прекращают обмен данными. Затем передающие станции запускают случайный таймер, который откладывает повторную передачу данных.

По мере увеличения сетей (количества станций) и возрастания потребления полосы пропускания, повышается вероятность того, что станции будут пытаться передавать данные одновременно, и произойдет коллизия. Чем больше коллизий, тем больше перегрузка и тем больше вероятность того, что сеть будет работать медленнее или не будет работать вовсе.

Добавление концентратора в ЛВС Ethernet может решить проблему ограничения по расстоянию, на которое может передаваться кадр до ослабления сигнала, но концентраторы не решают проблему коллизий.

Домены коллизий

При увеличении ЛВС Ethernet для поддержки работы большего числа пользователей с более высокими требованиями к полосе пропускания можно создавать отдельные физические сегменты сети, которые называются доменами коллизий. В результате коллизии ограничиваются отдельным доменом и не распространяются на всю сеть. В этом разделе описываются домены коллизий.



В традиционных сегментах Ethernet сетевые устройства конкурируют за общую полосу пропускания и только одно устройство может передавать данные в тот или иной момент времени. Сегменты сети, которые пользуются общей полосой пропускания, называются доменами коллизий, так как если два или более устройств в пределах этого сегмента пробуют передать данные одновременно – возникает коллизия.

Однако можно использовать другие сетевые устройства, работающие на уровне 2 и выше модели взаимодействия открытых систем для разделения сети на сегменты и уменьшения количества устройств, конкурирующих за полосу пропускания. В этом случае каждый новый сегмент становится новым доменом коллизий. Полоса пропускания, доступная устройствам в сегменте, и коллизии в одном домене не мешают работе других сегментов.

Широковещательный домен – еще одна ключевая концепция. Фильтрация кадров на основе MAC-адресов на коммутаторах *не* распространяется на фильтрацию широковещательных кадров. По своей природе широковещательные кадры *должны* пересылаться, поэтому набор соединенных коммутаторов создает отдельный широковещательный домен. Требуется элемент уровня 3, например маршрутизатор, чтобы ограничить широковещательный домен уровня 2.

Резюме

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

Резюме

- Сегмент – это сетевое соединение по отдельному непрерывному сетевому кабелю. Кабели и сегменты Ethernet могут охватывать ограниченное физическое расстояние, за пределами которого качество передачи ухудшается.
- Концентратор расширяет сетевые сегменты, принимая входящие биты, усиливая электрический сигнал и передавая биты данных через все порты на другие устройства в сети.
- Если две или более станции внутри одного сегмента передают данные одновременно, возникает коллизия.

Резюме (прод.)

- Сегменты сети, которые пользуются общей полосой пропускания, называются доменами коллизий, так как если два или более устройств в пределах этого сегмента пробуют передавать данные одновременно – возникает коллизия.
- Кроме того, можно использовать другие сетевые устройства, работающие на уровне 2 (или выше) модели OSI для разделения сети на сегменты и уменьшения количества устройств, конкурирующих за полосу пропускания в отдельно взятом сегменте. Это обеспечивает устройствам в сегменте большую полосу пропускания.

Занятие 2

Решение проблем сети путем применения технологии коммутируемых ЛВС

Обзор

По мере роста нагрузки на ЛВС действуют несколько факторов, которые ухудшают производительность сети. Процессоры современных ПК легко выполняют более 5 000 миллионов операций в секунду (MIPS), а самые новые – более 50 000 MIPS. Более быстрые процессоры увеличивают потребность в сетевых ресурсах. Для удовлетворения этой потребности требуются более быстрые соединения. При этом возникает ряд проблем. Технология коммутации предлагает решение этих проблем. Добавление мостов и коммутаторов в сеть может повысить ее скорость и эффективность за счет уменьшения перегрузки и увеличения полосы пропускания. В этом занятии описывается, как технология коммутации способствует повышению эффективности сетей.

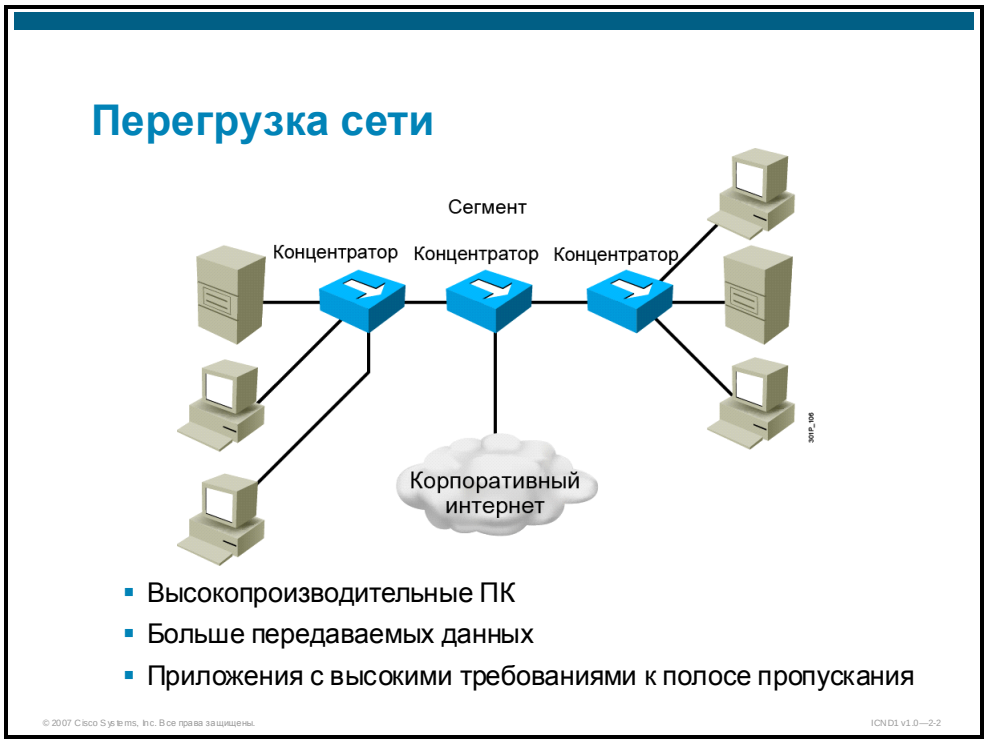
Задачи

По окончании этого занятия вы сможете находить решения проблем Ethernet с помощью технологии коммутируемых ЛВС. Это значит, что вы сможете выполнять следующие задачи:

- выявлять типовые причины перегрузки сети Ethernet;
- перечислять характеристики и функции моста, снижающие нагрузку на сеть;
- перечислять характеристики и функции коммутатора;
- сравнивать производительность коммутатора с производительностью моста;
- перечислять три функции коммутатора;
- описывать принцип работы коммутации;
- описывать, как современные ЛВС используют технологию коммутации.

Стандартные причины возникновения перегрузки в сети

Подобно быстро растущему городу, испытывающему проблему пробок на дорогах, сети сталкиваются с проблемой перегрузки по мере роста. В этом разделе описываются наиболее распространенные причины перегрузки сети.

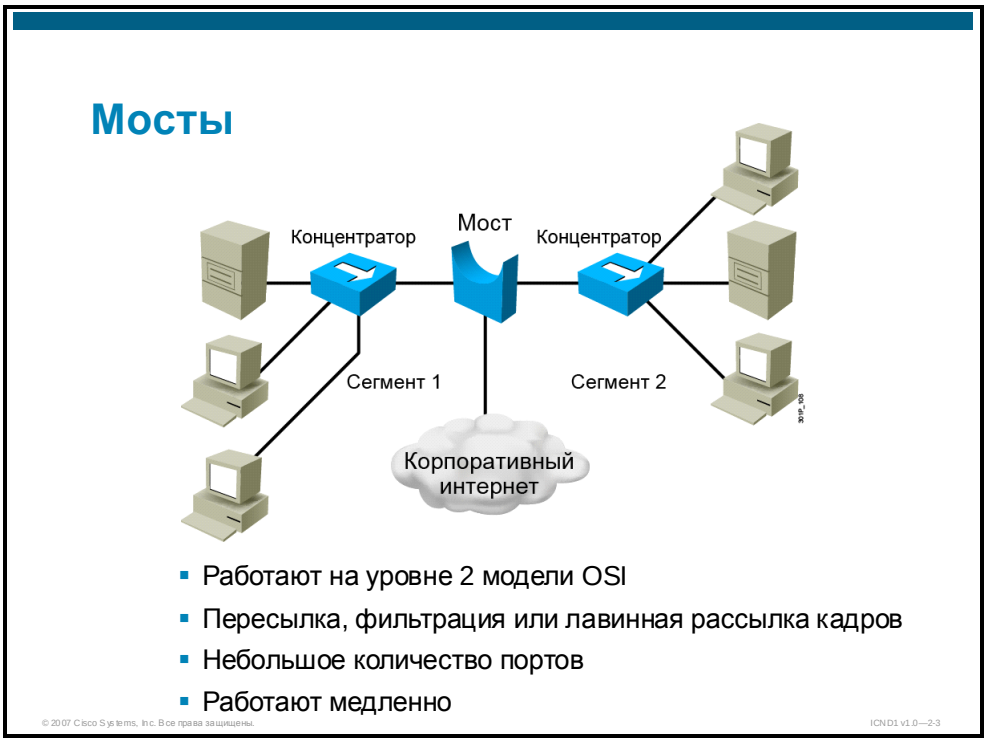


Наиболее распространенные причины перегрузки сети:

- **Рост вычислительной мощности компьютерных и сетевых технологий.** Современные ЦП, шины и периферийные устройства намного быстрее и мощнее, чем те, что использовались в первых ЛВС, поэтому они могут передавать по сети больше данных с более высокой скоростью.
- **Увеличивающийся объем сетевого трафика.** Передача данных по сети используется все чаще, поскольку для выполнения стандартных задач необходимы удаленные ресурсы. Кроме того, широковещательные сообщения могут неблагоприятно повлиять на производительность конечной станции и сети, хотя протоколы TCP/IP, в целом, нечасто используют широковещательную рассылку.
- **Приложения с высокими требованиями к полосе пропускания.** Приложения приобретают все больше функциональных возможностей и требуют все большей пропускной способности для нормальной работы. Настольная издательская система, техническое проектирование, видео по запросу (VoD), электронное обучение и потоковое видео – все эти приложения требуют высокой вычислительной мощности и скорости передачи. Управление передачей файлов этих приложений значительно увеличивает нагрузку на сети и требует совместного использования приложений пользователями.

Мосты – раннее решение проблемы перегрузки сети

Сегментация на уровне 2 модели взаимодействия открытых систем (OSI) может уменьшить перегрузку, и мосты стали первым средством такой сегментации. В этом разделе описывается, как мосты снижают перегрузки сети.



Мосты Ethernet используются для разделения локальной сети Ethernet на несколько сегментов. Это увеличивает количество доменов коллизий, что позволяет сократить перегрузку сети.

Некоторые важнейшие характеристики мостов:

- мосты работают на уровне 2 модели OSI;
- мосты более «разумны», чем концентраторы, они могут анализировать входящие кадры и пересылать (или удалять) их в зависимости от информации об адресе;
- мосты могут буферизовать кадры между двумя или более сегментами ЛВС;
- мосты увеличивают число доменов коллизий, позволяя сразу нескольким устройствам передавать данные, не вызывая коллизий;
- мосты ведут таблицы MAC-адресов.

Добавление мостов в сеть дает множество преимуществ, в том числе:

- изоляция потенциальных проблем сети внутри отдельных сегментов;
- минимизация ненужного сетевого трафика путем фильтрации кадров данных внутри сегментов ЛВС или между ними;
- расширение ЛВС на большие расстояния путем объединения нескольких сегментов.

Коммутаторы

Во многом схожие с мостами, сетевые коммутаторы обладают особыми характеристиками, которые делают их эффективным средством снижения перегрузки сетей. В этом разделе описываются характеристики коммутаторов.

Подобно мостам коммутаторы соединяют сегменты ЛВС, используют таблицу MAC-адресов, чтобы определить сегмент для передачи данных, и снижают объемы сетевого трафика. Однако коммутаторы работают на гораздо более высоких скоростях, чем мосты, и предлагают более совершенные функциональные возможности.

- **Высокая плотность портов.** По сравнению с мостами коммутаторы обладают более высокой плотностью портов. Достаточно распространены коммутаторы с 24 и 48 портами со скоростями 10 Мбит/с и 100 Мбит/с. Коммутаторы на крупных предприятиях могут поддерживать сотни портов.
- **Большие объемы буферов кадров.** Возможность сохранять больше принимаемых кадров перед их передачей весьма полезна, особенно если порты, серверы и другие элементы сети перегружены.
- **Скорости портов.** В зависимости от стоимости коммутатора возможна поддержка носителей с разными скоростями. Скорее всего будут доступны порты со скоростью 10 Мбит/с и 100 Мбит/с, порты 1 Гбит/с или 10 Гбит/с обеспечивают бóльшую гибкость.
- **Быстрая внутренняя коммутация.** Быстрая внутренняя коммутация обеспечивает поддержку нескольких портов 10 Мбит/с, 100 Мбит/с и 1 000 Мбит/с. Для этого может использоваться высокоскоростная внутренняя шина или общая память, которая влияет на всю работу коммутатора.

Коммутаторы используют один из следующих методов пересылки для коммутации данных между сетевыми портами.

- **Коммутация без буферизации кадров.** При использовании этого метода коммутатор обрабатывает данные, как только они начинают поступать, даже если передача не закончена. Коммутатор определяет, на какой порт необходимо передать данные, и начинает процесс передачи без буферизации данных, принимая решение на основе первого полученного кадра. Это наиболее быстрый из методов, но в этом методе не выполняется выявление ошибок, и нельзя гарантировать точность данных. Одним из вариантов коммутации без буферизации кадров является бесфрагментная коммутация, при которой кадр не передается, пока не исчезнет сама возможность коллизии.
- **Коммутация с буферизацией пакетов.** В этом методе коммутатор сохраняет данные в буферах при их получении до момента, пока не будет получен весь кадр. Во время сохранения коммутатор анализирует кадр, чтобы получить информацию о его адресате. В рамках этого процесса коммутатор также выполняет определение ошибок.
- **Бесфрагментная коммутация.** Коммутация без буферизации кадров обеспечивает малое время задержки. Однако в этом случае возможна пересылка поврежденных кадров. Коммутатор должен начать пересылку кадра прежде, чем сможет убедиться в отсутствии коллизии. Бесфрагментная коммутация гарантирует, что было принято достаточное количество байтов, чтобы обнаружить коллизию до передачи кадра.

Бесфрагментная коммутация может быть компромиссом между большим временем задержки и повышенной целостностью коммутации с буферизацией и пересылкой с небольшим временем задержки и пониженной целостностью коммутации без буферизации пакетов. На практике разница между коммутацией с буферизацией и без буферизации пакетов не важна, потому что несущественное уменьшение времени задержки при коммутации без буферизации пакетов компенсируется малым джиттером (колебаниями времени ожидания) при коммутации с буферизацией.

Сравнение коммутаторов и мостов

Во многом схожие с мостами, сетевые коммутаторы обладают особыми характеристиками, которые делают их эффективным средством снижения перегрузки сетей за счет увеличения фактической полосы пропускания. В этом разделе описываются сходства и различия коммутаторов и мостов.

Схожесть мостов и коммутаторов.

- И мосты, и коммутаторы соединяют сегменты ЛВС.
- И мосты, и коммутаторы используют таблицу MAC-адресов для идентификации сегмента, в который нужно переслать кадр с данными.
- И мосты, и коммутаторы помогают уменьшить сетевой трафик.

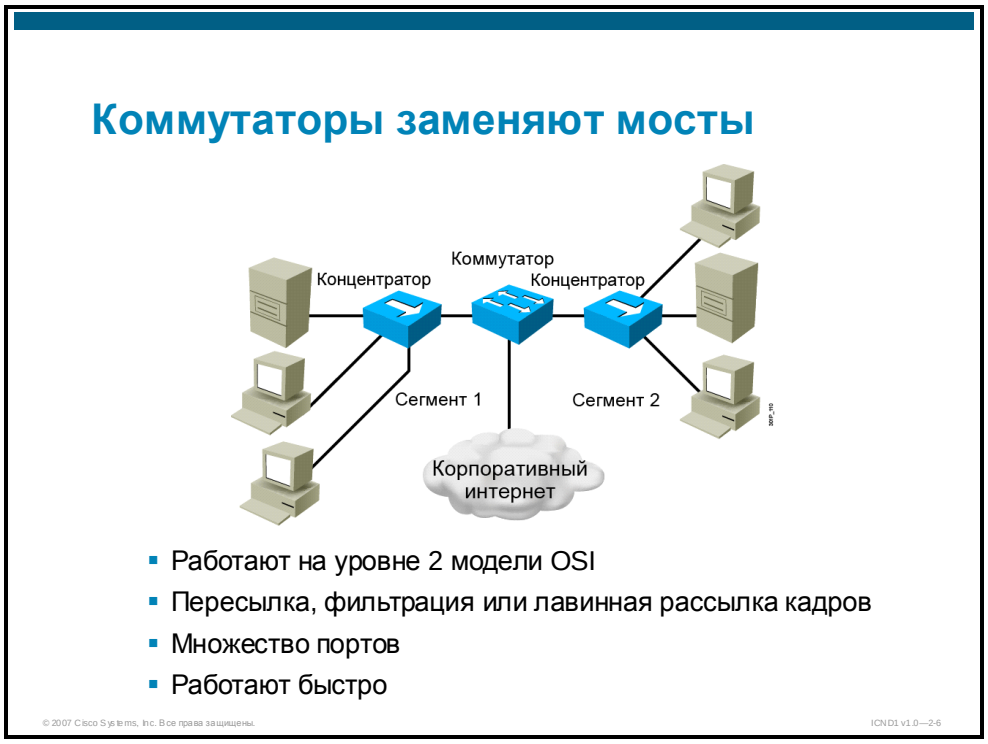
Однако коммутаторы предлагают следующие важные функции, которые обеспечивают дополнительные преимущества для устранения перегрузки сети.

- **Выделенный канал связи между устройствами.** Это увеличивает пропускную способность канала. Коммутаторы с наличием одного пользователя на порт выполняют микросегментацию сети. При таком типе конфигурации каждый пользователь получает доступ ко всей полосе пропускания и не должен конкурировать за доступную полосу пропускания с другими пользователями. В результате коллизии не возникают.

- **Многократные одновременные сеансы связи.** Многократные одновременные сеансы связи обеспечиваются путем одновременной пересылки или коммутации нескольких пакетов, что увеличивает полосу пропускания сети в соответствии с числом поддерживаемых сеансов связи. Например, когда кадры пересылаются между портами 1 и 2, другой сеанс связи может иметь место между портами 5 и 6. Это возможно из-за буферов ввода-вывода и быстрой внутренней передачи между портами. О коммутаторе, который может одновременно поддерживать все варианты передачи кадров между всеми портами, говорят, что он предлагает незаблокированную производительность со скоростью, соответствующей среде передачи данных. Конечно, этот класс коммутаторов относительно дорог.
- **Полнодуплексная система связи.** После того как подключение микросегментировано, в нем участвуют только два хоста (коммутатор и хост). Теперь можно настроить порты так, чтобы они могли получать и отправлять данные в одно и то же время. Это называется дуплексной связью. Например, соединения 100 Мбит/с типа «точка-точка» обладают скоростью передачи 100 Мбит/с и скоростью приема 100 Мбит/с, что обеспечивает эффективную полосу пропускания 200 Мбит/с на одном соединении. Конфигурация между полудуплексом и дуплексом автоматически согласуется во время создания канала. (Полудуплекс означает, что в отдельно взятый момент времени передача данных идет только в одном направлении.)
- **Адаптация к скорости среды.** Сетевой коммутатор с портами разных скоростей может автоматически выбирать между значениями 10 и 100 Мбит/с *или* между 100 и 1 000 Мбит/с, что позволяем автоматически выбирать полосу пропускания при необходимости. Без этой функции одновременная работа портов с разными скоростями была бы невозможна.

Как коммутаторы сегментируют сеть Ethernet

Коммутаторы заменили и вытеснили мосты. Коммутаторы выполняют три главные функции в сегментации сети Ethernet: пересылка, фильтрация и лавинная рассылка. В этом разделе описываются главные функции коммутаторов.



Коммутаторы формируют таблицу MAC-адресов, связанную с доступными портами. Затем коммутаторы используют эти MAC-адреса при принятии решения о дальнейших операциях над кадрами – фильтрация, пересылка или лавинная рассылка.

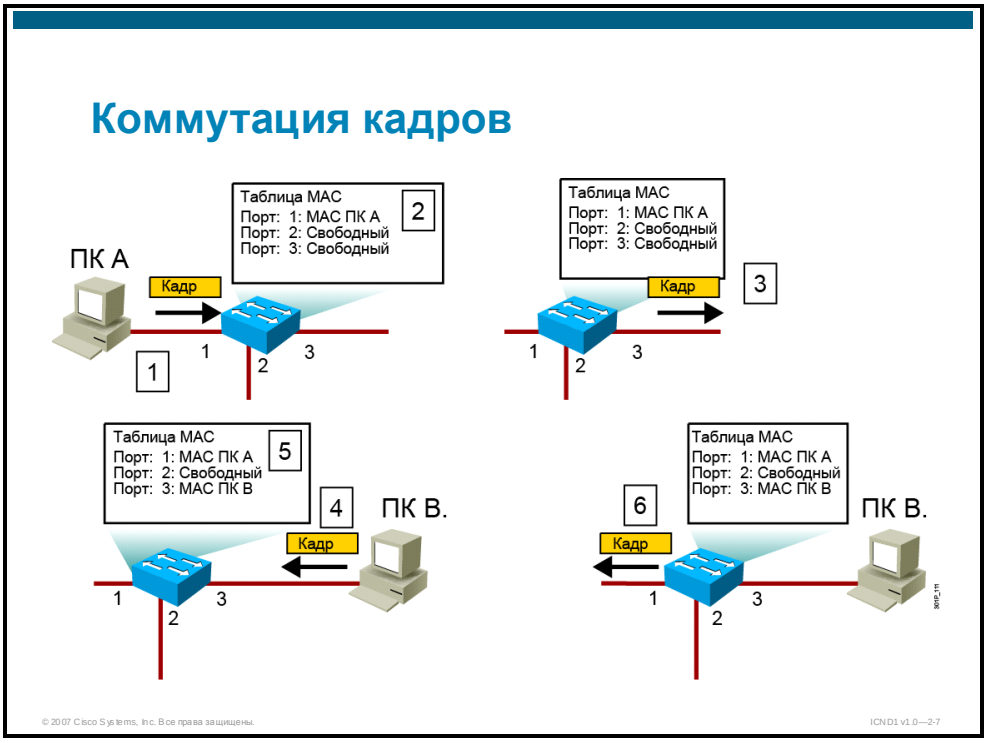
В таблице показано, как коммутаторы обрабатывают индивидуальные кадры.

Как коммутаторы обрабатывают индивидуальные кадры ЛВС Ethernet

№	Действие
1.	Когда порт принимает индивидуальный кадр, коммутатор сравнивает MAC-адрес назначения с адресами в таблицах.
2.	Если коммутатор решает, что MAC-адрес назначения кадра находится в том же сегменте сети, что и источник, он не пересылает кадр. Этот процесс называется фильтрацией, и с его помощью коммутаторы могут значительно уменьшить трафик между сегментами сети путем ликвидации ненужных кадров.
3.	Если коммутатор решает, что MAC-адрес назначения кадра находится в другом сегменте, он пересылает кадр в соответствующий сегмент.
4.	Если коммутатор *не* имеет записи адреса назначения, он передаст кадр всем портам, за исключением того, с которого кадр был получен. Это называется лавинной рассылкой (flooding).

Коммутация в действии

Коммутатор решает, как обработать кадр данных, используя таблицу MAC-адресов. В этом разделе описывается процесс на основе MAC-адресов, в ходе которого кадры передаются через коммутатор.



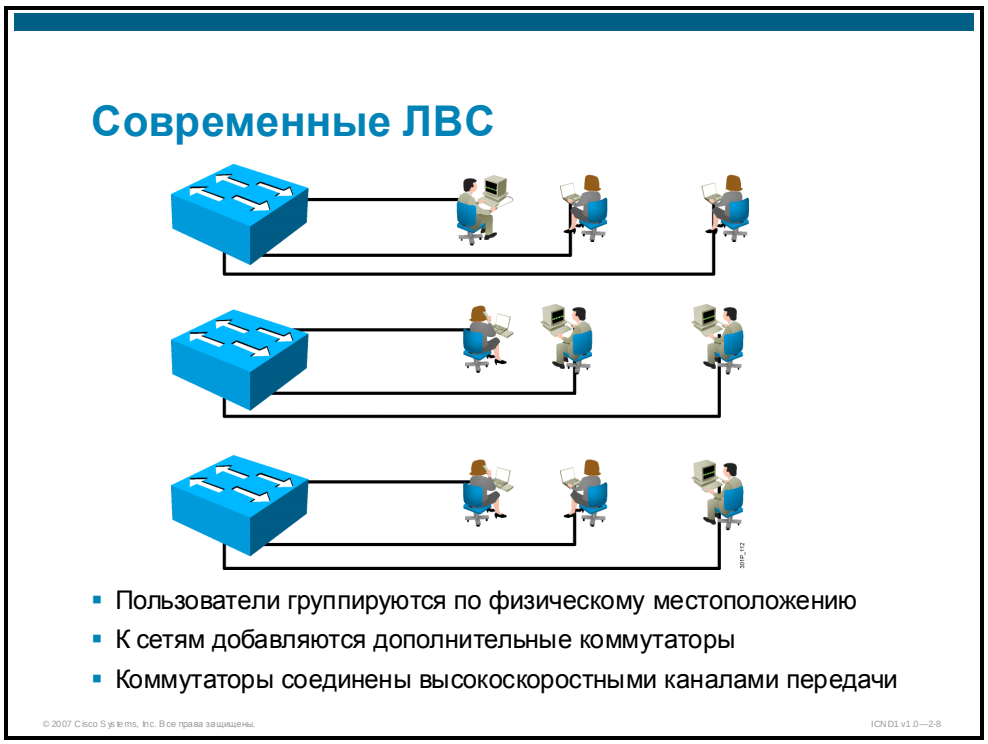
Когда адрес неизвестен, коммутатор изучает топологию сети, анализируя адрес источника входящих кадров от всех подключенных сетей. В таблице ниже описывается этот процесс.

Процедура коммутации кадров

№	Действие
1.	Коммутатор получает широковещательный кадр от ПК на порту 1.
2.	Коммутатор сохраняет MAC-адрес источника и номер порта коммутатора, который получил кадр, в таблицу MAC-адресов.
3.	Поскольку адрес назначения широковещательный, коммутатор рассылает кадр по всем портам, за исключением того, с которого он был получен.
4.	Устройство-получатель отвечает на широковещательную рассылку индивидуальным кадром по адресу ПК A.
5.	Коммутатор сохраняет выделенный их адреса источника кадра MAC-адрес ПК B и номер порта коммутатора, с которого кадр был получен, в таблицу MAC-адресов. В таблице MAC-адресов производится поиск адреса назначения кадра и связанного с ним порта.
6.	Теперь коммутатор может пересылать кадры между устройствами источника и назначения без выполнения лавинной рассылки, потому что у него есть записи в таблице MAC-адресов, которые идентифицируют соответствующие порты.

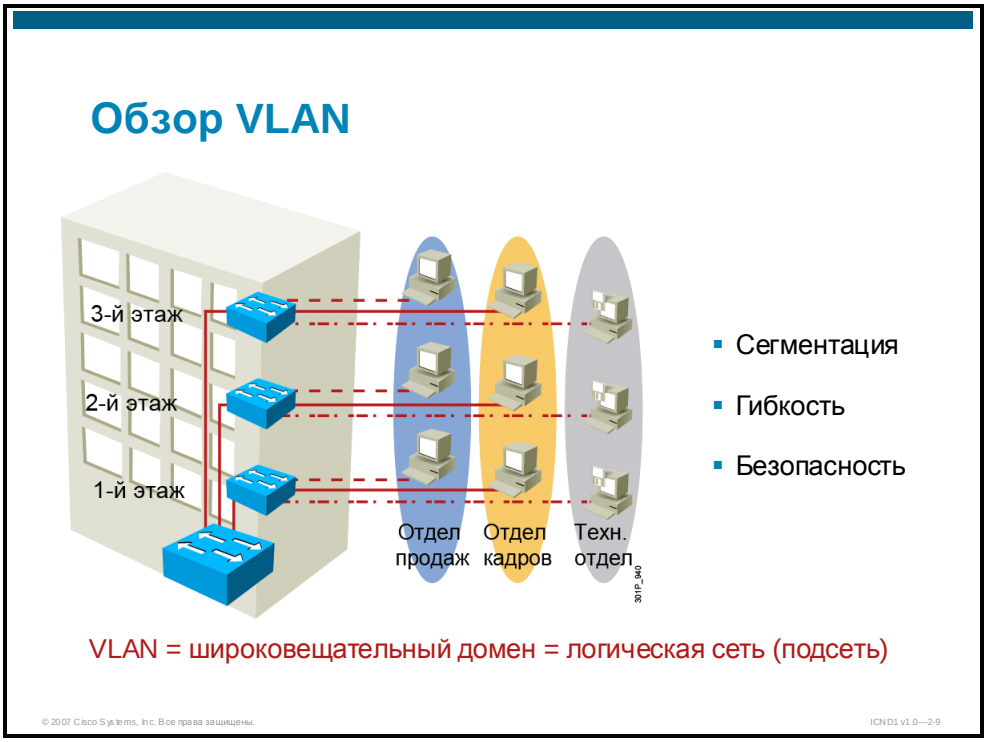
Использование технологии коммутируемых ЛВС

Коммутируемые сети – это самый распространенный тип ЛВС на сегодняшний день. Цена порта коммутатора уменьшилась настолько, что концентраторы и мосты больше не рассматриваются при принятии решения о покупке. Здесь описывается, как современные ЛВС используют технологию коммутации.



В коммутируемых сетях группировка пользователей в значительной степени определяется их физическим местоположением. Например, все пользователи, подключенные к коммутатору на первом этаже офисного здания будут принадлежать одной и той же рабочей группе, в то время как пользователи, подключенные к коммутатору на втором этаже, будут принадлежать к другой рабочей группе. Такая организация позволяет каждой группе обращаться к устройствам в сети, например серверам, с меньшей вероятностью коллизий и повышает общую производительность сети.

Для поддержки большего числа пользователей и удовлетворения более высоких требований к сетевым ресурсам и полосе пропускания, в сеть вводится все больше коммутаторов. Однако при добавлении дополнительных коммутаторов в сеть объем трафика между ними увеличивается. Поэтому возникает необходимость в увеличении скорости и производительности каналов связи между коммутаторами и другими сетевыми устройствами.



VLAN – это логический широковещательный домен, который может охватывать несколько физических сегментов локальной сети. В коммутируемых интерсетях VLAN обеспечивают сегментацию и гибкость организации сети. 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, при этом порты в других VLAN не участвуют в широковещательной рассылке. Ограничение широковещательной рассылки одной VLAN улучшает общую производительность сети.

В коммутируемых интерсетях VLAN обеспечивает сегментацию и гибкость организации сети. 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 существовать на одном коммутаторе или охватывать несколько коммутаторов. VLAN могут содержстанции внутри одного здания или инфраструктуры, развернутые в нескольких зданиях. Кроме того, VLAN могут связываться через распределенные сети (WAN).

Резюме

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

Резюме

- Основными причинами перегрузки ЛВС Ethernet являются непрерывно развивающиеся компьютерные и сетевые технологии, увеличивающийся объем сетевого трафика, а также приложения с высокими требованиями к полосе пропускания, такие как настольные издательские системы, системы электронного обучения и потоковое видео.
- Для разделения ЛВС Ethernet на несколько сегментов использовались мосты Ethernet. Такое разделение позволяет предотвратить коллизии между устройствами, расположенными в разных сегментах, а также снизить уровень перегрузки сети.
- Коммутаторы работают на гораздо более высоких скоростях, чем мосты, поддерживают высокую плотность портов с большими буферами кадров и обеспечивают быструю внутреннюю коммутацию. Кроме того, коммутаторы используют один из двух методов пересылки для коммутации данных между сетевыми портами: коммутация без буферизации и коммутация с буферизацией.

Резюме (прод.)

- Коммутаторы обеспечивают гораздо больше преимуществ с точки зрения устранения перегрузок сети, нежели мосты, так как обеспечивает выделенные каналы связи между устройствами, поддержку одновременных сеансов связи, полнодуплексную связь и адаптацию к скорости среды.
- Коммутаторы работают на уровне 2 модели OSI, анализируют входящие кадры, а затем выполняют пересылку, фильтрацию или лавинную рассылку кадров на основании информации об адресе назначения. Коммутаторы также собирают и передают кадры между двумя или более сегментами ЛВС, повышая количество доменов коллизий.
- Коммутаторы строят таблицы известных MAC-адресов в сегментах сети и сопоставляют их с соответствующими портами. Затем MAC-адреса используются коммутаторами во время коммутации кадров.

Резюме (прод.)

- В коммутируемых сетях группирование пользователей в значительной степени определяется их физическим местоположением. Многие коммутаторы используются, чтобы обеспечить доступ к устройствам в сети, таким как серверы, каждой группе пользователей. Коммутаторы должны соединяться через высокоскоростные порты для максимального повышения общей производительности сети.

Занятие 3

Изучение процесса доставки пакетов данных

Обзор

В модуле «Построение простой сети» мы рассмотрели связь между хостами и ввели понятие коммутатора. В этом занятии приводится графическое представление передачи данных между хостами, при которой данные проходят через коммутатор.

Задачи

По окончании этого занятия вы сможете описывать создание и поддержку обмена данными между хостами. Это значит, что вы сможете выполнять следующие задачи:

- описывать адресацию на уровне 2;
- описывать адресацию на уровне 3;
- описывать передачу пакетов данных между хостами.

Адресация уровня 2

Для обмена данными между хостами необходимы адреса уровня 2. В этом разделе рассматривается роль адресации уровня 2 в модели обмена данными между хостами.

Из модуля «Построение простой сети» вы помните, что MAC-адреса присваиваются конечным устройствам, таким как хосты. В большинстве случаев сетевым устройствам уровня 2, таким как мосты и коммутаторы, MAC-адрес не присваивается. Однако в отдельных случаях, коммутаторам могут быть назначены MAC-адреса. Эта ситуация будет рассматриваться позднее в этом курсе.

Адресация уровня 3

В этом разделе рассматривается роль адресации уровня 3 в модели обмена данными между хостами.

Каждая сетевая операционная система (NOS) обладает собственным форматом адреса уровня 3. Например, модель OSI использует точку доступа к сетевому сервису (NSAP), а стек TCP/IP использует IP-адрес.

Доставка пакетов от хоста к хосту

В этом разделе описываются самые распространенные средства связи между хостами.

В этом примере хосту 192.168.3.1 необходимо передать данные в хост 192.168.3.2. Приложение не нуждается в надежном соединении. Выбран протокол UDP.

Поскольку создание сеанса не требуется, приложение может начать отправку данных. UDP добавляет заголовок UDP и передает единицу информации протокола (PDU) на уровень IP (уровень 3) с инструкцией отправить PDU по адресу 192.168.3.2. IP инкапсулирует PDU в пакете уровня 3 и передает его на уровень 2.

Как и в примере, который приводится в модуле «Построение простой сети», протокол ARP не имеет соответствующей записи в таблице.

Хост 192.168.3.1 отправляет запрос ARP. Однако перед тем, как запрос попадет на удаленный хост, он попадает на коммутатор (в этом примере).

Когда коммутатор получает кадр, он должен переслать его на соответствующий порт. Однако в этом примере MAC-адреса источника и назначения не представлены в таблице MAC-адресов коммутатора. Коммутатор может получить привязку порта для хоста источника из MAC-адреса в кадре, а затем занести ее в таблицу привязок порта. (0800:0222:2222 = порт 1).

Поскольку адрес назначения является широковещательным, коммутатор должен разослать пакет на все порты.

Примечание Коммутатор не вносит никаких изменений в кадр.

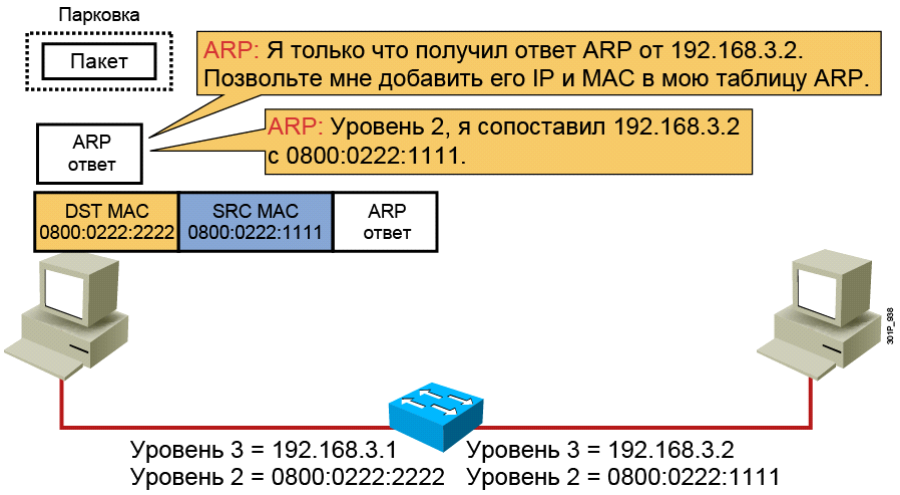
Хост назначения получает запрос ARP и возвращает ответ.

Коммутатор получает привязку порта для хоста источника из MAC-адреса в кадре. Таким образом, коммутатор добавляет привязку в таблицу привязок порта (0800:0222:1111 = порт 2).

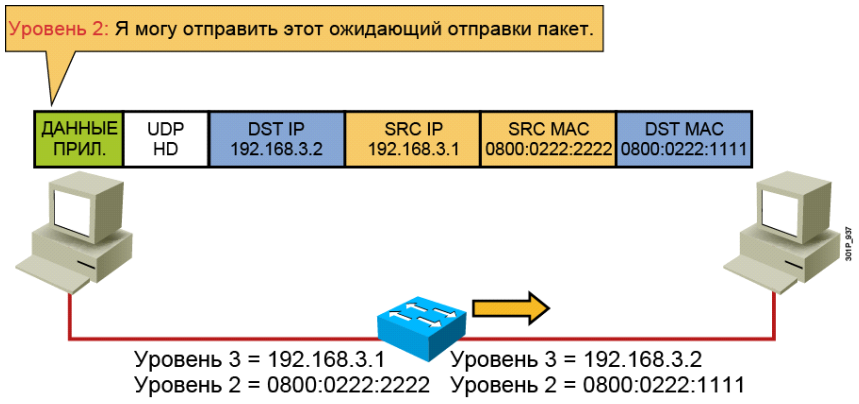
Поскольку место назначения уже занесено в таблицу MAC-адресов коммутатора, он может передать кадр на порт 1.

Примечание	Коммутатор не вносит никаких изменений в кадр.

Передача пакетов данных между хостами (9 из 10)



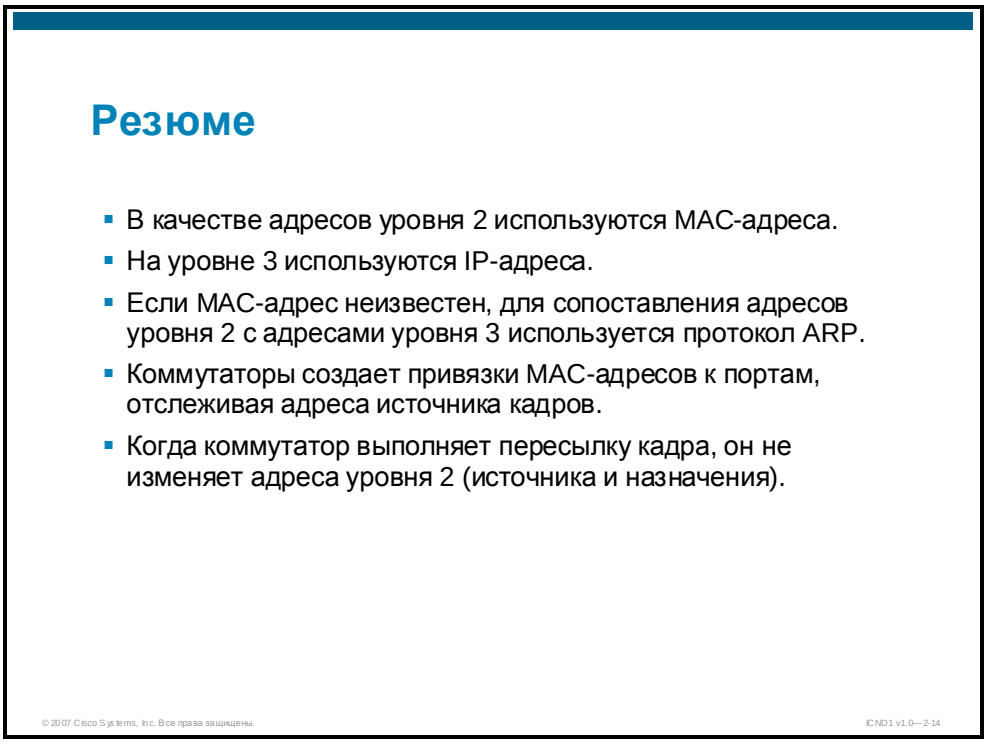
Передача пакетов данных между хостами (10 из 10)



Данные отправляются с коммутатора и принимаются хостом. Все кадры проходят через коммутатор без изменений.

Резюме

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



Занятие 4

Работа с программным обеспечением Cisco IOS

Обзор

Понимание окружения корпоративной сети ведет к осознанию необходимости в более широких функциональных возможностях и контроле над сетевыми компонентами, которые предоставляются более сложными сетевыми устройствами, такими как коммутаторы. Cisco IOS – это многофункциональное сетевое системное программное обеспечение, обеспечивающее сетевую интелектуальность в критически важных сетях. В этом занятии сравниваются функциональные возможности коммутаторов и устройств малых и домашних офисов (SOHO) с компонентами корпоративной сети и описываются функции программного обеспечения Cisco IOS.

Задачи

По окончании этого занятия вы сможете выполнять консольные подключения к сетевым устройствам Cisco посредством терминального ПО. Это значит, что вы сможете выполнять следующие задачи:

- перечислять функции и возможности ПО Cisco IOS в контексте корпоративной сети;
- описывать процедуру первого запуска сетевых устройств Cisco;
- описывать процедуру конфигурации сетевых устройств Cisco;
- определять функции интерфейса командной строки Cisco IOS;
- описывать запуск сеанса EXEC и изменение режима EXEC;
- определять функции интерактивной справки, связанные с интерфейсом командной строки устройства;
- описывать усовершенствованные функции редактирования интерфейса командной строки Cisco IOS;
- использовать функцию журнала команд устройства интерфейса командной строки.

Функции и возможности программного обеспечения Cisco IOS

ПО Cisco IOS – это ведущее и наиболее распространенное программное обеспечение для сетевых систем. В этом разделе описываются функции и возможности ПО Cisco IOS.

ПО Cisco IOS применяется на большинстве аппаратных платформ Cisco – коммутаторах и другие устройствах. Это программная архитектура внедрена на всех устройств Cisco, а также является операционной системой коммутаторов Cisco Catalyst.

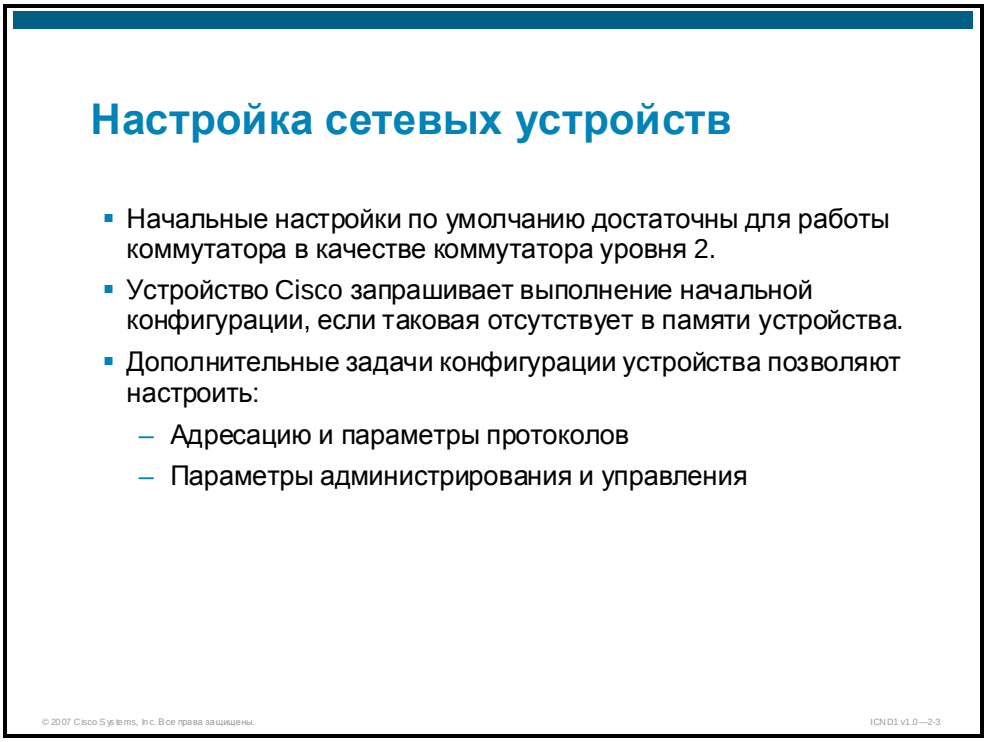
ПО Cisco IOS выполняет следующие сетевые сервисы продуктов Cisco:

- средства поддержки выбранных сетевых протоколов и функций;
- возможности подключения для высокоскоростной передачи трафика между устройствами;
- система безопасности для контроля доступа и предотвращения несанкционированного использование сети;
- масштабируемость для добавления интерфейсов и функции в соответствии с требованиями роста сети;
- надежность обеспечения доступа к сетевым ресурсам.

Доступ к интерфейсу командной строки ПО Cisco IOS осуществляется через консольное, модемное подключение или сеанс Telnet. Независимо от метода подключения доступ к ПО Cisco IOS обычно называется сеансом EXEC.

Настройка сетевых устройств

Интерфейс командной строки Cisco IOS используется для выполнения конфигурации устройств, отвечающей сетевым требованиям организации. В этом разделе описываются начальные действия по запуску и настройке сетевых устройств Cisco.

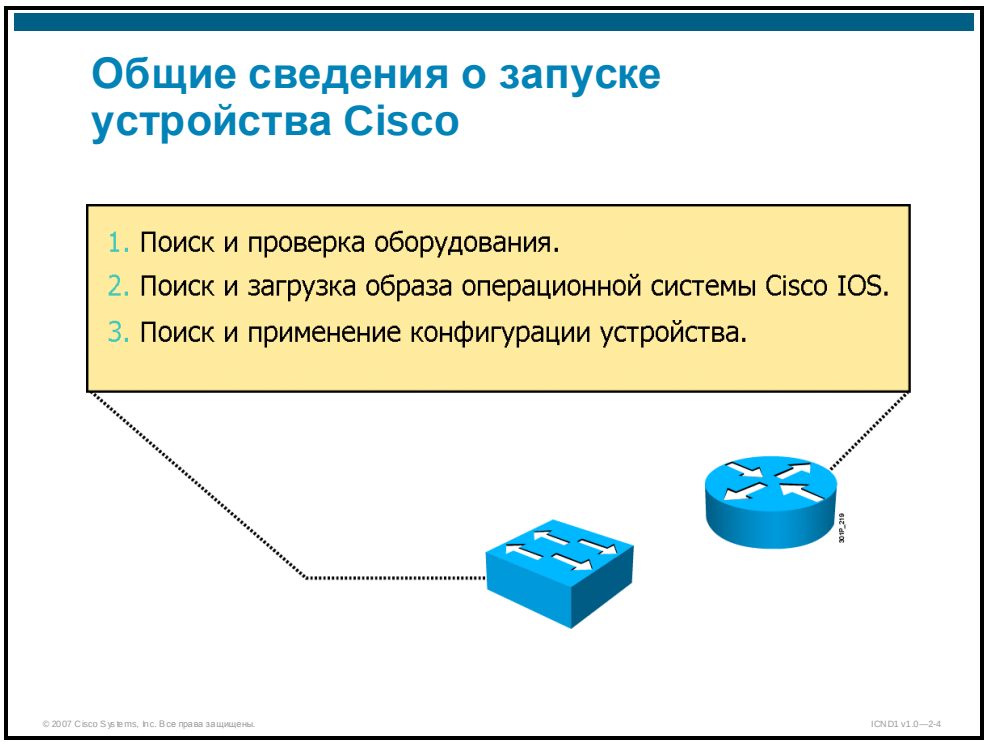


Если коммутатор Cisco IOS запускается впервые, его первоначальной конфигурации с параметрами по умолчанию достаточно, чтобы он мог работать на уровне 2 как коммутатор. Однако при первом запуске маршрутизатора Cisco, коммутатор не обладает достаточной информацией в его исходной конфигурации, чтобы работать на уровне 3, поскольку управление коммутатором требует как минимум информации об IP-адресе, поэтому программное обеспечение коммутатора запросит эту информацию посредством конфигурационного диалога.

Конфигурационная настройка определяет следующие параметры устройства:

- Адресацию протоколов и такие параметры, как IP-адрес и маска подсети интерфейса;
- параметры администрирования и управления, такие как настройка пароля и т. д.

В этом занятии рассматривается минимальная конфигурация устройства. Изменение этих минимальных настроек или параметров по умолчанию для выполнения тех или иных требований сети часто является основной задачей администратора.



При запуске сетевого устройства Cisco выполняются три главные операции.

1. Устройство выполняет проверку оборудования. Термин, часто используемый для описания этого набора процедур, – самотестирование после включения питания (POST – Power-On Self-Test).

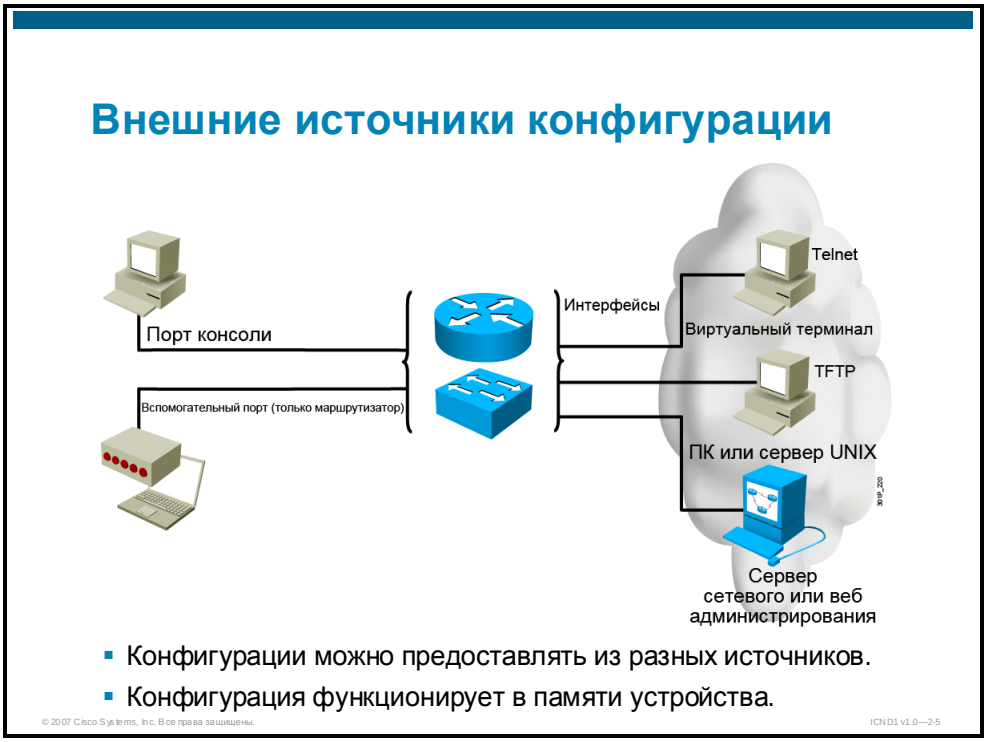
2. После подтверждения исправности оборудования, устройство выполняет процедуры запуска системы. Они инициализируют операционную систему устройства.

3. После загрузки операционной системы устройство пытается найти и применить инструкции конфигурации программного обеспечения, необходимые для работы сети.

Как правило, существует аварийный порядок, который обеспечивает альтернативные варианты запуска программного обеспечения, если это необходимо.

Внешние источники конфигурации

Коммутатор или устройство может настраиваться с использованием источников, которые являются внешними по отношению к устройству. В этом разделе описываются внешние источники конфигурации для настройки сетевых устройств Cisco.



Вы можете получить доступ к устройству с удаленной площадки, не подключаясь к сети, а путем прямого дозвона до консольного или вспомогательного порта устройства. Как правило, рекомендуется использовать консольный порт, потому что он показывает сообщения о запуске устройства, тогда как вспомогательный порт не предоставляет эту информацию. Устройства можно настраивать из следующими способами.

- **Консольный терминал.** На начальном этапе установки сетевые устройства можно настраивать с консольного терминала, который подключается через консольный порт. Для настройки устройства Cisco с консольного порта необходимо следующее:
  - Консольный кабель RJ-45-EIA/TIA-232
  - Персональный компьютер (ПК) или его эквивалент с коммуникационным программным обеспечением со следующими параметрами:
    - Скорость: 9 600 бит/с
    - Биты данных: 8
    - Контроль четности: нет
    - Стоповый бит: 1
    - Управление потоками: нет

- **Удаленный терминал.** Для поддержки удаленного устройства используется модемное подключение к вспомогательному порту устройства, которое позволяет настраивать удаленное устройство с удаленного терминала. Однако сначала вспомогательный порт устройства нужно настроить для работы с внешним модемом. Для удаленного подключения к вспомогательному порту на устройстве Cisco необходимо следующее:
  - Последовательный прямой кабель
  - Модем 14,4 кбит/с
  - ПК или его эквивалент с подходящим коммуникационным ПО

После первого запуска вы можете получить доступ к устройству и настраивать его следующими способами:

- создав терминальный сеанс с помощью Telnet;
- настраивать устройства через подключение или путем загрузки готового файла конфигурации с TFTP-сервера в сети.
- загрузка файла конфигурации помощью приложения для управления сетью, например CiscoWorks.

Примечание Некоторые сетевые устройства могут не иметь всех портов, изображенных на рисунке. Например, некоторые устройства Cisco для сегмента SOHO не поддерживают вспомогательный порт.

Функции интерфейса командной строки Cisco IOS

Программное обеспечение Cisco IOS использует интерфейс командной строки в качестве традиционной среды для ввода команд. ПО Cisco IOS является базовой технологией, которая используется во многих продуктах, однако особенности его эксплуатации могут меняться в зависимости от конкретного устройства. В этом разделе рассматриваются функции интерфейса командной строки Cisco IOS.

Чтобы ввести команду в интерфейсе командной строки, введите или вставьте текст в одном из нескольких режимов команд консоли. Все режимы конфигурации обозначаются собственным приглашением. Клавиша Enter (ВВОД) заставляет устройство обработать и выполнить команду.

В структуре режимов команд ПО Cisco IOS применяется иерархия команд. В каждом режиме команд 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.

Вход в режимы EXEC

Программное обеспечение Cisco IOS поддерживает два режима команд EXEC: пользовательский и привилегированный. В этом разделе описывается запуск сеанса EXEC и изменение режима EXEC.

Процедура в таблице описывает включение режима EXEC на коммутаторе или устройстве Cisco.

№	Действие	Результат и примечания
1.	Подключитесь к устройству, указав имя пользователя и пароль (если вход в систему предусмотрен конфигурацией). Это переведет устройство в пользовательский режим EXEC.	Появится приглашение, обозначающее пользовательский режим EXEC. Стрелка вправо (>) в приглашении указывает, что устройство или коммутатор находится на пользовательском уровне EXEC. `hostname>` Введите **exit**, чтобы выйти из пользовательского режима EXEC.
2.	Введите команду **?** в приглашении пользовательского уровня EXEC, чтобы вывести команды, доступные в пользовательском режиме EXEC.	Команда **?** в привилегированном режиме EXEC выводит больше команд, чем в пользовательском режиме. Эта функция называется контекстной справкой.

Пользовательский уровень EXEC не поддерживает команды для управления устройством. В частности пользовательский режим EXEC не позволяет перезагружать или настраивать устройство.

Критически важные команды, такие как команды конфигурации и управления, требуют привилегированного режима EXEC.

Чтобы перейти в привилегированный режим EXEC из пользовательского режима EXEC, введите команду **enable** в приглашении hostname>. Если настроен пароль «enable password» или «enable secret password», устройство запросит его.

После ввода правильного пароля приглашение устройства изменится на hostname#. Это значит, что пользователь перешел на привилегированный уровень EXEC. При вводе команды **?** в привилегированном режиме EXEC отображается больше команд, чем в пользовательском режиме EXEC.

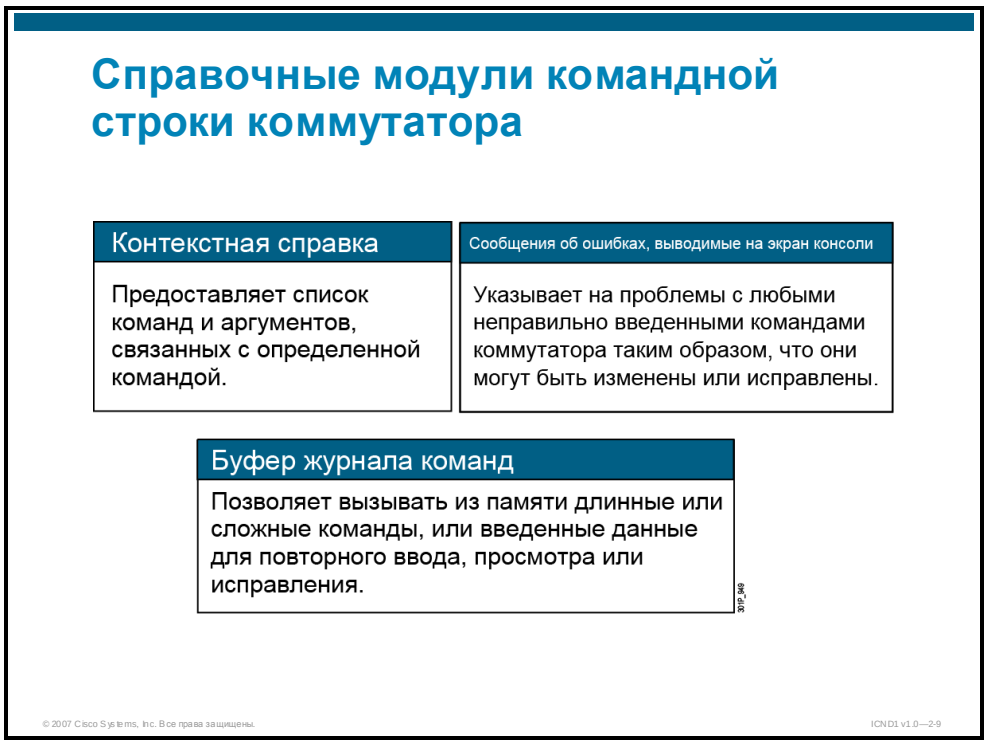
Чтобы вернуться к пользовательскому режиму EXEC, введите команду **disable** в приглашении hostname#.

Примечание	В целях безопасности сетевое устройство Cisco не будет отображать вводимый пароль на экране. Но если сетевое устройство настраивается через модемный канал или сеанс Telnet, пароль отправляется в виде нешифрованного текста. Telnet не не имеет методов для защиты пакетов.

Примечание	Протокол SSH, который используется в большинстве устройств Cisco, обеспечивает безопасную передачу данных по незащищенным каналам и использует «сильную» систему аутентификации. Сведения об использовании протокола SSH можно получить в документации по Cisco IOS.

Справка интерфейса командной строки

Устройства Cisco используют ПО Cisco IOS, которое имеет комплексные справочные средства для интерфейса командной строки, включая контекстную справку. В этом разделе описывается справка интерфейса командной строки, доступная в устройствах Cisco.



Интерфейс командной строки Cisco IOS на устройствах Cisco предлагает следующие виды справки.

- **Справка по словам.** Введите последовательность символов перед знаком вопроса. Не ставьте пробел между знаком вопроса и последовательностью символов. Устройство выведет список команд, которые начинаются с указанных символов. Например, введите команду **sh?**, чтобы получить список команд, которые начинаются с сочетания букв sh.
- **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 отобразит список доступных параметров команды, <cr> обозначает возврат каретки. Например, введите **show ?**, чтобы получить список поддерживаемых параметров команды **show**.

Примечание	Устройства Cisco и коммутаторы Cisco Catalyst предлагают аналогичные справочные средства командной строки. Все упоминания справочных средств для устройств, также относятся к коммутаторам Cisco Catalyst, если не указано иное.

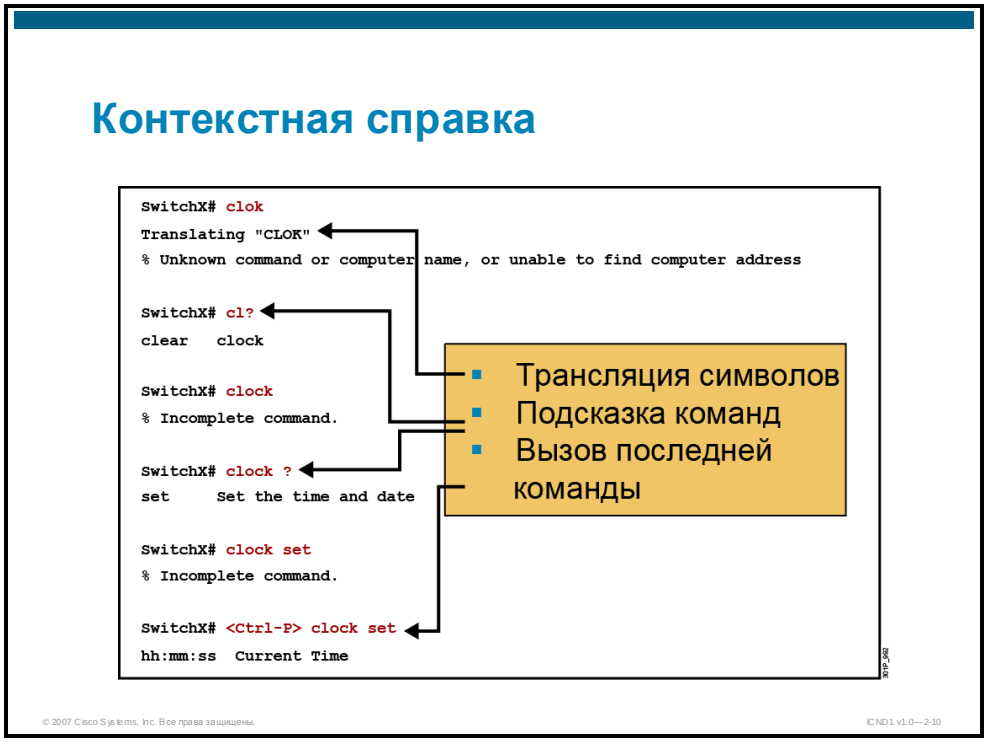
Последовательность Ctrl Escape устраняет необходимость в повторном вводе полных командных строк. ПО Cisco IOS предусматривает несколько команд и символов для вызова команд из буфера журнала, в котором хранятся последние

несколько команд, которые вы ввели. Эти команды могут использоваться многократно без повторного ввода.

Сообщения об ошибках консоли помогают выявить проблемы, связанные с неправильным вводом команд. Сообщения об ошибках, которые могут появиться при использовании интерфейса командной строки, показаны в таблице.

Сообщение об ошибке	**Значение**	**Как вызвать справку**
`% Ambiguous command (неопределенная команда): “show con”`	Вы ввели недостаточно символов, чтобы устройство могло распознать команду.	Введите команду еще раз с вопросительным знаком в конце (**?**) *без* пробела между командой и вопросительным знаком. Отобразятся возможные ключевые слова, которые вы можете ввести с командой.
`% Incomplete command (неполная команда)`	Вы ввели не все ключевые слова или значения, необходимые для этой команды.	Введите команду еще раз с вопросительным знаком в конце (**?**) *с* пробелом между командой и вопросительным знаком.
`% Invalid input detected at ‘^’ marker (недопустимый ввод обнаружен на месте метки ‘^’)`	Команда введена неверно. Символ (^) показывает место ошибки.	Введите вопросительный знак (**?**), чтобы вывести все доступные команды или параметры.

В буфере журнала команд сохраняются недавно введенные команды. Чтобы увидеть эти команды, введите команду Cisco IOS **show history**.



Вы можете использовать контекстную справку, чтобы определить синтаксис той или иной команды. Например, если нужно установить время устройства, но синтаксис команды установки времени не известен, контекстная справка позволит уточнить синтаксис команды для установки времени.

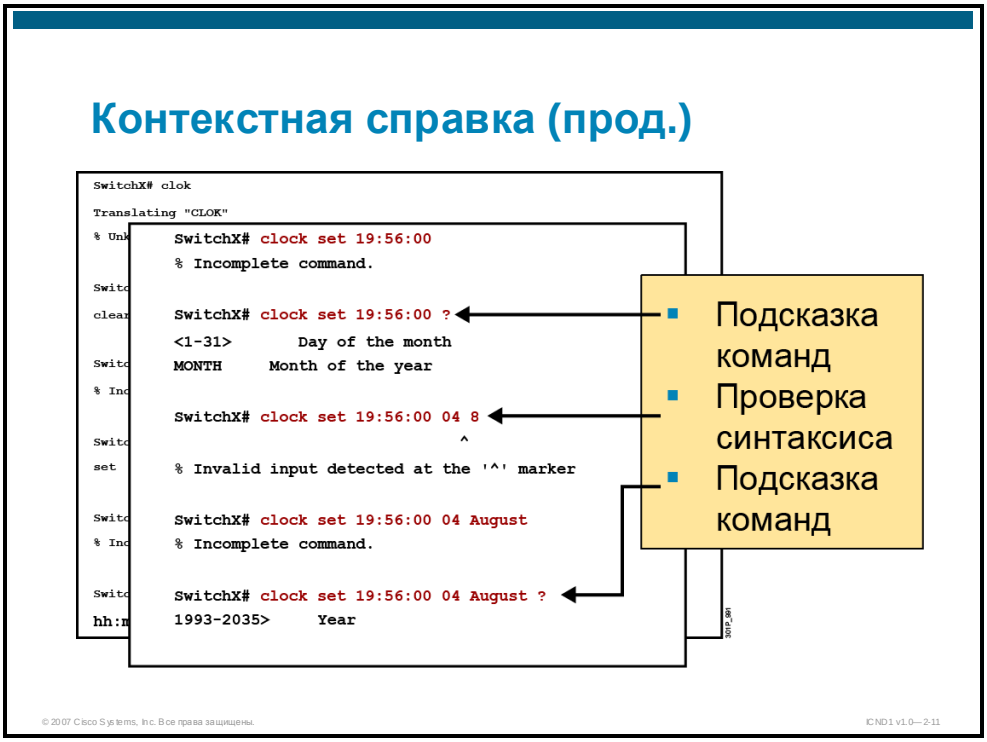
Если слово «clock» («часы») ввести с орфографической ошибкой, система выполнит символьное преобразование ошибочной команды в соответствии с синтаксическим анализом введенного текста ПО Cisco IOS. Если ни одна из команд, не соответствует введенной строке, появится сообщение об ошибке. Если в Cisco IOS нет команды, которая начинается с неправильно введенных символов, устройство воспримет неверную команду как имя хоста и попытается разрешить его в IP-адрес, а затем инициирует сеанс Telnet к этому хосту.

Контекстная справка выдает полную команду, даже если вы вводите только первую ее часть, например, **cl?**.

Если вы вводите команду **clock**, но появляется сообщение, что команда введена не полностью, введите **?** (перед «**?**» следует ввести пробел), чтобы определить, какие параметры требуются для этой команды. В примере с командой **clock?**, справка покажет, что после команды **clock** не хватает ключевого слова **set**.

Если теперь вы введете команду **clock set**, но опять появится сообщение, что команда введена не полностью, нажмите **Ctrl-P** (или **стрелку «Вверх»**), чтобы повторить ввод команды. Затем добавьте пробел и введите вопросительный знак (**?**), чтобы вывести список доступных параметров команды.

В примере показано, что после последнего вызова команды администратор использовал команду **?**, чтобы узнать дополнительные параметры, относящиеся к вводу текущего времени в часах, минутах и секундах.



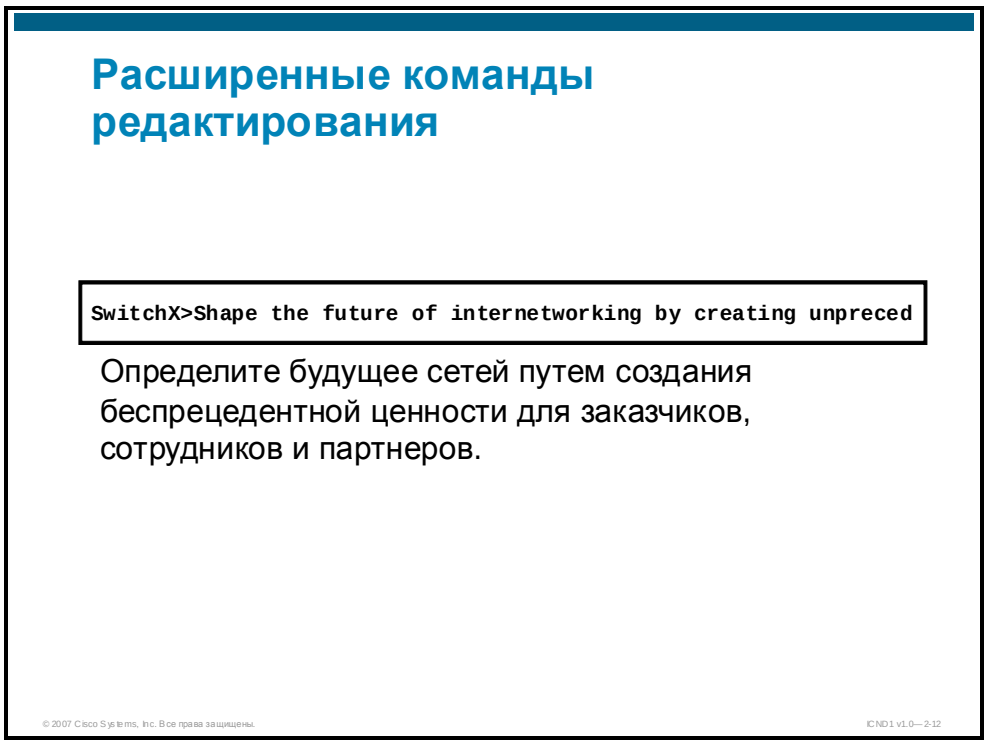
На рисунке показано, как продолжить установку времени устройства.

Если после ввода текущего времени вы все еще видите сообщение Cisco IOS о том, что команда введена не полностью, вызовите команду, добавьте пробел и вопросительный знак (**?**), чтобы вывести список параметров, доступных для данной команды в данный момент. В этом примере вам следует ввести день, месяц и год, используя правильный синтаксис, затем нажать клавишу **Return**, чтобы выполнить команду.

Система проверки синтаксиса использует символ каретки (^) в качестве индикатора положения ошибки. Символ каретки появляется в точке командной строки, в которой команда, ключевое слово или параметр введены неправильно. Индикатор положения ошибки и система интерактивной справки позволяют легко находить и исправлять синтаксические ошибки. В примере с часами символ каретки (^) указывает, что месяц был введен неправильно. Синтаксический анализатор ожидает корректного ввода месяца.

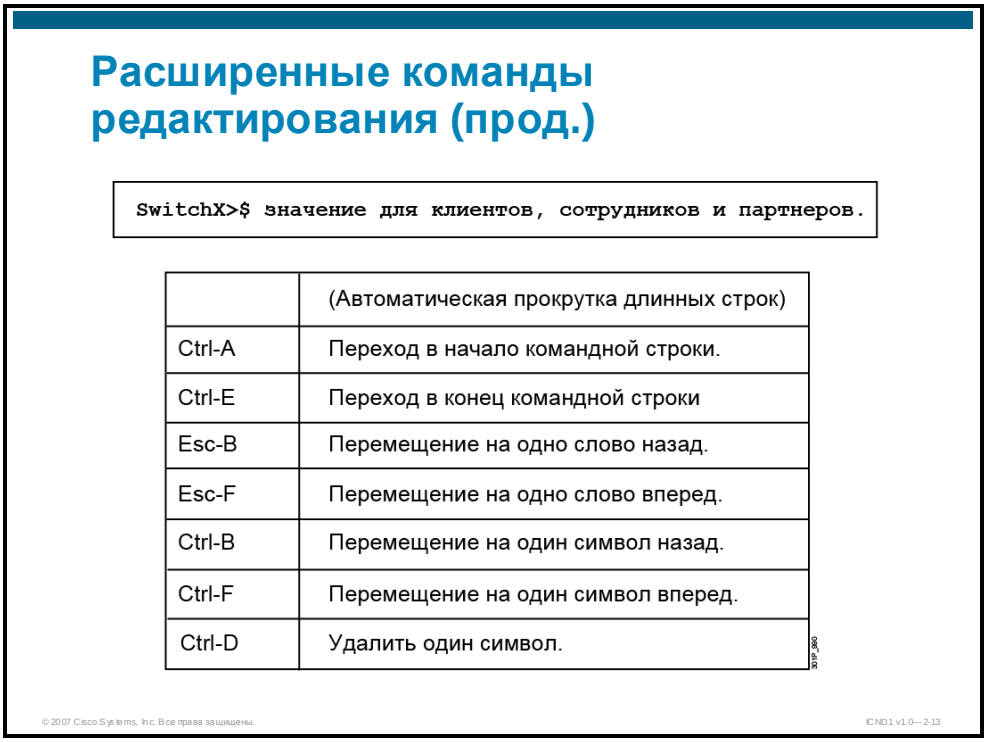
Расширенные команды редактирования

Интерфейс командной строки Cisco IOS поддерживает расширенный режим редактирования, который предлагает набор функциональных клавиш для редактирования. В этом разделе описываются расширенные функции клавиш для редактирования.



Хотя расширенный режим редактирования строки включается автоматически, его можно отключить. Расширенный режим редактирования лучше отключить, если используются сценарии, которые плохо взаимодействуют друг с другом, когда включен расширенный режим редактирования строки. Используйте команду EXEC **terminal editing**, чтобы включить расширенные функции редактирования строки и команду EXEC **terminal no editing**, чтобы отключить их.

Одна из расширенных функций редактирования строки обеспечивает горизонтальную прокрутку команд, которые выходят за пределы строки на экране. Когда курсор достигает правого поля, командная строка сдвигается на десять знаков влево. Первые десять символов строки становятся невидимыми, но вы можете прокрутить строку обратно, чтобы проверить синтаксис в начале команды.



В примере на рисунке команда выходит за пределы одной строки. Знак доллара ($) указывает на то, что строка была прокручена влево. Чтобы прокрутить строку назад, нажмите Ctrl-B или **стрелку влево** несколько раз, пока не попадете в начало команды, или нажмите Ctrl-A, чтобы сразу вернуться в начало строки.

Последовательности клавиш, указанные на рисунке, – это горячие клавиши интерфейса командной строки. Используйте эти клавиши для перемещения курсора по командной строке и внесения исправлений или изменений в команду.

В таблице перечислены все горячие клавиши, показанные на рисунке, а также некоторые дополнительные горячие клавиши для редактирования командной строки и управления вводом команды.

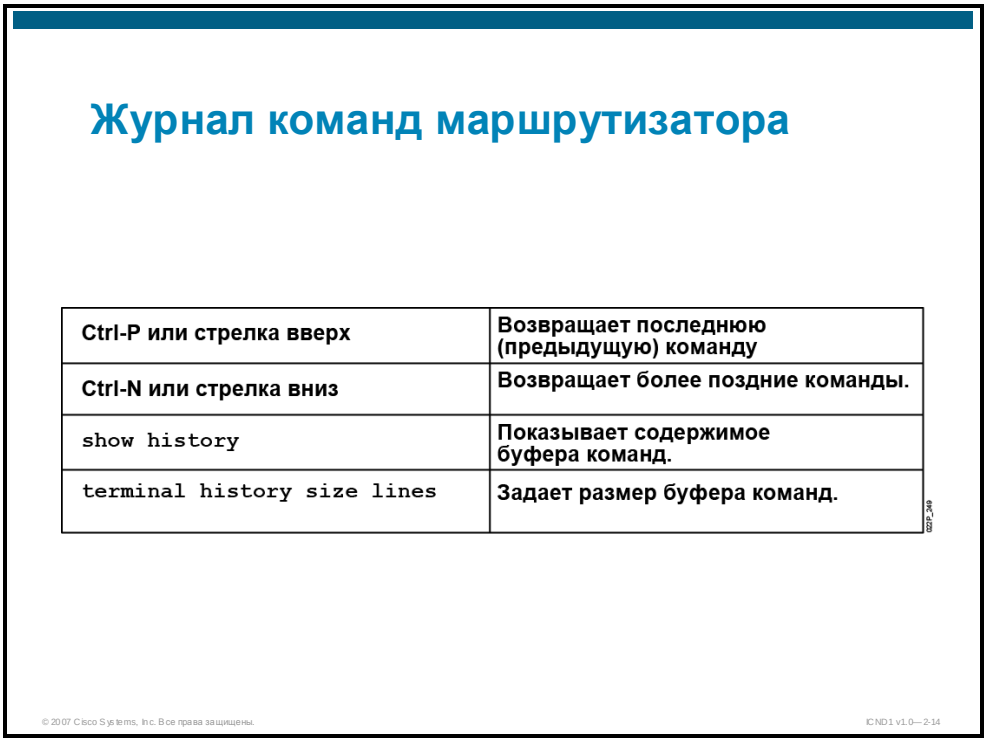
Сочетание клавиш в интерфейсе командной строки	**Описание**
Ctrl-A	Перемещает курсор в начало командной строки.
Ctrl-E	Перемещает курсор в конец командной строки.
Esc-B	Перемещает курсор на одно слово назад.
Esc-F	Перемещает курсор на одно слово вперед.
Ctrl-B	Перемещает курсор на один символ назад.
Ctrl-F	Перемещает курсор на один символ вперед.
Ctrl-D	Удаляет один символ слева от курсора.
Backspace	Удаляет один символ слева от курсора.
Ctrl-R	Повторно отображает текущую командную строку.
Ctrl-U	Стирает всю строку.

Сочетание клавиш в интерфейсе командной строки	Описание
Ctrl-W	Стирает слово слева от курсора.
Ctrl-Z	Закрывает режим конфигурации и возвращает в режим EXEC.
Tab	Дописывает частично введенную команду, если введенных символов достаточно для однозначного определения этой команды.

Примечание Клавиша Escape не является функциональной на всех терминалах.

Журнал команд

Интерфейс командной строки Cisco предусматривает журнал введенных команд. Эта функция под названием «журнал команд» особенно полезна для вывода длинных или сложных команд. В этом разделе описывается журнал команд устройства.



С помощью журнала команд можно выполнять следующие задачи:

- отображать содержимое буфера команд;
- устанавливать размер буфера журнала команд;
- вызывать ранее введенные команды, сохраненные в буфере журнала; существует буфер для режима EXEC и буфер для режима конфигурации.

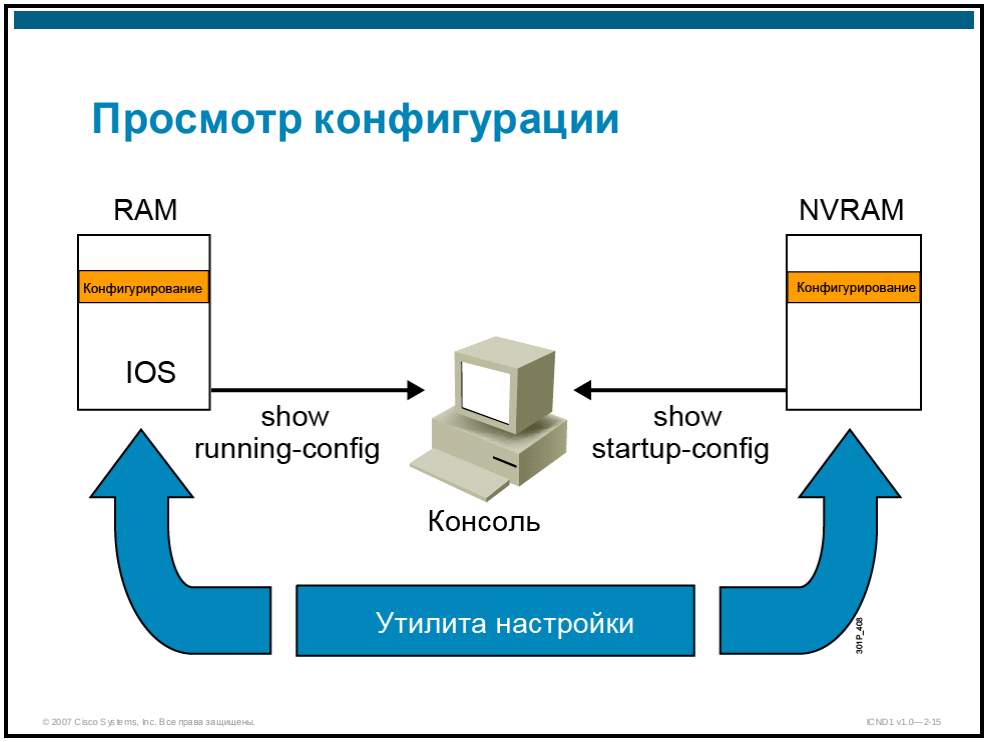
По умолчанию журнал команд включен, и система записывает последние десять командных строк в своем буфере журнала.

Чтобы изменить количество командных строк, которые система будет записывать в течение текущего терминального сеанса, используйте команду **terminal history** пользовательского режима EXEC.

Чтобы вызвать команды из журнала, начиная с последней, нажмите **Ctrl-P** или **стрелку вверх**. Повторяйте это сочетание клавиш для вызова каждой последующей, более старой команды.

Чтобы вернуться к более новым командам в буфере журнала после вызова более старых команд с помощью сочетания Ctrl-P или стрелки вверх, нажмите Ctrl-N или **стрелку вниз**. Повторяйте это сочетание клавиш для вызова каждой последующей, более новой команды.

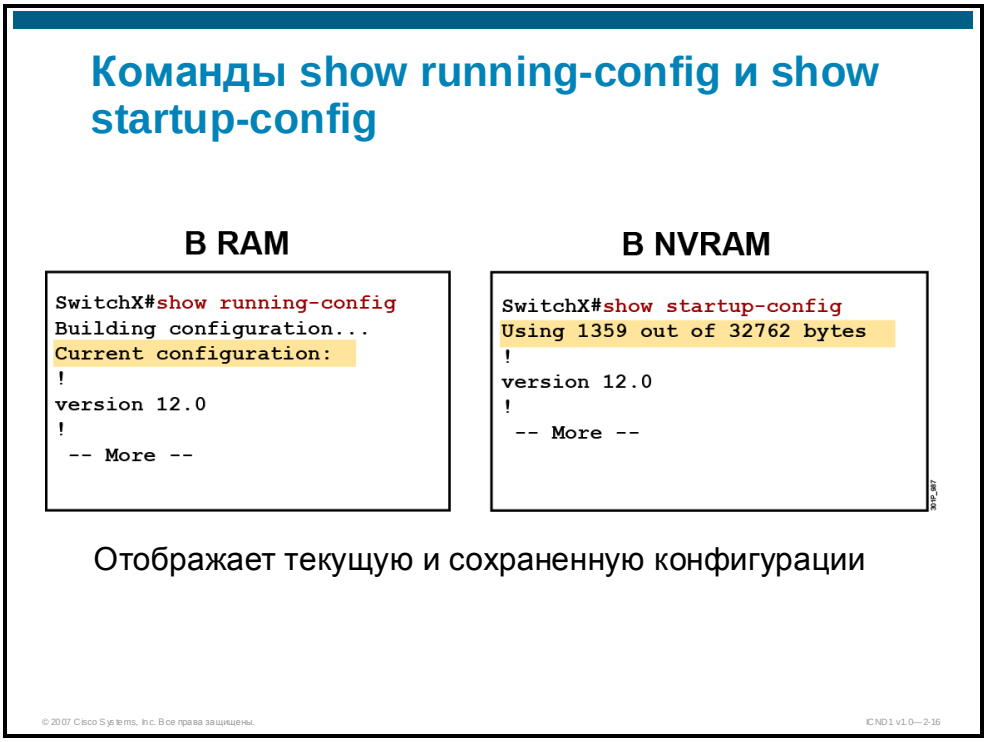
На большинстве компьютеров также доступны функции выбора и копирования. Скопируйте предыдущую командную строку, а затем вставьте ее как новую команду и нажмите клавишу **Return**.



Маршрутизатор Cisco включает три основных типа памяти:

- **RAM (оперативная память, ОЗУ):** в ней хранятся таблицы маршрутизации, кэш быстрой коммутации, текущую конфигурацию и т. д.
- **NVRAM (энергонезависимая память):** используется для постоянного хранения загрузочной конфигурации с возможностью перезаписи.
- **Флэш-память:** обеспечивает постоянное хранение образа ПО Cisco IOS, резервных конфигураций и любых других файлов на картах памяти.

Команда **show startup-config** отображает конфигурацию, сохраненную в NVRAM. Команда **show running-config** отображает конфигурацию в RAM.



Команда **show running-config** отображает текущую конфигурацию в RAM.

Сообщение «Building configuration.…» указывает на то, что действующая конфигурация формируется на основе активной конфигурации устройства, выполняющейся в RAM.

По окончании построения действующей конфигурации из RAM, появляется сообщение «Current configuration:», указывающее, что это – текущая конфигурация в RAM.

Первая строка вывода команды **show startup-config** содержит объем памяти NVRAM, используемой для хранения конфигурации, например, строка «Using 1 359 out of 32 762 bytes» означает полный объем NVRAM составляет 32 762 байта, а текущая конфигурация, сохраненная в NVRAM, занимает 1 359 байт.

Резюме

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

Резюме

- Cisco IOS – это встроенная программная архитектура всех устройств Cisco, а также операционная система для коммутаторов Cisco Catalyst. Его функции включают работу выбранных сетевых протоколов, средства подключения, безопасности, масштабируемости и надежности.
- Коммутатор или устройство IOS можно настраивать с локального терминала, подключенного к консольному порту или с удаленного терминала, подключенного к вспомогательному порту через модем.
- Интерфейс командной строки используется администраторами сети для мониторинга и настройки различных устройств Cisco IOS. Интерфейс командной строки поддерживает справочные средства, помогающие администраторам сети использовать команды проверки и конфигурации.

Резюме (прод.)

- Интерфейс командной строки поддерживает два режима EXEC: пользовательский и привилегированный. Привилегированный режим EXEC предлагает больше возможностей, чем пользовательский режим EXEC.
- Устройства Cisco IOS используют ПО Cisco IOS, которое включает комплексные справочные средства для интерфейса командной строки, включая контекстную справку.
- Интерфейс командной строки Cisco IOS поддерживает расширенный режим редактирования, который предлагает набор ключевых функций для редактирования.
- Интерфейс командной строки Cisco поддерживает журнал (список) введенных команд. Эта функция, которая называется журналом команд, особенно полезна для вывода длинных или сложных команд.

Занятие 5

Запуск коммутатора

Обзор

Коммутатор Cisco Catalyst проводит процедуру запуска при включении. Когда процедура запуска завершена, можно задать начальные параметры программного обеспечения. Понимание, что запуск коммутатора прошел без ошибок, – первый шаг при развертывании коммутатора Catalyst. Коммутатор должен запуститься успешно и иметь конфигурацию по умолчанию для работы в сети. На этом занятии описывается запуск коммутатора и проверка его начальной работоспособности.

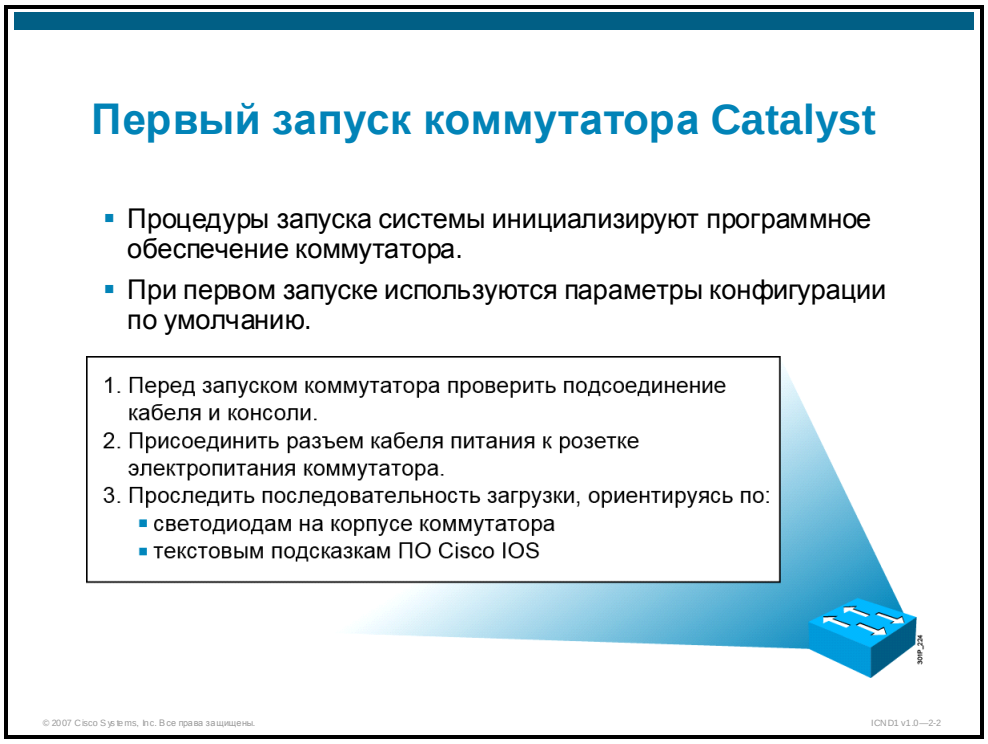
Задачи

По окончании этого занятия вы сможете запускать коммутатор уровня доступа и использовать интерфейс командной строки (CLI) для взаимодействия с программным обеспечением Cisco IOS. Это значит, что вы сможете выполнять следующие задачи:

- запускать коммутатор Cisco IOS;
- определять состояния, которые обозначаются светодиодами на коммутаторах Cisco IOS;
- описывать вывод начальной загрузки коммутатора Cisco IOS;
- выполнять вход в систему коммутатора Cisco IOS;
- настраивать коммутатор Cisco IOS из командной строки;
- проверять начальную работоспособность коммутатора;
- использовать соответствующую команду **show** для управления таблицей MAC-адресов.

Запуск коммутатора Catalyst

Для запуска коммутатора Catalyst необходимо проверить физическую установку, подключение питания и ознакомиться с выводом программного обеспечения Cisco IOS на консоли. В этом разделе описывается первый запуск коммутатора Catalyst.



Первоначальный запуск коммутатора Catalyst требует выполнения действий, перечисленных в таблице.

Шаг 1 Перед запуском коммутатора проверьте следующее:

- все сетевые кабельные подключения должны быть надежными;
- ваш терминал должен быть подключен к порту консоли;
- должно быть выбрано приложение консольного терминала, например HyperTerminal.

Шаг 2 Вставьте вилку кабеля питания коммутатора в розетку. Коммутатор запустится. На некоторых коммутаторах Catalyst нет выключателя «Вкл./выкл.», в том числе на Cisco Catalyst 2960.

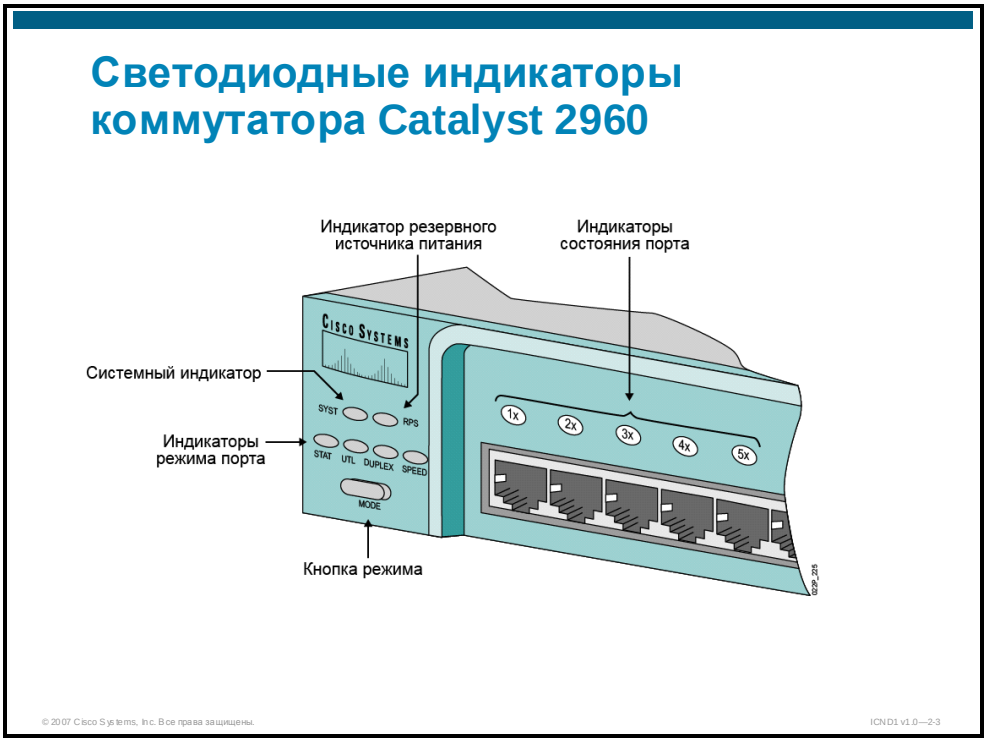
Шаг 3 Пронаблюдайте порядок загрузки:

- посмотрите на светодиоды на корпусе коммутатора;
- ознакомьтесь с текстом вывода программного обеспечения Cisco IOS на консоли.

Примечание В этом курсе описывается только коммутатор серии Catalyst 2960. Информационные команды и команды коммутации, представленные в этом документе, относятся к коммутатору серии Catalyst 2960. Ваш коммутатор может отличаться.

Светодиодные индикаторы коммутатора

Коммутаторы Catalyst оснащены несколькими светодиодными индикаторами состояния, которые светятся зеленым цветом, когда коммутатор функционирует нормально, и изменяют цвет на желтый при возникновении неисправности. В этом разделе описываются состояния светодиодов на коммутаторах серии Catalyst 2960.



Расположение светодиодов на коммутаторах Catalyst 2960-12 и 2960-24 показано на рисунке, а их функции объясняются в таблице.

Светодиод коммутатора	Описание
Системный светодиод	Выключен: система не включена. Зеленый: система включена и работоспособна. Желтый: системный сбой; при тестировании POST произошла одна или несколько ошибок .
Резервный источник питания	Выключен: резервный источник питания выключен или не установлен. Зеленый: резервный источник питания работоспособен. Мигающий зеленый: резервный источник питания подключен, но недоступен, так как обеспечивает питание другого устройства. Желтый: резервный источник питания установлен, но неработоспособен. Мигающий желтый: во внутреннем источнике питания произошел сбой, и коммутатор питается от резервного источника.

Режимы светодиодов порта приведены в таблице вместе со значениями цветов и режимов свечения светодиодов.

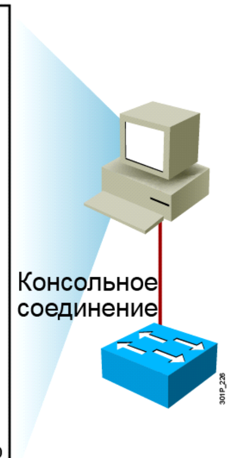
Режим светодиода порта	Описание
Состояние порта (светодиод STAT включен)	Выключен: нет канала. Зеленый: канал установлен, но бездействует. Мигающий зеленый: канал установлен, и есть трафик. Чередование зеленого и желтого: ошибка канала. Ошибочные кадры могут оказать негативное влияние на подключение. Повышенное число коллизий и ошибки циклического контроля избыточности (CRC), согласования и бессмысленные пакеты могут стать причиной срабатывания индикатора ошибки подключения. Желтый: порт не выполняет пересылку, так как был заблокирован администратором, приостановлен из-за нарушения безопасности адреса или протоколом «Spanning Tree» (STP) из-за петли коммутации.
Нагрузка общей полосы пропускания (светодиод UTL включен)	Зеленый: текущая нагрузка отображается на фоне желтого светодиода по логарифмической шкале. Желтый: максимальная нагрузка шины коммутатора при его включении. Чередование зеленого и желтого: зависит от модели: ■ **Catalyst 2960-12, 2960-24, 2960C-24 и 2960T-24:** если все светодиоды зеленые, коммутатор использует 50% общей полосы пропускания или выше. Если крайний правый светодиод выключен, коммутатор использует больше 25%, но меньше 50% общей полосы пропускания и так далее. Если только крайний левый светодиод горит зеленым цветом, коммутатор использует менее 0,0488% общей полосы пропускания. ■ **Catalyst 2960G-12-EI:** если все светодиоды зеленые, коммутатор использует 50% общей полосы пропускания или выше. Если светодиод слота 2 модуля GBIC выключен, коммутатор использует больше 25%, но меньше 50% общей полосы пропускания. Если светодиоды для обоих слотов GBIC выключены, коммутатор используют менее 25% полной полосы пропускания, и так далее. ■ **Catalyst 2960G-24-EI и 2960G-24-EI-DC:** если все светодиоды зеленые, коммутатор использует 50% общей полосы пропускания или выше. ■ **Слот 2 модуля GBIC:** если светодиод выключен, коммутатор использует больше 25%, но меньше 50% общей полосы пропускания. Если светодиоды для обоих слотов GBIC выключены, коммутатор используют менее 25% полной полосы пропускания, и так далее. ■ **Catalyst 2960G-48-EI:** если все светодиоды зеленые, коммутатор использует 50% общей полосы пропускания или выше. Если светодиод верхнего слота 2 модуля GBIC выключен, коммутатор использует больше 25%, но меньше 50% общей полосы пропускания. Если светодиоды для обоих слотов GBIC выключены, коммутатор используют менее 25% полной полосы пропускания, и так далее.
Полнодуплексный режим (светодиод FDUP включен)	Зеленый: порты настроены в полнодуплексном режиме. Выключен: порты настроены в полудуплексном режиме.

Отображение вывода начальной загрузки коммутатора

Если при начальном запуске во время тестирования POST обнаруживаются ошибки, они выводятся на консоль. Если тестирование POST выполняется успешно, вы можете настраивать коммутатор. В этом разделе описывается вывод данных начальной загрузки коммутатора Catalyst.

Вывод первой загрузки коммутатора Catalyst 2960

```
Base ethernet MAC Address: 00:19:30:38:bd:00
Xmodem file system is available.
The password-recovery mechanism is enabled.
Initializing Flash...
flashfs[0]: 598 files, 19 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 32514048
flashfs[0]: Bytes used: 8210432
flashfs[0]: Bytes available: 24303616
flashfs[0]: flashfs fsck took 9 seconds.
...done Initializing Flash.
Boot Sector Filesystem (bs) installed, fsid: 3
done.
Loading "flash:c2960-lanbasek9-mz.122-25.SEE2/c2960-lanbasek9
-mz.122-25.SEE2.bin"...@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@
File "flash:c2960-lanbasek9-mz.122-25.SEE2/c2960-lanbasek9-mz.
122-25.SEE2.bin" uncompressed and installed, entry point: 0x3000
executing...

!Rest of startup text omitted
```

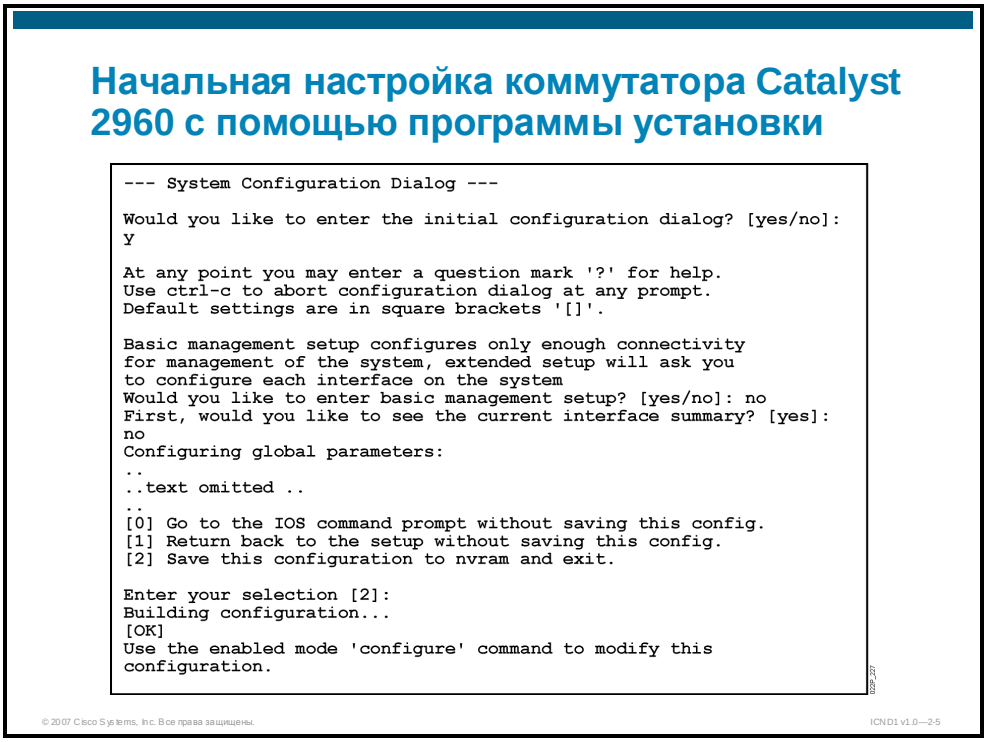


 ICND1 v1.0—2-4

После успешного завершения тестирования POST на коммутаторе Catalyst 2960 появится приглашение для ввода начальной конфигурации коммутатора. Программа автоматической установки может использоваться для задания IP-параметров коммутатора, имени хоста и кластера, паролей, а также для создания конфигурации по умолчанию для длительного использования. Позднее можно будет использовать интерфейс командной строки для задания конфигурации. Чтобы запустить программу установки, обратитесь к коммутатору с терминала ПК, подключенного к консольному порту.

Выполните начальную настройку, ответив на все вопросы по мере их появления, как показано ниже.

```
          --- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]: y
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Basic management setup configures only enough connectivity for
management of the system, extended setup will ask you to configure
each interface on the system
Would you like to enter basic management setup? [yes/no]: no
First, would you like to see the current interface summary? [yes]: no
Configuring global parameters:
  Enter host name [Switch]: SwitchX
  The enable secret is a password used to protect access to privileged
EXEC and configuration modes. This password, after entered, becomes
encrypted in the configuration.
  Enter enable secret: secret_password
  The enable password is used when you do not specify an enable secret
password, with some older software versions, and some boot images.
  Enter enable password: enable_password
  The virtual terminal password is used to protect access to the
router over a network interface.
  Enter virtual terminal password: vty_password
  Configure SNMP Network Management? [no]: no
Configuring interface parameters:
Do you want to configure Vlan1  interface? [yes]: yes
  Configure IP on this interface? [yes]: yes
    IP address for this interface: 10.1.1.140
    Subnet mask for this interface [255.0.0.0] : 255.255.255.0
    Class A network is 10.0.0.0, 24 subnet bits; mask is /24
Do you want to configure FastEthernet0/1  interface? [yes]: n
..text omitted ..
Do you want to configure FastEthernet0/24  interface? [yes]: n
Would you like to enable as a cluster command switch? [yes/no]: n
```

После задания всех необходимых параметров программа установки выводит конфигурацию, которую нужно подтвердить следующим образом:

```
The following configuration command script was created:
hostname SwitchX
enable secret 5 $1$oV63$8z7cBuveTibpCn1Rf5uI01
enable password enable_password
line vty 0 15
password vty_password
no snmp-server
!
!
interface Vlan1
ip address 10.1.1.140 255.255.255.0
!
interface FastEthernet0/1
..text omitted..
interface FastEthernet0/24
!
end
```

```
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.
Enter your selection [2]:2
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.
```

Введите **2**, чтобы завершить начальную настройку.

Вход в систему коммутатора

Когда коммутаторы Catalyst настраиваются через интерфейс командной строки посредством консоли или удаленного терминала, программное обеспечение Cisco IOS предоставляет интерфейс командной строки, именуемый EXEC. EXEC интерпретирует вводимые команды, и выполняет соответствующие операции. В этом разделе описывается вход в систему коммутатора Catalyst для начальной настройки.

В целях безопасности EXEC имеет два уровня доступа к командам:

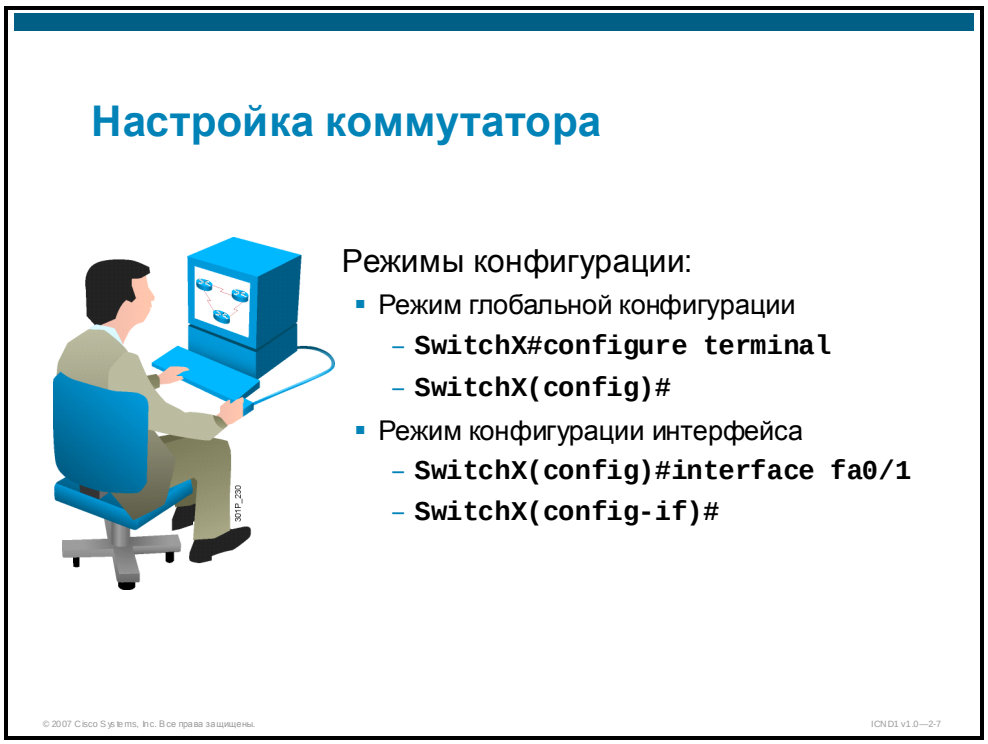
- **Пользовательский режим:** задачи ограничиваются проверкой состояния коммутатора.
- **Привилегированный режим:** задачи включают изменение конфигурации коммутатора. Этот режим также известен как режим «enable».

Чтобы перейти из пользовательского режима EXEC в привилегированный, введите команду **enable**. Затем коммутатор запрашивает пароль «enable password», если он настроен. Введите правильный пароль. По умолчанию пароль «enable password» не задан.

Примечание	В целях безопасности сетевое устройство не будет отображать вводимый пароль на экране. Но если вы настраиваете сетевое устройство через модемный канал или сеанс Telnet, пароль отправляется в виде нешифрованного текста. Telnet не поддерживает защиту пакетов. Для удаленного доступа следует использовать протокол SSH.

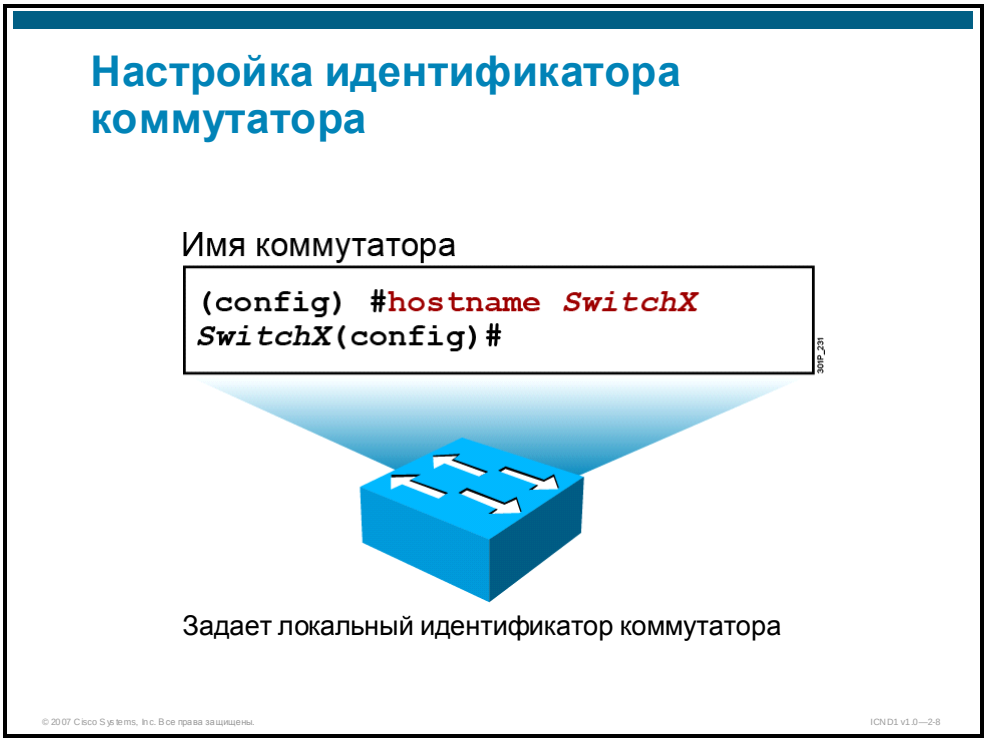
Настройка коммутатора из командной строки

Программное обеспечение коммутатора Catalyst поддерживает различные режимы конфигурации, в том числе режим глобальной конфигурации и режим конфигурации интерфейса. В этом разделе описывается начальная настройка коммутатора из обоих режимов.

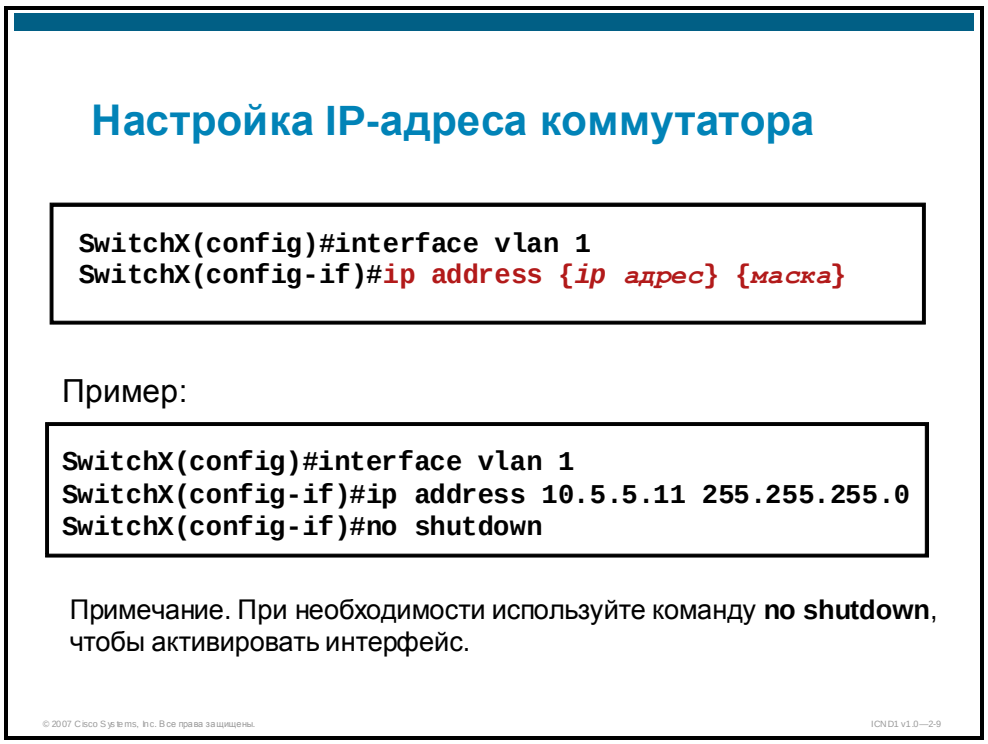


Для задания глобальных параметров коммутатора, например имени хоста и IP-адреса, используемого для управления коммутатором, следует применять режим глобальной конфигурации. Чтобы настроить определенный порт (интерфейс), используйте режим конфигурации интерфейса.

Примечание Дополнительные сведения о настройке коммутатора представлены далее в этом курсе. В этом разделе представлен обзор конфигурации коммутатора, который позволит вам выполнить начальную настройку своего коммутатора.



Одна из первых задач по настройке коммутатора состоит задании его имени. Задание имени коммутатора улучшает управление сетью за счет однозначной идентификации каждого коммутатора в сети. Имя коммутатора, в качестве которого используется имя хоста, отображается в системном приглашении. Имя коммутатора присваивается в режиме глобальной конфигурации. В примере на рисунке используется имя коммутатора **SwitchX**.



Интерфейс управления коммутатором работает как виртуальный хост уровня 3 в коммутаторе уровня 2. Удаленный доступ к интерфейсу управления коммутатором реализуется с помощью протокола уровня 3 и сетевых приложений TCP/IP. Поэтому коммутатору необходимо присвоить адрес 3-го уровня. Интерфейс управления находится по умолчанию в сети VLAN 1, поэтому IP-адрес назначается для VLAN 1.

Для настройки IP-адреса и маски подсети коммутатора необходимо перейти в режим конфигурации интерфейса VLAN 1, а затем использовать конфигурационную команду **ip address**. Коммутатор нуждается в IP-адресе для управления.

В частности IP-адрес следует назначить, если вы планируете использовать Telnet-подключение или если для управления коммутатором будет использоваться протокол SNMP.

Используйте команду конфигурации интерфейса **no shutdown**, чтобы включить интерфейс.

Настройка шлюза по умолчанию для коммутатора

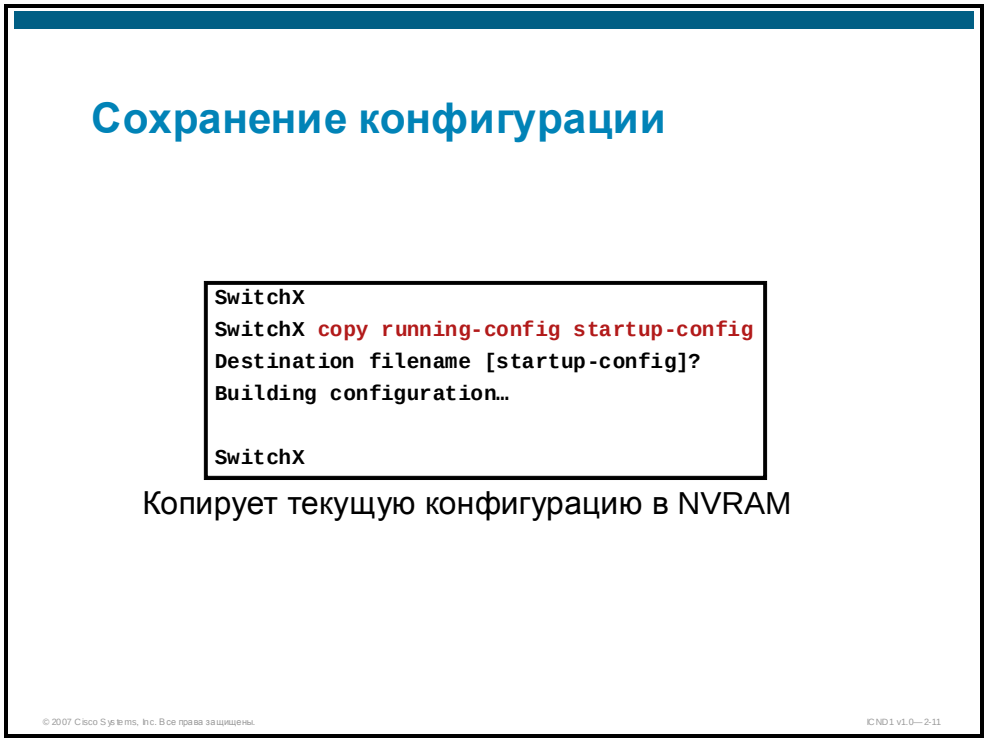

```
SwitchX(config)#ip default-gateway {ip-адрес}
```

Пример:

```
SwitchX(config)#ip default-gateway 172.20.137.1
```


Для настройки шлюза по умолчанию для коммутатора используйте команду **ip default-gateway**. Введите IP-адрес интерфейса следующего маршрутизатора, непосредственно подключенного к коммутатору, для которого настраивается шлюз по умолчанию. Шлюзу по умолчанию передаются IP-пакеты с неразрешенными IP-адресами назначения от процессов EXEC коммутатора.

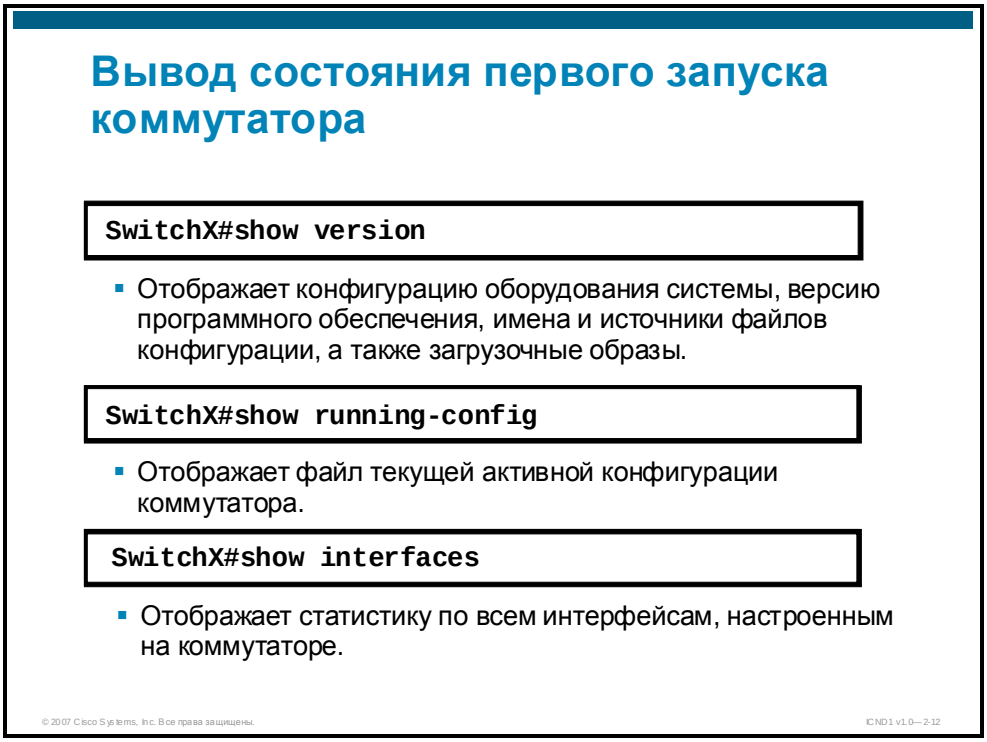
После настройки шлюза по умолчанию коммутатор сможет подключаться к удаленным сетям, с которыми ему необходимо взаимодействовать.



После ввода команд конфигурации необходимо сохранить текущую конфигурацию в NVRAM с помощью команды **copy running-config startup-config**. Если конфигурация не будет сохранена в NVRAM и устройство будет перезагружено, то конфигурация будет потеряна, и устройство вернется к последней конфигурации, сохраненной в NVRAM.

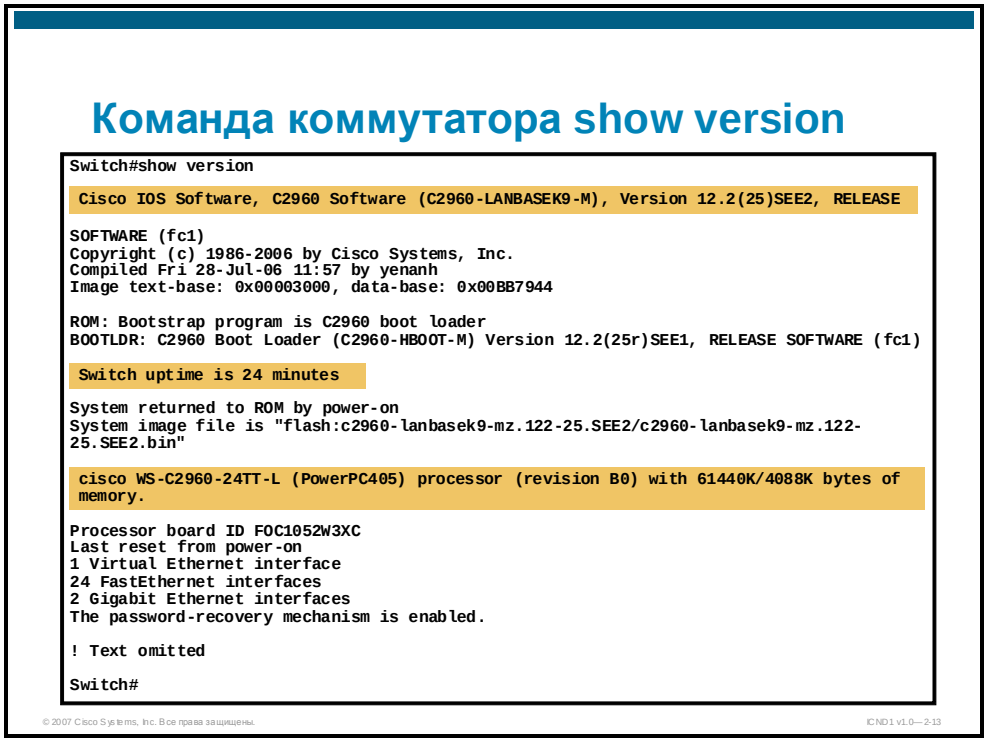
Вывод состояния первого запуска коммутатора

После входа в систему коммутатора Catalyst, состояние первого запуска коммутатора можно проверить с помощью следующих команд **show version**, **show running-config** и **show interfaces**. В этом разделе описываются команды состояния коммутатора, которые можно использовать для проверки начальной работоспособности коммутатора.



Команды состояния коммутатора:

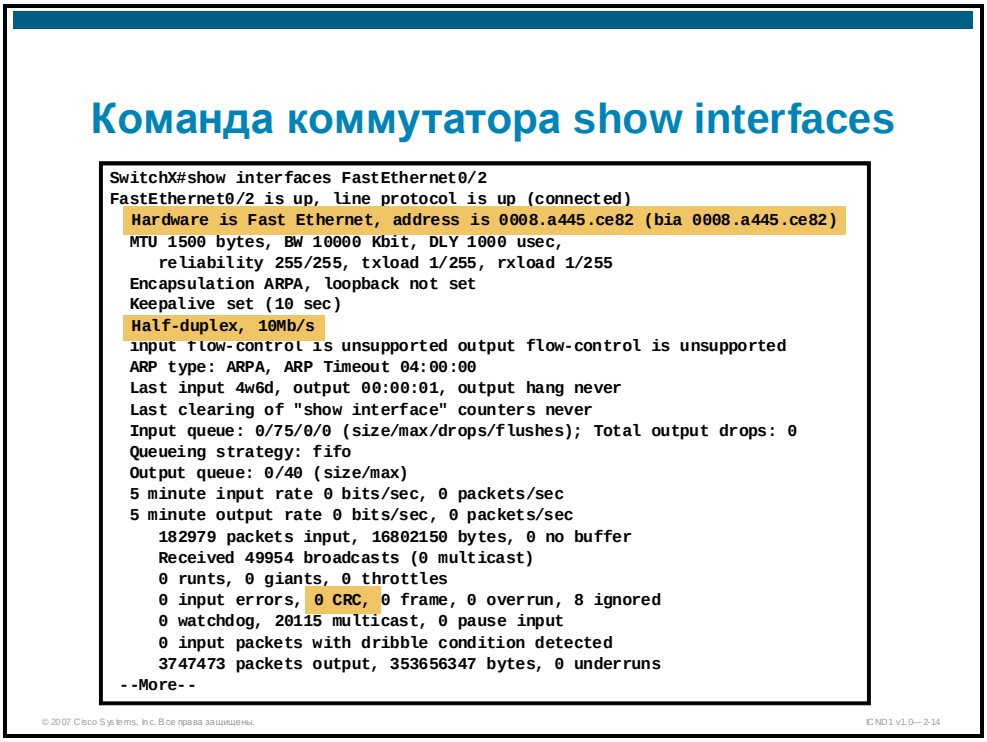
- **show version:** выводит конфигурацию аппаратного обеспечения системы и сведения о версиях программного обеспечения.
- **show running-config:** выводит файл текущей активной (действующей) конфигурации коммутатора. Эта команда требует доступа к привилегированному режиму EXEC. Здесь отображается IP-адрес, маска подсети и параметры шлюза по умолчанию.
- **show interfaces:** показывает статистику и сведения о состоянии всех интерфейсов коммутатора. Как транковые подключения, так и линейные порты коммутатора считаются интерфейсами. Вывод команды зависит от сети, для которой настроен интерфейс. Обычно эта команда вводится с параметрами *type (тип)* и *slot/number (слот/номер)*, где *type* позволяет выбрать между Ethernet и Fast Ethernet, а *slot/number* указывает слот 0 и номер порта на выбранном интерфейсе (например, e0/1).



Используйте команду EXEC **show version** для вывода конфигурации оборудования системы и сведения о версии ПО. В таблице описываются некоторые поля вывода команды **show version**.

Вывод	Описание
Cisco IOS version	Сведения о названии и номере версии программного обеспечения. Всегда указывайте весь номер версии, когда вы сообщаете о возможных проблемах ПО. В этом примере на коммутаторе работает программное обеспечение Cisco IOS версии 12.2(25)SEE2.
Switch uptime	Количество дней и времени, прошедшего с момента последней загрузки системы. В примере время работы коммутатора составляет 24 минуты.
Switch platform	Выводит информацию об аппаратной платформе, в том числе о версии и оперативной памяти.

Снимок экрана на рисунке получен на коммутатора Cisco Catalyst WS-C2960-24 с 24 портами Fast Ethernet.



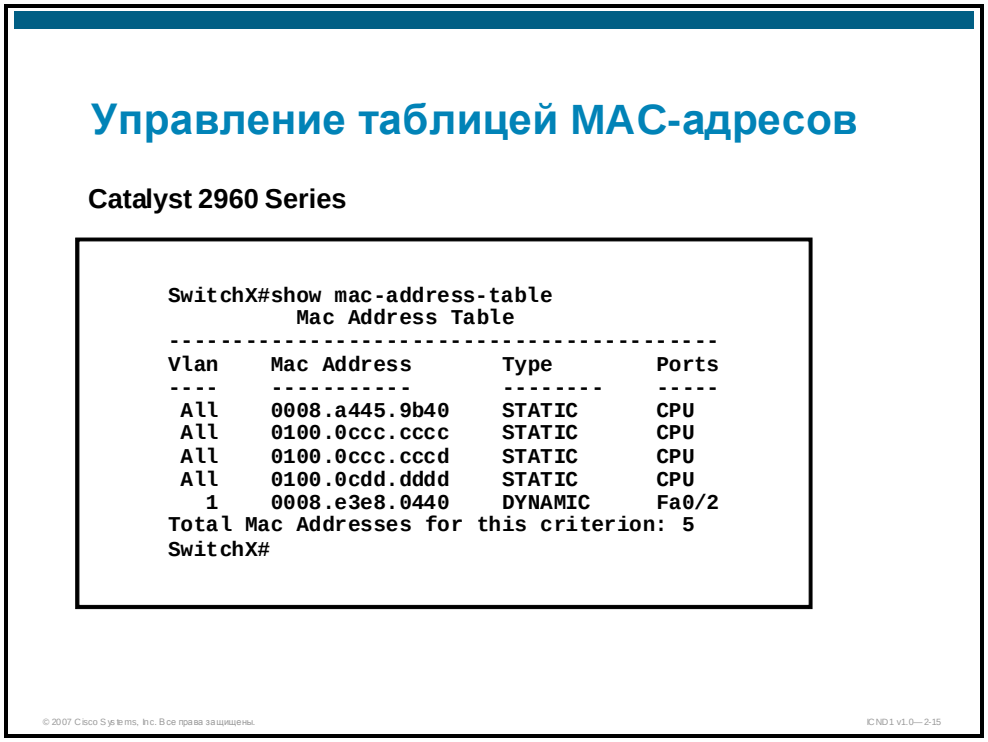
Команда **show interfaces** выводит сведения о состоянии и статистику сетевых интерфейсов коммутатора. В таблице приводятся некоторые поля вывода, которые можно использовать для проверки основных параметров коммутатора.

Вывод	Описание
FastEthernet0/2 is up	Указывает состояние аппаратного обеспечения интерфейса. В этом примере оно функционирует правильно. За состоянием аппаратного обеспечения следует состояние канального протокола, который в этом примере также исправен и активен.
address is 0008.a445.ce82…	Выводит MAC-адрес, который идентифицирует аппаратный интерфейс.
Half-duplex, 10 Mb/s	Показывает режим и тип подключения. Другие варианты: full duplex, 100 Mb/s.
CRC	Показывает, что выявлено 0 ошибок циклического контроля избыточности. Ошибки циклического контроля избыточности могут указывать на несоответствие дуплексного режима или на сбои адаптера Ethernet в подключенном устройстве.

Команда **show interfaces** будет часто использоваться при настройке и мониторинге сетевых устройств.

Управление таблицами MAC-адресов

В этом разделе описывается задание постоянных и статических адресов в таблице MAC-адресов.



Коммутаторы используют таблицы MAC-адресов для передачи данных между портами. Таблицы MAC-адресов содержат динамические, постоянные и статические адреса.

Динамические адреса – это MAC-адреса которые коммутатор получает из поля источника кадра, а затем удаляет, если они не обновляются и устаревают. Коммутатор реализует динамическую адресацию, изучая MAC-адрес источника каждого кадра, полученного с каждого порта, и добавляя MAC-адрес источника и соответствующий номер порта в таблицу MAC-адресов. По мере добавления или удаления станций в сети, коммутатор обновляет таблицу MAC-адресов, добавляя новые записи и переводя в разряд устаревших записи, которые не используются в настоящее время.

Администратор может присваивать постоянные адреса некоторым портам. В отличие от динамических адресов постоянные адреса не устаревают.

Максимальный размер таблицы MAC-адресов меняется в зависимости от модели коммутатора. Например, коммутаторы серии Catalyst 2960 могут хранить до 8 192 MAC-адреса. Когда таблица MAC-адресов переполняется, для трафика к новым неизвестным адресам выполняется лавинная рассылка.

Резюме

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

Резюме

- Запуск коммутатора Cisco IOS требует проверки физической установки, подключения питания и проверки вывода программного обеспечения Cisco IOS на консоли.
- Коммутаторы Cisco IOS оснащены несколькими светодиодными индикаторами состояния, которые светятся зеленым цветом, когда коммутатор функционирует нормально, и изменяют цвет на желтый при возникновении неисправности.
- Процедура Cisco Catalyst POST выполняется только при включении коммутатора.
- Если при начальном запуске во время тестирования POST обнаруживаются ошибки, они выводятся на консоль. Если процедура POST завершается успешно, можно приступать к процедуре настройки коммутатора.

Резюме (прод.)

- Чтобы запустить любой из режимов на коммутаторе Cisco IOS следует начать работу в пользовательском режиме EXEC. При переключения режимов необходимо ввести пароль.
- Коммутаторы Catalyst IOS можно настраивать с помощью режима глобальной конфигурации и других режимов, аналогично маршрутизаторам.
- Чтобы задать имя хоста и IP-адрес, настраивайте коммутатор Cisco IOS из командной строки.
- После входа в систему коммутатора Catalyst, состояние оборудования и программного обеспечения коммутатора можно проверить с помощью команд **show version**, **show running-config** и **show interfaces**.

Занятие 6

Общие сведения о безопасности коммутатора

Обзор

Помимо защиты физического доступа существует растущая потребность в обеспечении безопасности доступа к коммутатору через консольный порт и виртуальные порты VTY. Кроме того, важно гарантировать что неиспользуемые порты коммутатора не станут брешью в системе безопасности.

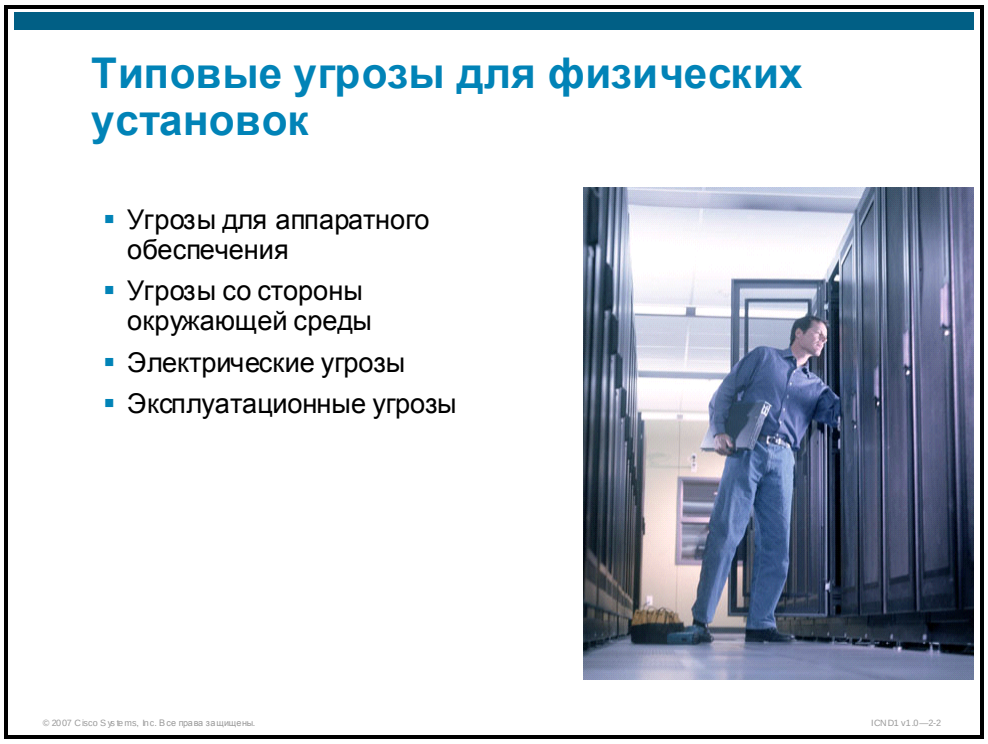
Задачи

По окончании этого занятия вы сможете создать базовую конфигурацию коммутатора Cisco. Это значит, что вы сможете выполнять следующие задачи:

- описывать способы минимизации аппаратных и электрических угроз, угрозы, связанных с обслуживанием, а также угроз со стороны окружающей среды, способных повредить безопасности коммутаторов Cisco;
- настраивать защиту на базе паролей;
- настраивать баннер входа в систему;
- описывать разницу между протоколами Telnet и SSH для удаленного доступа;
- настраивать безопасность портов;
- обеспечивать безопасность неиспользуемых портов.

Физические угрозы и угрозы со стороны окружающей среды

Часто угрозу безопасности сети представляет неверная или неполная установка сетевых устройств, причем эта угроза часто остается без внимания и приводит к печальным последствиям. Невозможно предотвратить преднамеренное или даже случайное повреждение сети в результате плохо проведенной установки только программными средствами безопасности. В этом разделе описывается, как минимизировать аппаратные и электрические угрозы, угрозы, связанные с обслуживанием, а также угрозы со стороны окружающей среды, способные ухудшить безопасность коммутаторов Cisco.

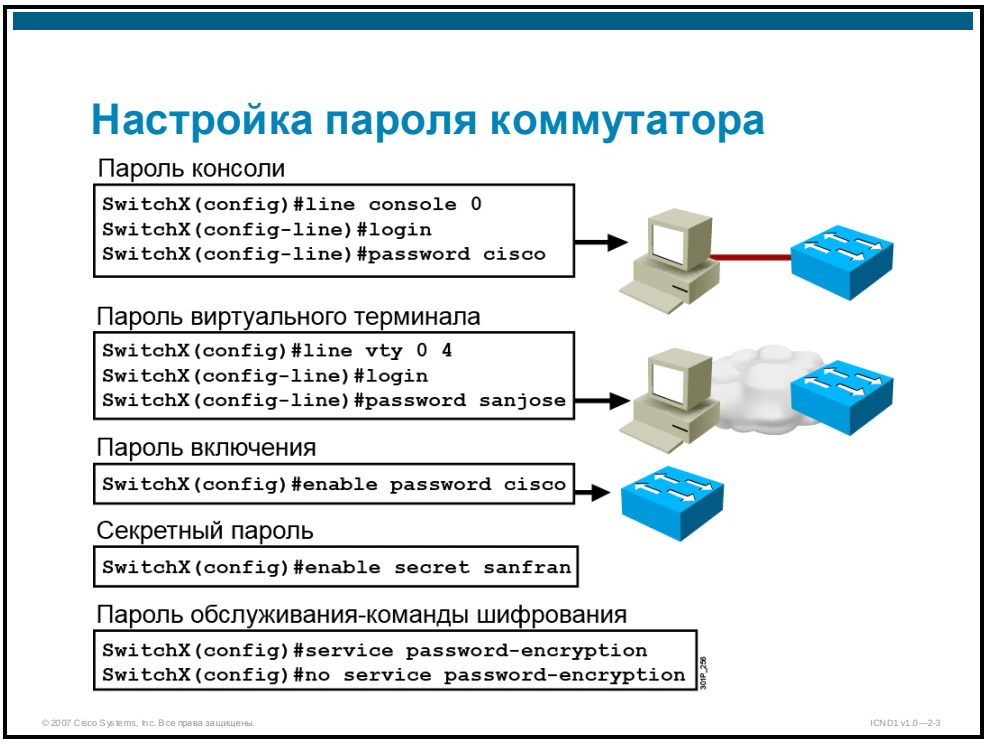


Существуют четыре класса угроз, связанных с небезопасной установкой или физическим доступом.

- **Угрозы для аппаратного обеспечения.** Это угрозы физического повреждения аппаратной части маршрутизатора или коммутатора.
- **Угрозы со стороны окружающей среды.** К ним относятся такие угрозы, как предельные температуры (слишком высокие или слишком низкие) или предельные значения влажности (слишком низкая или слишком высокая).
- **Электрические угрозы.** К ним относятся такие угрозы как пики напряжения, недостаточное напряжение в сети (провалы напряжения), колебания напряжения (шум) и полное отключение питания.
- **Эксплуатационные угрозы.** К ним относится неправильное обращение с основными электронными компонентами (электростатический разряд), отсутствие важных запасных частей, плохая прокладка кабеля, небрежная маркировка и т.д.

Настройка защиты паролем

Интерфейс командной строки (CLI) используется для настройки пароля и ввода других команд консоли. В этом разделе описывается одна из важнейших задач конфигурации – настройка пароля.



Внимание Пароли предоставляются только для учебных целей. Пароли, используемые в реальной ситуации, должны удовлетворять требования «сильного» пароля.

Вы можете обеспечить защиту коммутатора с помощью пароля, чтобы ограничить доступ к нему. Использование паролей и назначение уровней привилегий – это простой способ контроля терминального доступа в сети. Пароли можно задать для доступа к отдельным линиям, таким как консольная линия, и для доступа к привилегированному режиму EXEC. В паролях учитывается регистр.

Порты Telnet на коммутаторе известны как линии VTY. На коммутаторе может работать до шестнадцати виртуальных портов, обеспечивающих до шестнадцати одновременных сеансов Telnet. Виртуальные порты коммутатора пронумерованы от 0 до 15.

Используйте команду **line console 0** с подкомандами **password** и **login**, чтобы включить аутентификацию при входе в систему и установить пароль на консольном терминальном порту или порту VTY. По умолчанию аутентификация выключена на консольном терминальном порту а пароль не установлен консольном терминальном порту или порту VTY.

Команда **line vty 0 4** с подкомандами **password** и **login** включают аутентификацию при входе в систему и устанавливают пароль для сеансов Telnet.

С помощью команды **login local** можно включить аутентификацию на основе имени пользователя и пароля, указанного с помощью команды глобальной конфигурации **username**. Команда **username** включает аутентификацию по имени пользователя с использованием зашифрованных паролей.

Глобальная команда **enable password** ограничивает доступ к привилегированному режиму EXEC. Можно определить пароль доступа для сохранения в зашифрованной форме с помощью команды «enable secret». Для этого необходимо ввести команду **enable secret** с желаемым паролем в приглашении режима глобальной конфигурации. Если пароль «enable secret» настроен, он используется вместо простого пароля, а не вместе с ним.

Можно также добавить еще один уровень безопасности, который будет особенно полезен для паролей, пересылаемых по сети или хранящихся на TFTP-сервере. Cisco предоставляет возможность использования зашифрованных паролей. Чтобы установить шифрование пароля, введите команду **service password-encryption** в режиме глобальной конфигурации.

Отображаемые пароли и пароли, заданные после выполнения команды **service password-encryption**, будут зашифрованы.

Чтобы отключить команду, используйте версию «**no**» этой команды. Например, используйте команду **no service password-encryption**, чтобы отключить шифрование паролей.

Настройка баннера входа

Интерфейс командной строки используется для настройки «сообщения дня» и ввода других команд консоли. В этом разделе описываются некоторые задачи конфигурации, необходимые для включения баннера входа.

С помощью команды **banner login** в режиме глобальной конфигурации можно настроить баннер, который будет отображаться перед запросом имени пользователя и пароля. Чтобы отключить баннер входа, используйте версию «**no**» этой команды.

После ввода команды **banner login** поставьте за ней один или несколько пробелов и символ-разделитель по выбору. В этом примере в качестве символа-разделителя используется кавычка ("). После добавления текста баннера завершите сообщение таким же символом-разделителем.

Предупреждение	Необходимо осторожно выбирать слова, используемые в баннере входа. Выражения типа «добро пожаловать» могут означать, что доступ неограничен, что позволит хакерам оправдать свои действия.

Сравнение доступа через Telnet и SSH

В этом разделе рассматривается выбор режима удаленного доступа.

Telnet – это самый распространенный метод доступа к сетевому устройству. Однако Telnet является незащищенным методом доступа к сети, и поэтому его использование не рекомендуется. Протокол SSH – это безопасная замена Telnet, которая обеспечивает аналогичный тип доступа. Обмен данными между клиентом и сервером шифруется и в SSHv1, и в SSHv2. По возможности используйте SSHv2, так как в этом протоколе используется сложный алгоритм шифрования.

Сначала протестируйте аутентификацию без SSH, чтобы удостовериться, что аутентификация работает на коммутаторе. Аутентификация может выполняться с использованием локального имени пользователя и пароля или через сервер аутентификации, авторизации и учета (AAA) под управлением службы TACACS + или RADIUS. (Аутентификация на основе просто пароля не поддерживается в SSH.) В следующем примере показана локальная аутентификация, которая позволяет использовать протокол Telnet для получения доступа к коммутатору с помощью имени пользователя cisco и пароля cisco.

```
!--- The username command create the username and password for
the SSH session
username cisco password 0 cisco
ip domain-name mydomain.com
crypto key generate rsa
ip ssh version 2
line vty 0 4
  login local
  transport input telnet
```


Чтобы протестировать аутентификацию SSH, необходимо добавить к предыдущему сценарию инструкцию для включения SSH. Затем протестируйте SSH со станций PC и UNIX.

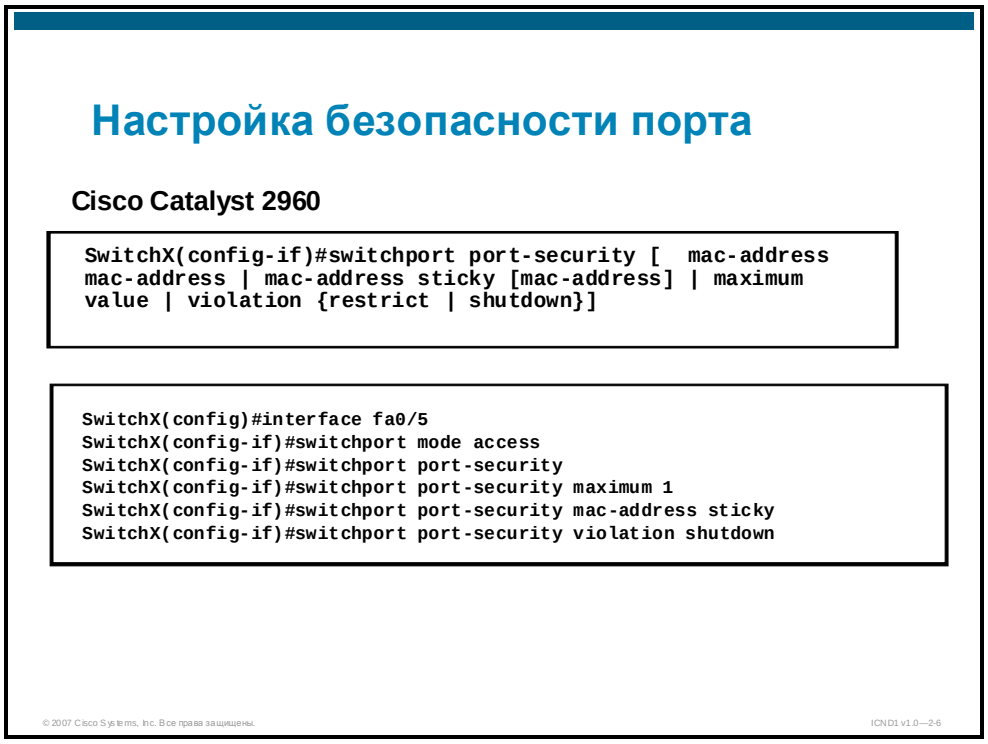
Если необходимо запретить подключение по всем протоколам, кроме SSH, добавьте команду **transport input ssh** для линии, чтобы ограничить средства подключения к коммутатору протоколом SSH. Прямое Telnet-подключение (не SSH) будет отклоняться.

```
line vty 0 4

!--- Prevent non-SSH Telnets.

transport input ssh
```

Протестируйте конфигурацию, чтобы удостовериться, что пользователи других протоколов (кроме SSH) не могут применять Telnet для получения доступа к коммутатору.

Настройка безопасности порта

В этом разделе описывается настройка безопасности порта.



Функцию безопасности порта можно использовать, чтобы ограничить подключение к интерфейсу путем ограничения и идентификации MAC-адресов станций, которым разрешен доступ к порту. После назначения безопасных MAC-адресов защищенному порту, он не будет пересылать пакеты с адресами источника, не входящими в группу заданных адресов.

Примечание Перед включением защиты порта, необходимо перевести его в режим доступа, используя команду switchport mode access.

На коммутаторе серии Cisco Catalyst 2960, используйте команду **switchport port-security** *без* ключевых слов, чтобы включить защиту порта на интерфейсе. Используйте команду интерфейса **switchport port-security** *с* ключевыми словами, чтобы настроить безопасный MAC-адрес, максимальное число безопасных MAC-адресов или режим безопасности. Используйте версию **no** с этой командой, чтобы отключить защиту порта или вернуться к параметрам по умолчанию.

Примечание Чтобы активировать защиту порта, необходимо перевести его в режим доступа.

Вы можете добавить безопасные адреса в таблицу адресов после того, как установите максимальное число безопасных MAC-адресов, разрешенных на порту. Это можно сделать следующими способами:

- Настроить все адреса вручную (**switchport port-security mac-address 0008.eeee.eeee**).

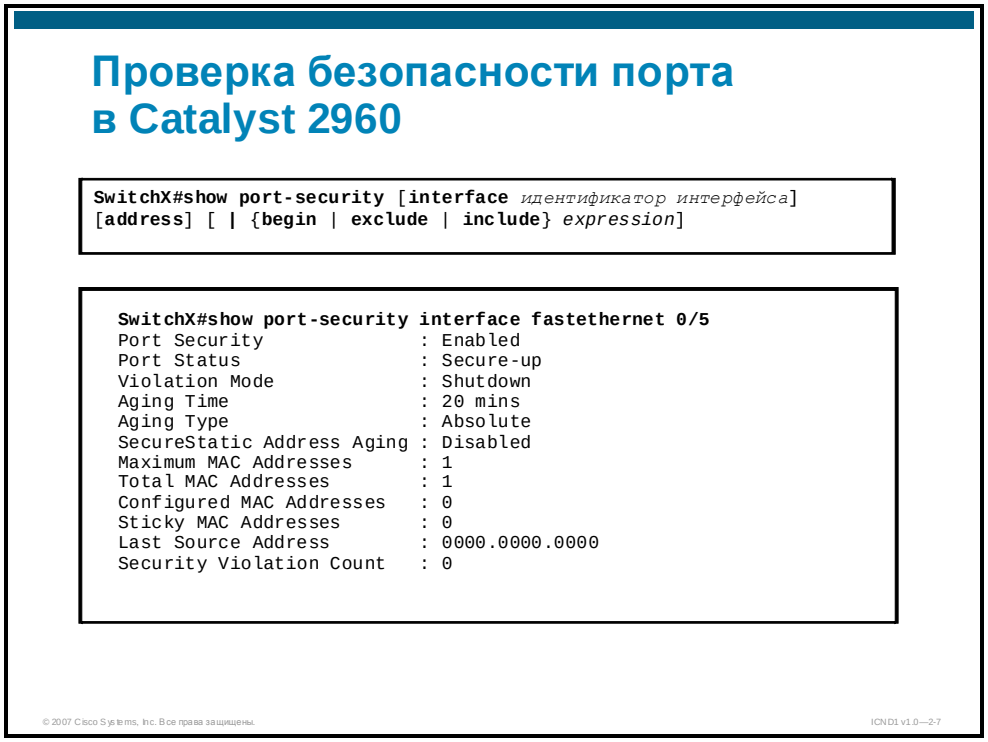
- Позволить порту динамически настраивать все адреса (**switchport port-security mac-address sticky**).
- Настроить несколько MAC-адресов и разрешить автоматическую настройку остальных адресов.

Вы можете настроить интерфейс на преобразование динамических MAC-адресов в «закрепленные» безопасные MAC-адреса и добавление этих адресов в текущую конфигурацию, включив функцию *sticky learning.* Чтобы включить функцию sticky learning, введите команду конфигурации интерфейса **switchport port-security mac-address sticky**. После ввода этой команды, интерфейс будет преобразовывать все динамические MAC-адреса в безопасные, включая адреса, которые были динамически получены до включения функции *sticky learning*, в «закрепленные» безопасные MAC-адреса.

Закрепленные безопасные MAC-адреса не добавляются в файл загрузочной конфигурации (который применяется при каждом перезапуске коммутатора). Если вы сохраните закрепленные безопасные MAC-адреса в файле конфигурации, при перезапуске коммутатора интерфейсу не придется повторно получать эти адреса. Если вы не сохраняете конфигурацию, MAC-адреса будут потеряны. Если режим sticky learning отключен, безопасные MAC-адреса преобразуются в динамические безопасные адреса и удаляются из текущей конфигурации. Защищенный порт может иметь от 1 до 132 безопасных адресов. Общее количество безопасных адресов, доступных на коммутаторе составляет 1 024.
Ситуации нарушения режима безопасности:

- В таблицу адресов добавлено максимальное число безопасных MAC-адресов, и станция, MAC-адрес которой не зафиксирован в таблице адресов, пытается получить доступ к интерфейсу.
- Адрес, полученный или настроенный на одном защищенном интерфейсе, замечен на другом защищенном интерфейсе в той же VLAN.

Примечание Защита порта отключена по умолчанию.

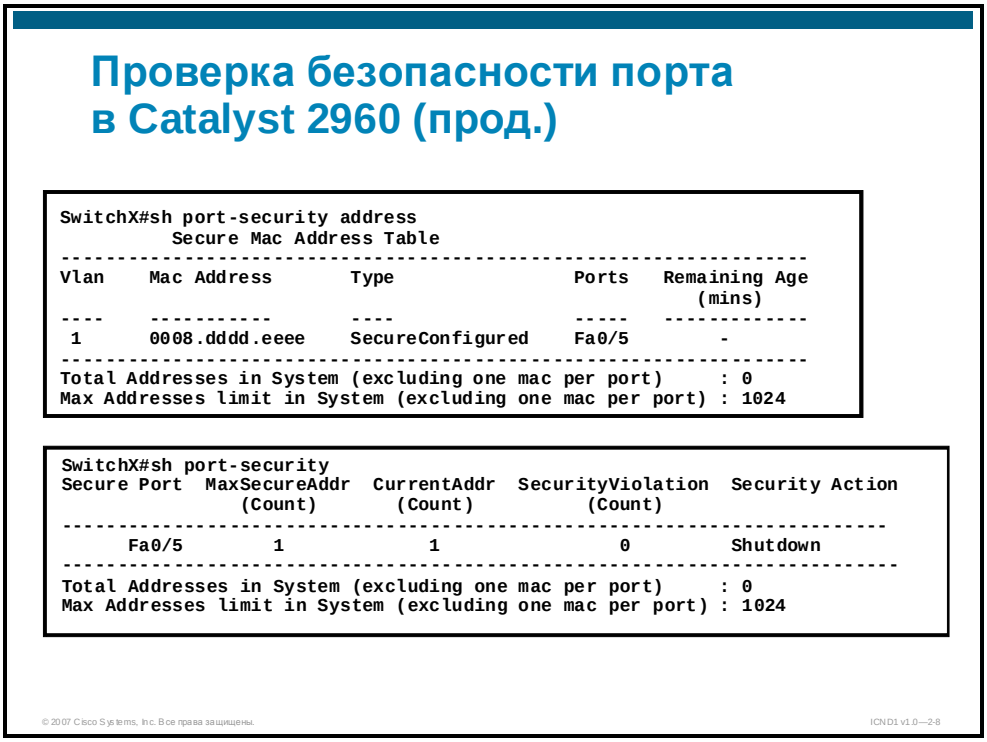


В коммутаторе Catalyst 2960 используйте команду **show port-security interface** в привилегированном режиме EXEC, чтобы вывести параметры безопаности порта, заданные для интерфейса.

Нарушение безопасности происходит, когда защищенный порт получает адрес источника, назначенный другому защищенному порту, или когда порт пробует получить адрес, который превышает ограничение на размер таблицы, установленное с помощью команды **switchport port-security maximum**.

В таблице перечислены параметры, которые можно использовать с командой **show port-security**.

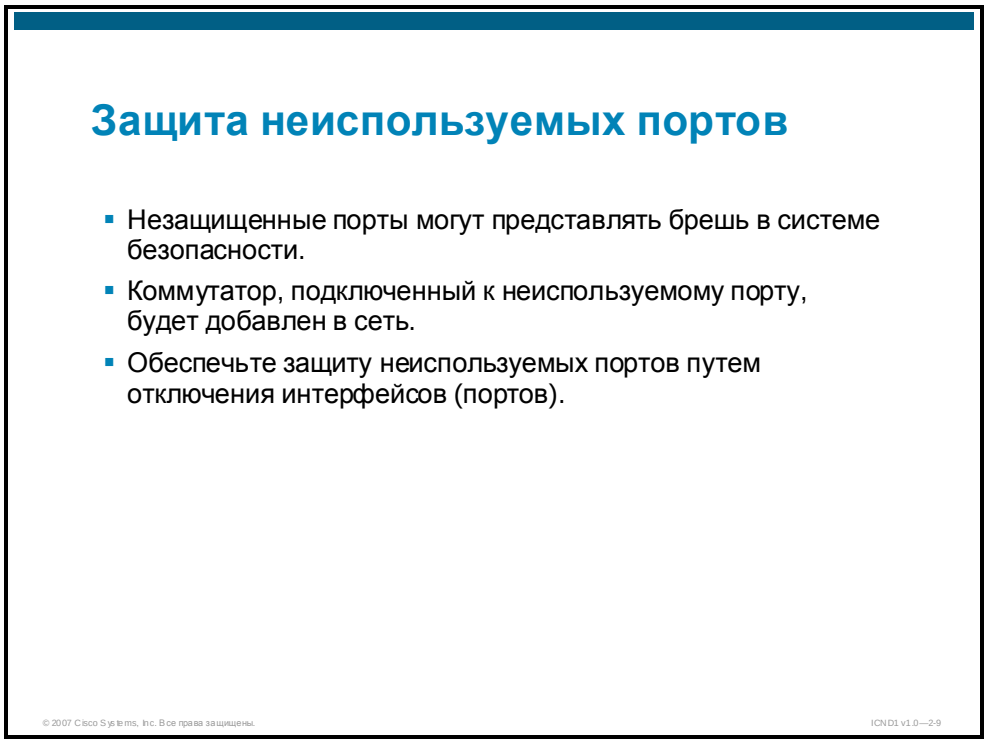
Команда	Описание
interface *идентификатор интерфейса*	(Необязательно) Выводит параметры защиты порта для указанного интерфейса.
address	(Необязательно) Выводит все безопасные адреса всех портов.
begin	(Необязательно) Настраивает вывод так, чтобы он начинался с линии, которая соответствует указанному выражению.
exclude	(Необязательно) Настраивает вывод так, чтобы линии, которые соответствует указанному выражению, исключались.
include	(Необязательно) Настраивает вывод так, чтобы линии, которые соответствует указанному выражению, включались.
expression	Вводит выражение, которое будет использоваться в качестве контрольной точки.



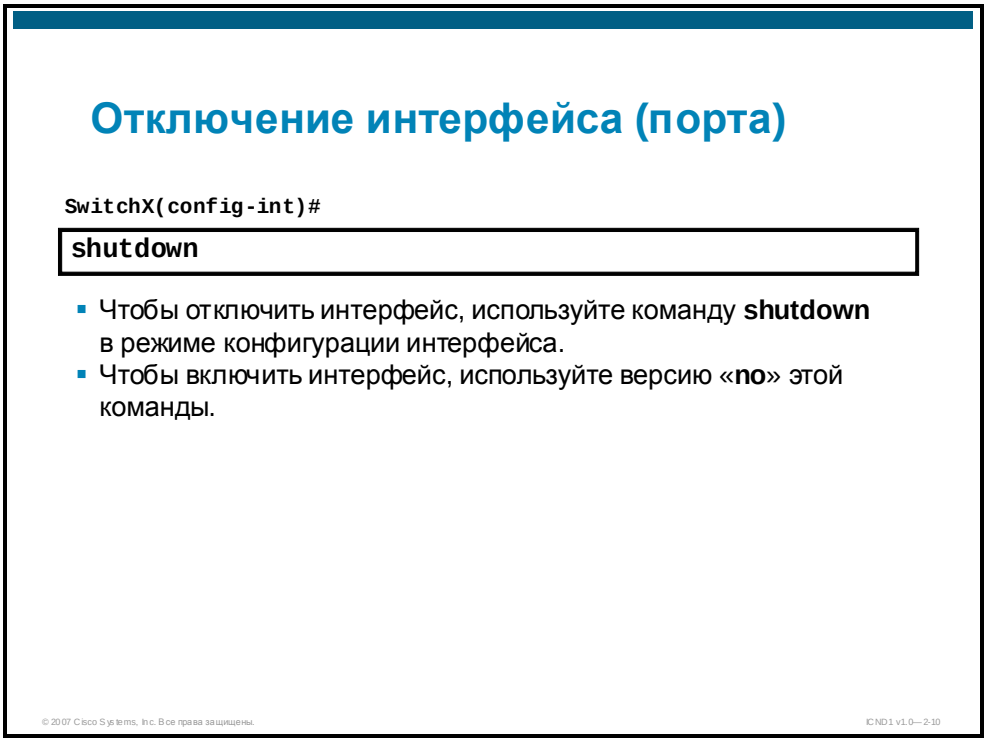
Используйте команду **show port-security address**, чтобы вывести безопасные MAC-адреса всех портов. Используйте команду **show port-security** без ключевых слов, чтобы вывести параметры безопасности порта для коммутатора.

Защита неиспользуемых портов

В этом разделе описывается потребность в защите неиспользуемых портов.



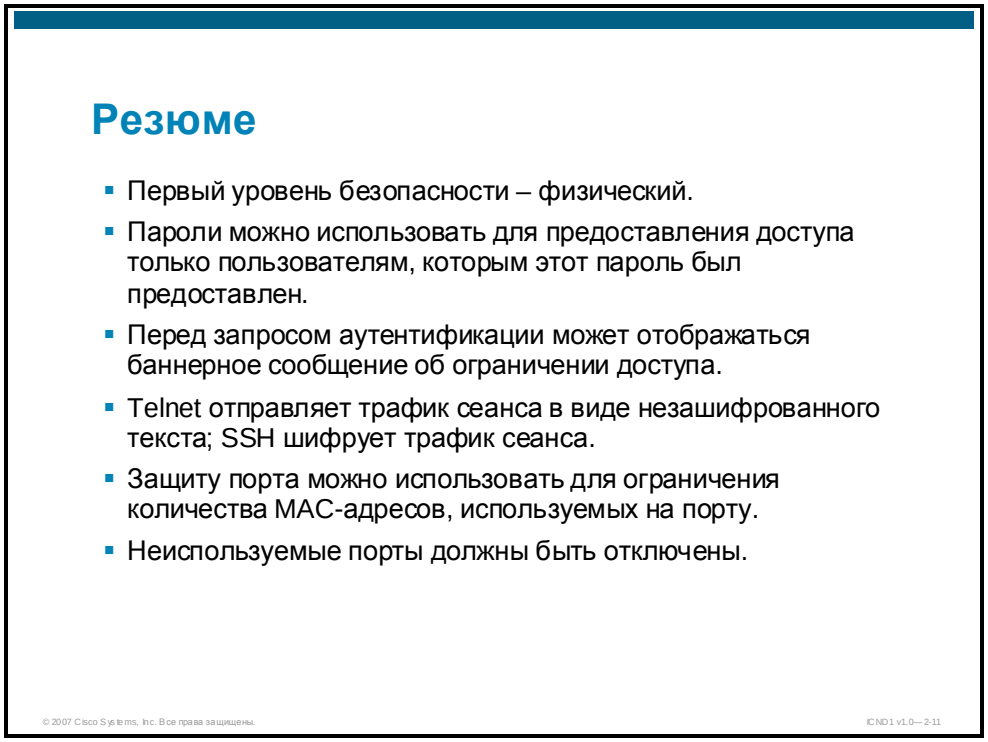
Дома незапертая дверь может быть угрозой безопасности. То же самое верно и в отношении неиспользуемых портов коммутатора. Хакер может подключить коммутатор к неиспользуемому порту и, таким образом, подключиться к сети. Поэтому незащищенные порты могут представлять брешь в системе безопасности. Чтобы решить эту проблему, необходимо защитить неиспользуемые порты (интерфейсы), отключив их.



Чтобы отключить интерфейс, используйте команду **shutdown** в режиме конфигурации интерфейса. Чтобы включить интерфейс, используйте версию «**no**» этой команды: **no shutdown**.

Резюме

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



Занятие 7

Максимизация преимуществ коммутации

Обзор

По мере добавления устройств к ЛВС для поддержки большего числа пользователей и увеличения полосы пропускания для растущего числа сетевых приложений, сохранение приемлемого уровня производительности сети становится все более насущной проблемой. Существует несколько способов усовершенствовать коммутируемые ЛВС Ethernet для удовлетворения требований пользователей к производительности и доступности. В этом занятии описывается несколько методов повышения производительности, включая микросегментацию, полнодуплексную связь и решения на основе протокола «Spanning Tree».

Задачи

По окончании этого занятия вы сможете перечислять способы оптимизации ЛВС Ethernet. Это значит, что вы сможете выполнять следующие задачи:

- перечислять характеристики и преимущества микросегментации;
- сравнивать полудуплексный и полнодуплексный режимы ЛВС Ethernet;
- выявлять потребность в разных скоростях среды в корпоративных сетях и описывать, как удовлетворить эту потребность в коммутируемой сети Ethernet;
- описывать влияние петель на работу коммутируемой ЛВС;
- описывать, как протокол STP предотвращает образование петель из-за физического резервирования ЛВС Ethernet.

Микросегментация

Микросегментация исключает появление коллизий в сегменте, обеспечивая ряд преимуществ, связанных с увеличением производительности сети. В этом разделе описывается работа микросегментации в коммутируемой ЛВС.

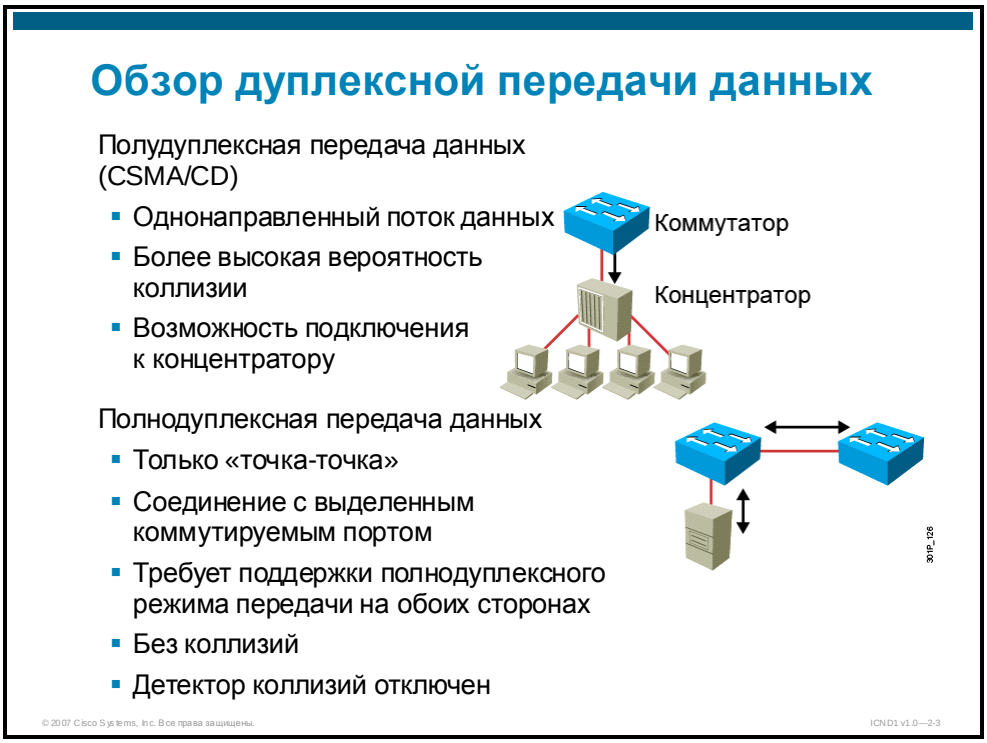
Микросегментация обеспечивается за счет внедрения коммутации ЛВС. Каждое устройство в сегменте сети подключается к порту коммутатора напрямую, и ему не приходится конкурировать с другими устройствами в сегменте за полосу пропускания. Эта важная функция исключает коллизии и увеличивает эффективную скорость передачи данных в полнодуплексном режиме, что обеспечивает существенное увеличение доступной полосы пропускания.

Пример: получение выделенного въезда на автомагистраль

Передачу данных можно сравнить с автомагистралью, кадры данных путешествуют по магистрали подобно автомобилям. Подобно тому, как автомобили используют наклонные въезды на автомагистраль, устройства подключаются к сети, когда им необходимо передать данные. Однако чем больше автомобилей на автомагистрали, тем сильнее загружены такие въезды, что позволяет лишь нескольким автомобилям получить доступ к магистрали, а также повышает вероятность столкновения (коллизии). Но если бы у каждого автомобиля был свой собственный въезд, все автомобили имели бы равный доступ к автомагистрали, и не было бы ни задержек ни столкновений. Микросегментация, которую обеспечивают коммутаторы ЛВС, дает каждому сетевому устройству свой собственный «въезд», и ему не приходится конкурировать с другими устройствами за место на сетевой «магистрали».

Дуплексная связь

Полнодуплексная связь увеличивает эффективную полосу пропускания, позволяя передавать данные одновременно в обоих направлениях. Однако этот метод оптимизации работы сети требует внедрения микросегментации до реализации полнодуплексной связи. В этом разделе описывается полудуплексная и полнодуплексная связь, а также улучшение работы коммутируемой ЛВС благодаря полнодуплексной связи.



В полудуплексном режиме используется метод Ethernet CSMA/CD. Традиционная общая ЛВС работает в полудуплексном режиме и уязвима к коллизиям при передаче данных по проводам.

Полнодуплексный Ethernet значительно повышает производительность сети *без* издержек на установку новых сред передачи данных. Полнодуплексная передача между станциями достигается за счет использования соединений Ethernet «точка-точка», Fast Ethernet и Gigabit Ethernet. Такая схема не подвержена действию коллизий. Кадры, пересылаемые двумя связанными конечными узлами, не могут столкнуться, потому что конечные узлы используют два отдельных канала связи по кабелю категории 5 или категории 3. Каждое полнодуплексное соединение использует только один порт.

Полнодуплексное соединение портов – это связь «точка-точка» между коммутаторами и конечными узлами, но не между общими концентраторами. Узлы, которые непосредственно подключены к выделенному порту коммутатора с помощью сетевых адаптеров, поддерживающих полнодуплексную связь, должны подключаться к портам коммутатора, настроенными для работы в полнодуплексном режиме. Большинство продаваемых сегодня сетевых адаптеров Ethernet, Fast Ethernet и Gigabit Ethernet работают в полнодуплексном режиме. В полнодуплексном режиме детектор коллизий отключен.

Узлы, которые подключены к концентраторам, совместно использующим подключение к порту коммутатора, должны работать в полудуплексном режиме, так как конечные станции должны иметь возможность обнаруживать коллизии.

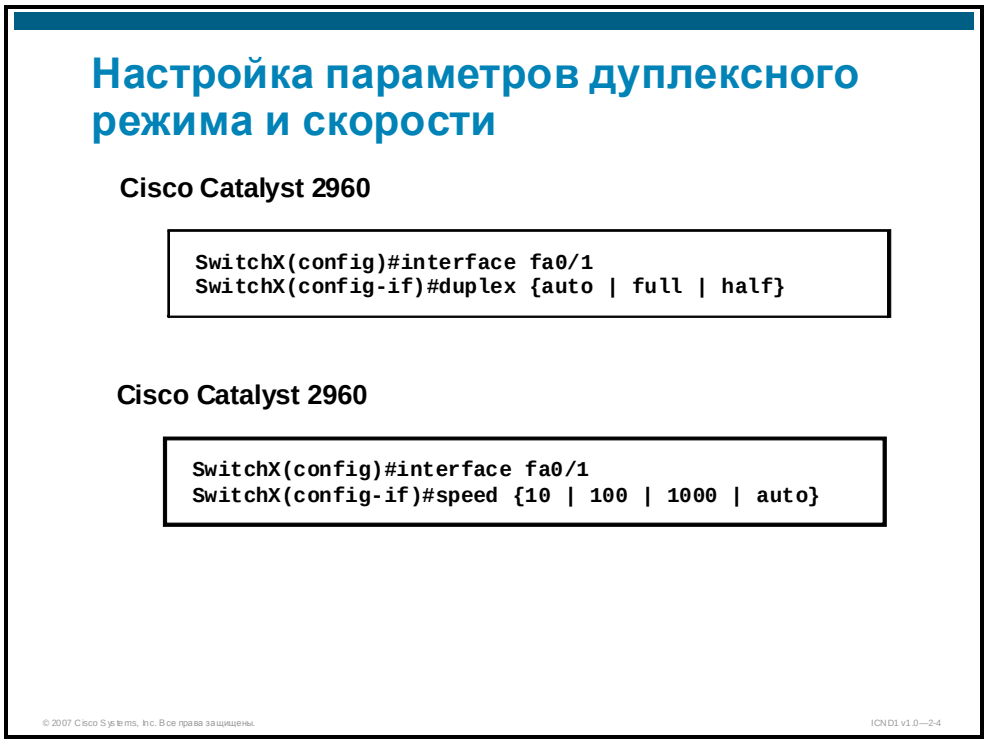
Эффективность конфигурации стандартной общей сети Ethernet обычно составляет 50 – 60% от полосы пропускания 10 Мбит/с. Полнодуплексная сеть Ethernet предлагает 100-процентную эффективность в обоих направлениях (скорость приема и скорость передачи равняются 10 Мбит/с).

Полнодуплексная система связи

Поскольку каждое устройство в микросегментированной коммутируемой ЛВС подключается непосредственно к порту коммутатора, порт коммутатора и данное устройство соединяются в режиме «точка-точка». В сетях с концентраторами вместо коммутаторов устройства могут обмениваться данными только в одном направлении в каждый отдельно взятый момент времени, так как им приходится конкурировать за полосу пропускания сети. Этот тип связи именуется полудуплексным, так как позволяет либо посылать, либо принимать данные, но не поддерживает параллельное выполнение этих операций. При этом микросегментированные порты коммутатора позволяют подключенным устройствам работать в полнодуплексном режиме, а это значит, что они могут отправлять и принимать данные одновременно. Эта возможность фактически удваивает полосу пропускания между устройствами.

Пример: диалог

Если вы используете устройство голосовой связи, например портативную радиостанцию, вы будете общаться в полудуплексном режиме. Вы можете говорить, но чтобы услышать, что говорит человек на другом конце вы должны будете замолчать. Однако по телефону вы можете общаться с другим человеком в полнодуплексном режиме: каждый абонент может говорить и одновременно слышать то, что говорит другой абонент.



Конфигурация дуплексного интерфейса

В этом разделе описывается задание и просмотр параметров дуплексной связи.

Используйте команду конфигурации интерфейса **duplex**, чтобы задать дуплексный режим для портов коммутатора.

Параметры дуплекса на коммутаторах серии Cisco Catalyst 2960:

- параметр **auto** обеспечивает автоматическое согласование дуплексного режима; при включении автоматического согласования два порта связываются друг с другом, чтобы определить наилучший режим работы;
- параметр **full** устанавливает дуплексный режим;
- параметр **half** устанавливает полудуплексный режим.

Для портов Fast Ethernet и 10/100/1000 по умолчанию выбирается параметр **auto**. Для портов 100BASE-FX по умолчанию выбирается параметр **full.** Порты 10/100/1000 функционируют либо в полудуплексном, либо в полнодуплексном режиме, когда работают со скоростью 10 или 100 Мбит/с, и только в полнодуплексном, когда работают со скоростью 1 000 Мбит/с.

Порты 100BASE-FX работают только со скоростью 100 Мбит/с и в полнодуплексном режиме.

Примечание Сведения о параметре дуплексного режима по умолчанию для портов модуля GBIC см. в документации по модулю GBIC.

Отображение параметров дуплексной передачи

```
SwitchX#show interfaces fastethernet0/2
FastEthernet0/2 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0008.a445.9b42 (bia 0008.a445.9b42)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 10Mb/s
  input flow-control is unsupported output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:57, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     323479 packets input, 44931071 bytes, 0 no buffer
     Received 98960 broadcasts (0 multicast)
     1 runts, 0 giants, 0 throttles
     1 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 36374 multicast, 0 pause input
     0 input packets with dribble condition detected
     1284934 packets output, 103121707 bytes, 0 underruns
     0 output errors, 2 collisions, 6 interface resets
     0 babbles, 0 late collision, 29 deferred
     0 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out
```

Пример: вывод параметров дуплексной связи

Проверьте параметры дуплексной связи с помощью команды **show interfaces** на коммутаторах серии Catalyst 2960. Команда **show interfaces** в привилегированном режиме EXEC выдает статистику и состояние всех или выбранных интерфейсов. На рисунке представлены параметры дуплексного режима интерфейса.

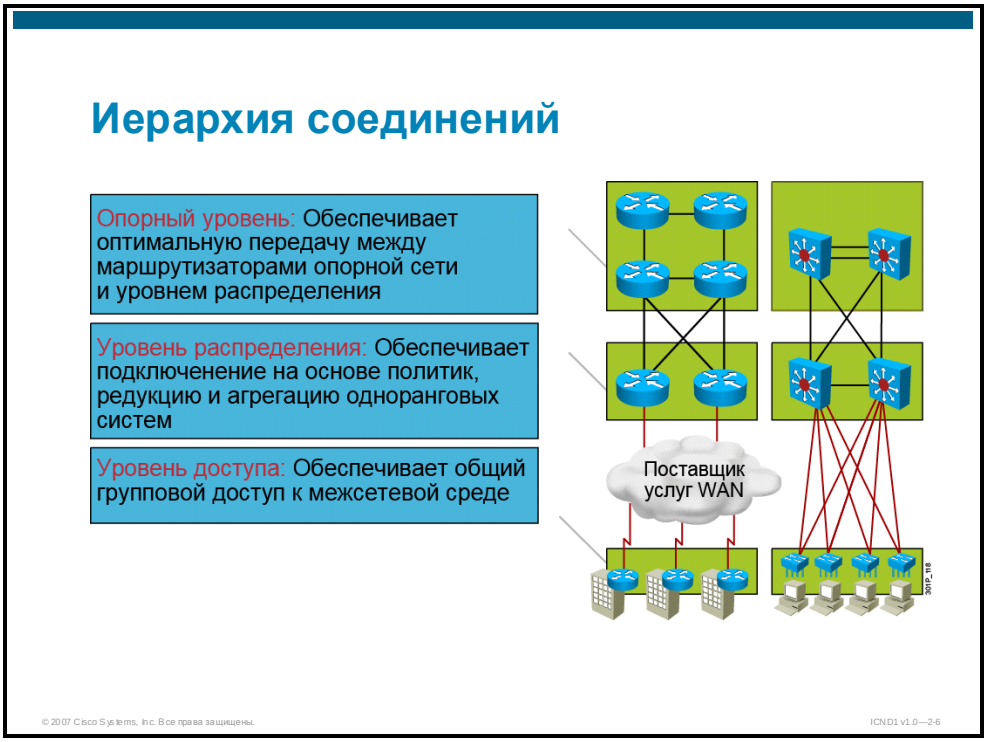
Автосогласование может приводить к непредсказуемым результатам. По умолчанию, если автосогласование завершается неудачно, коммутатор Catalyst переводит соответствующий порт коммутатора в полудуплексный режим. Это происходит, если подключенное устройство не поддерживает автосогласование. Если устройство вручную настроено в полудуплексном режиме, такой переход будет соответствовать режиму коммутатора по умолчанию. Однако ошибки автосогласования могут происходить, когда устройство вручную настроено в полнодуплексном режиме. Такая конфигурация – полудуплексный режим на одной стороне и полнодуплексный на другом – вызывает коллизии со стороны узла в полудуплексном режиме. Чтобы избежать этой ситуации, задайте параметры дуплексного режима коммутатора вручную в соответствии с подключенным устройством.

Если порт коммутатора работает в полнодуплексном режиме, а подключенное устройство – в полудуплексном режиме, поищите ошибки контрольной последовательности кадра (FCS) на полнодуплексном порту коммутатора.

Для выявления ошибок FCS можно использовать команду **show interfaces**.

Потребность в средах разной скорости в корпоративных сетях

Крупные сети содержат большое количество конечных систем, серверов и сетевых устройств, и каждое из них может требовать обмена данными на различных скоростях. В этом разделе описываются причины, по которым поддержка различных скоростей в корпоративной сети необходима.

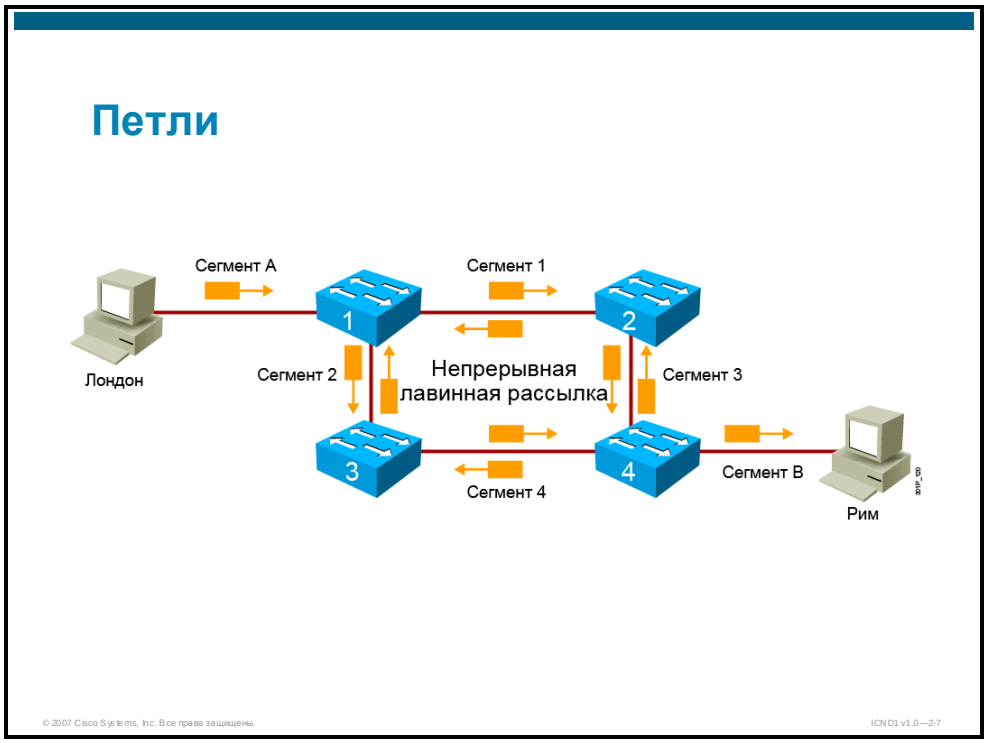


Существует несколько высокоскоростных Ethernet-протоколов (например, Fast Ethernet и Gigabit Ethernet), которые обеспечивают скорость, необходимую для адекватной работы крупных сетей. Однако стоимость внедрения высокоскоростных подключений во всех частях сети предприятия очень высока, такая сеть не будет постоянно использоваться всеми пользователями и устройствами. Поэтому иерархия соединений Ethernet – оптимальный способ предоставления скорости с учетом требований максимальной эффективности.

В стандартной иерархии соединений устройства конечного пользователя обычно называются системами уровня доступа, так как являются первичной точкой, в которой выполняется обращение к сети для передачи данных. Системы конечного пользователя объединены на уровне сервера или рабочей группы (уровень распределения), и при необходимости системы конечного пользователя будут использовать магистраль (или центральную часть сети), чтобы получить доступ к другому устройству уровня распределения. Соединения более высокой скорости обычно резервируется для устройств, которые передают большие объемы данных от многочисленных пользователей, особенно на распределительном и магистральном уровнях.

Физическое резервирование в ЛВС Ethernet

Когда множество коммутаторов работают в одной сети, существует вероятность образования преднамеренных или неумышленных физических петель. При возникновении петель возможно образование широковещательного шторма, который может распространиться по всей сети. В этом разделе описывается влияние петель на работу коммутируемой ЛВС.



Добавление коммутаторов в ЛВС может обеспечить преимущества резервирования, то есть подключение двух коммутаторов к одному и тому же сегменту сети обеспечивает непрерывную работу в случае неисправности одного из сегментов. Резервирование может обеспечить постоянную доступность сети. Однако при использовании коммутаторов для резервирования в сети существует вероятность возникновения петель. Когда хост одного сегмента сети передает данные хосту в другой сегмент сети и они связаны двумя или более коммутаторами, каждый коммутатор получает кадры, ищет местоположение принимающего устройства и пересылает кадр. Поскольку каждый коммутатор пересылает кадры, выполняется дублирование каждого кадра. Этот процесс приводит к образованию петли, и кадр циркулирует между двумя путями, без удаления из сети. Кроме того, в таблицы MAC-адресов может заноситься неверная информация об адресах, что приводит к ошибочной пересылке данных.

Помимо основных проблем подключения, быстрое распространение широковещательных сообщений в сетях с петлями также представляет серьезную проблему. Исходя из принципа работы коммутатора, для любого группового, широковещательного или неизвестного трафика будет выполняться лавинная рассылка по всем портам кроме порта, из которого принимается этот трафик. В результате возникает «шторм» трафика, бесконечно распространяющийся по всей сети и немедленно занимающий всю доступную полосу пропускания.

Пример: петли в коммутируемой сети

Предположим, что хост с именем London посылает кадр на хост с именем Rome. London находится в сегменте A, а Rome – в сегменте B. Между хостами установлены соединения с резервированием для продолжения работы на случай сбоя сегмента. В этом примере предполагается, что ни один из коммутаторов не получил адрес хоста B.

Коммутатор 1 получает кадр, предназначенный для хоста B, и передает его на коммутаторы 2 и 3. И коммутатор 2, и коммутатор 3 получают кадр от London (через коммутатор 1) и запоминают, что London находится в сегменте 1 и 2 соответственно. Оба коммутатора передают кадр на коммутатор 4.

Коммутатор 4 получает две копии кадра от London: одну копию через коммутатор 2 и вторую через коммутатор 3. Предположим, что кадр от коммутатора 2 прибывает раньше всех. Коммутатор 4 запоминает, что Лондон находится в сегменте 3. Поскольку коммутатор 4 не знает адрес хоста Rome, он пересылает кадр от коммутатора 2 хосту Rome и коммутатору 3. Когда кадр от коммутатора 3 приходит на коммутатор 4, коммутатор 4 обновляет свою таблицу адресов и фиксирует, что хост London находится в сегменте 4. Затем он передает кадр хосту Rome и коммутатору 2.

Теперь коммутаторы 2 и 3 изменяют свои внутренние таблицы и фиксируют, что хост London находится в сегменте 3 и 4 соответственно. Если бы исходный кадр хоста London был широковещательным, оба коммутатора пересылали бы кадр бесконечно, заняв всю доступную полосу пропускания сети и заблокировав передачу других пакетов в обоих сегментах. Такая ситуация называется широковещательным штормом.

Решение проблемы петель с помощью протокола STP

Протокол STP – это решение проблемы петель, которые возникают при резервировании сети. В этом разделе описывается принцип работы протокола STP.

Решением проблемы петель является протокол STP, который управляет физическими каналами доступа к сегментам сети. STP обеспечивает физическое резервирование путей, но при этом предотвращает нежелательное воздействие активных петель на сеть. На коммутаторах Catalyst протокол STP работает по умолчанию.

STP работает следующим образом:

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

Примечание Более подробно протокол STP рассматривается в курсе Interconnecting Cisco Networking Devices Part 2 (ICND2).

Резюме

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

Резюме

- Коммутируемые ЛВС поддерживают микросегментацию. Это означает, что каждое устройство в сегменте сети подключается напрямую к порту коммутатора и получает выделенную полосу пропускания. Устройствам не приходится конкурировать за полосу пропускания с другими устройствами в сети.
- Полудуплексная передача в ЛВС Ethernet позволяет передавать данные одновременно только в одном направлении (либо передавать, либо получать); полнодуплексная передача позволяет передавать и получать данные одновременно. Коммутаторы обеспечивают полнодуплексную связь.
- Использование иерархии соединений Ethernet, как правило, является наиболее эффективным способом предоставления скорости в сетях комплекса зданий, в которых порты Fast Ethernet и Gigabit Ethernet используется для подключения рабочих групп и магистральных соединений.

Резюме (прод.)

- Петли образуются, когда коммутаторы, подключенные к одному и тому же сегменту, выполняют передачу одних и тех же данных. Кадры данных циркулируют между двумя путями, оставаясь в сети, и могут привести к появлению ошибочных данных в таблицах MAC-адресов.
- Решением проблемы петель является протокол STP, который управляет путями к сетевым сегментам. Протокол STP обеспечивает резервирование путей в ЛВС Ethernet и предотвращает нежелательное воздействие активных петель в сети.

Занятие 8

Решение проблем, связанных с коммутаторами

Обзор

Большинство проблем коммутируемой сети возникает при первоначальном внедрении. Теоретически, однажды установленная сеть работает без проблем. Однако это только теоретически. Все меняется; повреждаются кабели, меняется конфигурация, к коммутатору подключаются новые устройства, которые требуют изменения его конфигурации. Текущее обслуживание – важный аспект существования сети.

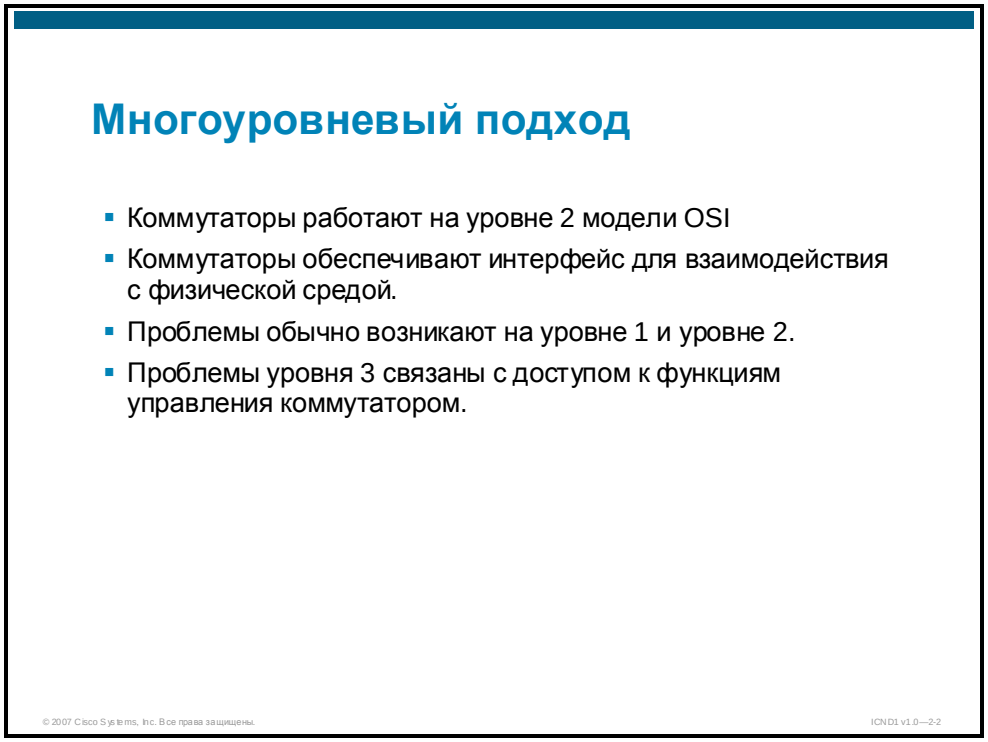
Задачи

По окончании этого занятия вы сможете выявлять и устранять типовые проблемы коммутируемой сети. Это значит, что вы сможете выполнять следующие задачи:

- описывать поиск и устранение неисправностей на основе многоуровневого подхода;
- выявлять и устранять типовые проблемы в среде передачи данных коммутируемой сети;
- выявлять и устранять типовые проблемы доступа к портам;
- выявлять и устранять типовые проблемы конфигурации.

Использование многоуровневого подхода

В этом разделе описывается использование многоуровневого подхода к выявлению типовых проблем коммутируемой сети.

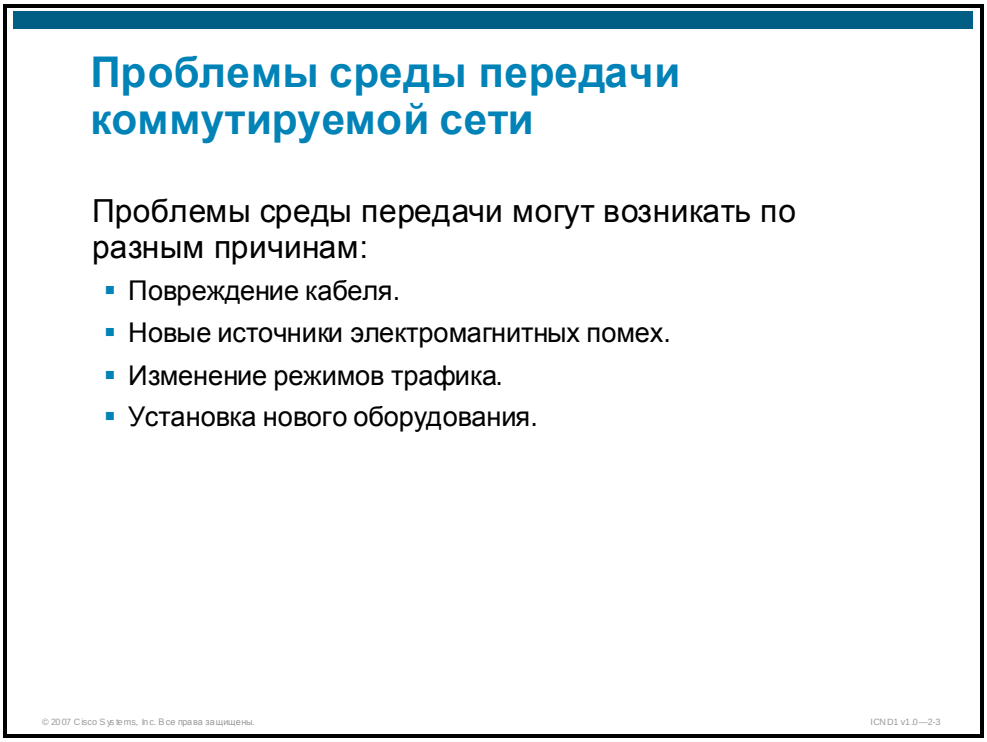


Коммутаторы работают на уровне 1 модели взаимодействия открытых систем (OSI), предоставляя интерфейс к физической среде. Коммутаторы также работают на уровне 2 модели OSI, обеспечивая передачу кадров по MAC-адресам. Поэтому проблемы, как правило, возникают на уровне 1 и уровне 2. На уровне 3 также могут возникать неполадки, связанные с подключением к коммутатору по протоколу IP для управления сетью.

Примечание Устранение неполадок уровня 3 будет рассмотрено подробно в модуле «Соединения локальных сетей».

Выявление и устранение проблем среды передачи данных

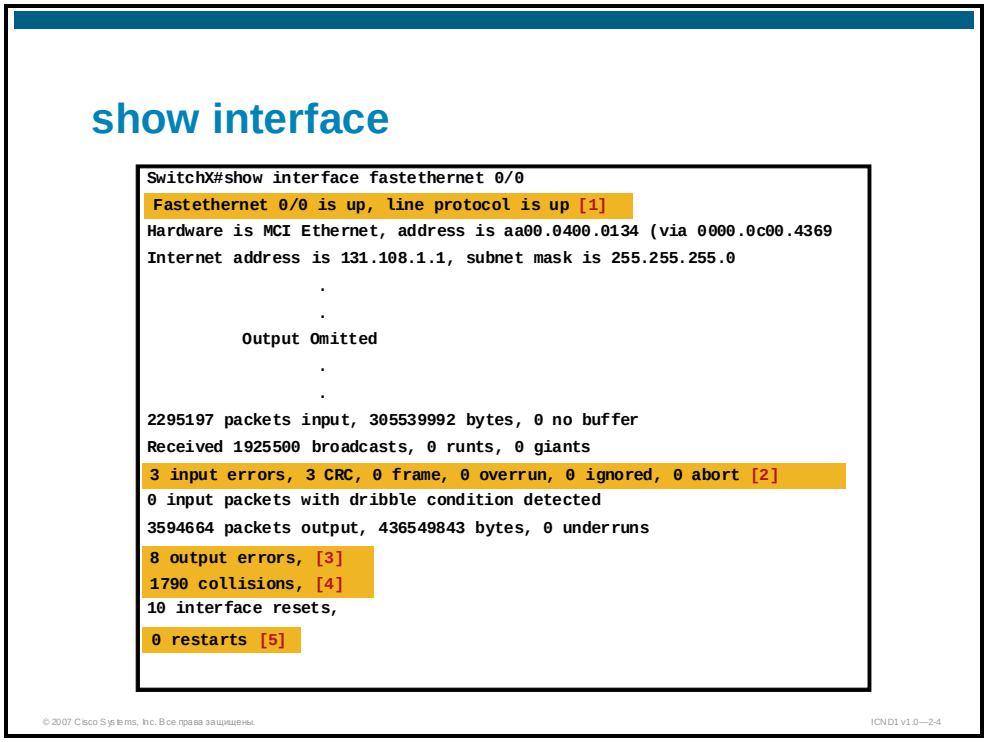
В этом разделе описываются методы выявления и решения типовых проблем среды передачи данных коммутируемой сети.



Проблемы среды – обычное явление. Иногда кабели повреждаются, и с этим ничего нельзя сделать. Далее перечислены некоторые примеры повседневных ситуаций, которые могут привести к возникновению проблем:

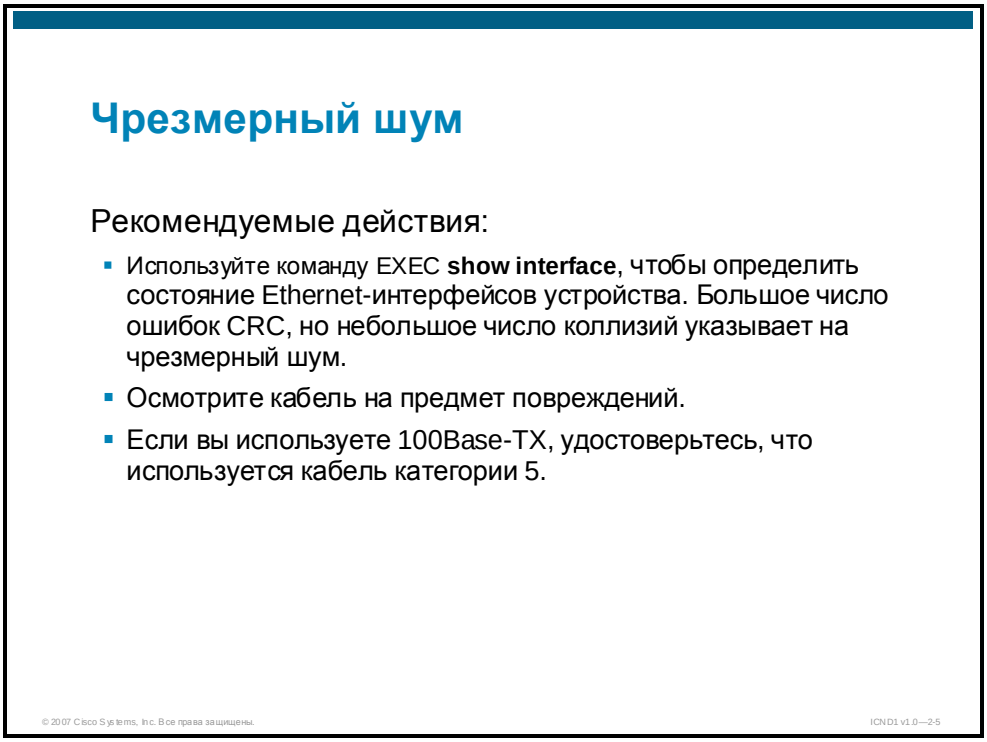
- в среде, использующей кабель категории 3, отдел обслуживания устанавливает новую систему кондиционирования воздуха, которая добавляет дополнительные источники электромагнитных помех;
- в среде, использующей кабель категории 5, кабель прокладывается слишком близко к двигателю лифта;
- плохая прокладка кабелей приводит к возникновению механического напряжения на разъемах RJ-45, что становится причиной повреждения одного или нескольких кабелей;
- новые приложения могут изменить режимы трафика.

Совсем простое действие, вроде подключения концентратора к порту коммутатора в офисе для подключения второго ПК, может вызвать увеличение количества коллизий.



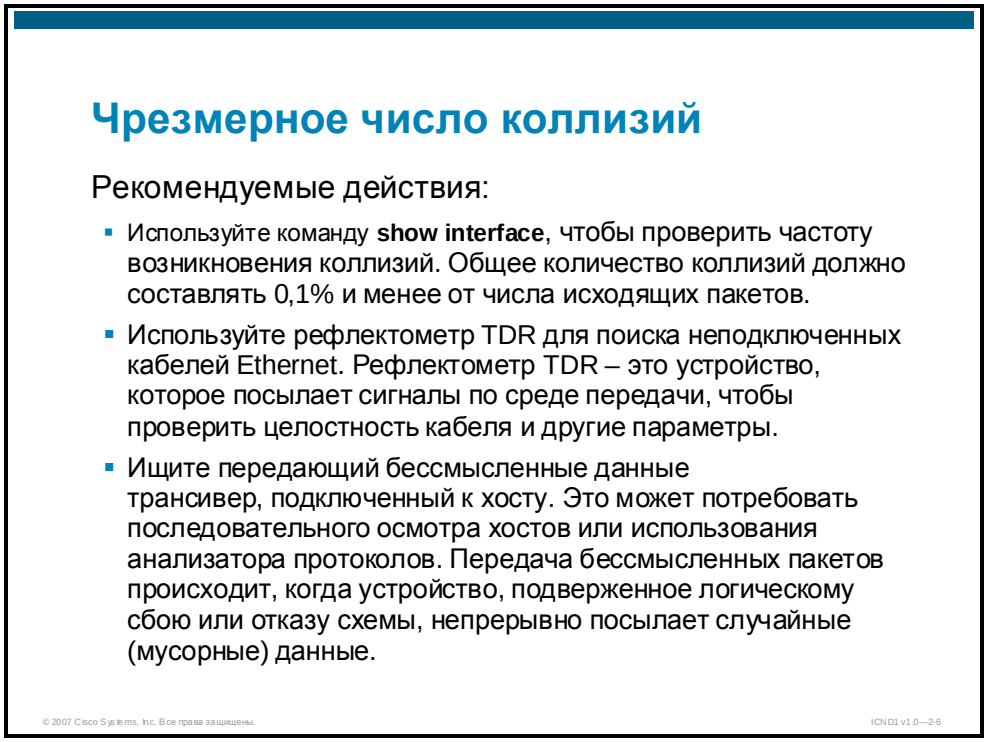
Поврежденный кабель и электромагнитные помехи обычно проявляются в виде чрезмерных коллизий и шума. Изменения в режимах трафика и установка концентратора может вызвать появление коллизий и кадров с недопустимо малой длиной. Эти признаки лучше всего отслеживаются с помощью команды **show interface**. В таблице ниже поясняется, что означают выделенные поля на рисунке.

Выноска	Поле	Описание
1	Состояние интерфейса и канального протокола	Указывает, активно ли оборудование интерфейса или оно заблокировано администратором. Если интерфейс имеет состояние «disabled», значит устройство получило более 5 000 ошибок за интервал Keepalive, который по умолчанию составляет 10 секунд. Если канальный протокол имеет состояние «down» или «administratively down», значит программные процессы, которые обрабатывают канальный протокол, считают интерфейс непригодным (отсутствуют Keepalive пакеты), или интерфейс был заблокирован администратором.
2	Ошибки на входе, включая ошибки циклического контроля избыточности (CRC) и формирования кадров	Общее количество ошибок, связанных с отказом буфера, кадрами с недопустимо малой длиной, кадрами с недопустимо большой длиной, циклическим контролем избыточности, формированием кадров, перегрузкой, пропуском и аварийным прекращением работы. Другие ошибки на входе также могут увеличить счетчик, поэтому сумма может не соответствовать другим счетчикам.
3	Ошибки выхода	Количество раз, когда принимающему устройству не удалось передать полученные данные в буфер из-за того, что интенсивность входящего потока данных превысила возможности приемника по обработке данных.
4	Коллизии	Количество сообщений, повторно переданных из-за коллизий Ethernet. Коллизии обычно возникают из-за чрезмерного размера ЛВС. Это может происходить, если кабель Ethernet или кабель трансивера имеет слишком большую длину или если между станциями установлено боле двух повторителей.
5	Перезагрузка	Количество перезагрузок контроллера Ethernet из-за ошибок.



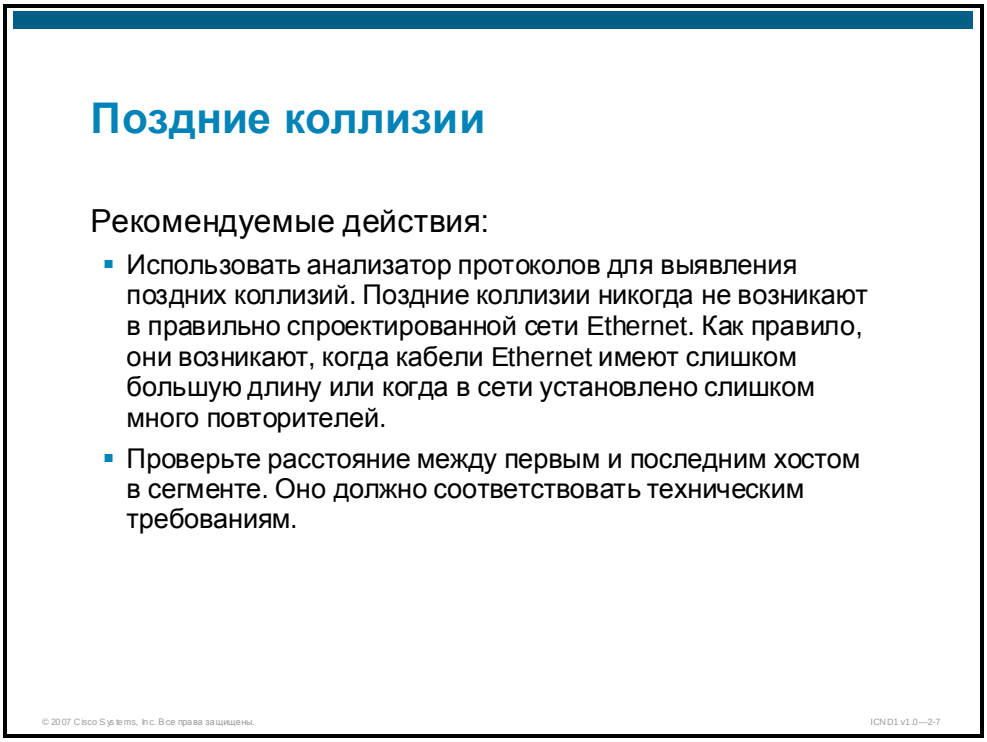
При поиске и устранении проблем, связанных с чрезмерным шумом, следует выполнить три действия.

- Используйте команду EXEC **show interface**, чтобы определить состояние Ethernet-интерфейсов устройства. Большое число ошибок циклического контроля избыточности, но небольшое число коллизий указывает на чрезмерный шум.
- Осмотрите кабель на предмет повреждений.
- Если вы используете 100Base-TX, удостоверьтесь, что применяется кабель категории 5.



При поиске и устранении проблем, связанных с чрезмерным числом коллизий, следует выполнить три действия.

- Используйте команду **show interface**, чтобы проверить частоту возникновения коллизий. Общее количество коллизий по сравнению с общим количеством исходящих пакетов должно быть 0,1% и менее.
- Рефлектометр TDR (Time-domain Reflectometer) – это устройство, которое посылает сигналы по среде передачи, чтобы проверить целостность кабеля и другие параметры. Используйте TDR для поиска неподключенных кабелей Ethernet.
- Передача бессмысленных пакетов происходит, когда устройство, подверженное логическому сбою или отказу схемы, непрерывно посылает случайные (мусорные) данные. Ищите передающий бессмысленные данные трансивер, подключенный к хосту. Это может потребовать последовательного осмотра хостов или использования анализатора протоколов.

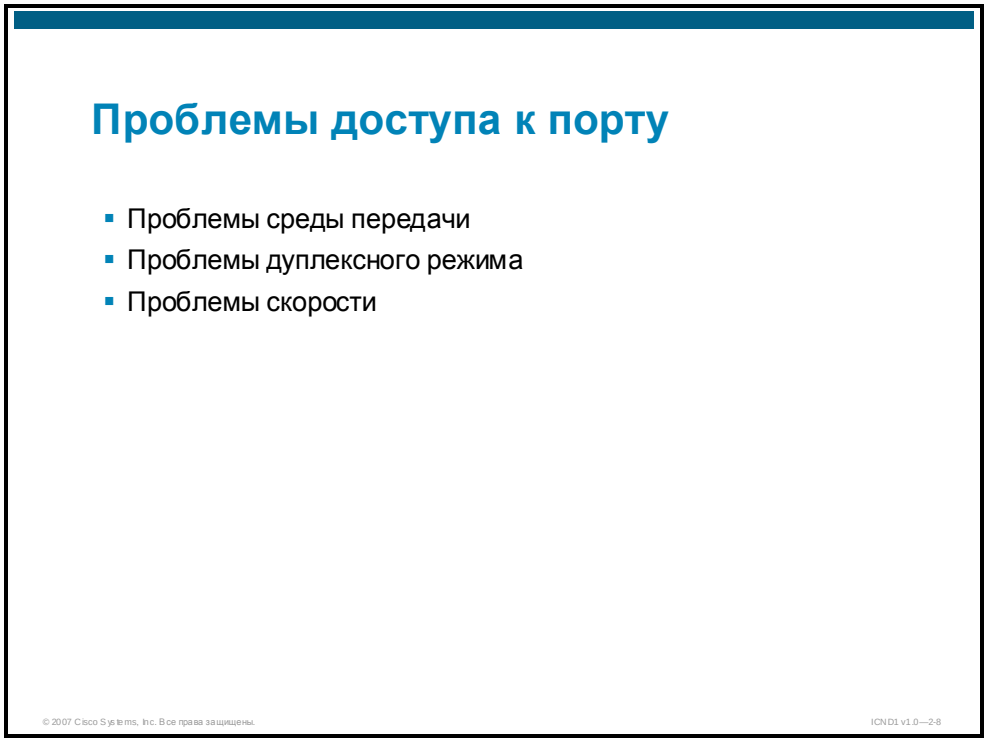


При поиске и устранении проблем, связанных с чрезмерным числом поздних коллизий, следует выполнить три действия.

- Использовать анализатор протоколов для выявления поздних коллизий. Поздние коллизии никогда не происходят в правильно спроектированной сети Ethernet. Как правило, они возникают, когда кабели Ethernet имеют слишком большую длину или когда в сети установлено слишком много повторителей.
- Проверьте расстояние между первым и последним хостом в сегменте. Оно должно соответствовать техническим требованиям.

Выявление и устранение типовых проблем доступа к портам

В этом разделе описываются методы выявления и решения типовых проблем доступа к портам.



Проблемы среды передачи можно назвать проблемами доступа (например, пользователь может сказать: «Я не могу получить доступ к сети»). Проблемы среды изолируются и решаются как описано в предыдущем разделе. Проблемы дуплексной передачи возникают при несовпадении параметров дуплексного режима. Проблемы скорости возникают при несовпадении параметров скоростного режима.

Проблемы дуплексного режима

Режимы дуплексной передачи:

- Одно конечное устройство работает в режиме полнодуплексной передачи, а другое – в режиме полудуплексной передачи, что приводит к несовпадению параметров.
- Одно конечное устройство работает в режиме полнодуплексной передачи, а другое – в режиме автоматического согласования:
  - Автоматическое согласование не выполняется, и конечное устройство переходит в режим полудуплексной передачи.
  - Это приводит к несовпадению параметров.
- Одно конечное устройство работает в режиме полудуплексной передачи, а другое – в режиме автоматического согласования:
  - Автоматическое согласование не выполняется, и конечное устройство переходит в режим полудуплексной передачи.
  - Оба конечных устройства работают в режиме полудуплексной передачи; несовпадение параметров не возникает.
- Оба конечных устройства работают в режиме автоматического согласования:
  - Одно конечное устройство не может работать в режиме полнодуплексной передачи, а второе не может работать в режиме полудуплексной передачи.
  - Пример: Интерфейс Gigabit Ethernet по умолчанию работает в режиме полнодуплексной передачи, в то время как 10/100 по умолчанию работает в режиме полудуплексной передачи.
- Оба конечных устройства работают в режиме автоматического согласования:
  - Автоматическое согласование завершается неудачей на обоих конечных устройствах, и они переходят в режим полудуплексной передачи.
  - Оба конечных устройства работают в режиме полудуплексной передачи; несовпадение параметров не возникает.

Используйте команду **show interface**, чтобы проверить параметры дуплексного режима.

Проблемы скорости

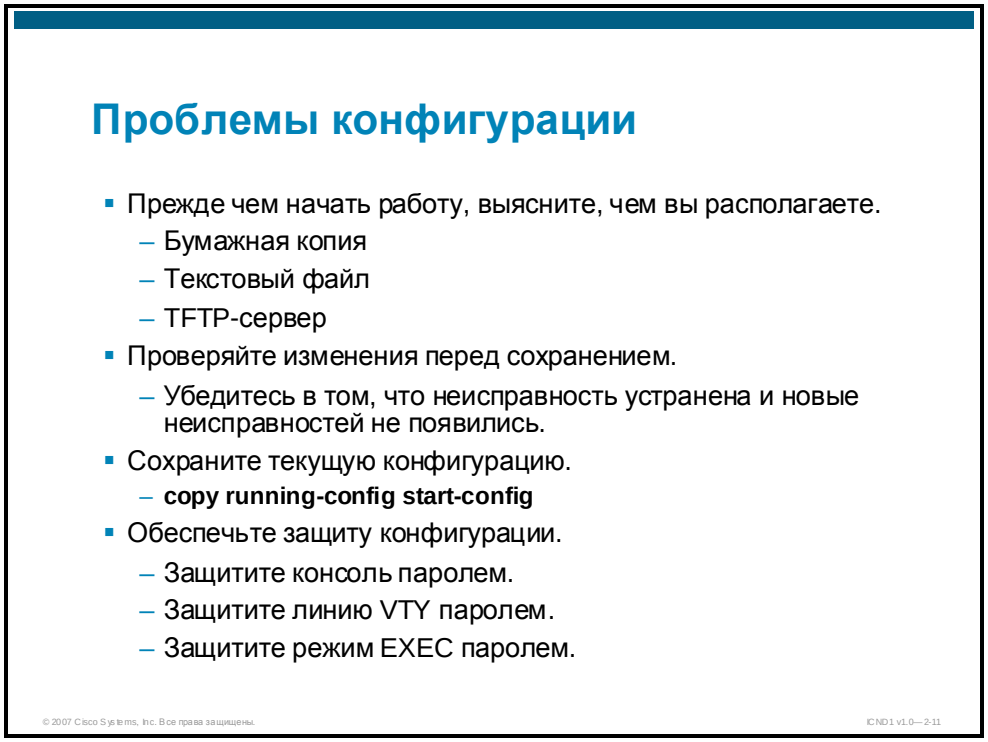
Скоростные режимы:

- Конечные устройства работают на разных скоростях, что приводит к несовпадению параметров.
- На одном конечном устройстве установлена более высокая скорость, а на другом задан режим автоматического согласования.
  - Если автоматическое согласование завершается неудачей, соответствующее конечное устройство возвращается к своей минимальной скорости.
  - Это приводит к несовпадению параметров.
- На обоих конечных устройствах выполняется автоматическое согласование:
  - Автоматическое согласование завершается неудачей на обоих конечных устройствах, и они возвращаются к своей минимальной скорости.

Используйте команду **show interface**, чтобы проверить параметры скоростного режима.

Выявление и устранение типовых проблем конфигурации

В этом разделе описываются методы выявления и решения типовых проблем конфигурации.



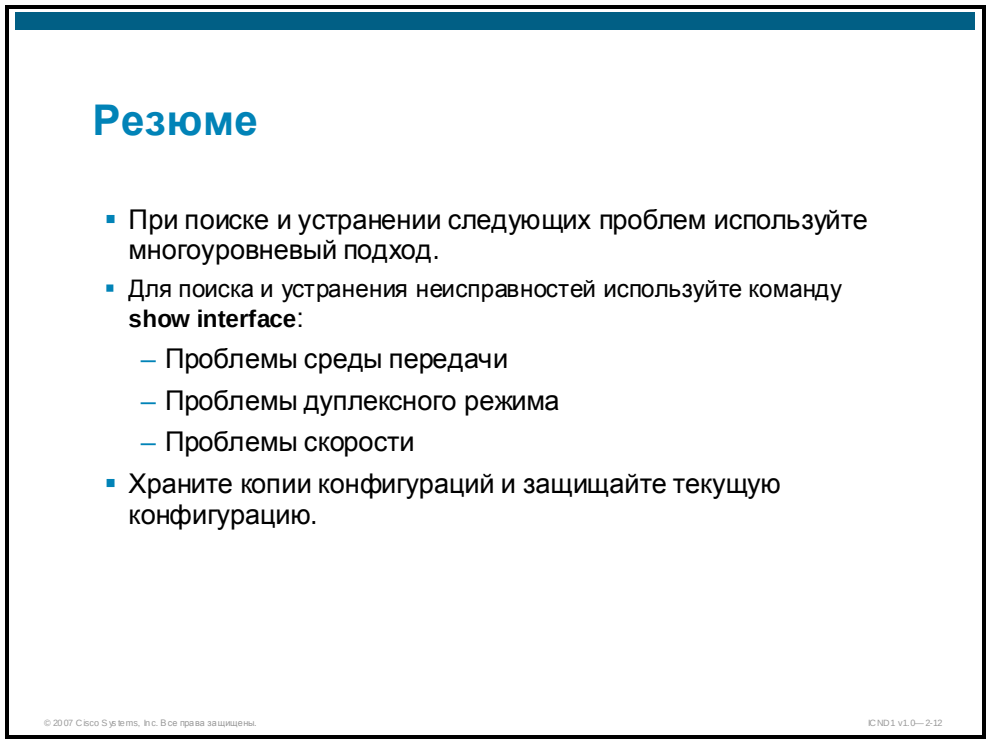
Начиная настройку устройств, оборудования и топологии вы должны знать существующую среду. Создав рабочую конфигурацию, сохраните копию. Например, сохраните и бумажную, и электронную копию: текстовый файл на PC или копию на TFTP-сервере.

При внесении изменений, убедитесь, что изменения именно те, которых вы хотели добиться, и что нет никаких неожиданных проблем, перед сохранением текущей конфигурации.

Изменения, сделанные посторонним лицом, намеренно или ненамеренно, могут быть катастрофическими. Чтобы гарантировать защиту конфигурации, необходимо защитить доступ к консольному порту и портам VTY сильным паролем. Также проследите, чтобы сильный пароль был задан для режима EXEC.

Резюме

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



Резюме модуля

В этом разделе приводится резюме вопросов, рассмотренных в модуле.

Резюме модуля

- Кабели и сегменты Ethernet могут охватывать ограниченное физическое пространство, но есть устройства, такие как повторители и концентраторы, которые можно добавлять в ЛВС Ethernet для расширения сегментов.
- Мосты и коммутаторы делят ЛВС на несколько сегментов. Однако коммутаторы работают на гораздо более высоких скоростях и поддерживают более широкий функционал, выполняя три основные функции в сегментации сети Ethernet: пересылка, фильтрация и лавинная рассылка.
- Существует несколько способов улучшения коммутируемых ЛВС Ethernet, в том числе микросегментация и иерархичность соединений. Однако существует вероятность образования преднамеренных или непреднамеренных физических петель, которые можно решить с помощью STP.

Резюме модуля (прод.)

- Интерфейс командной строки Cisco IOS используется для выполнения конфигурации устройств, отвечающих сетевым требованиям организации.
- Запуск коммутатора Cisco Catalyst требует проверки физической установки, подачи питания и проверки вывода сообщений ПО Cisco IOS на консоль.
- Интерфейс командной строки используется для настройки имени коммутатора и паролей, а также для ввода команд с консоли, например команд конфигурации интерфейсов устройства и IP-адресов.
- Повысьте уровень безопасности коммутатора с помощью паролей и функций безопасности порта
- Большинство проблем доступа к порту можно выявить с помощью команды **show interface**.

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».

B1) Какие два утверждения о функциях концентратора верны? (Выберите два варианта.) (Источник: общие сведения о проблемах разделяемых локальных сетей)

А) Концентратор расширяет ЛВС Ethernet.
Б) Концентратор уменьшает размер домена коллизий.
В) Добавление концентратора позволяет пользователям сегмента сети не конкурировать за полосу пропускания.
Г) Концентратор – это устройство канального уровня.
Д) Концентратор усиливает сигнал перед его ретрансляцией.

B2) Какие три утверждения лучше всего описывают коллизии? (Выберите три варианта.) (Источник: общие сведения о проблемах разделяемых локальных сетей)

А) Коллизии происходят, когда две или более станции в общей среде передают данные одновременно.
Б) Большие сегменты имеют меньшие шансы для возникновения коллизии.
В) Во время коллизий кадры разрушаются, каждая станция в сегменте запускает случайный таймер и выжидает некоторое время, прежде чем повторить попытку передачи данных.
Г) Добавление концентратора в сеть может решить проблему коллизий.
Д) Коллизии – это побочные явления общих ЛВС.
Е) Увеличение числа сегментов в сети повышает вероятность коллизий.

B3) Какой из вариантов лучше всего описывает домен коллизий? (Источник: общие сведения о проблемах разделяемых локальных сетей)

А) два или более устройств, пытающиеся передавать данные одновременно
Б) две соединенные сети
В) сегменты сети, которые совместно используют полосу пропускания
Г) ни один из вышеупомянутых вариантов не подходит

B4) Какие устройства помогают устранить коллизии? (Источник: решение проблем сети путем применения технологии коммутируемых ЛВС)

А) повторитель
Б) мост
В) концентратор
Г) удлинитель

B5) Какие три фактора чаще всего вызывают перегрузку сети? (Выберите три варианта.) (Источник: решение проблем сети путем применения технологии коммутируемых ЛВС)

А) приложения с высокими требованиями к полосе пропускания
Б) большое число сегментов сети
В) увеличивающийся объем сетевого трафика
Г) более мощные компьютерные и сетевые технологии
Д) небольшое число сегментов сети
Е) ЛВС, охватывающие большие расстояния

В6) Назовите три характеристики моста. (Выберите три варианта.) (Источник: решение проблем сети путем применения технологии коммутируемых ЛВС)

А) Мосты пересылают, но не фильтруют кадры между сегментами ЛВС.
Б) Мосты ведут таблицы MAC-адресов.
В) Мосты более «интеллектуальны», чем концентраторы.
Г) Мосты могут буферизировать и пересылать кадры между двумя или более сегментами ЛВС.
Д) Мосты создают меньше доменов коллизий.
Е) Мосты работают на уровне 2 модели OSI.

В7) Каковы два главных преимущества добавления моста к сети? (Выберите два варианта.) (Источник: решение проблем сети путем применения технологии коммутируемых ЛВС)

А) изоляция потенциальных проблем сети в отдельных сегментах
Б) увеличение скорости сети
В) расширение ЛВС для охвата больших расстояний путем соединения нескольких сегментов
Г) создание меньшего количества доменов коллизий
Д) передача кадров данных между сегментами ЛВС

В8) Сопоставьте термины, связанные с эксплуатацией коммутатора в сети, с их описанием. (Источник: решение проблем сети путем применения технологии коммутируемых ЛВС)

_____ 1. Если коммутатор решает, что MAC-адрес назначения кадра находится в том же сетевом сегменте, что и источник, он не пересылает кадр.

_____ 2. Если коммутатор решает, что MAC-адрес назначения кадра не находится в одном сетевом сегменте с источником, он пересылает кадр в соответствующий сегмент.

_____ 3. Если коммутатор *не* имеет записи адреса назначения, он передает кадр всем портам, кроме порта, с которого он получил кадр.

А) лавинная рассылка
Б) фильтрация
В) пересылка

В9) Какие три характеристики относятся к коммутатору? (Выберите три варианта.) (Источник: решение проблем сети путем применения технологии коммутируемых ЛВС)

А) использует таблицу MAC-адресов, чтобы определить порт, которому нужно передать данные
Б) соединяет сегменты ЛВС
В) уменьшает количество доменов коллизий
Г) увеличивает количество доменов коллизий
Д) фильтрует данные перед их пересылкой адресату в сети

В10) Какие три особенности отличают коммутаторы от мостов? (Выберите три варианта.) (Источник: решение проблем сети путем применения технологии коммутируемых ЛВС)

А) большие буферы кадров
Б) использует таблицы MAC-адресов, чтобы определить сегмент, которому нужно передать данные
В) поддержка сред передачи с разной скоростью
Г) высокая плотность портов
Д) способность сегментировать ЛВС

В11) Какие три утверждения о сравнении производительности коммутатора и моста верны? (Выберите три варианта.) (Источник: решение проблем сети путем применения технологии коммутируемых ЛВС)

А) Коммутаторы работают на гораздо более высоких скоростях, чем мосты.
Б) Коммутаторы работают на меньших скоростях, чем мосты.
В) Коммутаторы поддерживают более богатые функциональные возможности по сравнению с мостами.
Г) Коммутаторы поддерживают меньше функциональных возможностей по сравнению с мостами.
Д) Коммутаторы поддерживают выделенные соединения между устройствами.
Е) Коммутаторы не поддерживают выделенные соединения между устройствами.

В12) Какие три утверждения о микросегментации верны? (Выберите три варианта.) (Источник: максимизация преимуществ коммутации)

А) Внедрение моста в сети обеспечивает микросегментацию.
Б) Микросегментация увеличивает доступную полосу пропускания.
В) Каждое устройство в сегменте подключается напрямую к порту коммутатора.
Г) Микросегментация устраняет коллизии.
Д) Микросегментация ограничивает количество сегментов сети.
Е) Микросегментация использует полудуплексный режим работы.

В13) Сопоставьте описания функций с режимом передачи данных – полнодуплексным или полудуплексным. (Источник: максимизация преимуществ коммутации)

_____ 1. Сеть отправляет и принимает кадры данных поочередно, но не одновременно.

_____ 2. Этот вид связи удваивает полосу пропускания между устройствами.

_____ 3. Сеть посылает и принимает кадры данных одновременно.

А) полнодуплексная передача
Б) полудуплексная передача

B14) Сопоставьте функции соединения с соответствующими типами Ethernet. (Источник: максимизация преимуществ коммутации)

_____ 1. функционирует на уровне конечного пользователя, обеспечивает высокую производительность, доступ рабочей станции к серверу со скоростью 100 Мбит/с

_____ 2. не часто используется на уровне конечного пользователя; на уровне рабочей группы обеспечивает связь между конечным пользователем и рабочими группами; на магистральном уровне обеспечивает связь между коммутаторами для приложений малого и среднего объема

_____ 3. на уровне рабочей группы обеспечивает высокопроизводительную связь с корпоративным сервером

_____ 4. на магистральном уровне обеспечивает связь между магистралью и коммутаторами

_____ 5. на уровне конечного пользователя обеспечивает связь между конечным пользователем и коммутатором пользовательского уровня

_____ 6. обеспечивает связь между коммутаторами для приложений малого и среднего объема

А) Ethernet 10BASE-T
Б) Fast Ethernet
В) Gigabit Ethernet

B15) Когда устройство Cisco запускается, что оно использует для проверки оборудования? (Источник: работа с программным обеспечением Cisco IOS)

А) флэш-память
Б) RAM
В) POST
Г) TFTP

B16) При запуске коммутатора Catalyst или маршрутизатора Cisco какая операция выполняется первой? (Источник: работа с программным обеспечением Cisco IOS)

А) Устройство выполняет процедуры запуска системы.
Б) Устройство выполняет процедуры проверки оборудования.
В) Устройство пытается обнаружить другие устройства в сети.
Г) Устройство пытается найти и применить параметры конфигурации ПО.

B17) После начальной установки коммутатора или маршрутизатора Cisco администратор сети, как правило, настраивает сетевые устройства с помощью _____. (Источник: работа с программным обеспечением Cisco IOS)

А) CD-ROM
Б) TFTP-сервер
В) консольный терминал
Г) модемное соединение

B18) Если администратор сети поддерживает удаленное устройство, предпочтительнее использовать модемное подключение к _____ устройства для удаленной конфигурации. (Источник: работа с программным обеспечением Cisco IOS)

А) порт ЛВС
Б) восходящий порт
В) консольный порт
Г) вспомогательный порт

B19) Какой уровень доступа позволяют обращаться ко всем командам маршрутизатора и могут быть защищены паролем, для того чтобы только авторизованные пользователи могли иметь доступ к маршрутизатору? (Источник: работа с программным обеспечением Cisco IOS)

А) пользовательский уровень EXEC
Б) уровень установки EXEC
В) уровень enable EXEC
Г) привилегированный уровень EXEC

B20) Как заставить устройство Cisco проанализировать и выполнять введенную команду? (Источник: работа с программным обеспечением Cisco IOS)

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

B21) Какое приглашение интерфейса командной строки CLI обозначает привилегированный режим EXEC? (Источник: работа с программным обеспечением Cisco IOS)

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

B22) Какую команду нужно ввести в привилегированном режиме EXEC, чтобы вывести параметры команд? (Источник: работа с программным обеспечением Cisco IOS)

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

B23) Сопоставьте каждый этап процесса физического запуска коммутатора Catalyst с его описанием. (Источник: запуск коммутатора)

_____ 1. Этап 1

_____ 2. Этап 2

_____ 3. Этап 3

А) Вставьте вилку кабеля питания коммутатора в розетку.
Б) Пронаблюдайте последовательность загрузки, ознакомьтесь с текстом вывода программного обеспечения Cisco IOS на консоли.
В) Убедитесь, что все кабельные разъемы были подключены, терминал соединен с консольным портом, и выбрано приложение консольного терминала.

B24) Как включать коммутаторы серии Catalyst 2950? (Источник: запуск коммутатора)

А) Нажать кнопку «Вкл./выкл.».
Б) Включить резервный источник питания.
В) Подключить сетевой кабель к другому коммутатору в сети.
Г) Вставить вилку кабеля питания коммутатора в розетку.

B25) Если тестирование POST на коммутаторе Catalyst завершается успешно, какой вывод отображается в окне консоли? (Источник: запуск коммутатора)

А) приглашение «>»
Б) приглашение привилегированного режима EXEC
В) окно входа в консоль управления
Г) список команд, доступных на коммутаторе

B26) Какую команду интерфейса командной строки необходимо ввести, чтобы вывести список команд коммутатора Catalyst, которые начинаются с символа «c»? (Источник: запуск коммутатора)

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

B27) Какую команду интерфейса командной строки необходимо ввести, чтобы получить справку по синтаксису команд, и посмотреть варианты завершения команды, которая начинается с config? (Источник: запуск коммутатора)

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

B28) Какая команда Cisco IOS правильно настраивает IP-адрес и маску подсети на коммутаторе? (Источник: запуск коммутатора)

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**

В29) Какой режим конфигурации следует использовать для настройки порта на коммутаторе? (Источник: запуск коммутатора)

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

В30) Когда вы используете команду **show interface**, чтобы вывести состояние и статистику интерфейсов, настроенных на коммутаторе Catalyst, какие поля содержат MAC-адрес, идентифицирующий оборудование интерфейса? (Источник: запуск коммутатора)

А) MTU 1 500 bytes
Б) Hardware is … 10BaseT
В) Address is 0050.BD73.E2C1
Г) 802.1d STP State: Forwarding

В31) Какая команда **show** требует доступа к привилегированному режиму EXEC? (Источник: запуск коммутатора)

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

В32) Как включить маршрутизатор Cisco? (Источник: запуск коммутатора)

А) Нажать кнопку **Reset**.
Б) Перевести выключатель питания в положение «ВКЛ».
В) Подключить волоконно-оптический кабель к другому маршрутизатору.
Г) Вставить вилку кабеля питания маршрутизатора в розетку электропитания.

В33) Какие две ситуации можно считать физической угрозой? (Выберите два варианта.) (Источник: безопасность коммутаторов)

А) Пользователь, оставивший пароль на своем столе.
Б) Некто, выключивший питание коммутатора, чтобы блокировать доступ к сети.
В) Некто, выключивший систему кондиционирования воздуха сети.
Г) Некто, взломавший шкаф с документацией по сети.

В34) Какие четыре типа доступа можно защитить паролем? (Выберите четыре варианта.) (Источник: безопасность коммутаторов)

А) Консольный доступ
Б) Доступ к VTY
В) Доступ к TTY
Г) Пользовательский уровень доступа
Д) Уровень доступа Exec

В35) Какая из следующих функций позволяет настроить текст, который будет отображаться перед запросом имени пользователя и пароля для входа в систему? (Источник: безопасность коммутаторов)

А) сообщение дня
Б) баннер входа в систему
В) предупреждение о доступе
Г) пользовательский баннер
Д) предупреждающее сообщение

В36) Какой способ удаленного доступа к сетевому устройству наиболее безопасен? (Источник: безопасность коммутаторов)

А) HTTP
Б) Telnet
В) SSH
Г) RMON
Д) SNMP

В37) Какую из следующих функций Cisco IOS можно использовать для управления доступа к портам VTY? (Источник: безопасность коммутаторов)

А) отключение
Б) защита порта
В) список доступа
Г) брандмауэр

В38) Какая команда Cisco IOS может использоваться для управления доступом к порту коммутатора на основе MAC-адреса? (Источник: безопасность коммутаторов)

А) **shutdown**
Б) **port security**
В) **mac-secure**
Г) **firewall**

В39) Какой из следующих команд Cisco IOS можно использовать для повышения безопасности неиспользуемых портов коммутатора? (Источник: безопасность коммутаторов)

А) **shutdown**
Б) **port security**
В) **mac-secure**
Г) **firewall**

В40) Какая проблема возникает при резервировании сетевых подключений? (Источник: максимизация преимуществ коммутации)

А) микросегментация
Б) петли
В) ослабление
Г) коллизии

В41) Какое утверждение лучше всего описывает влияние петель на работу коммутируемой ЛВС? (Источник: максимизация преимуществ коммутации)

А) В результате появления петель могут возникать широковещательные штормы, которые препятствуют передаче данных по сети.
Б) Для любого группового, широковещательного или неизвестного трафика будет выполняться лавинная рассылка по всем портам.
В) Неправильная информация об адресе может заноситься в таблицы MAC-адресов, что приводит к ошибкам передачи кадров.
Г) Петля удаляет кадр из сети.

В42) Какое утверждение точно описывает протокол STP? (Источник: максимизация преимуществ коммутации)

А) STP присваивает роли мостам и портам, чтобы в отдельно взятый момент времени в сети был только один путь пересылки.
Б) STP автоматически сохраняет неактивный путь в неактивном состоянии.
В) STP устраняет проблемные сегменты.
Г) STP позволяет портам прослушивать, пересылать и выполнять лавинную рассылку.

В43) Какая команда Cisco IOS наиболее полезна при поиске неисправностей среды передачи? (Источник: решение проблем, связанных с коммутаторами)

А) **show controller**
Б) **show run**
В) **show interface**
Г) **show counters**

В44) Какая команда Cisco IOS наиболее полезна при поиске проблем доступа к порту? (Источник: решение проблем, связанных с коммутаторами)

А) **show controller**
Б) **show run**
В) **show interface**
Г) **show counters**

В45) Какие три способа используются для решения проблем конфигурации? (Выберите три варианта.) (Источник: решение проблем, связанных с коммутаторами)

А) Защита неиспользуемых портов.
Б) Защита конфигурации.
В) Проверка изменений перед сохранением.
Г) Знание существующей среды перед началом настройки.

Ответы на вопросы для самопроверки по модулю

В1)	А, Г
В2)	А, В, Г
В3)	В
В4)	Б
В5)	А, В, Г
В6)	Б, В, Г
В7)	А, В
В8)	1 = Б, 2 = В, 3 = А
В9)	А, Б, Г
В10)	А, В, Г
В11)	А, В, Д
В12)	Б, В, Г
В13)	1 = Б, 2 = А, 3 = А
В14)	1 = Б, 2 = В, 3 = Б, 4 = В, 5 = А, 6 = В
В15)	В
В16)	Б
В17)	В
В18)	Г
В19)	Г
В20)	Б
В21)	А
В22)	А
В23)	А, В, Б
В24)	Г
В25)	А
В26)	А
В27)	Б
В28)	Г
В29)	В
В30)	В
В31)	В
В32)	Б
В33)	Б, В
В34)	А, Б, В, Д
В35)	Б
В36)	В
В37)	В
В38)	Б
В39)	А
В40)	Б
В41)	А

B42) A

B43) B

B44) B

B45) Б, В, Г

Модуль 3

Беспроводные ЛВС

Обзор

Исторически локальные сети были ограничены физическими проводными сегментами. С появлением технологий, в которых инфракрасное излучение (ИК) и радиочастоты (РЧ) используются для передачи данных, локальные сети освободились от ограничений физических сред. В этом модуле описываются причины, по которым расширение доступности локальных сетей необходимо, и объяснять конкретные методы расширения локальных сетей , основанные на беспроводном РЧ-доступе.

Задачи модуля

По окончании этого модуля вы сможете описывать среду передачи беспроводной локальной сети. Это значит, что вы сможете выполнять следующие задачи:

- описывать бизнес-факторы и стандарты, влияющие на внедрение беспроводной локальной сети;
- описывать проблемы безопасности беспроводной локальной сети и методы уменьшения угроз;
- описывать другие факторы, влияющие на внедрение беспроводной локальной сети.

Занятие 1

Изучение беспроводной сети

Обзор

Беспроводной доступ к сетям был разработан подобно большинству новых технологий – потребности бизнеса определили технологические разработки, которые в свою очередь привели к появлению новых потребностей бизнеса, которые создали необходимость в новых технических разработках. Чтобы избежать бесконтрольного развития этого цикла, несколько организаций договорились о стандартах и системе сертификации для беспроводных локальных сетей. На этом занятии описываются тенденции и стандарты, влияющие на разработку беспроводных локальных сетей.

Задачи

По окончании этого занятия вы сможете описывать факторы, влияющие на беспроводные локальные сети, и стандарты, которые их регулируют. Это значит, что вы сможете выполнять следующие задачи:

- описывать бизнес-требования для служб беспроводной локальной сети (WLAN);
- описывать различия во внедрении проводных и беспроводных ЛВС;
- перечислять характеристики радиочастотной передачи, используемые в беспроводных локальных сетях;
- перечислять организации, определяющие стандарты беспроводных локальных сетей;
- описывать три нелицензируемых диапазона, разрешенных к использованию организациями FCC и ITU-R в локальных сетях;
- сравнивать различные стандарты IEEE 802.11;
- описывать сертификацию Wi-Fi.

Бизнес-требования для служб беспроводной локальной сети

В данном разделе описываются бизнес-требования для служб беспроводной локальной сети.

Производительность труда больше не ограничиваются стационарным рабочим местом или определенным периодом времени. Теперь подключение возможно в любое время и из любого места, от офиса до аэропорта или даже из дома. В деловых поездках сотрудникам приходилось оплачивать телефонную связь между рейсами для проверки сообщений и выполнения нескольких звонков. Теперь можно проверять электронную почту, голосовую почту и статус продуктов с использованием веб-доступа с помощью карманных ПК (КПК) во время посадки на рейс.

Даже дома образ жизни и способы обучения людей изменились. Интернет становится домашним стандартом наряду с телевидением и телефоном. Даже метод доступа к Интернету быстро изменился от временного коммутируемого подключения через модем до выделенных цифровых абонентских линий (DSL) или кабельных услуг с постоянным подключением, которые функционируют быстрее соединений по телефонным линиям. В 2005 году пользователи ПК приобрели больше портативных компьютеров с поддержкой беспроводного доступа, чем стационарных настольных компьютеров.

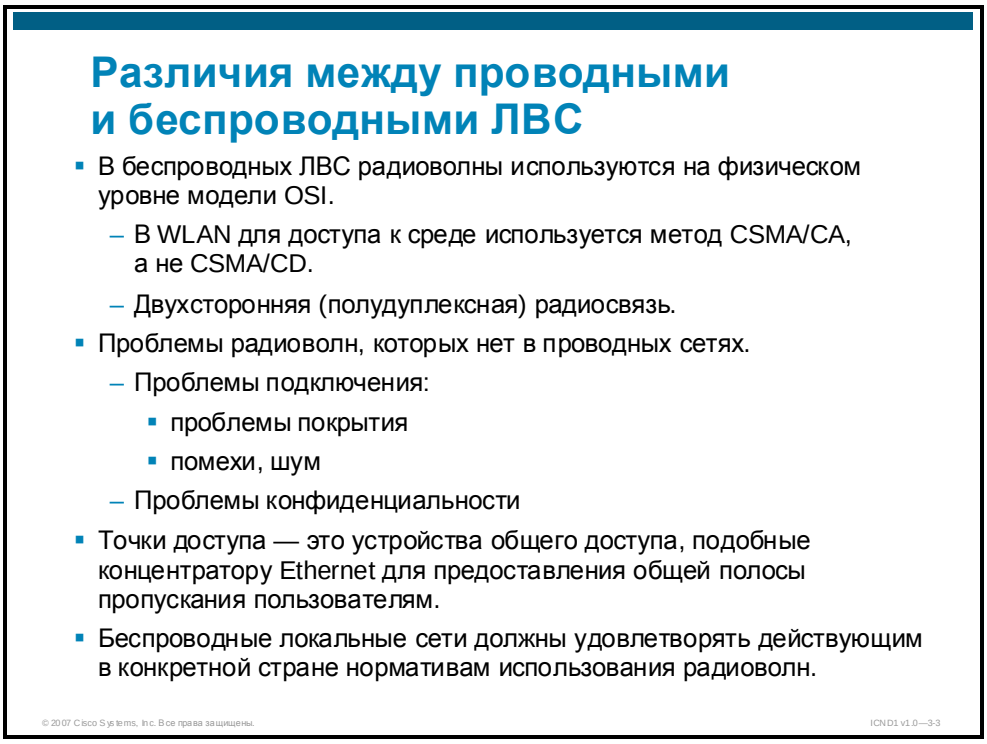
Наиболее осязаемое преимущество беспроводного доступа – снижение расходов. Это можно проиллюстрировать на двух примерах. В случае отлаженной инфраструктуры беспроводного доступа экономия проявляется при переходе пользователя от одного рабочего места к другому, реорганизации лаборатории или перемещении с временных площадок или мест реализации проекта. В среднем затраты на ИТ при перемещении сотрудника от одного рабочего места к другому составляют 375 долларов. Для данного примера предположим, что ежегодно рабочее место меняют 15 процентов персонала. В качестве другого примера рассмотрим ситуацию, когда компания переезжает в новое здание, в котором не развернута инфраструктура проводного подключения. В данном случае

экономия от беспроводного доступа еще более значительна, так как прокладка кабелей по стенам, потолкам и полам – довольно трудоемкий процесс.

И последнее, но не менее важное. Еще одно преимущество использования беспроводной локальной сети заключается в повышении степени удовлетворения сотрудников, что ведет к уменьшению текучки кадров и снижению затрат на найм новых сотрудников. Удовлетворенность сотрудников также приводит к улучшению обслуживания клиентов. Это преимущество нелегко оценить количественно, однако оно очень существенно.

Различия между проводными и беспроводными ЛВС

В этом разделе описываются различия во внедрении проводных и беспроводных ЛВС;



В беспроводных локальных сетях радиочастотный сигнал используется как физический уровень сети.

- В беспроводных локальных сетях используется множественный доступ с контролем несущей и предотвращением коллизий (CSMA/CA) вместо множественного доступа с контролем несущей и обнаружением коллизий (CSMA/CD), который применяется в локальных сетях. Обнаружение коллизий в беспроводных локальных сетях невозможно, так как передающая станция не может одновременно принимать то, что передает, и поэтому не может обнаруживать конфликты. Вместо этого в беспроводных локальных сетях используются протоколы готовности к передаче (RTS – Ready to Send) и готовности к приему (CTS – Clear to Send), что позволяет избегать коллизий.

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

Радиоволны вызывают проблемы, которых нет в проводных локальных сетях.

- В беспроводных локальных сетях неполадки подключения возникают из-за проблем покрытия, РЧ-передачи, искажений, вызванных наложением сигнала, и помех, возникающих из-за других беспроводных служб или локальных сетей.
- Проблемы с конфиденциальностью возникают из-за того, что радиоволны могут выходить за пределы объекта.

В беспроводных локальных сетях мобильные клиенты подключаются к сети через точку доступа, которая эквивалентна проводному концентратору Ethernet.

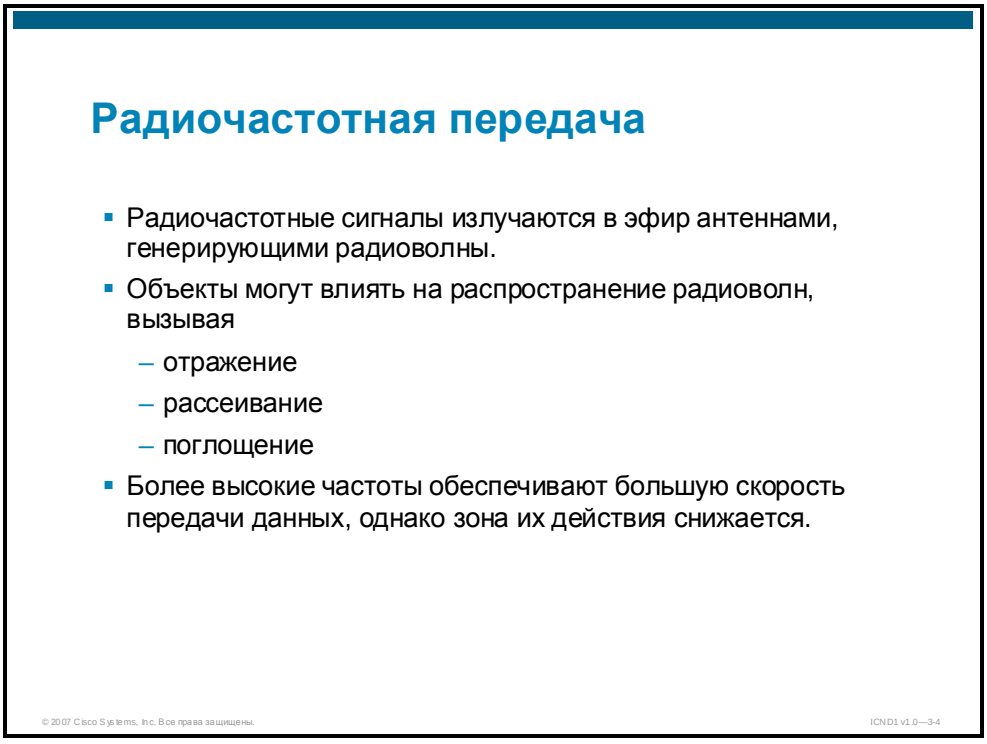
- У мобильных клиентов нет физического подключения к сети.
- Мобильные устройства зачастую работают от аккумулятора в отличие от устройств локальных сетей, подключенных к сети электропитания.

Беспроводные локальные сети должны удовлетворять действующим в конкретной стране нормативам по использованию РЧ-диапазона.

Цель стандартизации заключается в обеспечении доступности беспроводных локальных сетей по всему миру. Так как в беспроводных локальных сетях используется РЧ-диапазон, они должны соответствовать действующим в конкретной стране нормативам по использованию и мощности РЧ. Это требование отсутствует для проводных ЛВС.

РЧ-передача

Радиочастотный диапазон включает диапазоны от AM до частот, выделенных для мобильной связи. В этом разделе перечисляются характеристики радиочастотных сигналов, используемых в беспроводных локальных сетях.



Радиочастотные сигналы излучаются в эфир антеннами, генерирующими радиоволны. При распространении радиоволн через объекты они могут быть поглощены (например, стенами) или отражены (например, металлическими поверхностями). Поглощение или отражение может вызывать образование областей с низким уровнем или качеством сигнала.

На передачу радио волн влияют следующие факторы.

- **Отражение:** возникает, когда радиоволны отражаются от объектов (например, металлических или стеклянных поверхностей).
- **Рассеивание:** возникает, когда радиоволны попадают на неровную поверхность (например, шероховатую поверхность) и отражаются в разных направлениях.
- **Поглощение:** возникает, когда радиоволны поглощаются объектами (например, стенами).

При передаче данных с помощью радиоволн применяются следующие правила.

- При повышении скорости передачи данных дальность распространения, так как приемнику требуется более мощный сигнал с лучшим отношением сигнал/шум.
- При повышении мощности передачи увеличивается ее дальность. Для удвоения дальности необходимо увеличить мощность в 4 раза.
- Для более высокой скорости передачи требуется более широкая полоса пропускания. Увеличение полосы пропускания возможно за счет повышения частоты или использования более сложной модуляции.
- У радиоволн с более высокими частотами дальность передачи уменьшается из-за более высокого уровня ослабления и поглощения. Эту проблему можно решить с помощью более эффективных антенн.

Организации, определяющие беспроводные ЛВС

Несколько организаций договорились о стандартах и системе сертификации для беспроводных локальных сетей (WLAN). В данном разделе перечисляются организации, определяющие стандарты беспроводных локальных сетей.

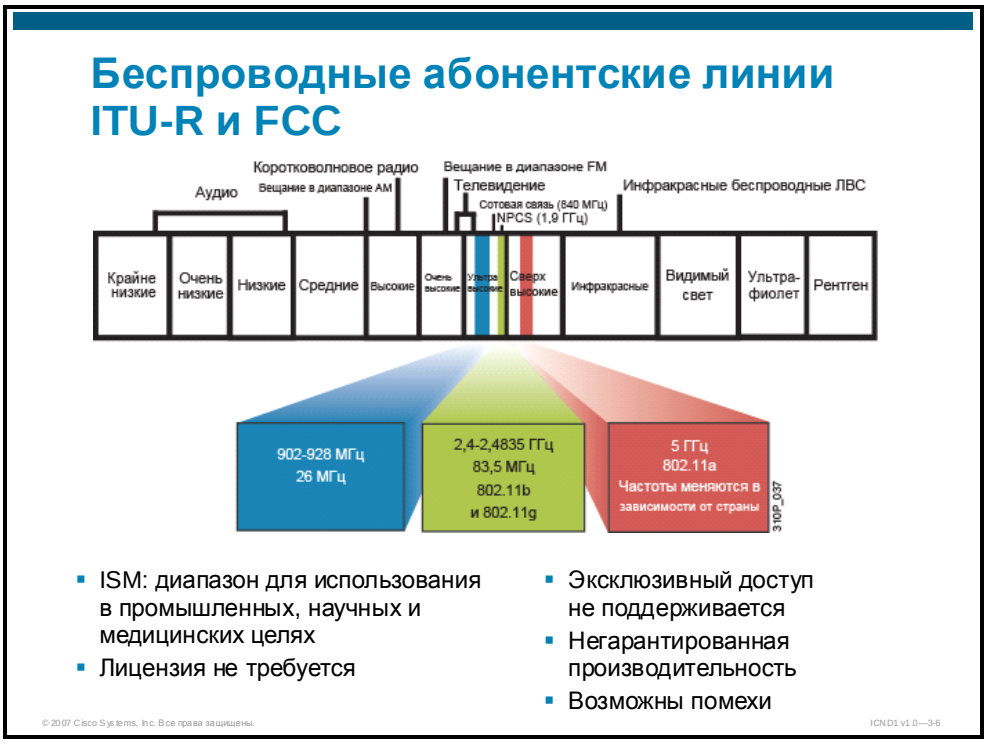
Использование радиочастотных диапазонов контролируется органами государственного регулирования. С момента ввода в действие 900-мегагерцового диапазона ISM (диапазон для использования в промышленных, научных и медицинских целях) в 1985 году началась разработка беспроводных локальных сетей. Новые сигналы, типы модуляции и частоты должны утверждаться органами государственного регулирования. Необходимо согласие по всему миру. Органы регулирования включают Федеральную комиссию по связи (FCC) для США (http://www.fcc.gov) и Европейский институт телекоммуникационных стандартов (ETSI) для Европы (http://www.etsi.org).

Стандарты определяются Институтом инженеров по электротехнике и радиоэлектронике (IEEE). IEEE 802.11 является частью процесса стандартизации сетей семейства 802. Одобренные стандарты можно загрузить с веб-сайта IEEE (http://standards.ieee.org/getieee802).

Ассоциация Wi-Fi Alliance предлагает сертификацию совместимости продуктов 802.11 различных поставщиков. Сертификация облегчает жизнь покупателям таких продуктов. Это также способствует развитию рынка технологий беспроводных локальных сетей за счет поощрения совместимости продуктов различных поставщиков. Сертификация включает все три РЧ-технологии 802.11 и беспроводной защищенный доступ (WPA), модель безопасности, выпущенную в 2003 г. и одобренную в 2004 г. Эта модель основана на новом стандарте безопасности IEEE 802.11i, который был одобрен в 2004 г. Ассоциация Wi-Fi Alliance продвигает стандарты беспроводных локальных сетей и влияет на их развитие. Список одобренных продуктов можно найти на веб-сайте (http://www.wi-fi.org).

Беспроводные абонентские линии, разрешенные ITU-R и FCC

В РЧ-диапазоне есть несколько нелицензируемых полос. В данном разделе описываются нелицензируемые полосы, которые используются в абонентских линиях, разрешенных ITU-R и FCC.



Существует три нелицензируемые полосы: 900 МГц, 2,4 ГГц и 5,7 ГГц. Полосы 900-МГц и 2,4-ГГц также называют диапазонами ISM, а полосу 5 ГГц обычно называют диапазоном UNII (нелицензируемая национальная информационная инфраструктура).

Ниже приводятся частоты для этих диапазонов.

- **Полоса 900 МГц:** 902 – 928 МГц.
- **Полоса 2,4 ГГц:** 2,400 – 2,483 ГГц (в Японии данный диапазон расширен до 2,495 ГГц).
- **Полоса 5 ГГц:** 5150 – 5350 МГц, 5725 – 5825 МГц, в некоторых странах поддерживается средний участок 5350 – 5725 МГц. Не во всех странах разрешен стандарт IEEE 802.11a, и доступный спектр меняется в широких пределах. Список стран, в которых разрешен стандарт 802.11a, пересматривается.

На данном рисунке показаны частоты, используемые для беспроводных локальных сетей. Рядом с частотами беспроводных ЛВС в спектре находятся частоты, используемые другими беспроводными службами, такими как сотовая связь и службы узкополосной двусторонней персональной связи (NPCS). Частоты, используемые для беспроводных локальных сетей, находятся в диапазонах ISM.

Для использования беспроводного оборудования на нелицензируемой полосе частот лицензия не требуется. Однако эксклюзивное использование какой-либо частоты не допускается. Например, полоса 2,4 ГГц используется для беспроводных локальных сетей, передачи видеоданных, Bluetooth, в микроволновых печах и портативных телефонах. Использование нелицензируемых диапазонов подразумевает негарантированную производительность, а также возможные помехи и ослабление сигнала.

Хотя для использования оборудования в этих трех диапазонах лицензия не требуется, использование подчиняются нормам конкретного государства. Регулируются такие параметры, как мощность передатчика, коэффициент усиления антенны (увеличивающий эффективную мощность), а также сумма потерь в передатчике и проводах, коэффициент усиления антенны.

Эффективная мощность изотропного излучения (EIRP) – важный параметр, контролируемый местными органами регулирования. Поэтому при замене компонентов беспроводного оборудования, например добавлении или модернизации антенны для увеличения дальности передачи, следует соблюдать осторожность. В результате может возникнуть ситуация, когда беспроводная локальная сеть становится нелегальной по местным законам.

Эффективная мощность изотропного излучения = мощность передатчика + коэффициент усиления антенны – потери в проводах

Примечание Используйте только антенны и кабели оригинального производителя, предписанные для конкретной реализации точки доступа. Работы должны выполняться только квалифицированными специалистами, которые знакомы с нормативными требованиями по использованию радиоволн в данной стране.

Сравнение стандартов 802.11

В этом разделе приводится сравнение различных стандартов IEEE 802.11.

Стандарты IEEE определяют физический уровень и подуровень MAC канального уровня модели OSI. Исходный беспроводной стандарт 802.11 был выпущен в июне 1997 г. Он был пересмотрен в 1999 г. для создания стандарта IEEE 802.11a/b, который затем был повторно пересмотрен в 2003 г. как стандарт IEEE 802.11g.

По замыслу разработчиков данный стандарт не предназначается для верхних уровней модели OSI. IEEE 802.11b был разработан на основе технологии DSSS (расширение спектра с применением кода прямой последовательности). В технологии DSSS используется только один канал, который передает данные по всем частотам, определенным для этого канала.

Стандарт IEEE 802.11 делит диапазон ISM 2,4-ГГц на 14 каналов, но разрешенные каналы определяются местными органами регулирования, такими как FCC, например, каналы 1–11 в США. Каждый канал в диапазоне ISM 2,4-ГГц имеет полосу 22 МГц с шагом в 5 МГц, что приводит к наложению соседних каналов. Поэтому для обеспечения уникальных неперекрывающихся каналов необходимо разделение, эквивалентное пяти каналам. Например, среди 11 каналов, разрешенных FCC, существует всего три неперекрывающихся канала: 1, 6 и 11.

Напомним, что в беспроводных средах используется полудуплексная связь, поэтому полоса пропускания составляет только половину скорости передачи. Основной целью разработки стандарта IEEE 802.11b было достижение более высоких скоростей передачи данных в диапазоне ISM 2,4-ГГц для развития

потребительского рынка беспроводного доступа и поощрения потребителей к переходу на беспроводной доступ.

Стандарт 802.11b определил использование технологии DSSS с обновленным кодированием и модуляцией CCK (Complementary Code Keying) для более высоких скоростей передачи данных – 5,5 и 11 Мбит/с, при сохранении кодирования Баркера для скоростей 1 и 2 Мбит/с. В стандарте 802.11b используется тот же диапазон ISM 2,4-ГГц, что и в более ранних стандартах 802.11, что делает его обратно совместимым со стандартом 802.11 и соответствующими скоростями передачи данных 1 и 2 Мбит/с.

В год принятия стандарта 802.11b институт IEEE разработал другой стандарт, известный как 802.11a. Целью этого стандарта было увеличение скорости передачи данных с помощью другой технологии расширения спектра под названием OFDM (мультиплексирование с ортогональным делением частот) и модуляции, а также использования менее «населенного» диапазона UNII 5 ГГц. Диапазон ISM 2,4-ГГц широко используется всеми устройствами беспроводных локальных сетей, такими как Bluetooth, беспроводные телефоны, мониторами, видеопроигрывателями и домашними игровыми приставками. Кроме того, эта частота нередко используется микроволновыми печами. Стандарт 802.11a не был широко принят, так как для производства микросхем, поддерживающих стандарт 802.11a, требовался менее доступный материал, что с самого начала увеличивало затраты. В большинстве приложений потребность в поддержке беспроводной связи была удовлетворена с помощью более дешевых и доступных стандартов 802.11b.

В более поздней разработке института IEEE поддерживается использование 802.11 MAC и более высокие скорости передачи данных в диапазоне ISM 2,4 ГГц. В дополнении IEEE 802.11g используется более новая, чем в 802.11a, технология OFDM для более высоких скоростей, при этом сохраняется обратная совместимость с 802.11b за счет технологии DSSS, в которой используется тот же диапазон ISM. Поддерживаются скорости передачи данных DSSS 1, 2, 5,5 и 11 Мбит/с, а также скорости передачи данных OFDM 6, 9, 12, 18, 24, 48 и 54 Мбит/с. Институт IEEE требует обязательной поддержки только скоростей передачи данных 6, 12 и 24 Мбит/с независимо от того, поддерживает устройство стандарт 802.11a или 802.11g OFDM.

Сертификация Wi-Fi

Даже после создания стандартов 802.11 было необходимо обеспечить совместимость продуктов 802.11. В данном разделе описывается, как сертификация Wi-Fi обеспечивает совместимость.

Сертификация Wi-Fi

Wi-Fi Alliance **сертифицирует** совместимость продуктов.

- Продукты включают 802.11a, 802.11b, 802.11g, продукты с поддержкой двух диапазонов и тестирование безопасности.
- Гарантирует клиентам возможность миграции и интеграции.

Cisco является членом-основателем Wi-Fi Alliance.

Список сертифицированных продуктов см. на веб-сайте http://www.wi-fi.com.

Ассоциация Wi-Fi Alliance – глобальная некоммерческая отраслевая ассоциация, деятельность которой направлена на поощрение развития и принятия беспроводных локальных сетей. Одно из основных преимуществ Wi-Fi Alliance заключается в обеспечении совместимости продуктов 802.11, предлагаемых различными поставщиками, за счет сертификации. Сертифицированная совместимость поставщиков облегчает жизнь покупателям. Сертификация включает все три РЧ-технологии IEEE 802.1, а также ранние версии черновых проектов IEEE, например стандарты безопасности. Ассоциация Wi-Fi Alliance приняла черновой вариант стандарта безопасности IEEE 802.11i в качестве стандарта беспроводного защищенного доступа (WPA), затем обновила его до версии WPA2 после финального выпуска стандарта IEEE 802.11i.

Резюме

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

Резюме

- Сегодня люди хотят подключаться к сети в любое время и из любого места. Наиболее осязаемое преимущество беспроводного доступа — снижение расходов.
- И в проводных и в беспроводных используется доступ CSMA. Однако в беспроводных сетях реализовано предотвращение коллизий, а в проводных сетях обнаружение коллизий.
- Радиочастотные сигналы излучаются в эфир антеннами. Эти сигналы подверженны отражению, рассеиванию и поглощению.
- Стандарты 802.11 определяются институтом IEEE.

Резюме (прод.)

- Беспроводные абонентские диапазоны, разрешенные ITU-R и FCC, не лицензируются.
- 802.11 представляет собой набор стандартов, определяющих частоты и радиодиапазоны для сетей беспроводных сетей.
- Одно из основных преимуществ Wi-Fi Alliance заключается в гарантии совместимости продуктов 802.11.

Занятие 2

Общие сведения о безопасности беспроводных ЛВС

Обзор

Наиболее осязаемое преимущество беспроводного доступа – снижение расходов. В дополнение к увеличению производительности беспроводные локальные сети (WLAN) повышают качество работы. Однако нарушения безопасности на одной незащищенной точке доступа, могут нивелировать часы работы, потраченные на обеспечение безопасности корпоративной сети и даже разорить организацию. Важно понимать угрозы безопасности беспроводных локальных сетей и способы их устранения.

Задачи

По окончании этого занятия вы сможете описывать проблемы безопасности беспроводных локальных сетей и функции, которые можно использовать для повышения безопасности таких сетей. Это значит, что вы сможете выполнять следующие задачи:

- описывать распространенные угрозы для беспроводных локальных сетей;
- описывать методы снижения угроз безопасности беспроводных локальных сетей;
- описывать эволюцию безопасности беспроводных локальных сетей;
- описывать процесс привязки беспроводного клиента;
- описывать, как стандарт IEEE 802.1X обеспечивает дополнительную безопасность беспроводных локальных сетей;
- описывать режимы беспроводного защищенного доступа.

Угрозы безопасности беспроводных локальных сетей

В этом разделе описываются распространенные угрозы безопасности беспроводных локальных сетей.

С внедрением недорогих систем IEEE 802.11b/g неизбежно то, что у хакеров появится значительно больший выбор незащищенных беспроводных локальных сетей. Известно множество примеров применения многочисленных приложений с открытым исходным кодом для обнаружения и использования уязвимостей стандартного механизма обеспечения безопасности IEEE 802.11 (Wired Equivalent Privacy, WEP). Анализатор беспроводных сигналов позволяет сетевым инженерам пассивно перехватывать пакеты, чтобы проверить их и устранить системные неполадки. Эти же анализаторы могут применяться злоумышленниками для использования известных недостатков безопасности.

Термин «вардрайвинг» (или «война на колесах») первоначально означал использование сотового сканирующего устройства для поиска номеров сотовых телефонов для последующего проведения атак. Теперь этот термин также означает передвижение на автомобиле с портативным компьютером и клиентской платой 802.11b/g с целью найти систему 802.11b/g для последующей атаки.

Большинство продаваемых сегодня беспроводных устройств уже готовы для подключения к беспроводной локальной сети. Конечные пользователи нередко оставляют значения по умолчанию при конфигурации устройств или применяют только стандартный механизм защиты WEP, который не оптимален для защиты беспроводных сетей. При включенном базовом WEP-шифровании (или, напротив, без шифрования) существует возможность сбора данных и получения конфиденциальной сетевой информации, такой как сведения об учетных данных пользователя, номера счетов и личные записи.

Вредоносная точка доступа – это точка доступа, расположенная в беспроводной локальной сети и используемая для вмешательства в обычные сетевые операции, например, для атак типа «отказ в обслуживании» (DoS). Если во вредоносной точке доступа запрограммирован правильный WEP-ключ, то клиентские данные могут быть перехвачены. Вредоносную точку доступа также можно настроить на предоставление неавторизованным пользователям такой информации, как MAC-адреса клиентов (как для беспроводных, так и для проводных сетей), на перехват и подделку пакетов данных или, в худшем случае, на получение доступа к серверам и файлам. Простой и распространенный вариант вредоносной точки доступа – точка, установленная авторизованными сотрудниками. Сотрудники устанавливают точки доступа, предназначенные для домашнего использования, без необходимой конфигурации безопасности корпоративной сети, что создает угрозу безопасности сети.

Уменьшение угроз безопасности

В этом разделе описаны способы уменьшения угроз безопасности беспроводных локальных сетей.

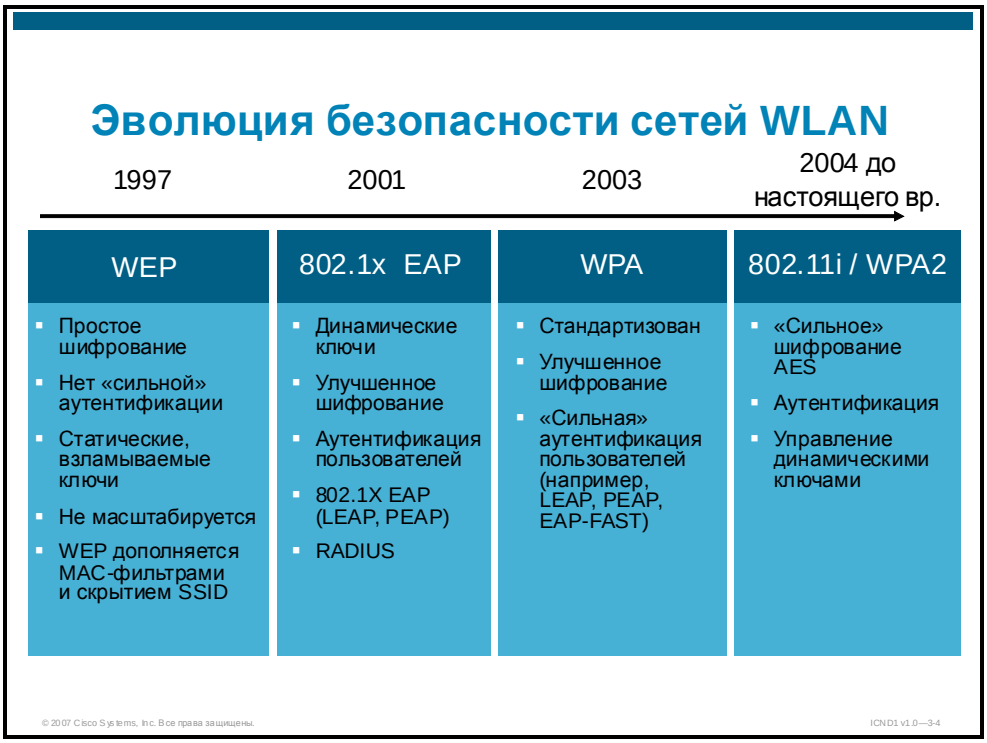
Для защиты беспроводной локальной сети необходимо настроить следующие параметры.

- Аутентификацию, для обеспечения доступа к сети через доверенные точки доступа только уполномоченным клиентам и пользователям.
- Шифрование, чтобы обеспечить секретность и конфиденциальность.
- Системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS) для защиты от угроз безопасности и доступности.

Фундаментальный подход к обеспечению безопасности беспроводных сетей подразумевает аутентификацию и шифрование для защиты беспроводной передачи данных. Существуют различные уровни внедрения этих методов защиты беспроводных сетей, однако оба метода применяются в беспроводных сетях малых офисов, домашних офисов и крупных предприятий. Для больших корпоративных сетей требуются дополнительные уровни безопасности, предлагаемые монитором IPS. Современные системы IPS могут не только обнаруживать атаки на беспроводные сети, но также предоставляет базовую защиту от неавторизованных клиентов и точек доступа. Во многих корпоративных сетях системы IPS используются для защиты главным образом не от внешних угроз, а от непреднамеренной установки небезопасных точек доступа сотрудниками, желающими воспользоваться мобильностью и преимуществами беспроводного доступа.

Эволюция безопасности беспроводных сетей

Почти сразу после создания первых стандартов беспроводных локальных сетей злоумышленники начали предпринимать попытки воспользоваться недостатками систем безопасности. Для борьбы с этой угрозой стандарты беспроводных локальных сетей развивались для предоставления более высокого уровня безопасности. В этом разделе описывается эволюция безопасности беспроводных локальных сетей.



На этом рисунке показана эволюция безопасности беспроводных локальных сетей.

Первоначально в стандарте безопасности 802.11 были определены только 64-битные статические WEP-ключи как для шифрования, так и для аутентификации. В этом 64-битном ключе содержался фактический 40-битный ключ и 24-битный вектор инициализации. Метод аутентификации не был «сильным», и такие ключи, в конце концов, были скомпрометированы. Так как эти ключи управлялись статически, данный метод обеспечения безопасности не мог масштабироваться на крупные корпоративные среды. Компании пытались бороться с этой слабостью с помощью таких методов, как скрытие идентификаторов наборов услуг (SSID) и фильтрация MAC-адресов.

SSID представляет собой схему сетевого именования и настраиваемый параметр, который должен быть общим для клиента и точки доступа. Если точка доступа настроена на широковещательную рассылку своего идентификатора SSID, клиент ассоциирует себя с данной точкой доступа, пользуясь идентификатором SSID, объявленным точкой доступа. Точку доступа можно настроить без широковещательной рассылки параметра SSID (скрытие SSID), чтобы обеспечить первый уровень защиты. Считалось, что если точка доступа себя не объявляет, то злоумышленнику будет труднее ее найти. Чтобы позволить клиентам получать идентификатор SSID точки доступа, стандарт 802.11 допускал использование беспроводными клиентами пустых строк (без значения в поле SSID), которые обозначали запрос к точке доступа на широковещательную

рассылку идентификатора SSID. Однако этот метод делает защиту, описанную выше, неэффективной, так как злоумышленнику достаточно отправлять пустую строку, для нахождения точки доступа. Точки доступа также поддерживали фильтрацию по MAC-адресу. В точках доступа вручную создавались таблицы, разрешающие или запрещающие доступ клиентов на основе их физических аппаратных адресов. Однако MAC-адреса легко подменить, поэтому фильтрация MAC-адресов не считается функцией безопасности.

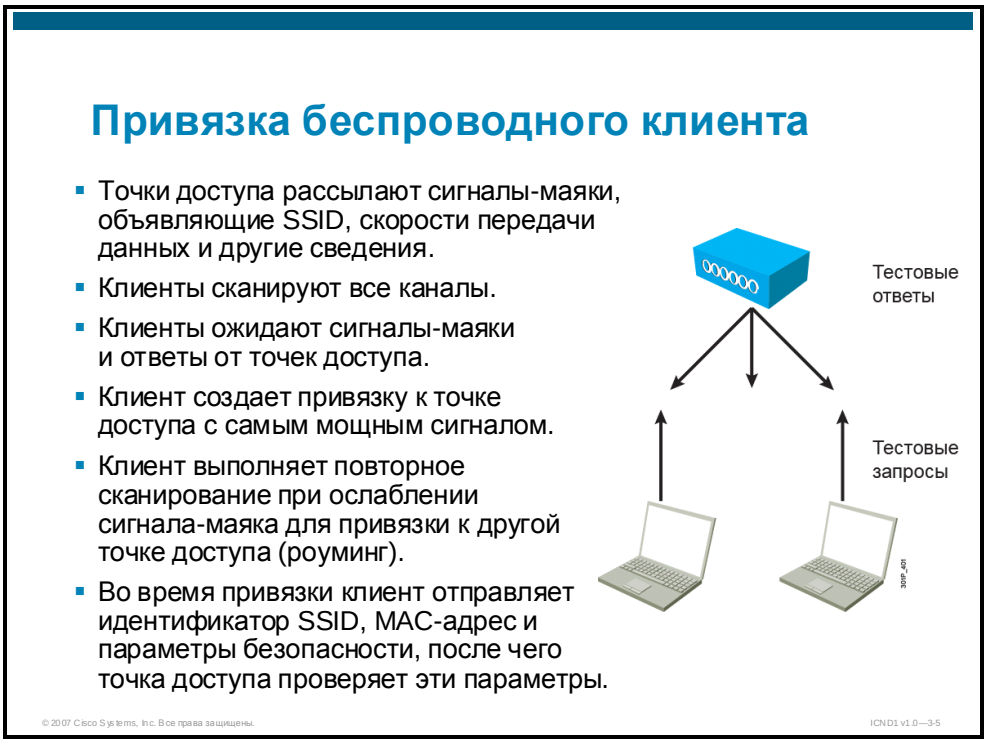
В то время как в комитетах 802.11 начинался процесс модернизации безопасности беспроводных локальных сетей, корпоративные заказчики нуждались в системе безопасности беспроводных сетей немедленно, чтобы сделать их развертывание возможным. Учитывая требования заказчиков, компания Cisco ввела собственные улучшения в WEP-шифровании, основанное на RC4. Для защиты WEP-ключей компания Cisco реализовала механизм попакетного формирования или хэширования ключей по протоколу Temporal Key Integrity Protocol (TKIP) и проверку целостности сообщений Cisco (Cisco MIC). Кроме того, компания Cisco адаптировала протоколы аутентификации проводных сетей 802.1X для беспроводных и динамических ключей с помощью протокола Cisco Lightweight Extensible Authentication Protocol (Cisco LEAP) для обеспечения централизованной базы данных.

Вскоре после внедрения беспроводной безопасности Cisco ассоциация Wi-Fi ввела беспроводной защищенный доступ WPA в качестве промежуточного решения. Это решение было частью ожидаемого стандарта безопасности IEEE 802.11i для беспроводных локальных сетей, в котором используется аутентификация и усовершенствования 802.1X для WEP-шифрования. Новый протокол TKIP с хэшированием ключей предлагает функции, аналогичные функциям протоколов Cisco KIP и MIC, однако эти три решения по безопасности несовместимы.

На данный момент стандарт 802.11i одобрен и улучшенный стандарт шифрования (AES) заменил WEP как самый последний и наиболее безопасный метод шифрования данных. Системы IDS для беспроводных сетей способны обнаруживать атаки и защищать беспроводные локальные сети от этих атак. Ассоциация Wi-Fi Alliance сертифицирует устройства 802.11i на соответствие новому стандарту беспроводного защищенного доступа WPA2.

Привязка беспроводного клиента

В этом разделе описывается процесс привязки беспроводного клиента.



Во время привязки клиента точки доступа рассылают сигналы-маяки, объявляющие один или несколько идентификаторов SSID, скорости передачи данных и другие данные. Клиент сканирует все каналы и ожидает сигналы-маяки и ответы от точек доступа. Клиент привязывается к точке доступа с самым мощным сигналом. Если мощность сигнала снижается, клиент возобновляет процесс сканирования, чтобы привязаться к другой точке доступа (этот процесс называется роумингом). Во время привязки клиент отправляет идентификатор SSID, MAC-адрес и параметры безопасности, после чего точка доступа проверяет эти параметры.

Привязка беспроводного клиента к выбранной точке доступа фактически является вторым этапом двухэтапного процесса. Сначала выполняется аутентификация, а затем привязка, которая позволяет клиенту 802.11 передавать трафик через точку доступа другому хосту в сети. Аутентификация в этом первичном процессе отличается от сетевой аутентификации (ввода имени пользователя и пароля для получения доступа к сети). Аутентификация клиента – это просто первый шаг (перед привязкой) между беспроводным клиентом и точкой доступа, который заключается в установлении соединения. Стандарт 802.11 определял только два метода аутентификации: открытая аутентификация и аутентификация с общим ключом. Открытая аутентификация – это просто обмен четырьмя пакетами приветствия без проверки клиента или точки доступа, обеспечивающий простое подключение. При аутентификации с общим ключом для проверки используется статически заданный WEP-ключ, известный клиенту и точке доступа. Этот же ключ можно использовать для шифрования передачи данных между беспроводным клиентом и точкой доступа в зависимости от пользовательской конфигурации.

Применение 802.1X в беспроводных локальных сетях

В этом разделе описывается, как стандарт IEEE 802.1X обеспечивает дополнительную безопасность беспроводных локальных сетей.

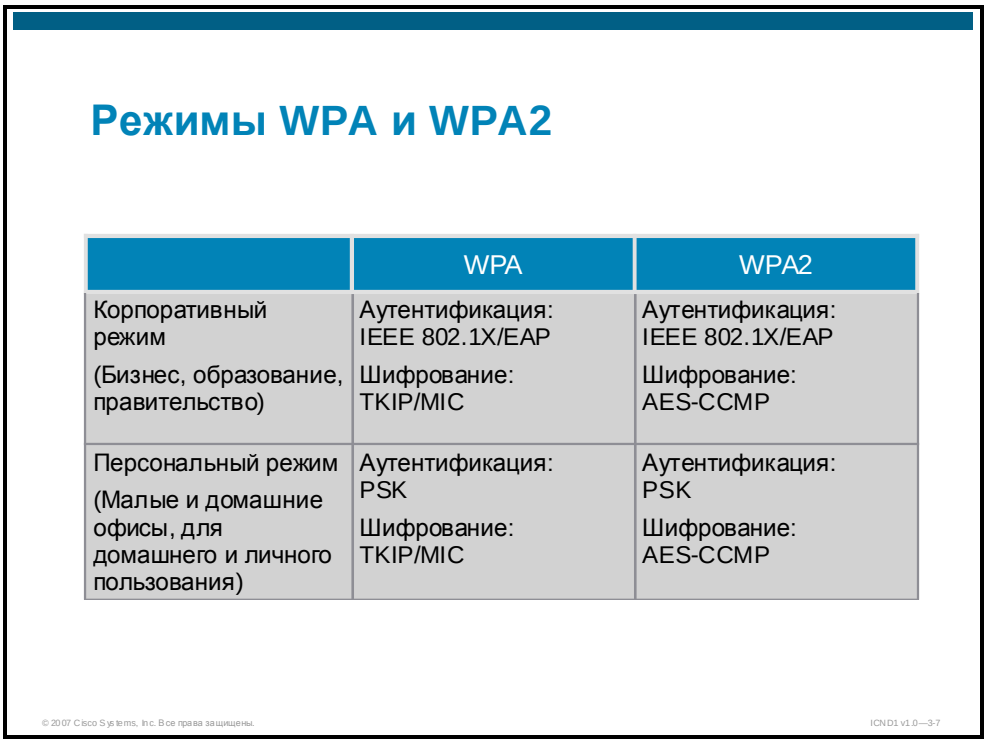
Точка доступа, выполняющая аутентификацию на стороне предприятия, разрешает клиенту создать привязку с использованием открытой аутентификации. Затем точка доступа инкапсулирует трафик 802.1X к серверу аутентификации и пересылается его серверу. Весь остальной сетевой трафик блокируется, т. е. блокируются все остальные попытки доступа к сетевым ресурсам.

При получении RADIUS-трафика для клиента точка доступа инкапсулирует его и пересылает клиенту. Хотя сервер аутентифицирует клиента как действующего пользователя сети, этот процесс также позволяет клиенту проверять сервер, что предотвращает подключение клиента к поддельному серверу.

Тогда как в корпоративных сетях используются централизованные серверы аутентификации, в малых офисах или предприятиях могут просто использовать точку доступа с предварительно сконфигурированными общими ключами вместо сервера аутентификации для беспроводных клиентов.

Режимы WPA и WPA2

В этом разделе описываются режимы защищенного беспроводного доступа (WPA).



Режим WPA предоставляет поддержку аутентификации на основе стандарта 802.1X и заранее сконфигурированного общего ключа (PSK). (Стандарт 802.1X рекомендуется использовать для корпоративных сред.) Режим WPA обеспечивает шифрование через TKIP. Протокол TKIP включает функции проверки целостности сообщений (MIC) и попакетного формирования ключей (PPK) путем хэширования вектора инициализации и ротации широковещательных ключей.

По сравнению с WPA проверка подлинности WPA2 не изменилась, но используется шифрование AES-Counter с протоколом CBC MAC (AES-CCMP).

Корпоративный режим

«Корпоративный режим» – это термин, используемый для продуктов, которые проверены на совместимость с режимами аутентификации PSK и 802.1X/EAP. При использовании стандарта 802.1X необходим сервер аутентификации, авторизации и учета (AAA) (протокол RADIUS для аутентификации и управления ключами, а также для централизованного управления учетными данными пользователей). Корпоративный режим ориентирован на корпоративные среды.

Персональный режим

«Персональный режим» – это термин, используемый для продуктов, которые проверены на совместимость только с режимом аутентификации PSK. В этом режиме требуется ручная настройка общих ключей на точке доступа и клиентах. В режиме PSK аутентификация пользователей осуществляется с помощью пароля или идентифицирующего кода как на стороне клиента, так и на стороне точки доступа. Сервер аутентификации не требуется. Персональный режим ориентирован на среды малых и домашних офисов.

Резюме

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

Резюме

- Незащищенные беспроводные ЛВС неизбежно подвергаются атакам.
- Фундаментальный подход к обеспечению безопасности беспроводных сетей подразумевает аутентификацию и шифрование для защиты беспроводной передачи данных.
- Стандарты развивались для повышения безопасности.
  - WEP
  - 802.1x EAP
  - WPA
  - 802.11i/WPA2
- Точки доступа рассылают сигналы-маяки, объявляющие SSID, скорости передачи данных и другие сведения.

Резюме (прод.)

- Точка доступа, выполняющая аутентификацию на стороне предприятия, разрешает клиенту создать привязку с использованием открытой аутентификации.
- WPA предоставляет поддержку аутентификации IEEE 802.1X и PSK.
  - Корпоративный режим — это термин, используемый для продуктов, которые проверены на совместимость с режимами аутентификации PSK и 802.1X/EAP.
  - Персональный режим — это термин, используемый для продуктов, которые проверены на совместимость только с режимом аутентификации PSK.

Занятие 3

Внедрение беспроводной локальной сети

Обзор

Внедрение беспроводной локальной сети не ограничивается выбором нужного стандарта. Размещение точки доступа может оказывать большее влияние на полосу пропускания, чем стандарты. Важно понимать, как такие аспекты, как топология, расстояние и расположение точки доступа влияет на эффективность беспроводной локальной сети.

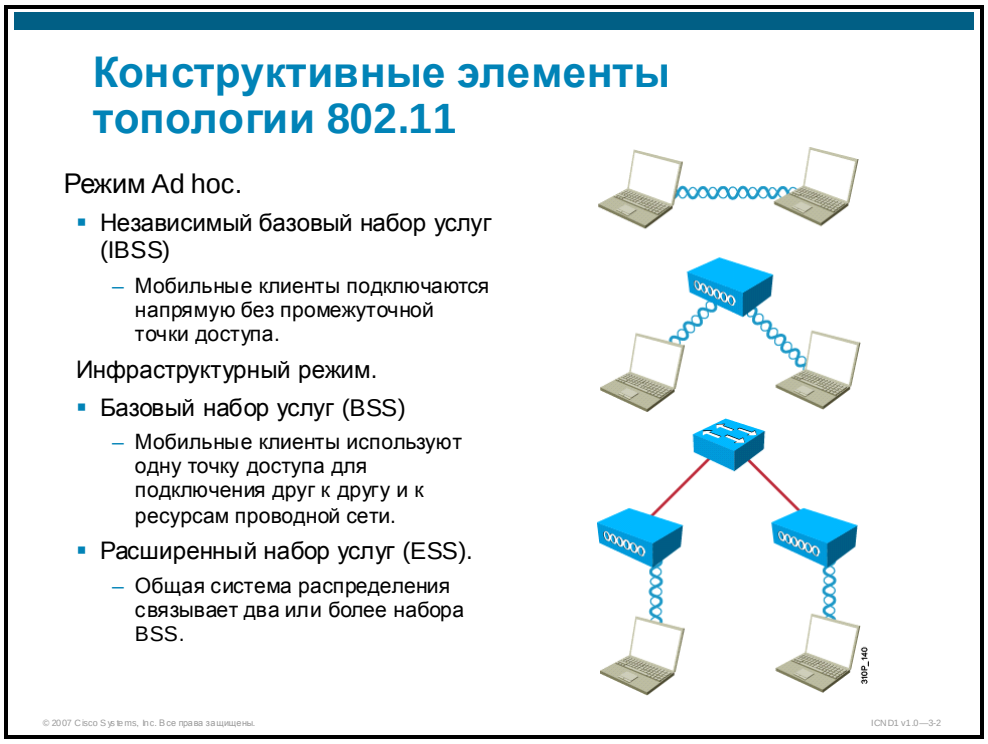
Задачи

По окончании этого занятия вы сможете описывать факторы, влияющие на внедрение беспроводных локальных сетей. Это значит, что вы сможете выполнять следующие задачи:

- описывать топологию IEEE 802.11;
- описывать службу BSA;
- описывать влияние расстояния и скорости на обслуживание в беспроводной локальной сети;
- описывать факторы, которые следует учитывать при внедрении точки доступа;
- описывать базовое внедрение беспроводной локальной сети;
- описать форм-факторы для внедрения беспроводного доступа на портативных компьютерах;
- описывать распространенные проблемы беспроводного доступа и методы их устранения.

Конструктивные элементы топологии 802.11

В этом разделе описываются топологии 802.11.



Стандарт 802.11 предоставляет несколько топологий (режимов), которые могут использоваться как конструктивные элементы беспроводной локальной сети.

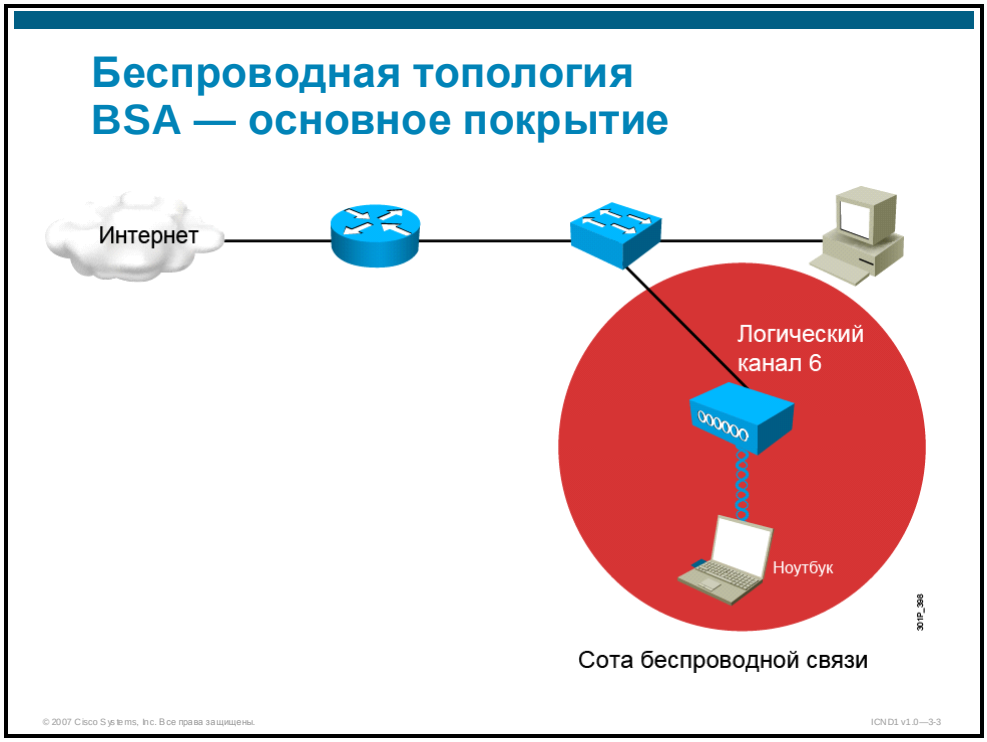
- **Режим Ad hoc.** Режим Ad hoc топологии – это независимый базовый набор услуг (IBSS). Мобильные клиенты подключаются напрямую без промежуточной точки доступа. Операционные системы, такие как Windows, упростили установку такой одноранговой сети. Такая установка может использоваться в малых офисах (или домашних офисах) для подключения портативного компьютера к основному ПК, или для совместного использования файлов группой пользователей. Зона покрытия ограничена. Каждый должен слышать каждого. Точка доступа не требуется. Недостаток одноранговых сетей заключается в сложности обеспечения безопасности.
- **Инфраструктурный режим.** В инфраструктурном режиме клиенты подключаются через точку доступа. Существует два инфраструктурных режима.
  - **Базовый набор услуг (BSS).** Устройства связи, формирующие BSS, являются мобильными клиентами, использующими одну точку доступа для подключения друг к другу и к ресурсам проводной сети. Идентификатор базового набора услуг (BSSID) – это MAC-адрес 2-го уровня радиоплаты точки доступа BSS. Хотя BSS является фундаментальным конструктивным элементом беспроводной топологии, а точка доступа BSS уникально идентифицируется значением BSSID, сама беспроводная сеть объявляется посредством идентификатора набора услуг (SSID), который сообщает мобильным клиентам о доступности беспроводной сети. SSID – это имя беспроводной сети, которое настраивается пользователем и может содержать до 32 символов с учетом регистра.

— **Расширенный набор услуг (ESS).** Беспроводная топология расширяется на два или более базовых набора услуг, связанных системой распределения или проводной инфраструктурой. Обычно ESS включает общий идентификатор SSID, обеспечивающий роуминг от одной точки доступа к другой без перенастройки клиента.

Эти топологии определены в исходном стандарте 802.11, в то время как другие топологии, такие как повторители, мосты и мосты рабочей группы, являются расширениями и определяются поставщиками.

Беспроводная топология BSA

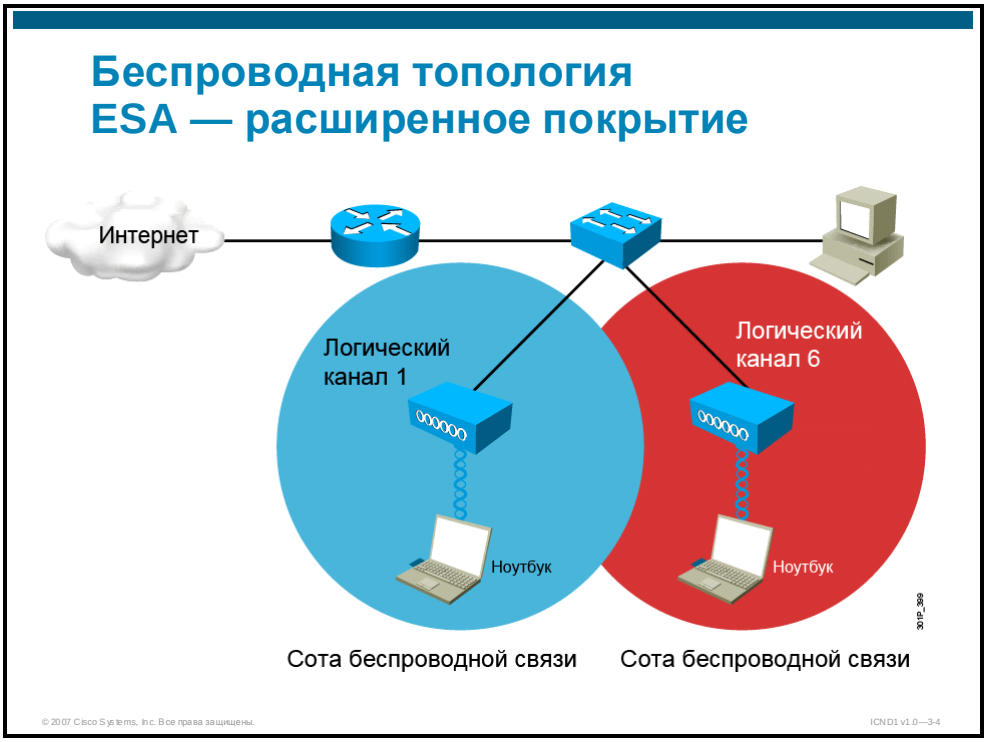
В этом разделе описываются топологии базовой области обслуживания (BSA) и расширенной области обслуживания (ESA) и ихроли в беспроводной локальной сети.



Базовая область обслуживания (BSA) — это физическая зона покрытия РЧ-сигнала, обеспечиваемая точкой доступа в BSS. Эта область зависит от формируемого энергетического радиочастотного поля с изменениями, обусловленными выходной мощностью точки доступа, типом антенны и физическим окружением, влияющим на распространение радиоволн. Эта зона покрытия также называется сотой. Хотя BSS является конструктивным элементом топологии, а BSA фактической зоной покрытия при обсуждении базовых беспроводных сетей эти термины взаимозаменяемы.

Точка доступа подключается к магистрали Ethernet и взаимодействует со всеми беспроводными устройствами текущей соты. Эта точка доступа является главной для данной соты, и контролирует входящий и исходящий трафик сети. Удаленные устройства не взаимодействуют напрямую друг с другом; они связываются только с точкой доступа. Уникальный РЧ-канал и идентификатор SSID настраиваются пользователем.

Точка доступа выполняет широковещательную рассылку сигналов-маяков с именем беспроводной соты в SSID. Сигналы-маяки рассылаются точками доступа, чтобы объявить о доступных службах. Идентификатор SSID используется для логического разделения беспроводных локальных сетей. Он должен устанавливать однозначное соответствие между клиентом и точкой доступа. Однако клиенты могут быть настроены без SSID (неопределенный SSID), тогда они обнаруживают все точки доступа и узнают SSID из сигналов-маяков точки доступа. Общим примером процесса обнаружения может служить процесс, используемый встроенной утилитой Wireless Zero Configuration (WZC) при перемещении беспроводного портативного компьютера в новое место. Пользователю показывается окно с найденными беспроводными службами и запрашивается подключение или соответствующий ключ для привязки. Широковещательные рассылки SSID можно отключить на точке доступа, но этот подход не работает, если клиенту необходимо получать SSID из сигнала-маяка.



Если одна сота не обеспечивает достаточной зоны покрытия, для ее расширения может быть добавлено любое число сот. Набор объединенных сот также известен как расширенная область обслуживания (ESA).

Рекомендуется, чтобы соты расширенной области обслуживания перекрывались на 10 – 15%, чтобы позволить удаленным пользователям выполнять роуминг без потери РЧ-соединений. Для беспроводных голосовых сетей рекомендуется перекрытие на 15 – 20%. Для улучшения производительности пограничные соты следует настроить на разные неперекрывающиеся каналы.

Скорости передачи данных для различных беспроводных топологий

Клиенты беспроводных локальных сетей способны изменять скорость передачи данных во время движения. В этом разделе описывается влияние расстояния и скорости на работу беспроводной локальной сети.

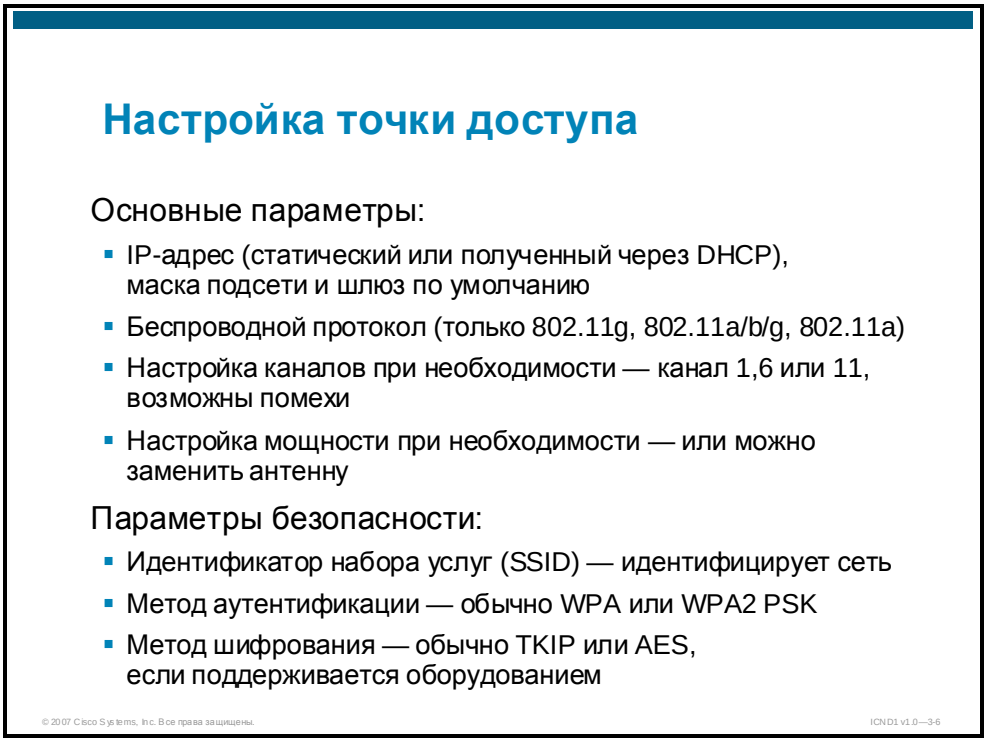
Клиенты беспроводных локальных сетей могут изменять скорость передачи данных во время движения. Этот метод позволяет клиенту, работающему на скорости 11 Мбит/с, переключиться на скорость 5,5 Мбит/с, затем на 2 Мбит/с, и оставаться на связи на внешнем кольце при скорости 1 Мбит/с. Такое переключение скорости передачи выполняется без потери соединения и участия пользователя. Кроме того, переключение скорости выполняется для каждой отдельной передачи, поэтому точка доступа может поддерживать несколько клиентов с различными скоростями в зависимости от расположения каждого из них.

- Для получения более высоких скоростей передачи данных требуется более мощный сигнал на приемнике. Поэтому при более низких скоростях дальность передачи увеличивается.
- Беспроводные клиенты всегда пытаются подключиться на максимально возможной скорости передачи.
- Клиент снижает скорость передачи данных только в случае возникновения ошибок или повторов передачи.

Это подход обеспечивает максимальную общую полосу пропускания в заданной беспроводной соте. На рисунке описывается стандарт IEEE 802.11b, однако эта концепция применима к скоростям передачи данных по стандартам 802.11a и 802.11g.

Настройка точки доступа

В этом разделе описываются факторы, которые следует учитывать при внедрении беспроводной локальной сети.



Беспроводные точки доступа можно настроить с помощью интерфейса командной строки (CLI) или, что более распространено, посредством графического пользовательского интерфейса посредством браузера. Однако режим настройки основных параметров беспроводного доступа одинаков. К основным параметрам беспроводных точек доступа относятся SSID, РЧ-канал с возможностью указания мощности, а также аутентификация (безопасность), основные параметры беспроводного клиента ограничиваются аутентификацией. Беспроводным клиентам требуется меньше параметров, так как беспроводной сетевой адаптер (NIC) сканирует все доступные радиочастоты (подразумевается, что плата IEEE 802.11b/g не сканирует диапазон 5 ГГц), чтобы обнаружить РЧ-канал, и, как правило, инициирует соединение с неопределенным идентификатором SSID, чтобы обнаружить доступные SSID. Поэтому в соответствии со стандартом 802.11 при использовании открытой аутентификации применяется режим plug-and-play. Если система безопасности настроена в режиме предварительно-сконфигурированных общих ключей (PSK) для старого или текущего механизма обеспечения безопасности (WEP или WPA соответственно) следует помнить о том, что для создания подключения требуется полное совпадение ключей.

В зависимости от выбранного оборудования ТД, точка доступа может поддерживать два диапазона частот (ISM 2,4 ГГц и UNII 5 ГГц) и все три реализации IEEE 802.11a/b/g. Точки доступа, как правило, позволяют выполнять тонкую настройку параметров, таких как предлагаемые частоты, выбор радиомодуля и стандарта IEEE, используемого на этом радиомодуле.

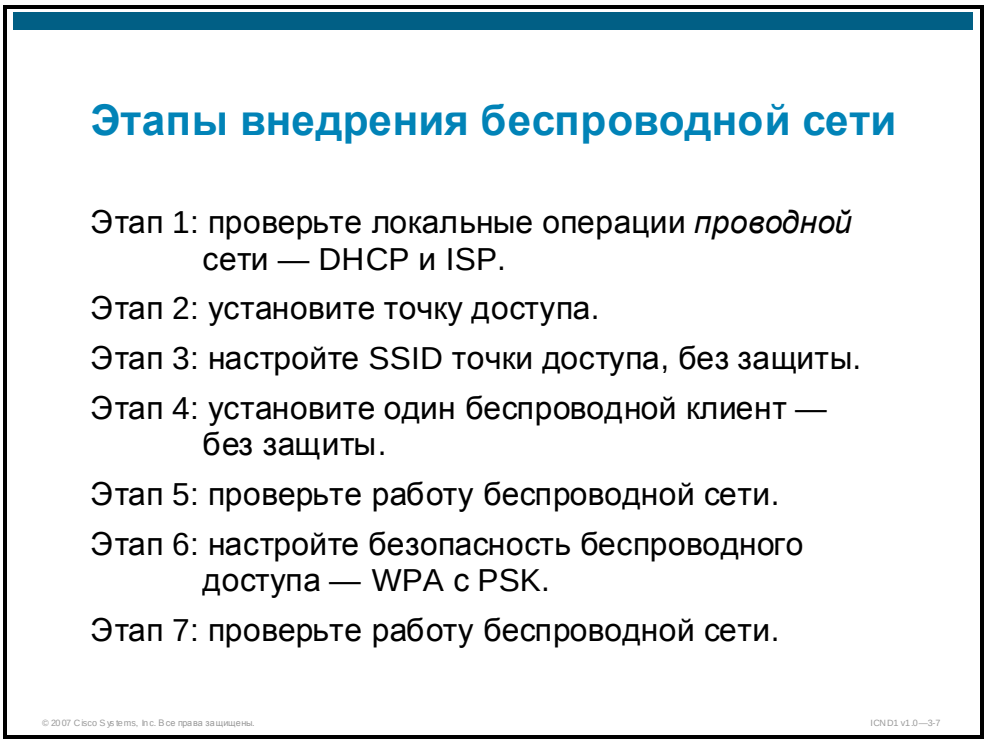
Примечание Подробные сведения об этих настройках не включены в данный курс.

При смешанном использовании беспроводных клиентов 802.11b и 802.11g полоса пропускания снижается, так как в точке доступа необходимо реализовать защитный протокол готовности к передаче/готовности к приему (RTS/CTS). Следовательно, при внедрении беспроводных клиентов только одного типа IEEE полоса пропускания будет выше, чем в смешанном режиме.

После настройки базовых обязательных параметров беспроводной точки доступа необходимо настроить дополнительные базовые параметры проводной сети – маршрутизатора по умолчанию и DHCP-сервера. В существующей локальной сети должен присутствовать маршрутизатор по умолчанию для выхода из сети и DHCP-сервер для выделения IP-адресов компьютерам, подключенным к проводной сети. Существующий маршрутизатор и DHCP-серверы используются точкой доступа для ретрансляции IP-адресов беспроводным клиентам. Из-за расширения сети следует убедиться, что существующий диапазон IP-адресов DHCP достаточно велик для включения новых беспроводных клиентов. В случае новой установки со всеми функциями маршрутизатора и точек доступа, реализованными на одном оборудовании, следует просто настроить все необходимые параметры на этом оборудовании.

Этапы внедрения беспроводной сети

В этом разделе описывается базовый подход к внедрению беспроводной сети.

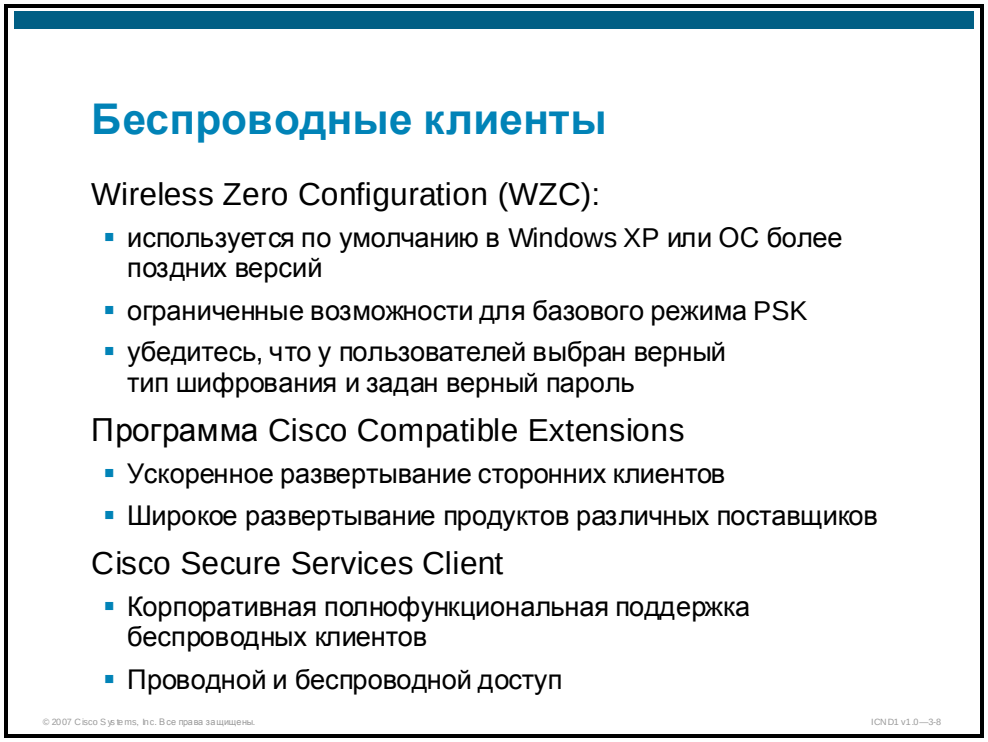


Базовый подход к внедрению беспроводной сети (как и к базовой организации любой сети) заключается в поэтапной настройке и тестировании.

Перед внедрением беспроводной сети проверьте существующую сеть и доступ к Интернету для проводных хостов. Внедрите беспроводной доступ только с одной точкой доступа и одним клиентом без механизмов безопасности беспроводной сети. Убедитесь, что беспроводной клиент получает IP-адрес от DHCP-сервера и может отправить эхо-запрос локальному проводному маршрутизатору, а затем выйти во внешний Интернет. Наконец, настройте механизм безопасности беспроводного доступа WPA. Режим WEP используется только в том случае, если оборудование не поддерживает WPA.

Беспроводные клиенты

В этом разделе описываются форм-факторы для внедрения беспроводного доступа на портативных компьютерах.



В настоящее время доступно множество форм-факторов для внедрения беспроводного доступа на портативных компьютерах. Наиболее распространены USB-устройства со встроенными фиксированными антеннами и ПО для беспроводного доступа, которые позволяют использовать оборудование беспроводного доступа и предоставляют средства безопасности для аутентификации и шифрования. Большинство портативных компьютеров содержат средства беспроводного доступа. Такая доступность беспроводной технологии привела к расширению рынка беспроводной связи и упрощению ее использования. Новые операционные системы Microsoft Windows включают базового клиента беспроводного доступа (WZC), обеспечивающего беспроводное подключение по методу «plug-and-play». Он обнаруживает широковещательную рассылку идентификаторов SSID и позволяет пользователю вводить предварительный общий ключ, например, для WEP или WPA. Основных возможностей WZC достаточно для простых сред малых и домашних офисов.

В крупных корпоративных сетях требуется более широкие возможности беспроводных клиентов, не поддерживаемые встроенными утилитами ОС. В 2000 году компания Cisco запустила программу совершенствования важных функций посредством безвозмездной программы сертификации. Более 95% продаваемых сегодня портативных компьютеров с беспроводным доступом совместимы с расширениями Cisco. Подробные сведения и информацию о состоянии версий и функций можно найти на веб-сайте http://www.cisco.com. В следующей таблице приводится сводка версий и функций.

Версии и функции

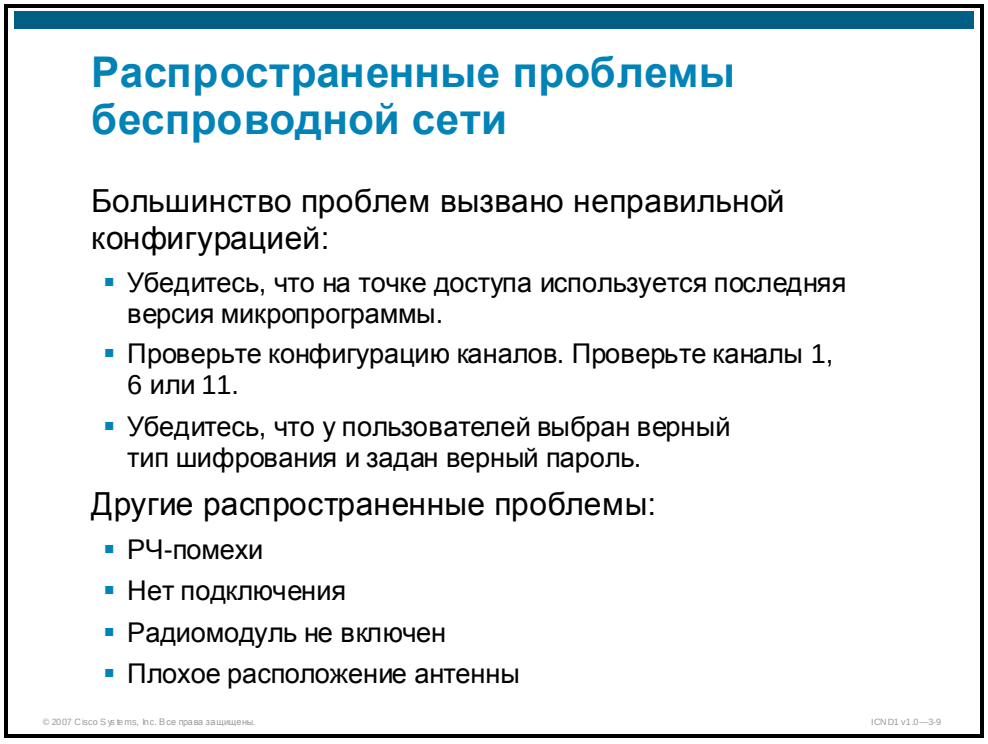
Версия	Тема	Пример
v1	Безопасность	Wi-Fi-совместимость; 802.1X, LEAP, протокол Cisco Key Integrity Protocol
v2	Масштабирование	WPA, роуминг с помощью точек доступа
v3	Производительность и безопасность	WPA2, Wi-Fi-мультимедиа (WMM)
v4	Передача голоса по беспроводным ЛВС	Управление приемом вызовов (CAC), метрики голосовой связи
v5	Управление и система предотвращения вторжений (IPS)	Защита кадров управления (Management Frame Protection), отчеты по клиентам

До тех пор, пока компания Cisco не предложила полнофункциональную поддержку и проводных, и беспроводных клиентов в продукте, который называется Cisco Secure Services Client, в корпоративных сетях проводные и беспроводные клиенты управлялись по отдельности. Преимущество для пользователей заключается в едином клиенте для проводного или беспроводного подключения и безопасности.

Дополнительные сведения см. на странице http://www.cisco.com/go/ciscocompatible/wireless.

Устранение неполадок беспроводного доступа

В этом разделе описываются распространенные проблемы беспроводного доступа и методы их устранения.



Если следовать рекомендуемым действиям по внедрению беспроводной сети, метод поэтапной настройки скорее всего позволит выявить причину проблемы. Наиболее распространенные причины проблем конфигурации:

- настройка определенного идентификатора SSID на клиенте (в противоположность методу обнаружения SSID), который не соответствует данной точке доступа (регистр учитывается);
- настройка несовместимых методов безопасности.

На беспроводном клиенте и точке доступа должны использоваться одинаковые методы аутентификации (EAP или PSK) и шифрования (TKIP или AES).

Другие распространенные проблемы могут быть связаны с установкой радиочастотного модуля, поэтому следует найти ответы на следующие вопросы:

- Настроен ли радиомодуль точки доступа и клиента на правильный РЧ-канал (ISM 2,4 ГГц или UNII 5 ГГц)?
- Подключена ли внешняя антенна и верно ли ее направление?
- Находится ли антенна слишком высоко или слишком низко по отношению к беспроводным клиентам (предпочтительная высота – 6 м над клиентом)?
- Есть ли в помещении металлические объекты, отражающие радиоволны и ухудшающие прием и передачу?
- Не пытаетесь ли вы работать на слишком большом расстоянии?

Устранение неполадок беспроводного доступа

- Устанавливайте точку доступа рядом с центром дома или офиса.
- Не монтируйте точку доступа рядом с металлическими объектами.
- Точка доступа не должна находиться в зоне прямой видимости с устройствами, содержащих металл
- Проверьте подключение без аутентификации PSK.
- Избегайте РЧ-помех от другого оборудования (игровых приставок, мониторов, телефонов).
- В большом доме или офисе может потребоваться две или более точки доступа.
- Убедитесь, что точка доступа работает на уникальном канале, который не используется расположенными по соседству точками доступа.

Первый шаг в устранении предполагаемой проблемы беспроводного доступа состоит в разделении среды на проводную и беспроводную. Затем отделите проблемы настройки беспроводной сети от проблем, связанных с радиоволнами. Сначала проверяется правильность работы существующей проводной инфраструктуры и связанных с ней служб. Необходимо убедиться, что существующие узлы, подключенные к Ethernet, способны обновлять свои DHCP-адреса и выходить в Интернет.

Затем следует расположить поблизости точку доступа с беспроводным клиентом, чтобы проверить конфигурацию и исключить возможность проблем с радиоволнами. Всегда запускайте беспроводного клиента с открытой аутентификацией. Установите подключение. Затем внедрите необходимые меры безопасности беспроводного доступа.

Если беспроводной клиент работает в этот момент, то остаются только неполадки, связанные с радиоволнами. Сначала проверьте наличие металлических препятствий. Если такие есть, переместите их или измените расположение точки доступа. Если расстояние слишком велико, рассмотрите возможность добавления другой точки доступа с тем же SSID, но уникальным РЧ-каналом. Наконец, проанализируйте среду распространения радиоволн. Канал РЧ 2,4 ГГц может быть перегружен трафиком (чаще, чем канал 5 ГГц), так же, как проводная сеть. Проверьте работу других беспроводных устройств, использующих частоту 2,4 ГГц.

Проблемы производительности, возникающие в определенное время суток, указывают на интерференцию с излучением какого-либо устройства. Например, в обеденное время может снижаться производительность в офисе, расположенном рядом с микроволновой печью, часто используемой сотрудниками. Хотя большинство микроволновых печей перекрываются с РЧ-каналом 11, некоторые из них перекрываются со всеми РЧ-каналами. Еще одним источником проблем могут быть РЧ-устройства, которые резко меняют частоты, например, при скачкообразной смене рабочей частоты с расширением спектра (FHSS), используемой в беспроводных телефонах. Так как может существовать много источников интерференции радиоволн, всегда следует начинать с близкого расположения точки доступа и беспроводного клиента, а затем перемещать беспроводной клиент, пока не возникнет проблема. На большинстве беспроводных клиентов установлено вспомогательное программное обеспечение, которое помогает устранять неполадки, предоставляя сведения об мощности и качестве радиосигнала.

Резюме

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

Резюме

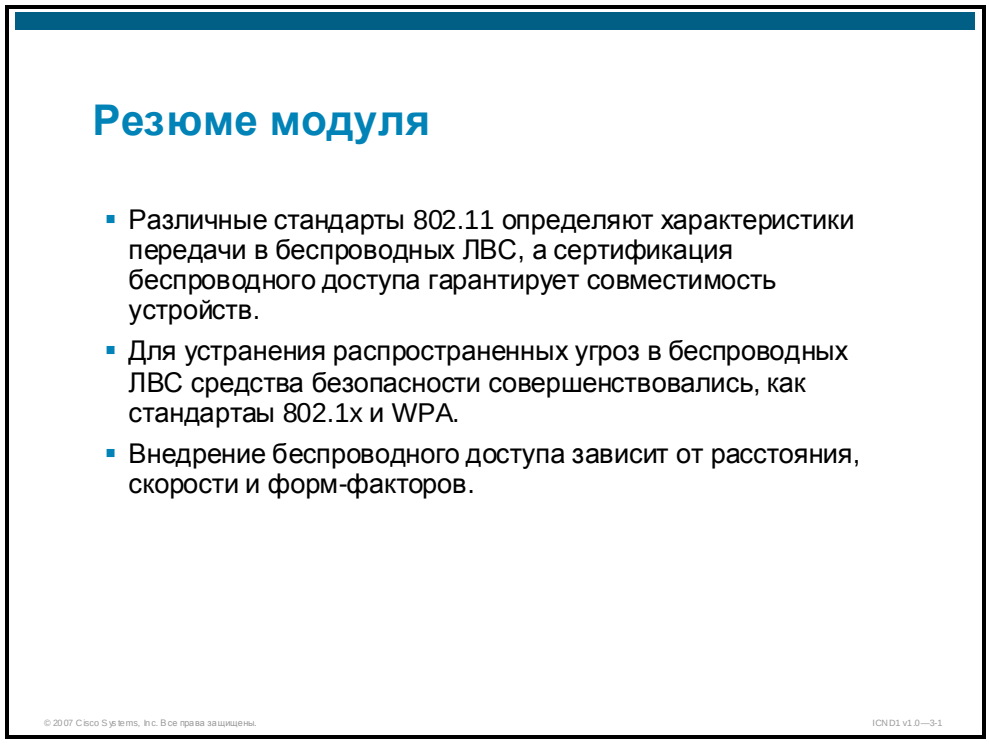
- Топологии 802.11 используются в различных режимах
  - В режиме ad hoc клиенты подключаются напрямую без промежуточной точки доступа.
  - В инфраструктурном режиме клиенты подключаются через точку доступа. Существует два подрежима, базовый набор услуг (BSS) и расширенный набор услуг (ESS).
- Беспроводная топология BSS состоит из основной области обслуживания (BSA) и расширенной области обслуживания (ESA).

Резюме (прод.)

- Беспроводные точки доступа можно настроить с помощью интерфейса командной строки (CLI) или, что более распространено, посредством графического пользовательского интерфейса через браузер.
- Основной подход к внедрению беспроводной сети (как и к базовой организации любой сети) заключается в поэтапной настройке и тестировании.
- В настоящее время доступно множество форм-факторов для внедрения беспроводного доступа на портативных компьютерах.
  - Wireless Zero Configuration
  - Cisco Compatible Extensions
  - Cisco Secure Services Client
- Устранение неполадок выполняется путем разделения среды на проводную и беспроводную сети.
- Скорости передачи данных WLAN зависят от стандартов, расположения точек доступа и расстояния.

Резюме модуля

В этом разделе приводится резюме вопросов, рассмотренных в модуле.



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 Каково наиболее заметное преимущество от внедрения беспроводного доступа? (Источник: изучение беспроводной сети)

А) снижение расходов
Б) повышенная мобильность
В) повышенная производительность
Г) улучшенная безопасность

В2 Какой метод используется в беспроводных ЛВС для управления передачей? (Источник: изучение беспроводной сети)

А) CSMA/CA (множественный доступ с контролем несущей и предотвращением коллизий)
Б) CSMA/CA (множественный доступ с контролем несущей и обнаружением коллизий)
В) CSMA/CR (множественный доступ с контролем несущей и отклонением коллизий)
Г) CSMA/CW (множественный доступ с контролем несущей и оценкой коллизий)

В3 Сопоставьте каждый фактор, влияющий на передачу радиоволн, соответствующему описанию. (Источник: изучение беспроводной сети)

_____ 1. возникает, когда радиоволны отражаются от металлических или стеклянных поверхностей

_____ 2. возникает, когда радиоволны задерживаются стенами

_____ 3. возникает, когда радиоволны попадают на неровную поверхность и отражаются в разных направлениях

А) поглощение
Б) отражение
В) рассеивание

В4 Какие органы регулирования контролируют стандарт 801.11, определяющий беспроводные локальные сети? (Источник: изучение беспроводной сети)

А) Wi-Fi Alliance
Б) IEEE
В) EMA
Г) WISC

В5 Какая организация предлагает сертификацию совместимости продуктов 802.11 различных поставщиков? (Источник: изучение беспроводной сети)

А) Wi-Fi
Б) IEEE
В) EMA
Г) WISC

В6 Какие три нелицензируемых диапазона используются в беспроводных локальных сетях? (Выберите три варианта.) (Источник: изучение беспроводной сети)

А) Диапазон 2,4 МГц
Б) Диапазон 900 МГц
В) Диапазон 2,4 ГГц
Г) Диапазон 5 ГГц
Д) Диапазон 900 ГГц

В7 Какие два из стандартов 802.11 обладают самой наибольшей скоростью передачи данных? (Выберите два варианта.) (Источник: изучение беспроводной сети)

А) 802.11
Б) 802,11a
В) 802.11b
Г) 802.11d
Д) 802.11g

В8 В каком стандарте 802.11 для передачи используется диапазон 5 ГГц? (Источник: изучение беспроводной сети)

А) 802.11
Б) 802,11a
В) 802.11b
Г) 802.11d
Д) 802.11g

В9 Какое утверждение о Wi-Fi Alliance является верным? (Источник: изучение беспроводной сети)

А) Это глобальная организация по стандартам, которая контролирует совместимость продуктов беспроводного доступа.
Б) Она работает только в США и обеспечивает совместимость продуктов беспроводного доступа.
В) Глобальная некоммерческая отраслевая ассоциация, деятельность которой направлена на поощрение развития и принятия беспроводных локальных сетей.
Г) Это глобальная некоммерческая отраслевая ассоциация, деятельность которой направлена на поощрение установки беспроводных локальных сетей в торговых павильонах.

В10 Что такое «вредоносная точка доступа»? (Источник: общие сведения о безопасности беспроводных ЛВС)

А) точка доступа с открытым ключом WEP
Б) точка доступа, рассылающая свой SSID в широковещательной рассылке
В) небезопасная точка доступа, размещенная в беспроводной локальной сети
Г) точка доступа, в которой произошел сбой оборудования, вызывавший безостановочную широковещательную рассылку ее SSID

В11 Какие три действия следует выполнить для защиты беспроводной локальной сети? (Выберите три варианта.) (Источник: общие сведения о безопасности беспроводных ЛВС)

А) внедрить шифрование для секретности и конфиденциальности
Б) внедрить аутентификацию, чтобы обеспечить доступ к сети через доверенные точки доступа только уполномоченным клиентам и пользователям
В) внедрить средства управления мощностью передачи, чтобы ограничить область покрытия точки доступа в границах собственности организации
Г) внедрить защиту от угроз безопасности и доступности с помощью систем обнаружения и предотвращения вторжений для беспроводных локальных сетей

В12 Какой стандарт предлагает самый высокий уровень безопасности беспроводных локальных сетей? (Источник: общие сведения о безопасности беспроводных ЛВС)

А) EAP
Б) WEP
В) WPA
Г) 802.11i/WPA2

В13 Какие факторы определяют точку доступа, к которой будет привязываться клиент? (Источник: общие сведения о безопасности беспроводных ЛВС)

А) точка доступа с минимальным SSID
Б) точка доступа с максимальным SSID
В) точка доступа, SSID которой получен первым
Г) точка доступа с самым мощным сигналом

В14 Как выполняется аутентификация клиента при использовании 802.1X? (Источник: общие сведения о безопасности беспроводных ЛВС)

А) Аутентификация клиента выполняется по локальной базе данных, расположенной в точке доступа.
Б) Весь сетевой трафик пересылается от точки доступа к серверу, где он проходит аутентификацию или блокируется.
В) Точка доступа инкапсулирует трафик 802.1X к серверу аутентификации и пересылается его серверу.
Г) Клиент инкапсулирует трафик аутентификации 802.1X перед отправкой точке доступа. В результате точка доступа пересылает его серверу.

В15 Какое утверждение о сравнении WPA и WPA2 является верным? (Источник: общие сведения о безопасности беспроводных ЛВС)

А) В WPA используются предварительные общие ключи, а в WPA 2 – PSK.
Б) В WPA используются аутентификация EAP, а в WPA 2 – 802.11X.
В) В WPA используются персональный режим, а в WPA 2 – корпоративный.
Г) В WPA используется шифрование TKIP/MIC, а в WPA 2 – шифрование AES-CCMP.

В16 Сопоставьте каждую топологию 802.11 с ее описанием. (Источник: внедрение беспроводной локальной сети)

_____ 1. Мобильные клиенты подключаются напрямую без промежуточной точки доступа.

_____ 2. Устройства связи используют одну точку доступа для подключения друг к другу и к ресурсам проводной сети.

_____ 3. Беспроводная топология представляет собой два или несколько наборов услуг, связанных системой распределения или чаще проводной инфраструктурой.

А) Режим Ad hoc
Б) Базовый набор услуг (BSS)
В) Расширенный набор служб (ESS)

В17 Что такое физическая зона покрытия РЧ точки доступа? (Источник: внедрение беспроводной локальной сети)

А) зона обслуживания РЧ
Б) основная зона обслуживания
В) зона обслуживания «ad hoc»
Г) расширенная зона обслуживания

В18 Какое перекрытие рекомендуется при внедрении расширенных областей обслуживания? (Источник: внедрение беспроводной локальной сети)

А) 5 – 10%
Б) 10 – 15%
В) 15 – 20%
Г) 25 – 30%

В19 Что позволяет клиенту поддерживать связь во время движения? (Источник: внедрение беспроводной локальной сети)

А) способность к переключению скорости передачи данных
Б) способность к изменению уровней передачи
В) способность к сопоставлению уровня передачи к уровню приема
Г) способность к коррекции ошибок при изменениях уровня сигнала

В20 Какие три из перечисленных ниже вариантов являются основными параметрами точки беспроводного доступа? (Выберите три варианта.) (Источник: внедрение беспроводной локальной сети)

А) SSID
Б) аутентификация
В) скорости обмена данными
Г) выбор диапазона передачи
Д) РЧ-канал с возможностью указания мощности

В21 Когда следует использовать WEP при внедрении беспроводной локальной сети? (Источник: внедрение беспроводной локальной сети)

А) только если доступен AAA-сервер
Б) когда требуется повышенная безопасность, предлагаемая WEP
В) когда планируется использовать аутентификацию 802.11x
Г) только если оборудование не поддерживает WPA

В22 Сопоставьте каждый беспроводной клиент его описанию. (Источник: внедрение беспроводной локальной сети)

_____ 1. полнофункциональный клиент с поддержкой как проводного, так и беспроводного доступа

_____ 2. базовый клиент поддержки беспроводного доступа в операционных системах Windows

_____ 3. более совершенные функции беспроводного клиента, превосходящие возможности встроенных клиентов ОС

А) WZC
Б) Cisco Compatible Extensions
В) Cisco Secure Services Client

Ответы на вопросы для самопроверки по модулю

B1	А
B2	А
B3	1 = Б, 2 = А, 3 = В
B4	Б
B5	А
B6	Б, В, Г
B7	Б, Д
B8	Б
B9	В
B10	В
B11	А, Б, Г
B12	Г
B13	Г
B14	В
B15	Г
B16	1 = А, 2 = Б, 3 = В
B17	Б
B18	Б
B19	А
B20	А, Б, Д
B21	Г
B22	1 = В, 2 = А, 3 =Б

