ICND1

Interconnecting Cisco Networking Devices Part 1

Том 2

Версия 1.0

Руководство для студента

Номер текста по каталогу: 97-2568-0–

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 2

Модуль 4

Соединения локальных сетей

Обзор

Помимо соединения нескольких устройств в сети можно соединять сами сети. По сути, Интернет – это объединение огромного количества связанных между собой сетей. Соединенные сети – это распространенная коммуникационная инфраструктура в крупных организациях. Соединение сетей с различными устройствами, архитектурами и протоколами требует более сложных компонентов, чем простые локальные сети. В более сложной сетевой среде используются маршрутизаторы, а передачей данных управляет стек протоколов TCP/IP. В этом модуле описаны функции маршрутизаторов при соединении сетей и используемые ими методы передачи данных между сетями с использованием TCP/IP.

Задачи модуля

По окончании этого модуля вы сможете соединять несколько сетей с помощью шлюза по умолчанию. Это значит, что вы сможете выполнять следующие задачи:

- описывать функцию маршрутизации в сетевой модели;
- преобразовывать десятичное число в двоичное и двоичное число в десятичное;
- описывать принципы формирования сетевых адресов в IP-сетях;
- запускать маршрутизатор и пользоваться интерфейсом командной строки для настройки и мониторинга маршрутизатора;
- выполнять базовую настройку маршрутизатора Cisco;
- описывать прохождение пакетов с одного хоста на другой через маршрутизатор;
- внедрять базовые средства безопасности маршрутизатора;
- описывать основные функции Cisco SDM;
- использовать Cisco SDM для включения DHCP-сервера на маршрутизаторе;
- получать удаленный доступ к маршрутизатору с помощью протоколов Telnet и SSH.

Занятие 1

Изучение функций маршрутизации

Обзор

Маршрутизация – это процесс пересылки пакетов данных между сетями или подсетями с помощью устройства 3-го уровня (маршрутизатора или шлюза). Процесс маршрутизации использует таблицы, протоколы и алгоритмы маршрутизации, чтобы определить наиболее эффективный путь для пересылки IP-пакета. Маршрутизаторы значительно увеличивают масштабируемость сетей, ограничивая широковещательные домены и домены коллизий второго уровня. Понимание того, как работают маршрутизаторы позволяет лучше понять принципы соединения сетей и передачи данных по ним. В этом занятии рассматривается принцип работы маршрутизации.

Задачи

По окончании этого занятия вы сможете описывать работу маршрутизаторов Cisco при соединении сетей. Это значит, что вы сможете выполнять следующие задачи:

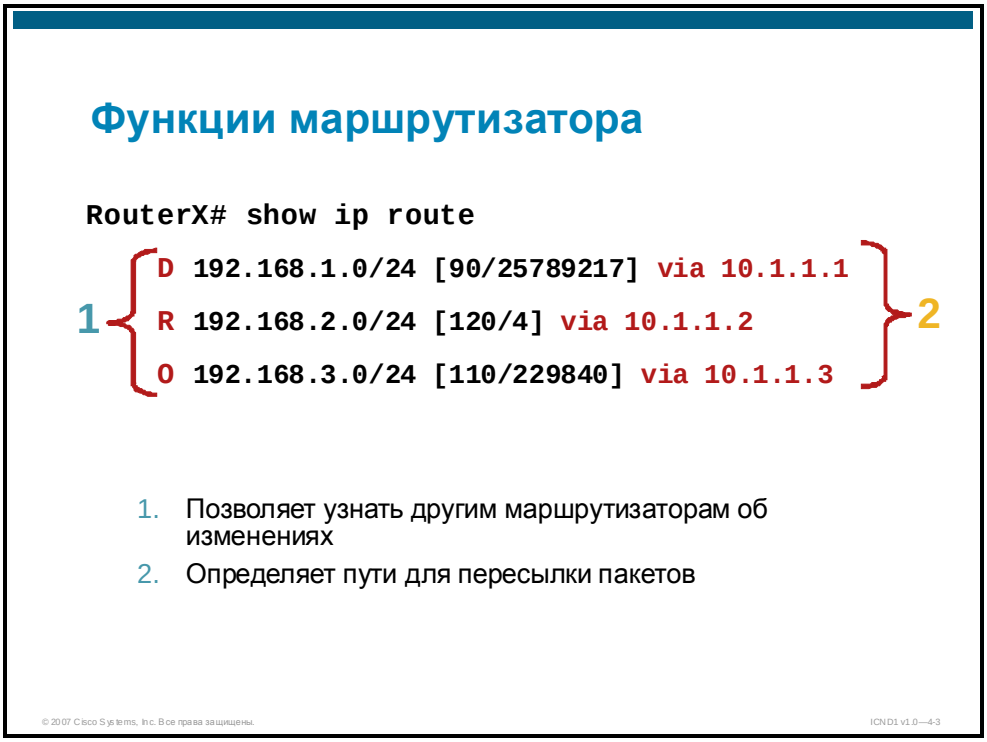
- описывать физические характеристики маршрутизатора и его функции в процессе доставки IP-пакета;
- описывать метод, используемый при определении оптимального пути для пересылки IP-пакетов между сетями;
- перечислять характеристики таблиц маршрутизации и их функции при определении пути;
- сопоставлять характеристики статического маршрута, динамического маршрута, маршрута непосредственного подключения и маршрута по умолчанию с соответствующим типом маршрута;
- перечислять характеристики протоколов маршрутизации, которые автоматически создают и занимаются обработкой таблиц маршрутизации.

Маршрутизаторы

Маршрутизатор или шлюз – это сетевое устройство, которое определяет оптимальный путь для передачи данных из одной сети в другую. Определенные характеристики являются общими для всех маршрутизаторов. В этом разделе описываются характеристики маршрутизаторов.

Маршрутизаторы являются важными компонентами крупных сетей, функционирующих на основе стека протоколов TCP/IP, так как они позволяют обеспечить протяженность сетей на обширные географические расстояния. Следующие характеристики относятся ко всем маршрутизаторам:

- Маршрутизаторы обладают компонентами, которыми также обладают компьютеры и коммутаторы:
  - ЦП,
  - системная плата,
  - ОЗУ,
  - ПЗУ.
- В маршрутизаторах установлены сетевые адаптеры, которым присваиваются IP-адреса.
- Маршрутизаторы могут включать порты следующих типов:
  - **Консольный порт.** Маршрутизатор использует консольный порт для подключения терминала, который применяется для управления, настройки и контроля. У некоторых маршрутизаторов может не быть консольного порта.
  - **Сетевой порт.** На маршрутизаторе присутствуют несколько сетевых портов, включая порты локальных (LAN) и глобальных (WAN) сетей различных типов.

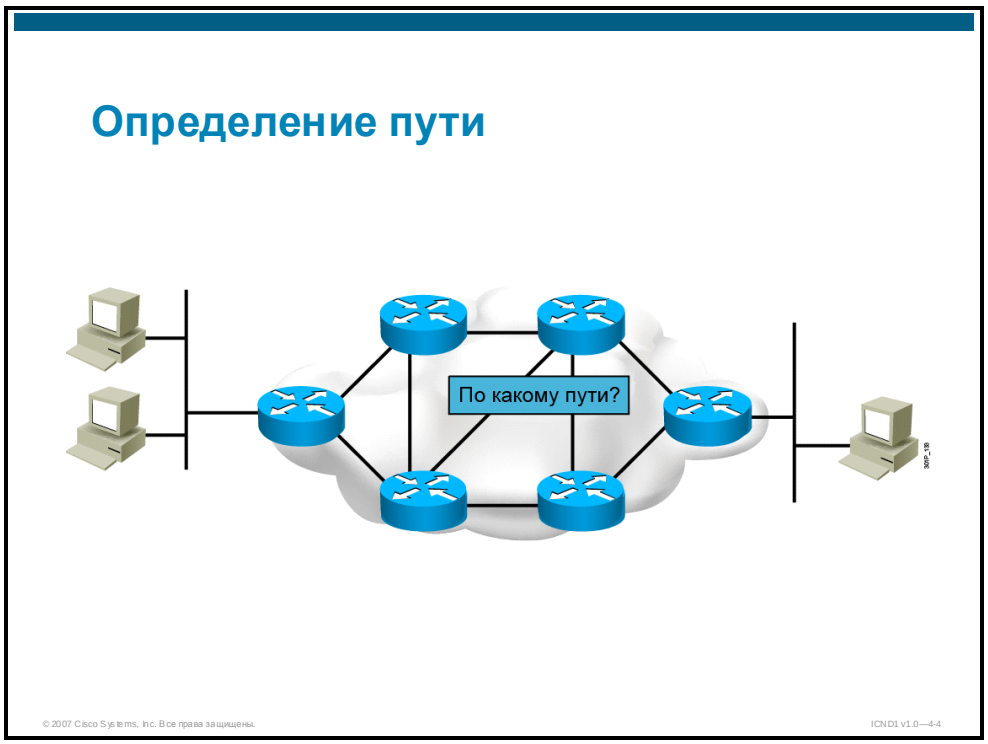


Две основные функции маршрутизатора:

- **Определение пути.** Маршрутизаторы должны вести свои таблицы маршрутизации и предоставлять другим маршрутизаторам информацию об изменениях в сети. С помощью протокола маршрутизации информация о сети из таблицы маршрутизации одного маршрутизатора передается другим маршрутизаторам. Можно статически заполнять таблицы маршрутизации, но статическое заполнение не масштабируется и приводит к проблемам из-за проектирования или в результате изменения топологии сети или в случае отказа на участке сети.
- **Пересылка пакетов.** Маршрутизаторы используют таблицу маршрутизации, чтобы определить место назначения пересылки пакетов. Маршрутизаторы пересылают пакеты через сетевой интерфейс к сети назначения, которая определяется по IP-адресу назначения в пакете.

Определение пути

На этапе определения пути при передаче данных через сеть маршрутизаторы анализируют доступные пути к удаленным получателям. В этом разделе описываются методы определения наиболее эффективного пути для пересылки пакетов.



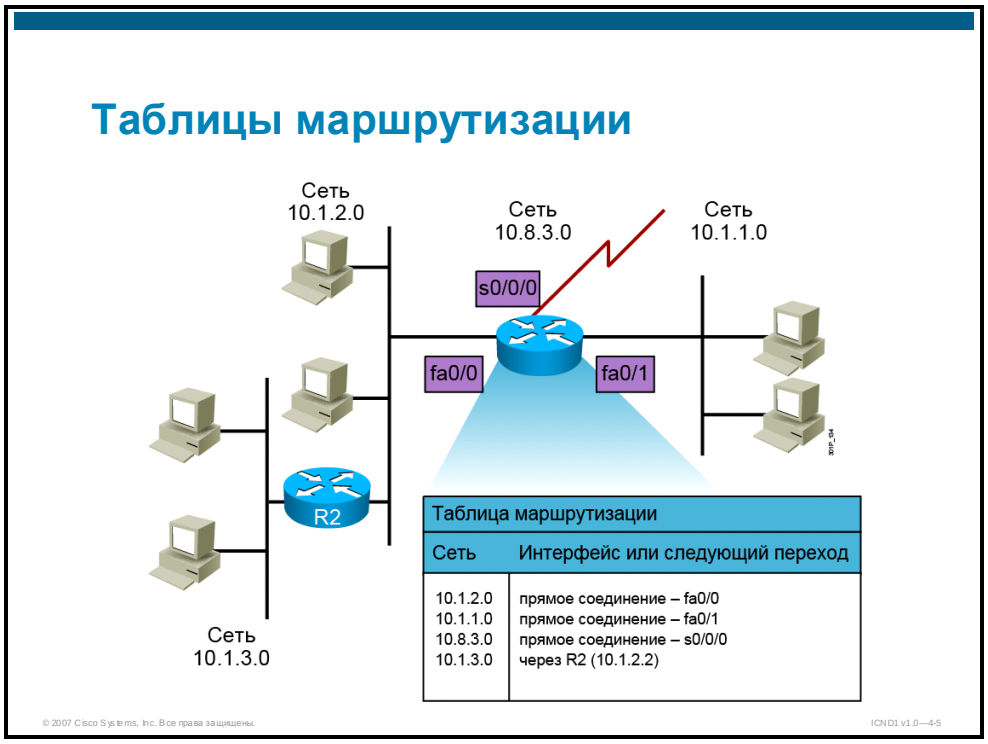
Для выбора оптимального пути к удаленному месту назначения могут использоваться три следующих типа записей в таблицах маршрутизации:

- **Статическая маршрутизация.** Этот тип маршрутизации требует ручного ввода информации о маршруте в таблицу маршрутизацию.
- **Динамическая маршрутизация.** При использовании этого типа маршрутизации таблица маршрутизации создается динамически, на основе данных маршрутизации, полученных по протоколам маршрутизации.
- **Маршрутизация по умолчанию.** Этот тип маршрутизации исключает необходимость установки явно заданного маршрута к каждой сети. Запись маршрута по умолчанию может настраиваться статически или приниматься по протоколу динамической маршрутизации.

В таблице маршрутизации сохраняется только одна запись для каждой сети. При наличии нескольких источников информации о пути к определенному месту назначения, процесс маршрутизации должен иметь возможность выбора источника информации для использования в таблице маршрутизации. Несколько источников появляются при использовании нескольких протоколов динамической маршрутизации, а также статических маршрутов и маршрутов по умолчанию. Протоколы маршрутизации используют различные метрики для определения расстояния и приемлемости пути к сети назначения. Поскольку невозможно непосредственно выбрать нужные данные на основе информации, предоставляемой различными протоколами маршрутизации, процесс маршрутизации Cisco присваивает определенный вес, называемый административным расстоянием, каждому источнику информации. Самому лучшему и надежному источнику присваивается наименьшее значение.

Таблицы маршрутизации

При определении пути процесс маршрутизации создает таблицу маршрутизации, в которой определяются известные сети и способы их достижения. В этом разделе рассматривается роль таблицы маршрутизации в процессе маршрутизации.



Метрики маршрутизации зависят от используемого протокола маршрутизации. На рисунке показано, как маршрутизаторы ведут таблицу данных, на основе которой принимаются решения о пересылке пакетов.

Данные таблицы маршрутизации

Таблица маршрутизации содержит упорядоченный список «известных» сетевых адресов, то есть тех адресов, которые были динамически получены процессом маршрутизации или статически заданы для непосредственно подключенных сетей. Таблицы маршрутизации также содержат данные о местах назначения и связях со следующими переходами. С помощью этих связей маршрутизатор узнает о том, можно ли достичь определенного пункта назначения напрямую или только через другой маршрутизатор, называемый маршрутизатором следующего перехода. Когда маршрутизатор получает входящий пакет, он использует адрес назначения для поиска оптимального пути в таблице маршрутизации. Если запись не находится, маршрутизатор отклоняет этот пакет после отправки сообщения ICMP (Internet Control Message Protocol) к адресу источника пакета.

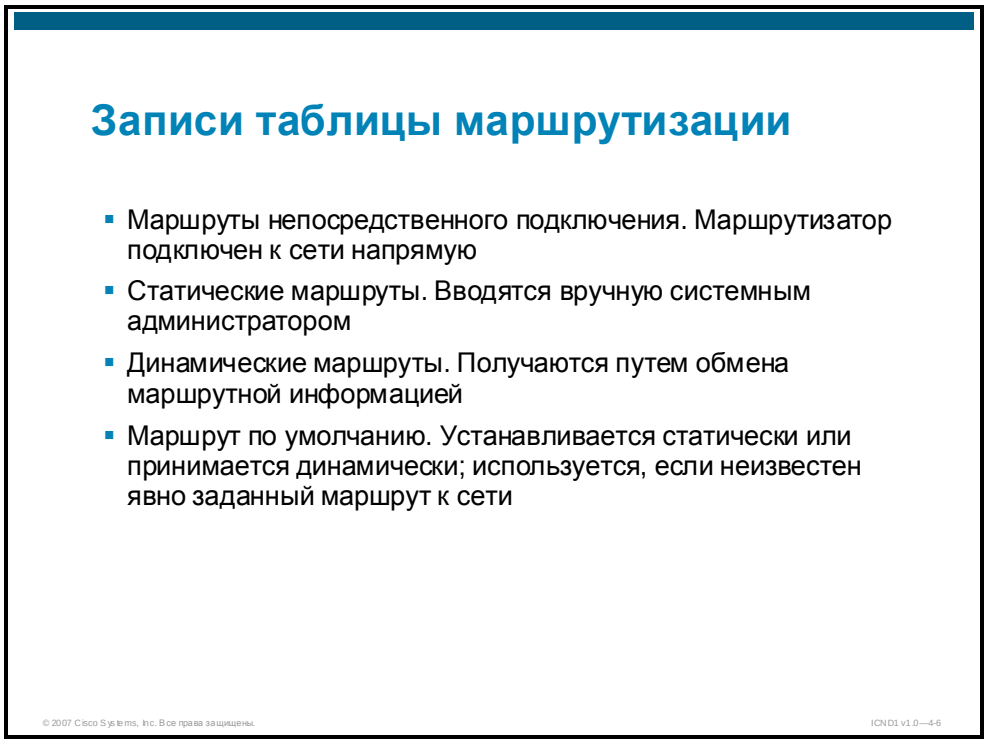
На рисунке в середине таблицы маршрутизации данного маршрутизатора показано, что при получении пакета с адресом назначения из сети 10.1.3.0 этот пакет должен пересылаться маршрутизатору R2.

Сообщения об обновлении маршрутизации

Маршрутизаторы обмениваются информацией друг с другом и ведут свои таблицы маршрутизации путем передачи сообщений об обновлении маршрутизации. В зависимости от протокола маршрутизации сообщения об обновлении маршрутизации могут отправляться периодически или только при изменении топологии сети. В сообщениях об обновлении маршрутизации приводится информация о сетях назначения, которых может достичь маршрутизатор, и метрика маршрутизации, характеризующая достижимость каждого места назначения. Анализируя обновления маршрутизации, полученные от соседних маршрутизаторов, маршрутизатор может создавать и вести таблицу маршрутизации.

Статические, динамические и маршруты непосредственного подключения, а также маршруты по умолчанию

Маршрутизаторы могут получать сведения о других сетях с помощью статических, динамических, маршрутов непосредственного подключения, а также маршрутов по умолчанию. В этом разделе описываются все эти типы маршрутов.



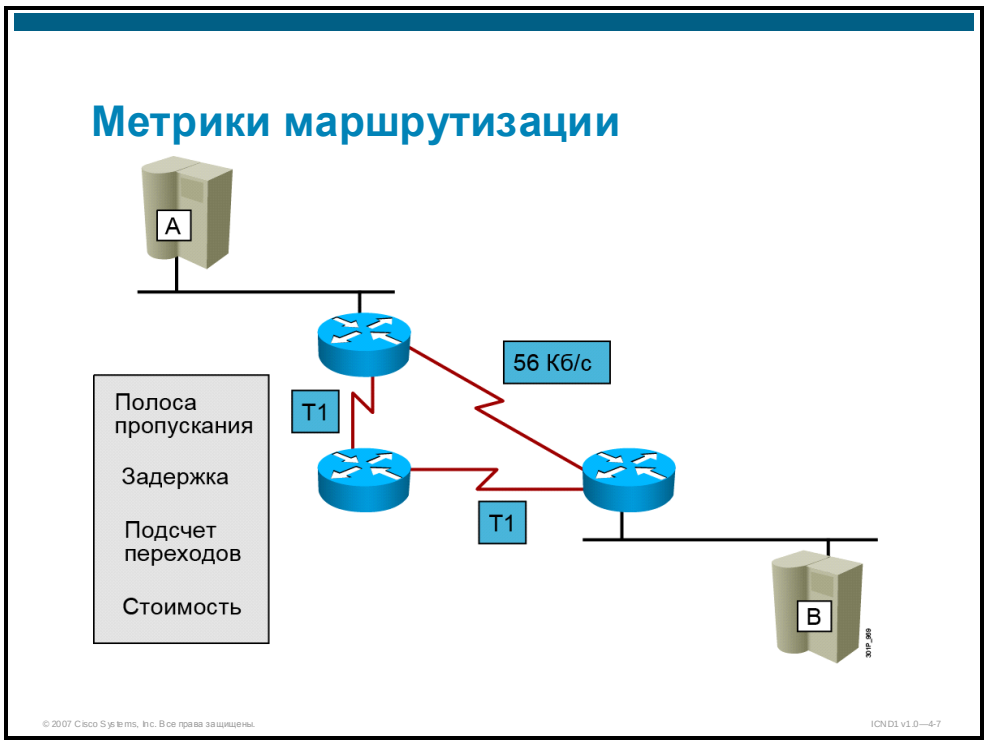
Для заполнения таблиц маршрутизации могут использоваться следующие методы:

- **Маршруты непосредственно подключенных сетей.** Эти маршруты создаются на основе информации интерфейсов маршрутизатора, которые непосредственно подключены к сегментам сети. Этот метод заполнения таблицы маршрутизации является самым надежным. В случае сбоя или административного отключения интерфейса маршрут к этой сети удаляется из таблицы маршрутизации. Административное расстояние таких маршрутов равно «0», поэтому этот маршрут имеет приоритет перед всеми остальными маршрутами к этой сети назначения, поскольку маршрут с наименьшим административным расстоянием является оптимальным и самым надежным.
- **Статические маршруты.** Статические маршруты вводятся системным администратором вручную непосредственно в конфигурацию маршрутизатора. Административное расстояние по умолчанию для статического маршрута равно «1»; поэтому статические маршруты включаются в таблицу маршрутизации, если нет прямого соединения с данной сетью. Статические маршруты эффективны для сетей небольшого размера, которые редко изменяются.

- **Динамические маршруты.** Маршрутизаторы обучаются динамическим маршрутам. Они могут изменяться в соответствии с изменениями в сети. Однако между изменением сети и получением сообщений об этом изменении всеми маршрутизаторами всегда существует задержка. Эта задержка во времени согласования данных маршрутизатора с изменениями сети называется временем сходимости. Чем меньше время сходимости, тем лучше. Для различных протоколов маршрутизации это время отличается. Для крупных сетей необходимо использовать динамическую маршрутизацию, так как они содержат множество адресов и постоянно меняются, и если на эти изменения немедленно не отреагировать, возможны перерывы связи.
- **Маршрут по умолчанию.** Маршрут по умолчанию – необязательный маршрут, используемый в случае, если в таблице маршрутизации не найден явно заданный маршрут к пункту назначения. Маршрут по умолчанию может вводиться вручную или приниматься по протоколу динамической маршрутизации.

Протоколы динамической маршрутизации

Существует несколько протоколов маршрутизации, в которых используются собственные правила и метрики для автоматического создания и обновления таблиц маршрутизации. В этом разделе описаны метрики и методы маршрутизации, используемые протоколами маршрутизации.



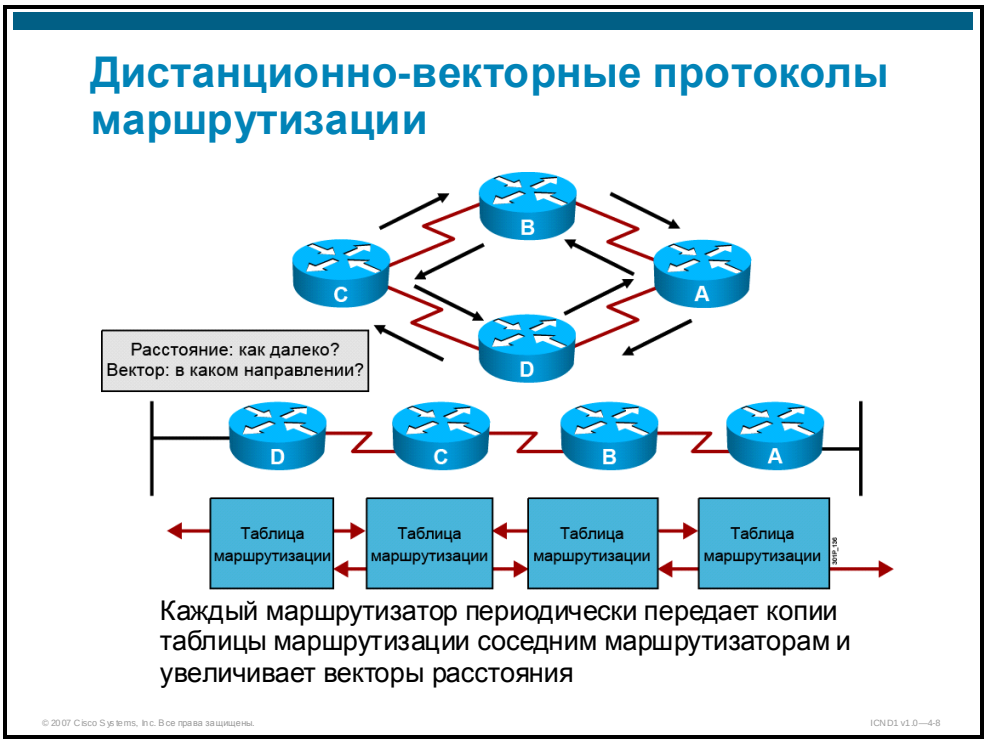
Метрики маршрутизации

Когда протокол маршрутизации обновляет таблицу маршрутизации, его основной задачей является выбор наилучшего маршрута для включения в таблицу. Алгоритм маршрутизации генерирует численное значение, называемое метрикой, для каждого маршрута в сети. Сложный протокол маршрутизации может выбирать маршрут на основе нескольких метрик, объединяя их в одну метрику. Обычно чем меньше значение метрики, тем более оптимальным является путь.

Метрики могут основываться на одной или нескольких характеристиках пути. В протоколах маршрутизации наиболее часто используются следующие метрики:

- **Полоса пропускания.** Пропускная способность канала (соединения между двумя сетевыми устройствами)
- **Задержка.** Интервал времени, который требуется для перемещения пакета по всем каналам между источником и получателем, зависит от полосы пропускания промежуточных каналов, очередей портов на каждом маршрутизаторе, перегрузки сети и физического расстояния.
- **Число переходов.** Количество маршрутизаторов на пути к месту назначения пакета (на следующем рисунке число переходов от узла A до узла B будет равно 2 для каждого пути).

- **Стоимость.** Произвольное значение, назначаемое сетевым администратором, которое обычно основано на полосе пропускания, предпочтениях администратора или других показателях.



Методы маршрутизации

Во многих протоколах маршрутизации используется один из следующих методов маршрутизации:

- **Маршрутизация на базе векторов расстояния.** При использовании маршрутизации на базе векторов расстояния маршрутизатор не должен знать весь путь к каждому сегменту сети, ему необходимо знать только направление или вектор для отправки пакета. В методе маршрутизации на базеG векторов расстояния определяется направление (вектор) и расстояние (число переходов) до любой сети в интерсети. Алгоритмы векторов расстояния периодически (например, каждые 30 секунд) отправляют все данные таблиц маршрутизации или их часть смежным соседним маршрутизаторам. Маршрутизатор, на котором выполняется дистанционно-векторный протокол маршрутизации периодически отправляет обновления, даже при отсутствии изменений в сети. Маршрутизатор может проверить все известные маршруты и внести изменения в свою локальную таблицу маршрутизации в соответствии с обновленной информацией, полученной от соседнего маршрутизатора. Этот процесс также называется «routing by rumor» (маршрутизацией по слухам), поскольку представление маршрутизатора о топологии сети основано на таблице маршрутизации соседнего маршрутизатора.

  В качестве примера дистанционно- векторного можно привести широко распространенный протокол RIP (Routing Information Protocol), в котором в качестве метрики маршрутизации используется количество переходов.

- **Маршрутизация на базе состояния канала.** В маршрутизации на базе состояния канала каждый маршрутизатор пытается создать собственную внутреннюю схему топологии сети. Как только каждый из маршрутизаторов становится активным, он отправляет сообщения со списком всех непосредственно подключенных маршрутизаторов, и данными о том, активен ли канал с каждым маршрутизатором. Другие маршрутизаторы используют эту информацию для создания схемы сети, а затем применяют эту схему для выбора оптимального пути к месту назначения. Протоколы маршрутизации на базе состояния канала быстро реагируют на изменения сети, так как триггерно отправляют обновления, в момент изменения сети, и периодические обновления (обновления состояния канала) через более продолжительные интервалы времени, например через 30 минут.

  При изменении состояния канала устройство, обнаружившее это изменение, создает сообщение об обновлении этого канала (маршрута), и это сообщение передается всем маршрутизаторам (на которых выполняется этот протокол маршрутизации). Каждый маршрутизатор получает копию сообщения об обновлении, обновляет свои таблицы маршрутизации и пересылает сообщение об обновлении всем соседним маршрутизаторам. Эта лавинная рассылка сообщений об обновлении обеспечивает обновление баз данных всех маршрутизаторов для создания измененной таблицы маршрутизации, в которой отражена новая топология.

  В качестве примеров протоколов маршрутизации на базе состояния канала можно привести OSPF (Open Shortest Path First) и IS-IS (Intermediate System-to-Intermediate System).

Примечание Компанией Cisco разработан протокол EIGRP (Enhanced Interior Gateway Routing Protocol), объединяющий лучшие характеристики протоколов маршрутизации на базе векторов расстояния и состояния канала.

Резюме

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

Резюме

- Маршрутизаторы содержат компоненты, которые также являются компонентами компьютеров и коммутаторов, такие как ЦП, системная плата, ОЗУ и ПЗУ.
- В процессе доставки IP-пакетов маршрутизаторы выполняют две основных функции: ведение таблиц маршрутизации и определение оптимального пути для пересылки пакетов.
- Маршрутизаторы определяют оптимальный путь для пересылки IP-пакетов между сетями. Маршрутизаторы могут использовать различные типы маршрутов к сетям назначения, включая статические и динамические маршруты, а также маршруты по умолчанию.
- Таблицы маршрутизации содержат упорядоченный список оптимальных путей к известным сетям и информацию о получателях, связях со следующими переходами и метриках маршрутизации.
- Алгоритмы маршрутизации обрабатывают полученные обновления и устанавливают в таблицу маршрутизации оптимальные маршруты.

Резюме (прод.)

- Обычно используются следующие метрики маршрутизации: полоса пропускания, задержка, число переходов и стоимость.
- Дистанционно-векторные протоколы маршрутизации автоматически создают и обновляют таблицы маршрутизации, отправляя всю таблицу маршрутизации или ее часть соседям. В методе маршрутизации на базе векторов расстояния определяется направление (вектор) и расстояние до любой сети в интерсети.
- Протоколы маршрутизации на базе состояния канала автоматически создают и обновляют таблицы маршрутизации, применяя алгоритмы к базам данных состояния каналов для определения оптимального пути, и рассылают информацию о своих каналах всем маршрутизаторам в сети.
- Компанией Cisco разработан протокол EIGRP, объединяющий лучшие характеристики протоколов маршрутизации на базе векторов расстояния и состояния канала.

Занятие 2

Общие сведения о двоичной системе счисления

Обзор

Все функции компьютера используют систему триггеров, которые могут находиться в одном из двух положений: включенном или выключенном. Эта система называется двоичной системой, где положение «выкл.» представлено цифрой 0, а положение «вкл.» – цифрой 1. Двоичное число может состоять только из 0 и 1.

Сетевые адреса устройств также используют двоичную систему для задания местоположения в сети. IP-адреса основываются на точечно-десятичном представлении двоичного числа. Чтобы понять принципы построения сетей, необходимы базовые знания математических свойств двоичной системы счисления. В этом занятии рассматриваются математические соотношения, используемые в двоичной системе счисления, а также преобразование десятичного числа (основание 10) в двоичное (основание 2) и наоборот.

Задачи

По окончании этого занятия вы сможете преобразовать десятичные числа в двоичные и двоичные числа в десятичные. Это значит, что вы сможете выполнять следующие задачи:

- описывать системы двоичного и десятичного счисления;
- описывать процесс «возведения 2 в степень»;
- преобразовывать десятичное число в двоичное;
- преобразовывать двоичное число в десятичное.

Десятичная и двоичная системы счисления

Десятичная система счисления (основание 10) используется в обычных математических операциях, а двоичная система счисления (основание 2) является основой компьютерных вычислений. В этом разделе рассматриваются десятичная и двоичная системы счисления.

Десятичные и двоичные числа

- Для представления десятичных чисел используются цифры от 0 до 9.
- Двоичные числа записываются при помощи последовательности двух цифр – 0 и 1.

Десятичное	Двоичное
0	0
1	1
2	10
3	11
4	100
5	101
6	110
7	111
8	1000
9	1001

Десятичное	Двоичное
10	1010
11	1011
12	1100
13	1101
14	1110
15	1111
16	10000
17	10001
18	10010
19	10011

В десятичной системе счисления используются цифры 0, 1, 2, 3, 4, 5, 6, 7, 8 и 9. Для представления чисел больше 9, используется число 10, затем значения увеличиваются на единицу до 99. Затем используется число 100 и значения последовательно увеличиваются, причем в каждой колонке слева значение увеличивается на +1.

В двоичной системе счисления используются только цифры 0 и 1. Поэтому первая цифра 0, а за ней следует 1. Для представления числа больше 1 в двоичной системе используется значение 10, затем 11. Затем используются следующие значения: 100, 101, 110, 111, затем 1000 и т. д. На рисунке показаны эквиваленты десятичных чисел от 0 до 19 в двоичной системе счисления.

Младший и старший разряды

Большинство людей привыкли к десятичной системе счисления. В любой системе счисления важна позиция цифры в числе, которая отражает его значение. Число 10 представлено 1 в позиции десятков и 0 в позиции единиц. Число 100 представлено 1 в позиции сотен, 0 в позиции десятков и 0 в позиции единиц.

В двоичной системе крайняя справа цифра является младшим разрядом (LSB), а крайняя слева – старшим разрядом (MSB). Значимость любых цифр, находящихся между этими крайними цифрами, зависит от их близости к LSB или MSB.

Система преобразования двоичных чисел (основание 2)

Важно понять основы двоичной системы счисления, поскольку IP-адреса версии 4 (IPv4) включают 32 двоичных бита. Каждая цифра – это 1 бит. 32 бита разделены на 4 группы по 8 бит, называемые октетами. Для разделения октетов используется точка. (8 бит также называются байтом, однако в данном модуле группы из 8 бит будут называться октетами.)

Различные классы адресов основаны на границах октетов, поэтому студентам следует привыкнуть к таким группам. Кроме того, их удобнее использовать, так как 8-битные двоичные числа проще преобразовывать, чем 32-битные. При преобразовании двоичного представления IP-адреса октеты преобразуются последовательно, а не одновременно. Максимальное значение двоичного октета 11111111 соответствует десятичному числу 255.

Степени двойки

Чтобы уяснить принцип использования двоичных чисел в адресации, необходимо разобраться в математическом процессе преобразования десятичного числа в двоичное и обратно. В этом разделе рассматривается метод степеней двойки.

Батарейки калькулятора могут разрядиться, а таблицы – потеряться, но если известны математические принципы, для преобразования двоичных чисел в десятичные и обратно достаточно листка бумаги и карандаша. Существуют таблицы для упрощения процесса преобразования десятичных чисел в двоичные, в которых, например, указано, что 2^0 – это десятичная 1, 2^1 – это десятичная 2, 2^2 – это десятичная 4 и т.д. На рисунке показано формирование некоторых десятичных чисел.

Преобразование десятичного числа в двоичное

Для преобразования десятичных чисел в двоичные можно использовать специальную процедуру. В этом разделе описывается метод преобразования десятичных чисел в двоичные.

На рисунке показано простое преобразование десятичного числа 35 в двоичное. В строке степеней основания показаны различные степени двойки (2 * 2 = 4 * 2 = 8 и т.д.). Десятичное значение для определенной степени числа 2 приведено во второй строке, а двоичное значение – в третьей строке. В таблице приводится последовательность действий для определения двоичного числа. Обратите внимание, что 2 первых бита двоичного числа равны 0; они называются начальными нулями. На самом деле десятичное число 35 является шестиразрядным двоичным числом. Поскольку IP-адреса разделены на четыре группы октетов, для представления этого двоичного числа в виде октета добавлены нули слева от шестиразрядного числа.

В следующей таблице приведена последовательность действий для преобразования числа 35 в двоичный формат.

Процедура преобразования десятичного числа в двоичное

№	Действие
1.	Глядя на рисунок, определите, какая степень числа 2 меньше или равна 35. Сколько раз по 128 в числе 35? Нисколько, поэтому поставьте 0 в этот столбец.
2.	Сколько раз по 64 в числе 35? Нисколько, поэтому поставьте 0 в этот столбец.
3.	2^5 (32) меньше 35. Сколько раз по 32 в числе 35? Один. Поставьте 1 в этом столбце.
4.	Для определения остатка вычтите 32 из 35. Остаток равен 3.
5.	Проверьте, сколько раз по 16 (следующая в порядке убывания степень 2) в значении 3. Нисколько, поэтому поставьте 0 в данный столбец.
6.	Следующее значение равно 8. 8 больше 3, поэтому в этом столбце также поставьте 0.
7.	Следующее значение равно 4. 4 тоже больше 3, поэтому опять поставьте 0.
8.	Следующее значение 2. 2 меньше 3. Сколько раз по 2 в числе 3? Один. Поставьте 1 в этот столбец.
9.	Если из 3 вычесть 2, получится 1.
10.	Десятичное значение последнего бита равно 1, что соответствует остатку. Поэтому поставьте 1 в последний столбец. Двоичный эквивалент десятичного значения 35 – 100011.

Преобразование двоичного числа в десятичное

Как и в случае преобразования десятичного значения в двоичное, существует несколько способов преобразования двоичных чисел в десятичные. В этом разделе описан один из методов преобразования.

Преобразование двоичного числа в десятичное

Основание^Степень	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Значение разряда	128	64	32	16	8	4	2	1
Пример: двоичное число	1	0	1	1	1	0	0	1
Десятичное число – сумма: 185	128	0	32	16	8	0	0	1

1 0 1 1 1 0 0 1 = (128 * 1) + (64 * 0) + (32 * 1) + (16 * 1) + (8 * 1) + (4 * 0) + (2 * 0) + (1 * 1)
1 0 1 1 1 0 0 1 = 128 + 0 + 32 + 16 + 8 + 0 + 0 + 1
1 0 1 1 1 0 0 1 = 185

Для преобразования двоичных чисел в десятичные можно использовать позиционные значения, основанные на степенях двойки и определить столбцы с ненулевыми значениями, а затем суммировать эти значения для получения окончательного результата.

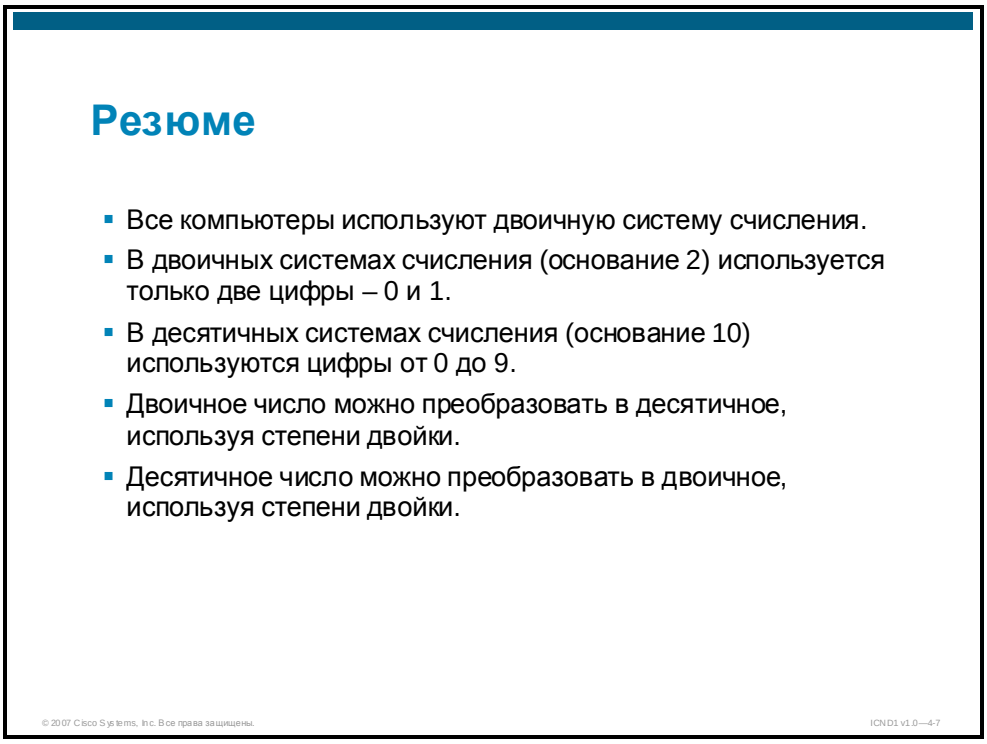
В следующей таблице приведена последовательность действий для преобразования числа 10111001 в десятичный формат.

Процедура преобразования двоичного числа в десятичное

№	Действие
1.	Определите значение разряда, соответствующее биту 1 в двоичном числе, в зависимости от его позиции. Например, на рисунке показано, что бит в столбце 2^7 равен 1, поэтому суммарное значение в десятичном формате равно 128.
2.	В столбце 2^6 (64) указано значение 0. Для расчета десятичного значения используется следующая формула 128 + 0 = 128.
3.	В столбце 2^5 (32) указано значение 1. Для расчета десятичного значения используется следующая формула 128 + 32 = 160.
4.	В столбце 2^4 (16) указано значение 0. Прибавив это значение к суммарному значению в десятичном формате, получим 160 + 16 = 176.
5.	В следующем столбце 2^3 указано значение 1, поэтому прибавляем 8 к суммарному значению в десятичном формате и получаем 176 + 8 = 184.
6.	В столбцах 2^2 и 2^1 указаны значения 0. Прибавляем нули к суммарному значению в десятичном формате: 184 + 0 + 0 = 184.
7.	И, наконец, в столбце 2^0 (1) установлена 1. Теперь прибавим 1 к 184 и получим 185. Десятичным эквивалентом двоичного значения 10111001 является значение 185.

Резюме

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



Занятие 3

Построение схемы сетевой адресации

Обзор

Подсети используются практически во всех (за исключением самых малых) сетевых средах для разбиения сети на более мелкие сегменты с собственными адресами. Для создания адресов подсетей заимствуется нескольких бит из хостовой части IP-адреса. В этом занятии описывается принцип работы и расчет подсетей.

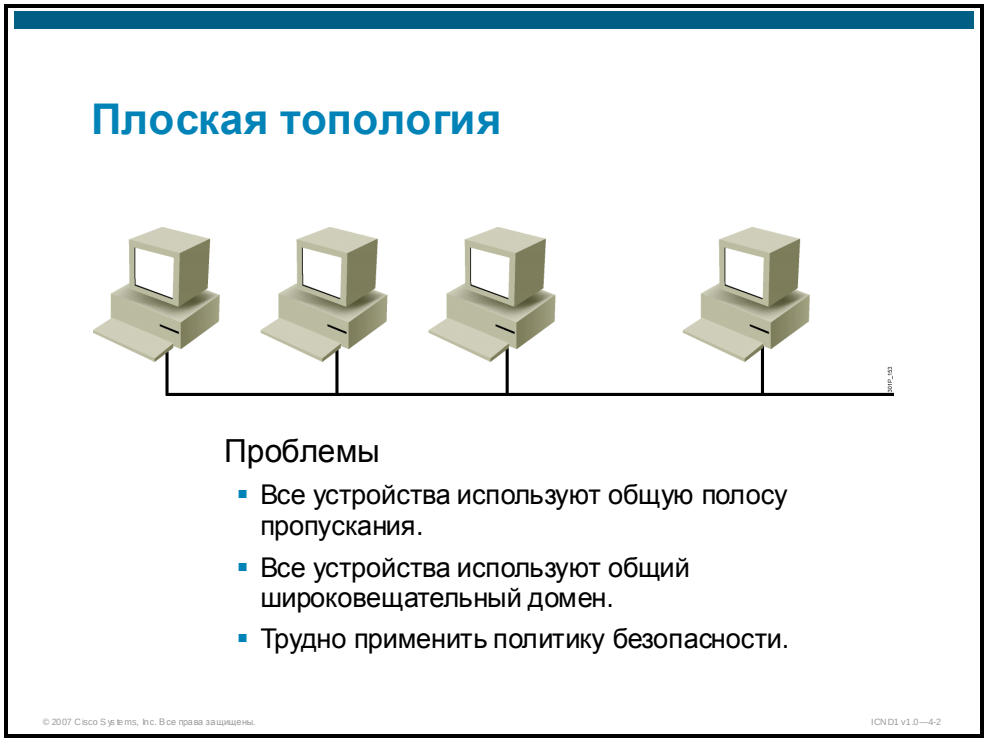
Задачи

По окончании этого занятия вы сможете описывать и рассчитывать адреса подсетей. Это значит, что вы сможете выполнять следующие задачи:

- определять назначение и функции подсети;
- описывать процесс расчета доступной подсети и адресов хостов;
- описывать использование масок подсетей конечными системами для обнаружения устройства назначения;
- описывать использование масок подсетей маршрутизаторами для маршрутизации пакета к месту назначения;
- описывать механизм работы масок подсетей;
- применять маски подсети к IP-адресам классов A, B и C.

Подсети

Сетевым администраторам часто приходится делить сети, особенно сети большого размера, на подсети для обеспечения гибкости адресации. В этом разделе описывается назначение и функции подсетей, а также схемы их адресации.



Сеть организации, занимающей трехэтажное здание, можно разделить на подсети по этажам, а затем по офисам. С точки зрения сети этажи можно рассматривать как подсети, а офисы как отдельные адреса хостов.

Подсеть сегментирует хосты внутри сети. Сети без подсетей имеют плоскую топологию. Для доставки пакетов в сети с плоской топологией используется короткая таблица маршрутизации и MAC-адреса второго уровня. Структура MAC-адресов неиерархическая. По мере расширения сети использование полосы пропускания сети становится все менее эффективным.

Плоская сеть имеет следующие недостатки:

- все устройства используют общую полосу пропускания;
- все устройства используют общий широковещательный домен второго уровня;
- из-за отсутствия границ между устройствами трудно применить политики безопасности.

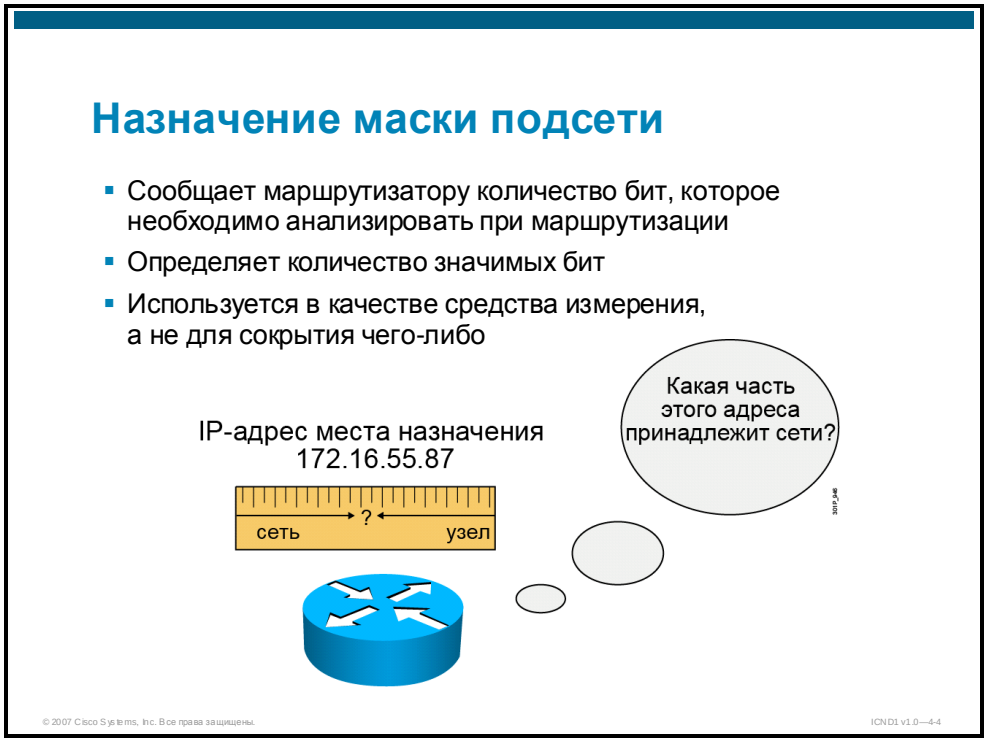
В сети Ethernet, соединяемой с помощью концентраторов, каждый хост в единой физической сети видит все пакеты в этой сети. В сети, соединенной коммутатором, хост видит все широковещательные пакеты. При интенсивном трафике может возникать множество коллизий, связанных с одновременной передачей данных несколькими устройствами. Устройство обнаруживает коллизию, останавливает передачу, а затем начинает ее снова через случайный интервал времени. Для пользователей этот процесс воспринимается как замедление работы сети. В таких случаях для разделения сетей на несколько подсетей можно использовать маршрутизаторы.

Использование подсетей обеспечивает следующие преимущества:

- небольшие сети проще организовывать в соответствии с географическими или функциональными потребностями, кроме того, ими легче управлять;
- уменьшается общий трафик сети, что позволяет повысить производительность;
- меры безопасности проще применять не на уровне всей сети, а на уровне соединений между подсетями.

Как показано на рисунке, в многосетевой среде каждая из подсетей может подключаться к сети Интернет через единственный маршрутизатор. В этом примере сеть разделена на несколько подсетей. Фактические подробности внутренней сетевой среды и способ ее деления на несколько подсетей несущественны для других IP-сетей.

Маска подсети определяет сетевую часть (префикс) IP-адреса. Сетевая часть IP-адреса определяет сеть, к которой подключен хост (то есть сетевой адрес). Она важна для эффективной маршрутизации.



Двухуровневые и трехуровневые адреса

Когда для определения адресов и классов адресов был разработан метод IPv4, казалось, что будет достаточно двухуровневого адреса (сеть и узел). С каждым классом адреса (A, B и C) связана маска по умолчанию, и поскольку эта маска определена заранее, ее не нужно настраивать в явном виде.

По мере увеличения количества подключенных к сети устройств стало ясно, что в этом методе сетевые адреса используются неэффективно. Для решения этой проблемы был разработан метод трехуровневой адресации, включающей подсети.

Адрес подсети содержит исходное классовое сетевое поле и поле подсети. Полный префикс сети, состоящий из сетевого поля и поля подсети, получил название расширенного сетевого префикса. Поле подсети и поле хоста образуются из исходной хостовой части классового адреса. Для создания адреса подсети можно «заимствовать» биты из исходной хостовой части адреса и использовать их в качестве поля подсети.

Однако для работы подсетей необходим метод определения сетевой и хостовой частей адреса. Для этого маска подсети должна быть задана в явном виде.

Создание подсети

Адрес подсети создается путем заимствования бит из хостовой части адресов класса A, B и C. Обычно сетевой администратор назначает адрес подсети локально. Как и IP-адрес, каждый адрес подсети должен быть уникальным.

При создании подсетей многие уникальные адреса хостов (конечных точек) становятся недоступными. Поэтому следует уделять особое внимание проценту адресов, которые теряются при создании подсетей. В алгоритме, используемом для расчета подсетей, используются степени двойки.

При заимствовании бит из хостовой части важно обратить внимание на число создаваемых дополнительных подсетей при каждом заимствовании 1 бита. При заимствовании 2 битов возможно создание четырех подсетей ($2^2 = 4$). При заимствовании каждого дополнительного бита из хостовой части количество создаваемых подсетей *увеличивается* в 2 раза, а число уникальных адресов хостов *уменьшается* в 2 раза. Ниже приводится несколько примеров:

- Использование 3 битов для поля подсети позволяет создать 8 подсетей ($2^3 = 8$).
- Использование 4 битов для поля подсети позволяет создать 16 подсетей ($2^4 = 16$).
- Использование 5 битов для поля подсети позволяет создать 32 подсети ($2^5 = 32$).
- Использование 6 битов для поля подсети позволяет создать 64 подсети ($2^6 = 64$).

В общем случае для расчета количества доступных подсетей на основе заданного количества битов для подсети можно использовать следующую формулу:

Количество подсетей = 2^s (где *s* – это количество битов, заимствованных из хостовой части для создания подсетей)

Расчет числа доступных подсетей и хостов

При создании подсетей важно определить оптимальное количество подсетей и хостов. В этом разделе описывается процесс планирования подсетей.

Расчет хостов для подсети класса C

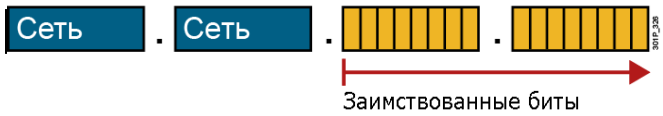
Каждый раз, когда бит заимствуется из хостовой части, количество бит в поле, которое можно использовать для номеров хостов, уменьшается. При этом число адресов хостов, доступных для назначения, уменьшается на два.

В качестве примера рассмотрим сеть класса C, в которой все 8 бит в последнем октете используются для идентификатора хоста. Поэтому существует 256 возможных значений. Фактически для назначения хостам можно использовать 254 адреса (256 – 2 зарезервированных адреса).

Теперь представим, что эта сеть класса C разделена на подсети. Если из используемых по умолчанию 8 бит хостовой части заимствуются 2 бита, размер хостовой части уменьшится до 6 битов. Все возможные комбинации 0 и 1 для оставшихся 6 битов образуют совокупное число доступных хостов, которое можно назначить каждой подсети. Теперь исходное число 256 уменьшилось до 64. Количество доступных номеров хостов уменьшилось до 62 (64 – 2).

Если в той же сети класса C заимствовать 3 бита, размер хостовой части сократится до 5 бит и доступное количество хостов для каждой подсети уменьшится до 32 (2^5). Количество доступных номеров хостов уменьшается до 30 (32 – 2). Количество доступных адресов хостов, которое можно назначить подсети, зависит от количества созданных подсетей. Например, если в сети класса C создается 8 подсетей, в каждой из них можно использовать 30 (32 – 2) адресов хостов.

Доступные подсети и хосты для сети класса B



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

Расчет хостов для подсети класса B

Теперь рассмотрим сетевой адрес класса B, в котором 16 бит используется для идентификатора сети и 16 бит для идентификатора хоста. В этом случае доступно 65 536 (2^{16}) адресов для назначения хостам (после вычитания двух адресов для широковещательного и сетевого адресов, которые использовать нельзя, остается 65 534 адреса).

Теперь представим, что сеть класса B разделена на подсети. Если из используемых по умолчанию 16 бит хостовой части заимствуются 2 бита, размер хостовой части уменьшится до 14 бит. Все возможные комбинации 0 и 1 для оставшихся 14 бит образуют совокупное число доступных хостов, которое можно назначить каждой подсети. Таким образом, каждой подсети можно назначить только 16 382 хоста.

Если в той же сети класса B заимствовать 3 бита, размер хостовой части сократится до 13 бит и доступное количество хостов для каждой подсети уменьшится до 8 192 (2^{13}). Количество доступных номеров хостов уменьшается до 8 190 (8 192 – 2). Например, если в сети класса B создается 6 подсетей, в каждой из них можно использовать 8 190 (8 192 – 2) адресов хостов.

Доступные подсети и хосты для сети класса A

Количество заимствованных бит (s)	Количество возможных подсетей (2^s)	Количество бит, оставшихся в идентификаторе узла (24 - s = h)	Количество узлов, допустимых в подсети (2^h - 2)
1	2	23	8 388 606
2	4	22	4 194 302
3	8	21	2 097 150
4	16	20	1 048 574
5	32	19	524 286
6	64	18	262 142
7	128	17	131 070
...	...	...	...

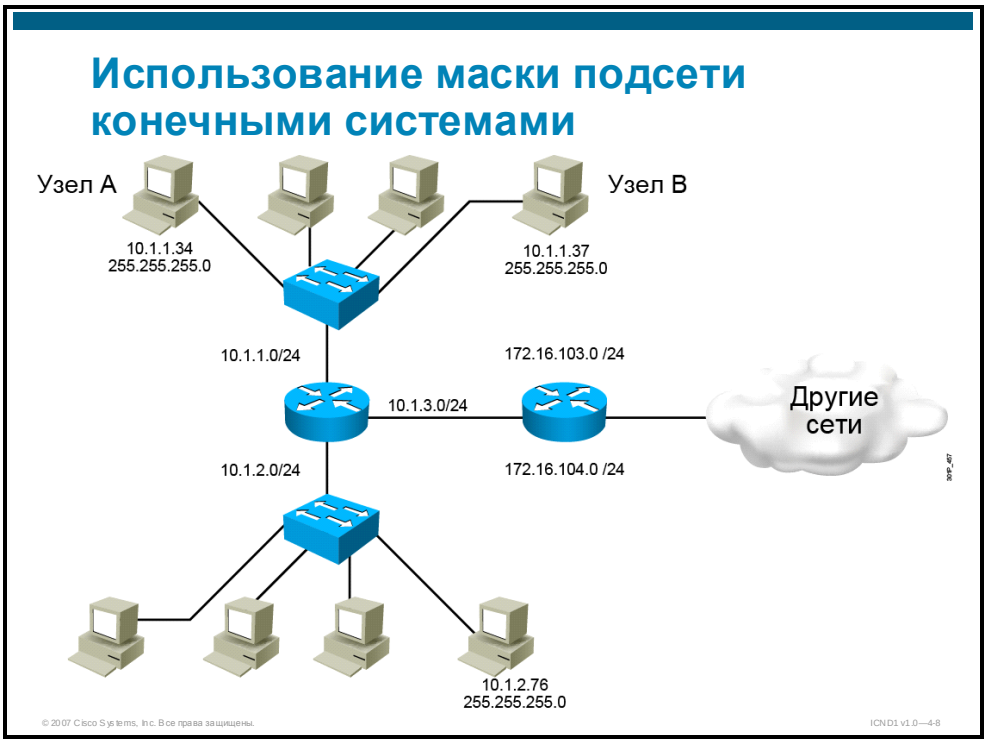
Расчет хостов для подсети класса A

Теперь рассмотрим сетевой адрес класса A, в котором 8 бит используется для идентификатора сети и 24 бита для идентификатора хоста. В этом случае доступно 16 777 216 (2^{24}) адресов для назначения хостам (после вычитания двух адресов для широковещательного и сетевого адресов, которые использовать нельзя, остается 16 777 214 адресов).

Теперь представим, что эта сеть класса A разделена на подсети. Если из используемых по умолчанию 24 бит хостовой части заимствуются 2 бита, размер хостовой части уменьшится до 18 бит. Все возможные комбинации 0 и 1 для оставшихся 18 битов образуют совокупное число доступных хостов, которое можно назначить каждой подсети. Теперь исходное число 16 777 216 уменьшилось до 262 142. Количество хостовых адресов, которое можно использовать, уменьшилось до 262 140 (262 142 – 2).

Использование масок подсетей конечными системами

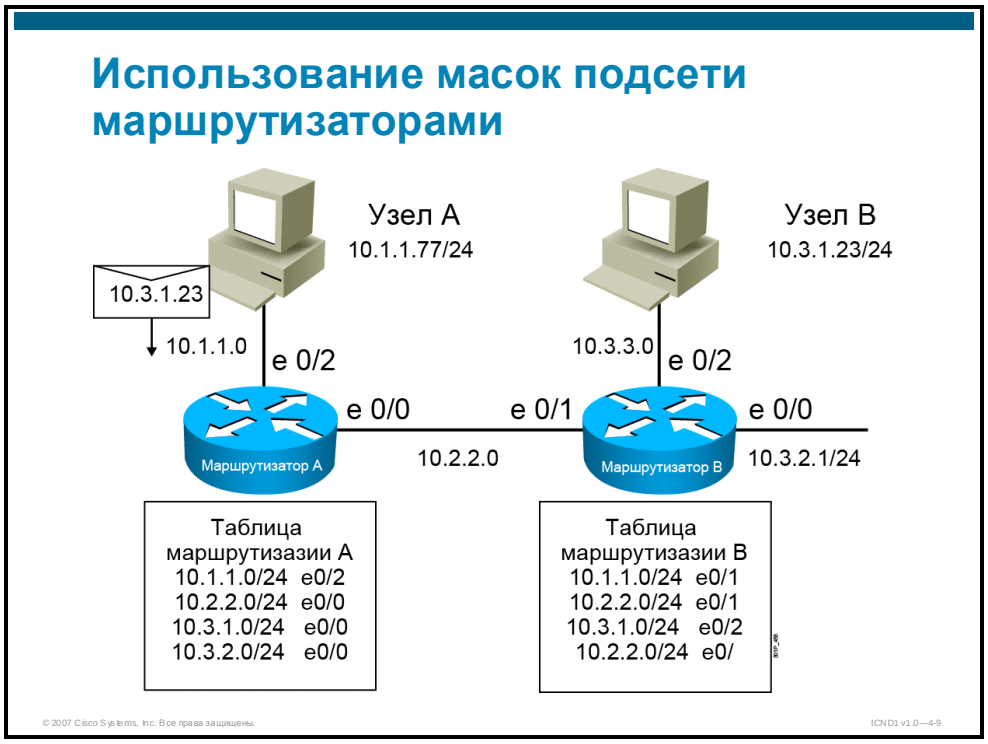
Конечная система использует маску подсети для сравнения сетевой части локального сетевого адреса с сетевым адресом назначения отправляемого пакета. В этом разделе описано использование масок подсети конечными системами.



Перед тем, как конечная система отправит пакет по месту назначения, она должна определить, относится ли этот адрес назначения к данной локальной сети. Если относится, конечная система будет использовать процесс Address Resolution Protocol (ARP) для привязки IP-адреса к MAC-адресу. В противном случае пакет должен пересылаться маршрутизатору, используемому в качестве шлюза по умолчанию, для передачи в сеть назначения.

Использование масок подсети маршрутизаторами

Маска подсети определяет сетевую часть (префикс) IP-адреса. С помощью этой информации маршрутизаторы могут определить, как доставить пакет в нужный пункт назначения. В этом разделе описывается, как маршрутизаторы используют маски подсети.

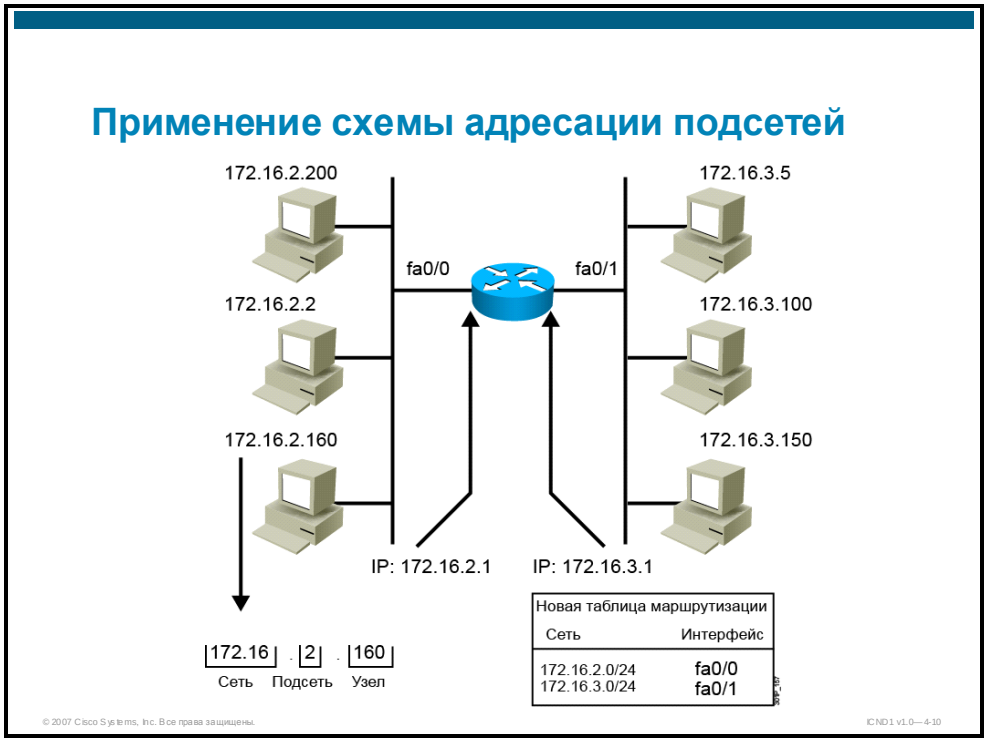


Все маршрутизаторы ведут таблицы маршрутизации. В зависимости от расположения маршрутизатора в иерархии сети эта таблица может быть небольшой и простой или большой и сложной.

Маршрутизатор вносит в таблицу маршрутизации сетевые части адресов всех известных сетей для сравнения с сетевыми адресами назначения пакетов, которые необходимо переслать. Если сеть не имеет непосредственного подключения к маршрутизатору, он хранит адрес маршрутизатора следующего перехода, которому должен пересылаться пакет. Чтобы маршрутизаторам не приходилось сохранять *все* сети назначения в своих таблицах, они используют маршрут по умолчанию для пересылки пакетов, которые не соответствуют записям в таблице маршрутизации.

Процедура маршрутизации с использование масок подсети

№	Действие	Примечания
1.	Хост A определяет, что для сети назначения необходимо использовать маршрутизатор, являющийся шлюзом по умолчанию (маршрутизатор A).	У маршрутизатора A есть маршрут к сети назначения 10.3.1.0, и он пересылает пакет маршрутизатору B через указанный интерфейс.
2.	Поскольку сеть 10.3.1.0/24 непосредственно подключена к интерфейсу fa0/2 маршрутизатора B, маршрутизатор B будет использовать протокол ARP для определения MAC-адреса хоста B.	



При настройке маршрутизатора, каждый интерфейс соединяется с отдельным сегментом сети или подсети. Интерфейсу маршрутизатора необходимо назначить доступный адрес хоста из каждой сети или подсети, к которой он подключен (см. рисунок). В этом примере маршрутизатор имеет два интерфейса Ethernet. Интерфейсу, который подключен к подсети 172.16.2.0, присваивается IP-адрес 172.16.2.1, а другому интерфейсу, который подключен к подсети 172.16.3.0, присваивается IP-адрес 172.16.3.1. У всех подключенных хостов должны быть собственные адреса из диапазона данной подсети. Все хосты, для которых заданы адреса, не относящиеся к подсети, будут *недоступны*.

Принцип действия масок подсетей

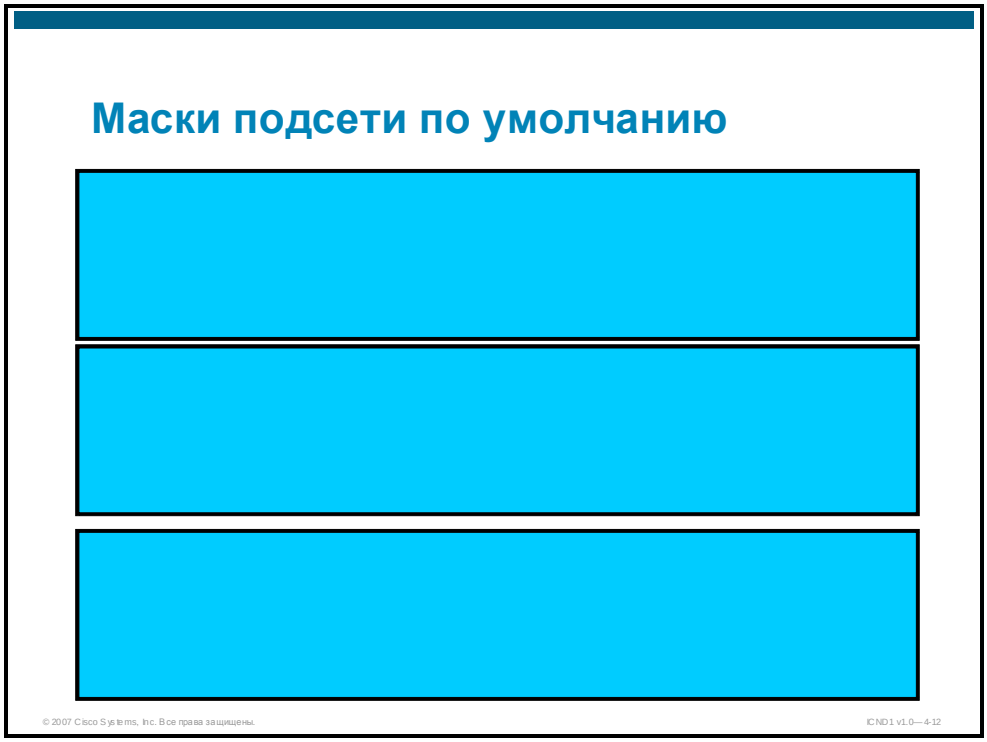
В предыдущих разделах мы обсудили, зачем нужны маски подсети и как они используются конечными системами и маршрутизаторами. В этом разделе разъясняется, как маски подсети создаются и функционируют.

Хотя в масках подсети используется тот же формат, что и в IP-адресах, они не являются IP-адресами. Каждая маска подсети имеет 32 бита, разделенных на 4 октета, которые обычно представлены в точечно-десятичном представлении, как и IP-адреса. В двоичном представлении маски подсети содержат единицы в разрядах, относящихся к части сети и подсети, и нули в разрядах хостовой части.

Значения октетов маски подсети

Существует только восемь допустимых значений маски подсети на октет. Поле подсети всегда расположено сразу после номера сети. То есть заимствоваться должны первые *n* бит, начиная со старшего бита (MSB) исходной хостовой части, где *n* – число бит, определяющее область подсетей (см. рисунок). С помощью маски подсети маршрутизатор определяет, какие биты определяют маршрут (сеть и подсеть), а какие биты являются битами хостов.

Если во всех 8 битах октета в двоичном представлении установлены 1, в десятичном формате этот октет будет представлен как 255. Поэтому в десятичном представлении подсети по умолчанию используются значения 255. В классе A по умолчанию используется адрес подсети 255.0.0.0 или 11111111.00000000.00000000.00000000. Если заимствовать три старших бита из второго по старшинству октета, в десятичном представлении мы получим число 224. Адрес подсети преобразуется в 255.224.0.0 или 11111111.11100000.00000000.00000000.

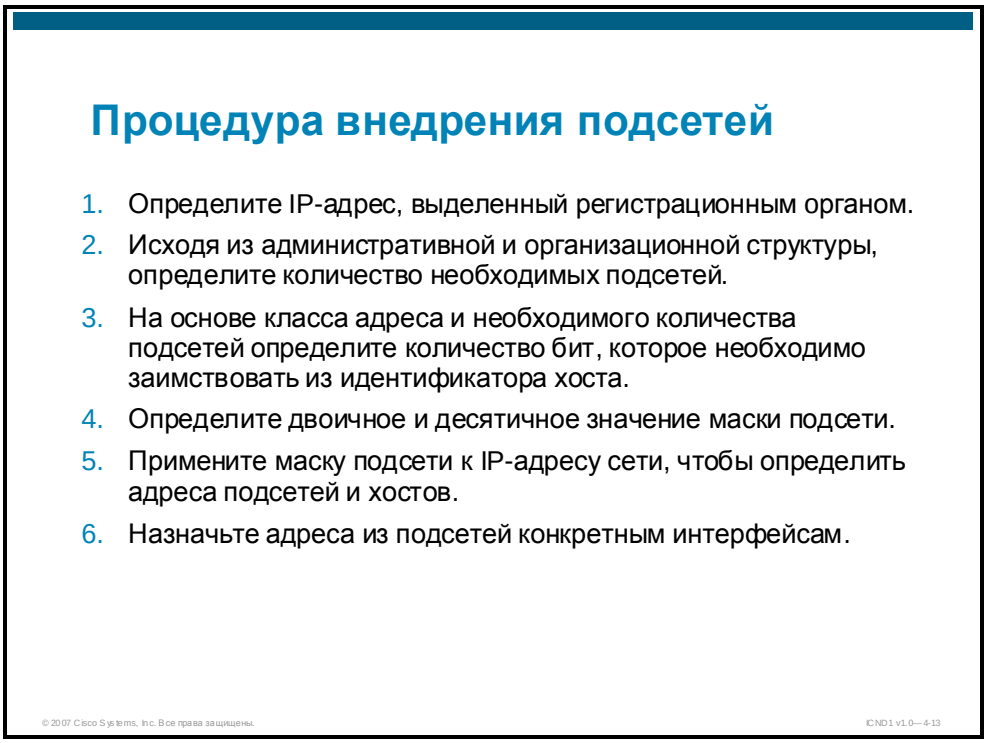


При использовании IP-адресации маска подсети определяет адресную информацию, которая необходима для отправки пакетов по месту назначения. Маска подсети указывает, какие биты в IP-адресе являются битами сети и подсети.

На рисунке приводятся маски подсети по умолчанию для классов A, B и C. Маска подсети задается с единицами в битах, относящихся к сети, и нулями в остальных битах.

Применение маски подсети

Большинство сетевых администраторов работают с существующими сетями, для которых уже определены подсети и подходящие маски подсети. Сетевые администраторы должны уметь определять, какая часть существующего IP-адреса относится к сети, а какая – к подсети. Эту информацию можно получить, применив маску подсети. В этом разделе описано, как применить маску подсети.



В приведенной на рисунке процедуре разъясняется, как выбрать необходимое количество подсетей для определенной сети, а затем применить маску для внедрения подсетей.

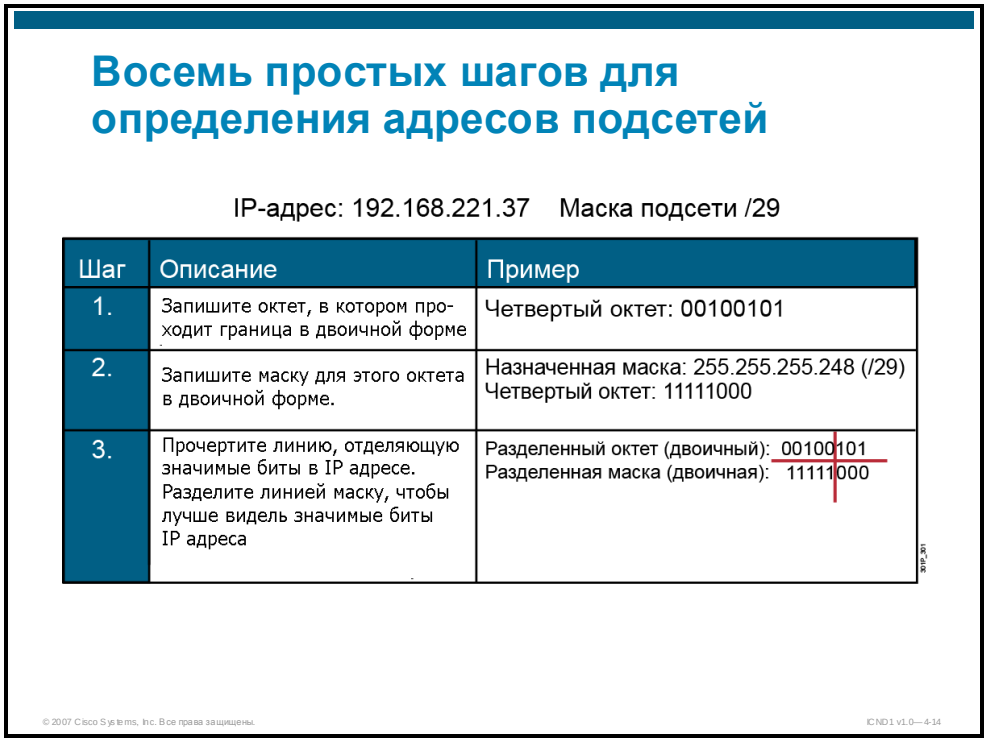
Процедура внедрения подсетей

№	Действие	Пример
1.	Определите IP-адрес для вашей сети, выделенный соответствующим регистрационным органом.	Предположим, что выделен адрес 172.16.0.0 класса B.
2.	Исходя из административных потребностей и структуры организации, определите, сколько подсетей необходимо для сети. Обязательно учтите возможный рост и развитие сети.	Предположим, что вы управляете всемирной сетью в 25 странах. В каждой стране в среднем четыре филиала. Поэтому вам необходимо 100 подсетей.
3.	На основе класса адреса и выбранного количества подсетей определите количество бит, которое необходимо заимствовать из хостовой части.	Для создания 100 подсетей необходимо позаимствовать 7 бит ($2^7 – 2 = 126$).

№	Действие	Пример
4.	Определите двоичное и десятичное значение выбранной маски подсети.	Для адреса класса B с 16 битами в идентификаторе сети после заимствования 7 бит образуется маска /23. Двоичное значение этой маски: 11111111.11111111.11111110.00000000 Десятичное значение этой маски: 255.255.254.0
5.	Примените эту маску подсети к IP-адресу сети, чтобы определить адреса подсетей и хостов. Кроме того, необходимо определить сетевой и широковещательный адрес для каждой подсети.	
6.	Назначьте адреса подсетей конкретным подсетям в вашей сети.	

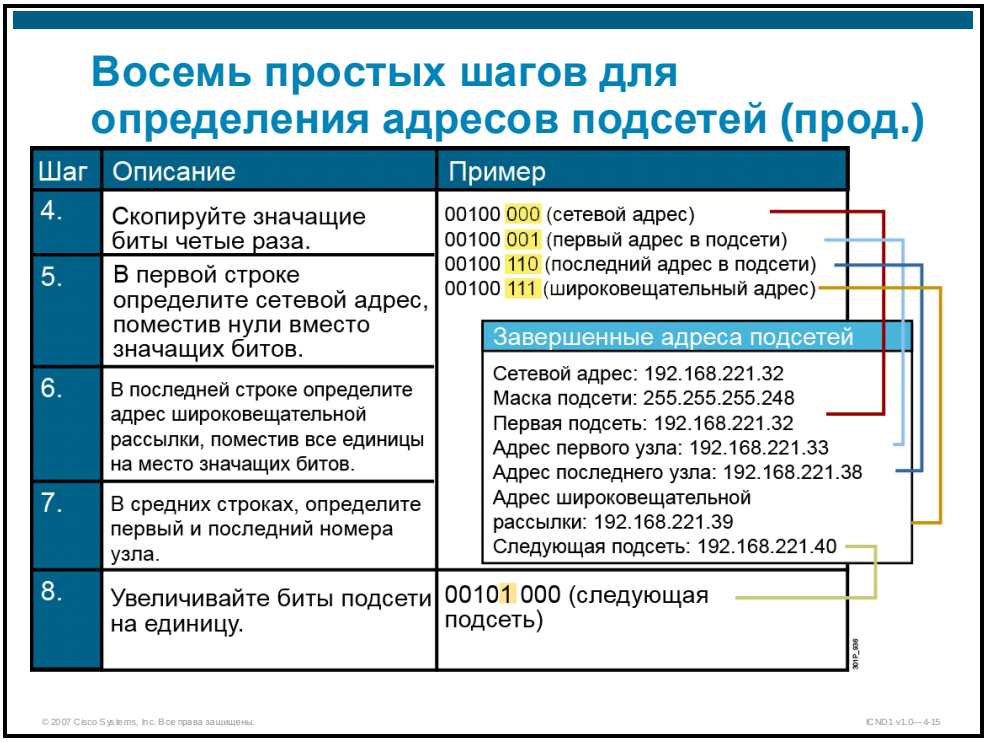
Определение схемы сетевой адресации

При работе в классовой сетевой среде, в которой используется маски подсетей фиксированных размеров, можно определить всю схему адресации сети на основе одного IP-адреса и соответствующей ему маски подсети.



На рисунке приводятся три первых действия (из восьми), используемых для определения подсети заданного IP-адреса. В этом примере используются следующие IP-адрес и маска подсети:

- **Сетевой адрес:** 192.168.221.37
- **Маска подсети:** 255.255.255.248



На этом рисунке показаны последние пять из восьми действий, используемых для определения подсети заданного IP-адреса.

После преобразования двоичных значений в десятичные будут получены следующие адреса для подсетей:

- **Адрес первой подсети:** 192.168.221.32
- **Адрес первого хоста:** 192.168.221.33
- **Адрес последнего хоста:** 192.168.221.38
- **Широковещательный адрес:** 192.168.221.39
- **Адрес следующей подсети:** 192.168.221.40

Обратите внимание, что диапазон блока адресов, включая адрес подсети и широковещательный адрес в этом примере, начинается с адреса 192.168.221.32 и заканчивается адресом 192.168.221.39, то есть включает восемь адресов. Размер блока адресов соответствует количеству бит хостовой части ($2^h = 2^3 = 8$).

Пример для класса C

Если известен адрес 192.168.5.139 и маска подсети 255.255.255.224, номер подсети равен 11111111.11111111.11111111.11100000 или /27.

Действия по определению адресов подсетей класса C

№	Описание	Пример
1.	Укажите разделяемый октет в двоичном формате.	10001011
2.	Укажите маску или длину классового префикса в двоичном формате.	11100000
3.	Отделите линией значимые биты в назначенном IP-адресе. Разделите линией маску, чтобы выделить значимые биты IP-адреса.	100 | 01011 111 | 00000
4.	Скопируйте значимые биты четыре раза.	100 00000 (адрес первой подсети) 100 00001 (адрес первого хоста) 100 11110 (адрес последнего хоста) 100 11111 (широковещательный адрес)
5.	В первой строке укажите сетевой адрес, поставив 0 в оставшиеся биты хоста.	
6.	В последней строке укажите широковещательный адрес, поставив 1 в битах хоста.	
7.	В средних строках укажите идентификатор первого и последнего хостов подсети.	
8.	Чтобы определить следующий адрес подсети, увеличивайте биты подсети на единицу. Повторите шаги с 4 по 8 для всех подсетей.	101 00000 (адрес следующей подсети)

Таблица адресов подсетей

Номер подсети	Идентификатор подсети	Диапазон адресов хостов	Широковещательный адрес
Все 0	192.168.5.0	с 192.168.5.1 по 192.168.5.30	192.168.5.31
1	192.168.5.32	с 192.168.5.33 по 192.168.5.62	192.168.5.63
2	192.168.5.64	с 192.168.5.65 по 192.168.5.94	192.168.5.95
3	192.168.5.96	с 192.168.5.97 по 192.168.5.126	192.168.5.127
4	192.168.5.128	с 192.168.5.129 по 192.168.5.158	192.168.5.159
5	192.168.5.160	с 192.168.5.161 по 192.168.5.190	192.168.5.191
6	192.168.5.192	с 192.168.5.193 по 192.168.5.222	192.168.5.223
Все 1	192.168.5.224	с 192.168.5.225 по 192.168.5.254	192.168.5.255

Пример для класса B

Если известен адрес 172.16.139.46 и маска подсети 255.255.240.0 или /20, можно определить адреса подсети и хостов для этой сети.

Пример. Применение маски подсети для адреса класса B

IP-адрес 172.16.139.46 Маска подсети /20

IP-адрес	172	16	139	46	
IP-адрес	10101100	00010000	10001011	00101110	
Маска подсети	11111111	11111111	11110000	00000000	/20
Подсеть	10101100	00010000	10000000	00000000	
Подсеть	172	16	128	0	
Первый узел	172	16	10000000	00000001=128.1	
Последний узел	172	16	10001111	11111110=143.254	
Направленная широковещательная рассылка	172	16	10001111	11111111=143.255	
Следующая подсеть	172	16	10010000	00000000=144.0	

Действия по определению адресов подсетей класса B

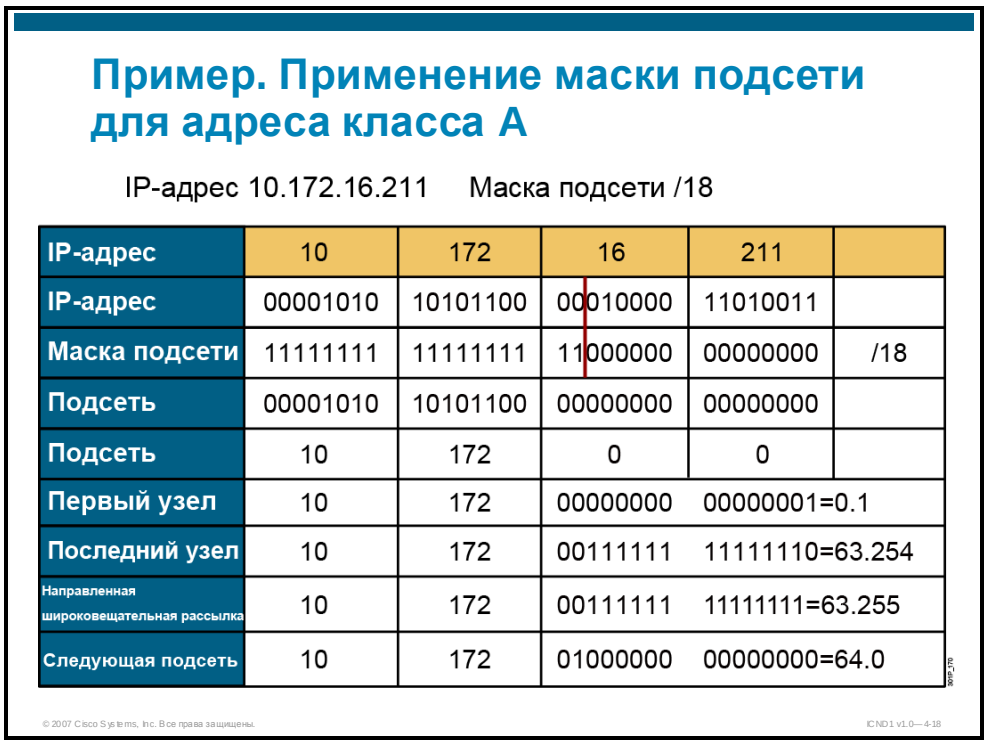
№	Описание	Пример
1.	Укажите разделяемый октет в двоичном формате.	10001011
2.	Укажите маску или длину классового префикса в двоичном формате.	11110000
3.	Отделите линией значимые биты в назначенном IP-адресе. Разделите линией маску, чтобы выделить значимые биты IP-адреса.	1000 | 1011 1111 | 0000
4.	Скопируйте значимые биты четыре раза.	1000 0000 (адрес первой подсети)
5.	В первой строке укажите сетевой адрес, поставив 0 в оставшиеся биты хоста.	1000 0001 (адрес первого хоста)
6.	В последней строке укажите широковещательный адрес, поставив 1 в битах хоста.	1000 1110 (адрес последнего хоста) 1000 1111 (широковещательный адрес)
7.	В средних строках укажите идентификатор первого и последнего хостов подсети.	
8.	Чтобы определить следующий адрес подсети, увеличивайте биты подсети на единицу. Повторите шаги с 4 по 8 для всех подсетей.	1001 0000 (адрес следующей подсети)

Таблица адресов подсетей

Номер подсети	Идентификатор подсети	Диапазон адресов хостов	Широковещательный адрес
Все 0	172.16.0.0	с 172.16.0.1 по 172.16.15.254	172.16.15.255
1	172.16.16.0	с 172.16.16.1 по 172.16.31.254	172.16.31.255
2	172.16.32.0	с 172.16.32.1 по 172.16.47.254	172.16.47.255
…….			
13	172.16.208.0	с 172.16.208.1 по 172.16.223.254	172.16.223.255
14	172.16.224.0	с 172.16.224.1 по 172.16.239.254	172.16.239.255
Все 1	172.16.240.0	с 172.16.240.1 по 172.16.255.254	172.16.255.255

Пример для класса A

Если известен адрес 10.172.16.211 и маска подсети /18, можно определить адреса подсетей и хостов для этой сети.



Действия по определению адресов подсетей класса A

№	Описание	Пример
1.	Укажите разделяемый октет в двоичном формате.	00010000
2.	Укажите маску или длину классового префикса в двоичном формате.	11000000
3.	Отделите линией значимые биты в назначенном IP-адресе. Разделите линией маску, чтобы выделить значимые биты IP-адреса.	00 | 010000 11 | 000000
4.	Скопируйте значимые биты четыре раза.	00 000000 (адрес первой подсети) 00 000001 (адрес первого хоста) 00 111110 (адрес последнего хоста) 00 111111 (широковещательный адрес)
5.	В первой строке укажите сетевой адрес, поставив 0 в оставшиеся биты хоста.	
6.	В последней строке укажите широковещательный адрес, поставив 1 в битах хоста.	
7.	В средних строках укажите идентификатор первого и последнего хостов подсети.	
8.	Чтобы определить следующий адрес подсети, увеличивайте биты подсети на единицу. Повторите шаги с 4 по 8 для всех подсетей.	01 000000 (адрес следующей подсети)

Таблица адресов подсетей

Номер подсети	Идентификатор подсети	Диапазон адресов хостов	Широковещательный адрес
Все 0	10.0.0.0	с 10.0.0.1 по 10.0.63.254	10.0.63.255
1	10.0.64.0	с 10.0.64.1 по 10.0.127.254	10.0.127.255
2	10.0.128.0	с 10.0.128.1 по 10.0.191.254	10.0.191.255
…….			
1021	10.255.64.0	с 10.255.64.1 по 10.255.127.254	10.255.127.255
1022	10.255.128.0	с 10.255.128.1 по 10.255.191.254	10.255.191.255
Все 1	10.255.192.0	с 10.255.192.1 по 10.255.255.254	10.255.255.255

Резюме

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

Резюме

- Сети, особенно большого размера, часто делят на меньшие по размеру подсети. Использование подсетей позволяет повысить производительность сети и улучшить управление.
- Адрес подсети расширяет сетевую часть адреса. Для этого из исходной хостовой части заимствуются биты и используются как область подсети.
- Определение оптимального количества подсетей и хостов зависит от типа сети и количества необходимых адресов хостов.
- Формула для расчета количества подсетей – 2^s, где s – это количество битов подсети.

Резюме (прод.)

- С помощью маски подсети маршрутизатор определяет, какие биты определяют маршрут (сеть и подсеть), а какие являются битами хостов.
- Конечные системы используют маски подсети для сравнения сетевой части локальных сетевых адресов с адресами назначения отправляемых пакетов.
- Маршрутизаторы используют маски подсети, чтобы определить, указана ли сетевая часть IP-адреса в соответствующей таблице маршрутизации и нужно ли отправлять пакет следующему маршрутизатору.

Резюме (прод.)

Выполните следующие действия для определения адресов подсетей и хостов, используя маску подсети:

1. Укажите разделяемый октет в двоичном формате.
2. Укажите маску в двоичном формате и отделите чертой значимые биты.
3. Разделите линией маску, чтобы выделить значимые биты IP-адреса.
4. Скопируйте биты подсети четыре раза.
5. Определите сетевой адрес, поместив нули во все биты хоста.
6. Определите широковещательный адрес, поместив единицы во все биты хоста.
7. Определите первый и последний номера хостов.
8. Добавьте к битам подсети единицу.

Занятие 4

Запуск маршрутизатора Cisco

Обзор

Процедура запуска выполняется при первом включении маршрутизатора Cisco, если в нем нет сохраненной конфигурации. После запуска можно выполнить начальную настройку программного обеспечения. Распознавание корректного запуска маршрутизатора – первый этап установки маршрутизатора Cisco. Для работы в сети необходим успешный запуск и корректная конфигурация маршрутизатора. На этом занятии приводятся инструкции по запуску маршрутизатора и проверке его работы на начальном этапе.

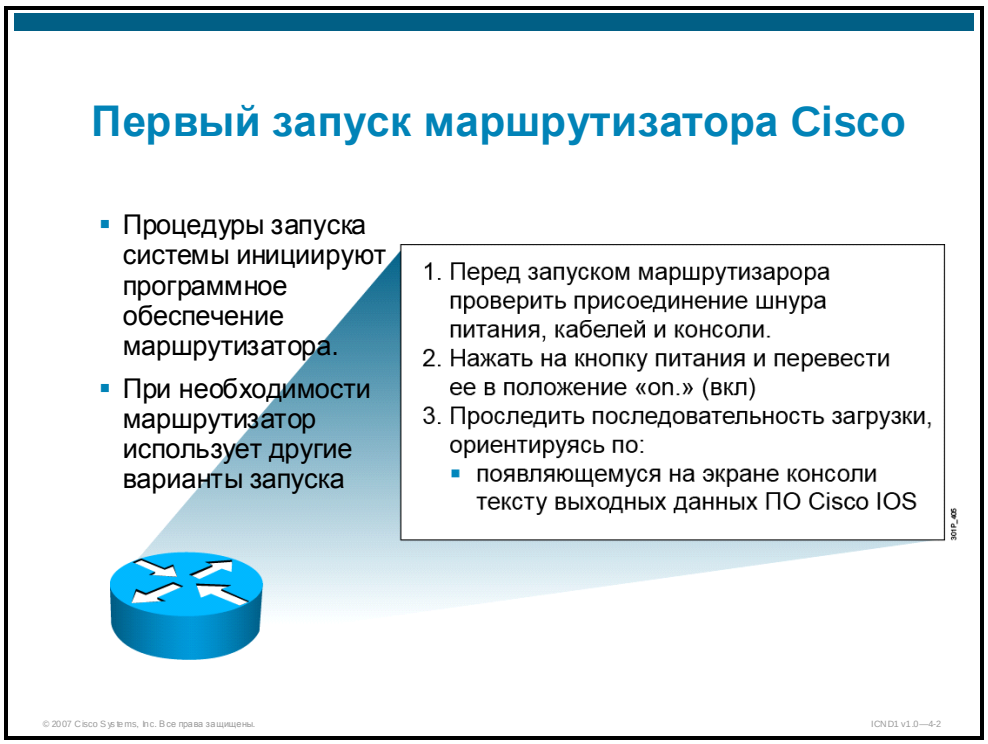
Задачи

По окончании этого занятия вы сможете запускать маршрутизатор под управлением ПО Cisco IOS и пользоваться командами интерфейса командной строки (CLI) для настройки и мониторинга маршрутизатора Cisco. Это значит, что вы сможете выполнять следующие задачи:

- запускать маршрутизатор Cisco;
- запускать процесс начальной установки маршрутизатора Cisco;
- входить в систему маршрутизатора Cisco;
- выводить сведения о состоянии аппаратного и программного обеспечения маршрутизатора Cisco.

Запуск маршрутизатора Cisco

Для запуска маршрутизатора Cisco необходимо проверить физическую установку, убедиться, что подключено питание к маршрутизатору, и ознакомится с выводом программного обеспечения Cisco IOS на консоли. В этом разделе описывается начальный запуск маршрутизаторов Cisco.



Для запуска маршрутизатор выполняет следующие задачи:

- выполняет процедуру самотестирования при включении питания (POST) для проверки аппаратного обеспечения;
- находит и загружает программное обеспечение Cisco IOS, используемое в качестве операционной системы маршрутизатора;
- находит и применяет инструкции конфигурации, касающиеся функций протоколов, адресов интерфейсов и атрибутов маршрутизатора.

При включении питания маршрутизатор Cisco выполняет процедуру POST. Во время тестирования POST маршрутизатор выполняет диагностические процедуры для проверки основных операций центрального процессора (ЦП), памяти и схем интерфейсов.

После проверки функционирования аппаратного обеспечения маршрутизатор возобновляет инициализацию программного обеспечения, в ходе которой он находит и загружает образ ПО Cisco IOS, а затем находит и загружает файл конфигурации (если он существует).

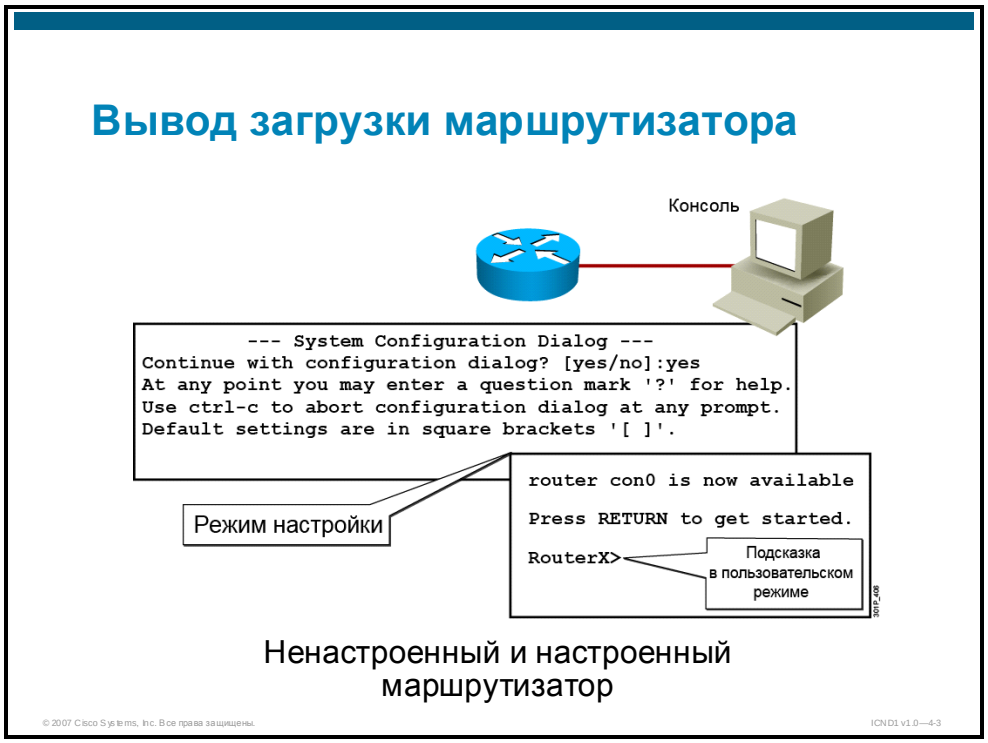
В следующей таблице перечислены действия, которые необходимо выполнить для начального запуска маршрутизатора Cisco.

Запуск маршрутизаторов Cisco

№	Действие
1.	Перед запуском маршрутизатора убедитесь, что выполнены следующие операции: ■ все сетевые кабельные подключения должны быть надежными; ■ ваш терминал должен быть подключен к порту консоли; ■ выбрано приложение консольного терминала, например HyperTerminal.
2.	Нажмите кнопку включения питания маршрутизатора.
3.	Пронаблюдайте последовательность загрузки, ознакомьтесь с текстом вывода программного обеспечения Cisco IOS на консоли.

Начальная установка маршрутизатора Cisco

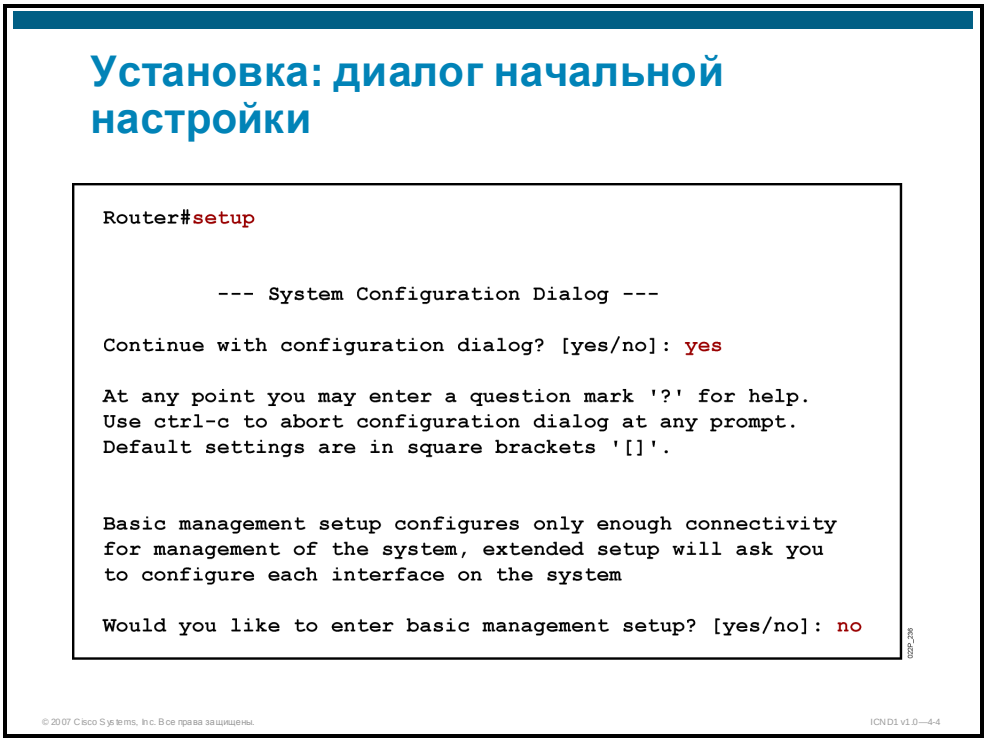
После запуска маршрутизатор ищет файл конфигурации устройства. Если он не найден, маршрутизатор выполняет процедуру начальной установки на основе вопросов, которая называется «setup». В этом разделе описывается начальный вывод командной строки и приводятся инструкции по заполнению диалога настройки.



После выполнения процедуры POST и загрузки образа ПО Cisco IOS маршрутизатор ищет файл конфигурации устройства в памяти NVRAM. Память NVRAM маршрутизатора является энергонезависимой, то есть ее содержимое сохраняется даже при отключении питания. Если в памяти NVRAM маршрутизатора найден файл конфигурации, появляется приглашение пользовательского режима. На рисунке показано приглашение RouterX>.

При запуске нового маршрутизатора Cisco файл конфигурации отсутствует. Если в памяти NVRAM нет допустимого файла конфигурации, операционная система выполняет процедуру начальной настройки, на основе вопросов. Эта процедура называется диалогом конфигурации системы или режимом установки.

Режим установки не предназначен для ввода функций сложных протоколов на маршрутизаторе. Режим установки используется для создания минимальной конфигурации. Вместо режима «setup» для настройки маршрутизатора можно использовать другие режимы конфигурации.



Основная задача режима установки – быстрое создание конфигурации с минимальным количеством функций для любого маршрутизатора, которому не удалось найти файл конфигурации в других источниках. В режим установки можно войти при загрузке маршрутизатора, не имеющего конфигурации, или в любой момент времени после загрузки и начала работы маршрутизатора с помощью команды **setup** привилегированного режима EXEC.

После многих вопросов в диалоге команды **setup** в квадратных скобках ([ ]) приведены значения по умолчанию. Чтобы использовать значения по умолчанию, нажимайте клавишу **Enter**.

При выводе вопроса «Would you like to enter basic management setup?» можно ввести **no** для завершения диалога настройки системы. Чтобы начать процесс начальной настройки, введите **yes**. Обычно в ответ на запрос «basic management setup» вводится **no** для перехода к расширенной настройке конкретных параметров системы.

В любой момент для прекращения и перезапуска этого процесса можно нажать **Ctrl-C**. При использовании командного режима установки (Router#setup) нажмите **Ctrl-C**, чтобы вернуться к приглашению привилегированного режима EXEC (Router#).

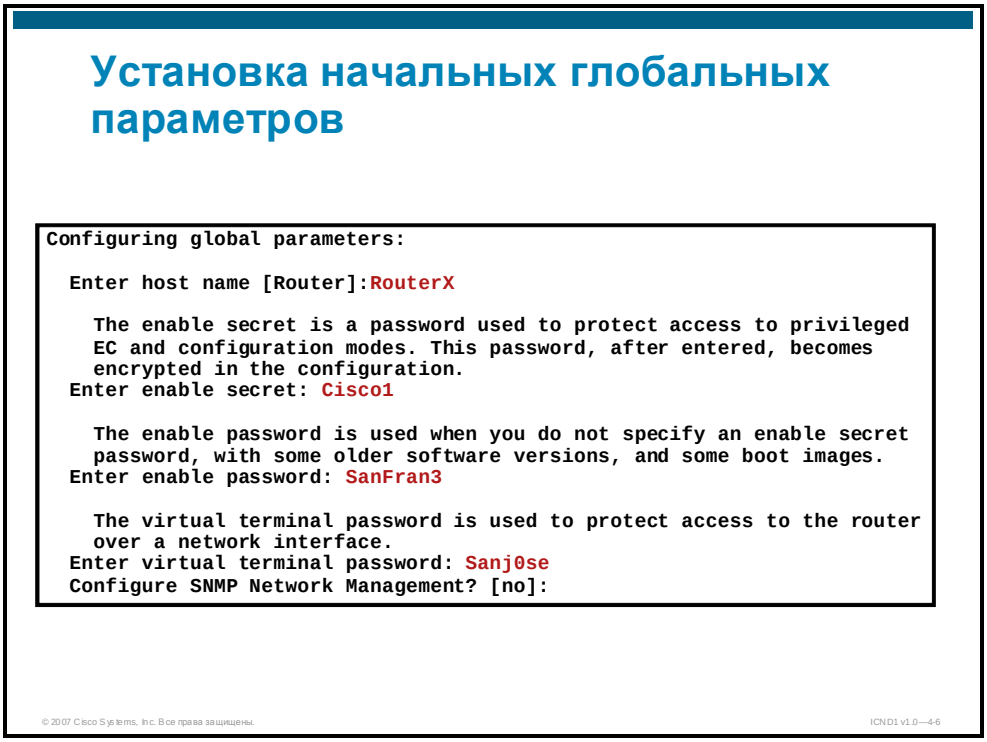
Сводка по настройке интерфейсов

```
Any interface listed with OK? value "NO" does not have a valid configuration

Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            unassigned      NO  unset  up                    up
FastEthernet0/1            unassigned      NO  unset  up                    up
Serial0/0/0                unassigned      NO  unset  up                    up
Serial0/0/1                unassigned      NO  unset  down                  down
```

Интерфейсы, обнаруженные при запуске

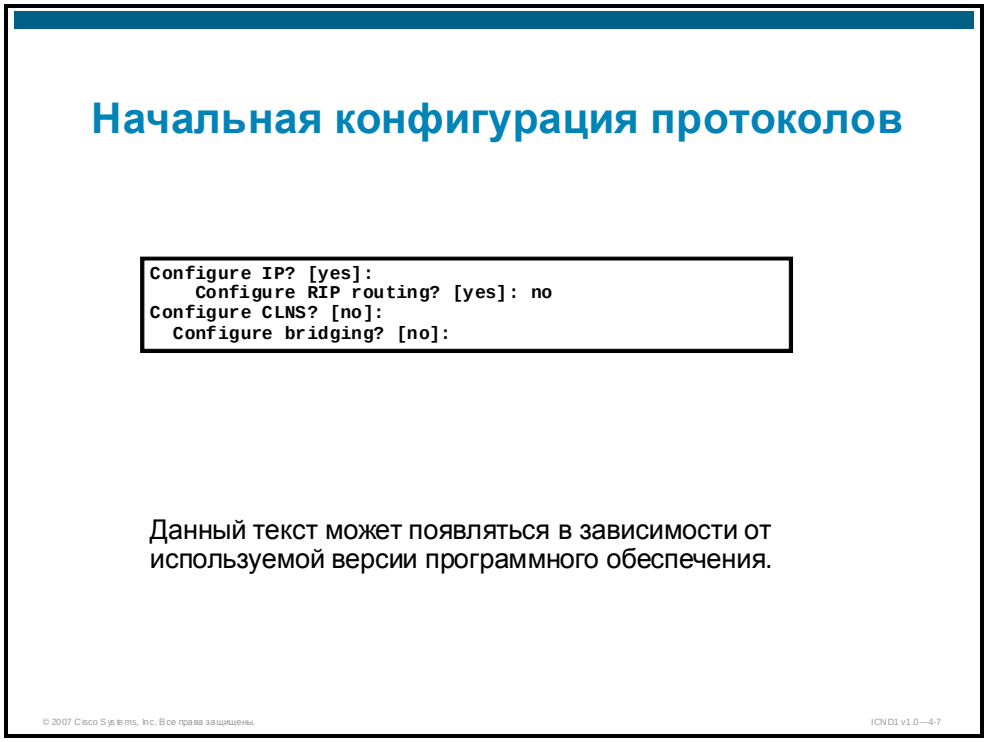
Если ввести **yes** в ответ на запрос «Would you like to enter basic management setup?», появится запрос «First, would you like to see the current interface summary?». Введите **yes** для просмотра интерфейсов маршрутизатора. На рисунке приводится вывод, в котором указывается текущее состояние каждого интерфейса маршрутизатора. Отображается IP-адрес и текущая конфигурация интерфейса.



Далее в диалоге установки будут запрашиваться глобальные параметры. При запросе глобальных параметров используйте значения конфигурации, которые были определены для маршрутизатора.

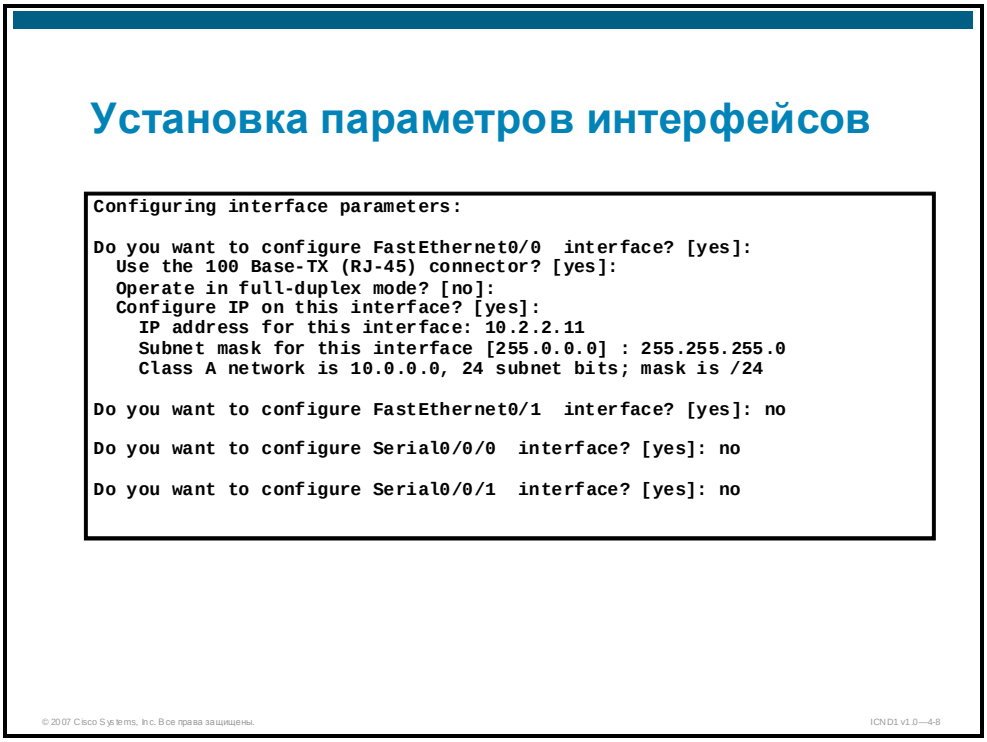
Первый глобальный параметр задает имя хоста для маршрутизатора. Это имя будет выводиться перед приглашениями Cisco IOS для всех режимов конфигурации. Имя маршрутизатора по умолчанию указывается в квадратных скобках [Router].

Используйте следующие глобальные параметры для задания различных паролей, используемых на маршрутизаторе.

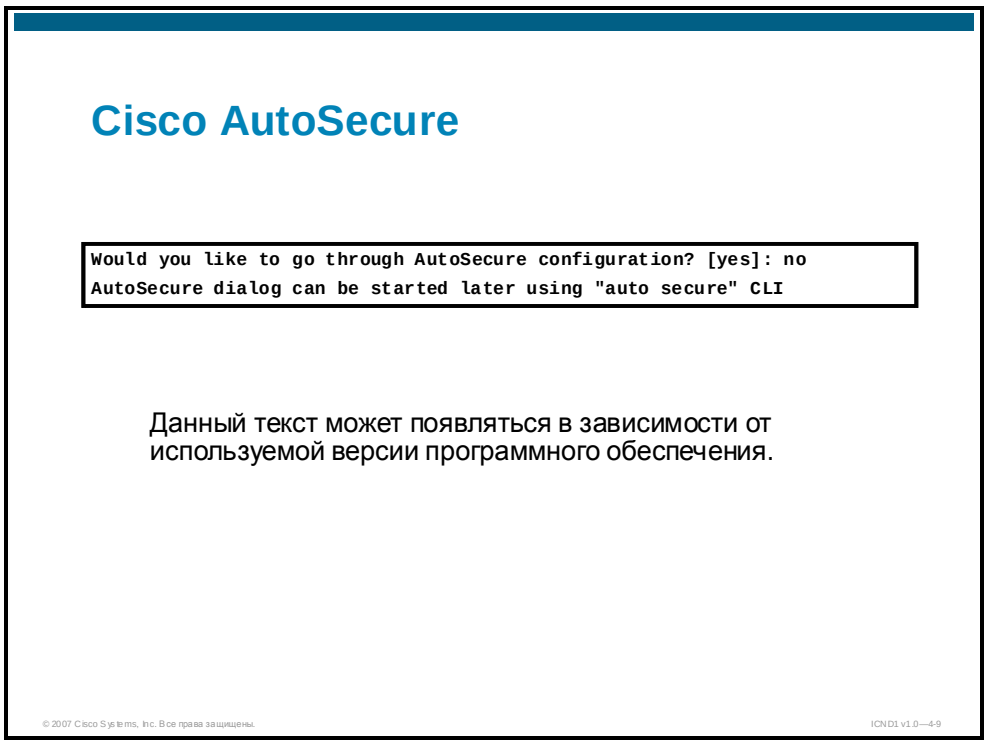


Далее в диалоге установки будут запрашиваться дополнительные глобальные параметры. При запросе глобальных параметров используйте значения конфигурации, которые были определены для маршрутизатора. В этом примере показаны запросы для протоколов маршрутизации в диалоге установки.

В запросе на настройку протокола необходимо ввести **yes**. Появятся дополнительные вспомогательные вопросы об этом протоколе.



Далее в диалоге установки будут запрашиваться параметры для каждого установленного интерфейса. Для правильного ввода запрашиваемых параметров используйте значения конфигурации, которые были определены для интерфейса.



Cisco AutoSecure – это функция обеспечения безопасности интерфейса командной строки Cisco IOS. В зависимости от потребностей среды можно использовать один из двух следующих режимов:

- **Интерактивный режим:** Пользователю предоставляется возможность включения и отключения служб и других функций безопасности.
- **Автоматический режим:** Автоматически выполняется команда Cisco AutoSecure с рекомендуемыми Cisco параметрами по умолчанию.

Внимание Cisco AutoSecure пытается обеспечить максимальную безопасность, отключая сервисы, которые наиболее часто используются хакерами для атак на маршрутизатор. Однако некоторые из этих сервисов могут быть необходимы для успешной работы в сети. Поэтому не следует использовать функцию Cisco AutoSecure, до тех пор пока вы полностью не поняли ее принципы работы и не определились с потребностями вашей сети.

Cisco AutoSecure выполняет следующие функции:

- Отключает следующие глобальные сервисы:
  - Finger;
  - Packet assembler/disassembler (PAD);
  - Small servers;
  - серверы BOOTP;
  - служба HTTP;
  - служба идентификации;
  - протокол CDP;

- протокол NTP;
- Source routing (маршрутизация от источника).

- Включает следующие глобальные сервисы:
  - служба шифрования паролей;
  - настройка выделения ресурсов и интервала планировщика;
  - время ожидания «synwait time» протокола TCP;
  - сообщения «keepalive» протокола TCP;
  - настройка базы данных политик безопасности (SPD);
  - сообщения о недостижимости протокола ICMP;
- Отключает следующие сервисы для интерфейса:
  - ICMP;
  - Proxy Address Resolution Protocol (ARP);
  - Directed broadcast (направленная широковещательная рассылка);
  - служба Maintenance Operation Protocol (MOP);
  - ICMP unreachables (сообщение о недостижимости места назначения ICMP);
  - ICMP mask reply messages (сообщения об отклике ICMP с маской).
- Обеспечивает ведение журналов системы безопасности, включая следующие функции:
  - включает последовательную нумерацию и метку времени;
  - обеспечивает ведение журнала консоли;
  - задает размер буфера журнала;
  - обеспечивает интерактивный диалог для настройки IP-адреса сервера журналов.
- Защищает доступ к маршрутизатору, включая следующие функции:
  - проверка баннер и предоставляет возможность добавить текст для автоматической настройки;
  - логин и пароль;
  - передача входных и выходных данных;
  - команды **exec-timeout**;
  - включает локальную авторизацию, аутентификацию и учет (AAA)
  - таймауты Secure Shell (SSH) и команды **ssh authentication-retries**;
  - использование только SSH и Secure Copy Protocol (SCP) для доступа и передачи файлов на маршрутизатор и с маршрутизатора;
  - отключает протокол SNMP, если он не используется.
- Защищает уровень коммутации (forwarding plane), включая следующие функции:
  - включает технологию ускоренной пересылки Cisco Express Forwarding или распределенной ускоренной пересылки Cisco Express Forwarding на маршрутизаторе, если они доступны;
  - включает антиспуфинг (защита от подделки пакетов);

— блокирует всех блоки IP-адресов, зарезервированные организацией IANA (Internet Assigned Numbers Authority);

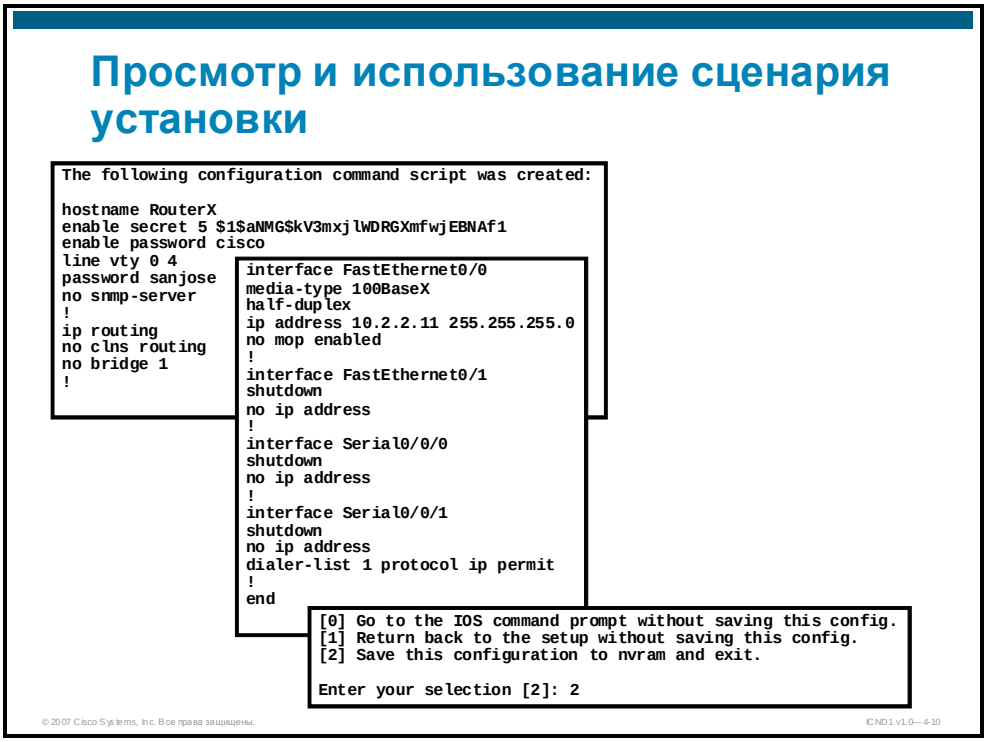
— блокирует блоки частных адресов по просьбе клиента;

— устанавливает маршрут по умолчанию в Null0, если не используется маршрутизатор по умолчанию;

— настраивает по просьбе клиента время ожидания перехвата TCP соединений, если доступна функция перехвата TCP;

— запускает функцию интерактивной настройки Context-Based Access Control (CBAC) на интерфейсах, связанных с сетью Интернет, при использовании образа Cisco IOS Firewall;

— включает NetFlow на уровне программной коммутации.



После завершения настройки для всех установленных интерфейсов маршрутизатора команда **setup** выводит созданный сценарий команд конфигурации.

Команда **setup** предлагает три следующих варианта:

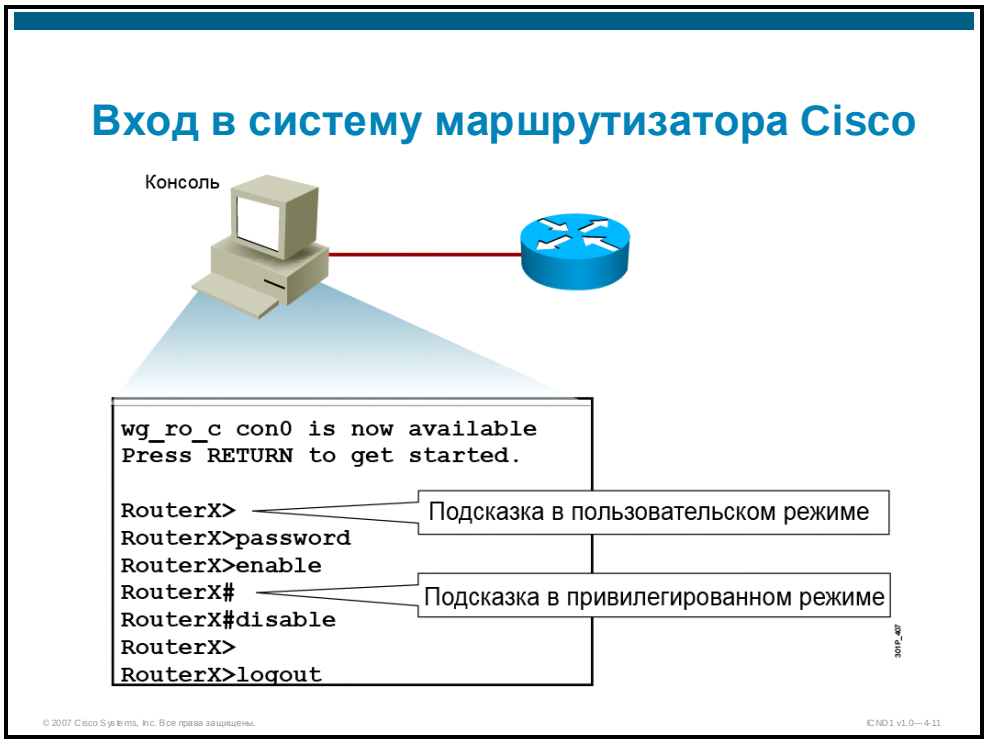
- **[0]:** Переход к приглашению EXEC без сохранения созданной конфигурации.
- **[1]:** Возвращение к началу установки без сохранения созданной конфигурации.
- **[2]:** Принятие созданной конфигурации, ее сохранение в памяти NVRAM и выход в режим EXEC.

Если выбран вариант **[2]**, после выполнения настройки и сохранения созданной конфигурации в памяти NVRAM система будет готова к использованию. Для изменения конфигурации необходимо внести изменения вручную.

Файл сценария, созданный командой **setup**, является аддитивным. С помощью команды **setup** можно *включать* функции, но *не отключать*. Кроме того, команда **setup** не поддерживает многие расширенные функции маршрутизатора и функции, которые требуют более сложной настройки.

Вход в систему маршрутизатора Cisco

При настройке маршрутизатора Cisco через интерфейс командной строки на консоли или удаленном терминале ПО Cisco IOS предоставляет интерпретатор, который называется EXEC. EXEC интерпретирует вводимые команды и выполняет соответствующие операции. В этом разделе приведены инструкции по входу в систему маршрутизатора Cisco для запуска начальной настройки.



После настройки маршрутизатора Cisco с помощью команды setup можно перенастроить конфигурацию или внести дополнения с помощью интерфейса пользователя, подключившись к консоли маршрутизатора или вспомогательному порту. Кроме того, для настройки маршрутизатора Cisco можно использовать приложение удаленного доступа, например SSH.

Интерпретатор команд ПО Cisco IOS EXEC интерпретирует вводимые команды и выполняет соответствующие операции. Перед вводом команды EXEC необходимо аутентифицироваться на маршрутизаторе.

В целях безопасности EXEC предлагает два уровня доступа к командам:

- **Пользовательский режим.** Обычно поддерживает задачи для проверки состояния маршрутизатора.
- **Привилегированный режим.** Обычно поддерживает задачи по изменению конфигурацию маршрутизатора.

При первом входе в систему маршрутизатора выводится приглашение пользовательского режима. В пользовательском режиме доступна только часть команд EXEC, которые можно выполнить в привилегированном режиме. С помощью этих команд можно выводить информацию, не изменяя параметры конфигурации маршрутизатора.

Для доступа ко всему набору команд необходимо перейти в привилегированный режим с помощью команды **enable** и пароля «enable password», если он настроен.

Внимание Пароль «enable password» отображается в незашифрованном виде при использовании команды **show run**. Пароль «enable secret» шифруется, поэтому он не отображается в незашифрованном виде. Если настроены оба пароля, пароль «enable secret» переопределяет пароль «enable password».

При использовании привилегированного режима в приглашении EXEC отображается знак решетки (#). Из привилегированного режима можно перейти в режим глобальной конфигурации и другие специальные режимы конфигурации, такие как режим конфигурации интерфейса, подинтерфейса, линии, протокола динамической маршрутизации, route-map и т. д.

Для возвращения из привилегированного режима в пользовательский режим EXEC используется команда **disable**. Для завершения текущего сеанса используется команда **exit** или **logout**.

Список команд пользовательского режима маршрутизатора

```
RouterX>?
Exec commands:
  access-enable     Create a temporary Access-List entry
  access-profile    Apply user-profile to interface
  clear             Reset functions
  connect           Open a terminal connection
  disable           Turn off privileged commands
  disconnect        Disconnect an existing network connection
  enable            Turn on privileged commands
  exit              Exit from the EXEC
  help              Description of the interactive help system
  lat               Open a lat connection
  lock              Lock the terminal
  login             Log in as a particular user
  logout            Exit from the EXEC
-- More --
```

Команда может быть сокращена до нескольких символов, которые ее однозначно определяют.

Введите вопросительный знак (**?**) в приглашении пользовательского или привилегированного режима для отображения списка команд, доступных в текущем режиме.

Внимание Список доступных команд меняется в зависимости от используемой версии ПО Cisco IOS.

Обратите внимание на строку «-- More --» в нижней части примера экрана. Она указывает, что можно вывести один или несколько дополнительных экранов. В этот момент вы можете выполнить одно из следующих действий:

- Нажать клавишу ПРОБЕЛ для отображения следующего доступного экрана.
- Нажать клавишу Return (на некоторых клавиатурах клавишу Enter) для вывода следующей строки.
- Нажать любую другую клавишу для возвращения к приглашению.

Список команд привилегированного режима маршрутизатора

```
RouterX#?
Exec commands:
  access-enable    Create a temporary Access-List entry
  access-profile   Apply user-profile to interface
  access-template  Create a temporary Access-List entry
  bfe              For manual emergency modes setting
  cd               Change current directory
  clear            Reset functions
  clock            Manage the system clock
  configure        Enter configuration mode
  connect          Open a terminal connection
  copy             Copy from one file to another
  debug            Debugging functions (see also 'undebug')
  delete           Delete a file
  dir              List files on a filesystem
  disable          Turn off privileged commands
  disconnect       Disconnect an existing network connection
  enable           Turn on privileged commands
  erase            Erase a filesystem
  exit             Exit from the EXEC
  help             Description of the interactive help system
-- More --
```

Вы можете дописывать команды автоматически, введя уникальную последовательность символов и нажав клавишу **Tab**.

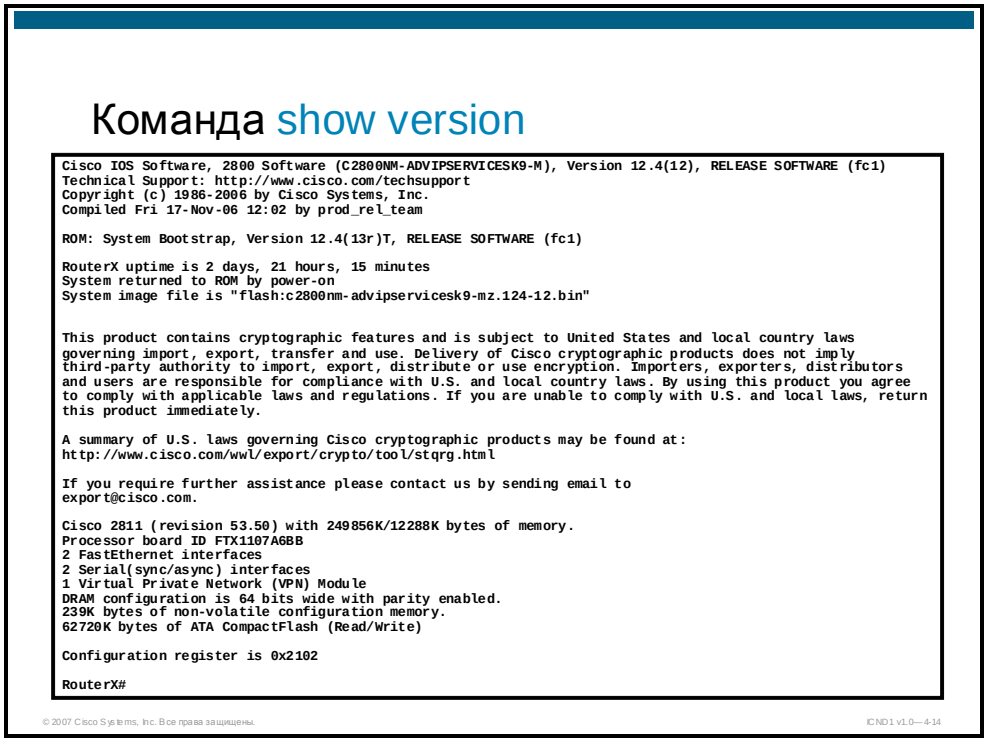
Введите в пользовательском режиме команду **enable** для перехода в привилегированный режим EXEC. Обычно, если настроен пароль «enable password», его необходимо ввести для доступа к привилегированному режиму EXEC.

Введите команду **?** в приглашении привилегированного режима для вывода списка доступных команд привилегированного режима EXEC (см. рисунок).

Внимание Список доступных команд меняется в зависимости от используемой версии ПО Cisco IOS.

Просмотр состояния маршрутизатора после первой загрузки

После входа в систему маршрутизатора Cisco можно проверить состояние программного и аппаратного обеспечения этого маршрутизатора с помощью следующих команд состояния маршрутизатора: **show version**, **show running-config** и **show startup-config**. В этом разделе описываются команды состояния маршрутизатора.



Введите команду **show version** в приглашении EXEC для вывода информиции об аппаратном обеспечении системы, версии программного обеспечения, объема памяти и значения конфигурационного регистра.

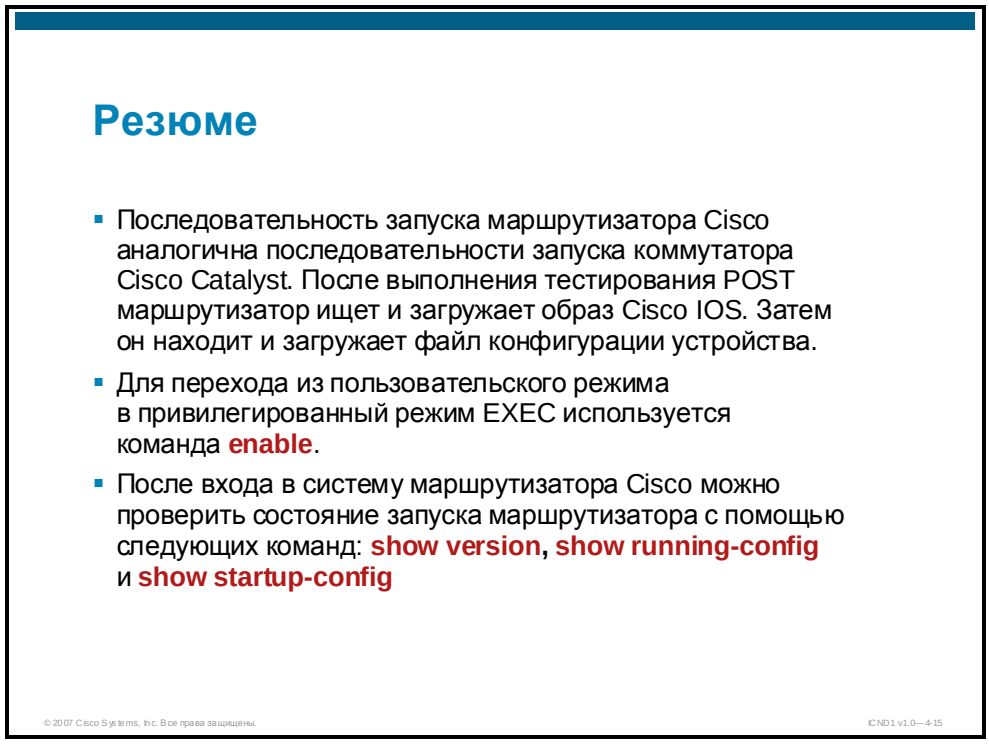
В примере, показанном на рисунке, в ОЗУ выделено 249 856 килобайт для основной памяти и 12 288 килобайт для памяти ввода-вывода (совместно используемой всеми интерфейсами). Память ввода-вывода используется для хранения маршрутизируемых пакетов.

В маршрутизаторе есть два интерфейса Fast Ethernet и два последовательных интерфейса. С помощью этой команды легко убедиться, что необходимые интерфейсы распознаны при запуске и функционируют на аппаратном уровне.

Маршрутизатор использует 239 КБ для хранения загрузочной конфигурации в памяти NVRAM и 62 720 КБ во флэш-памяти для хранения образа ПО Cisco IOS.

Резюме

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



Занятие 5

Настройка маршрутизатора Cisco

Обзор

После завершения установки оборудования и выполнения начальной конфигурации маршрутизатора Cisco можно приступить к настройке маршрутизатора для определенной интерсети. Для настройки расширенных функций, таких как IP-маршрутизация, студенты должны освоить интерфейс командной строки (CLI) ПО Cisco IOS, его режимы и принципы эксплуатации. На этом занятии приводятся инструкции по созданию базовой конфигурации маршрутизатора Cisco.

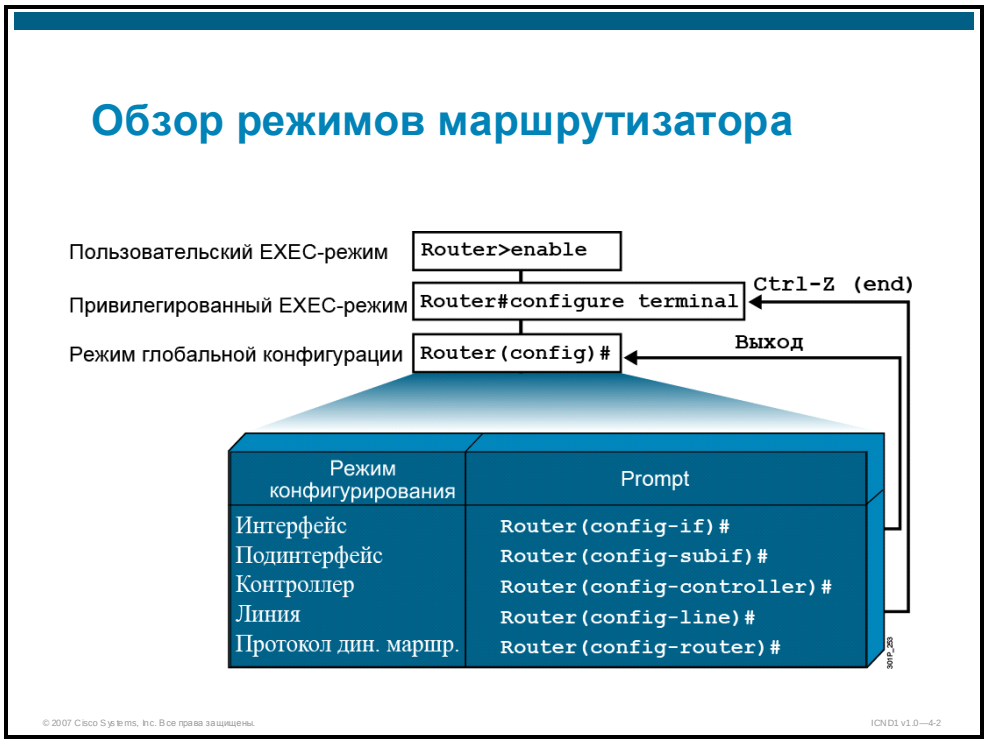
Задачи

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

- описывать режимы конфигурации маршрутизатора;
- настраивать маршрутизатор с помощью интерфейса командной строки;
- настраивать интерфейсы маршрутизатора;
- настраивать IP-адрес маршрутизатора;
- проверять конфигурацию интерфейса маршрутизатора.

Режимы конфигурации маршрутизатора Cisco

Из привилегированного режима EXEC можно перейти в режим глобальной конфигурации, предоставляющий доступ к специализированным режимам конфигурации маршрутизатора. В этом разделе описываются режимы конфигурации маршрутизатора и приводятся инструкции по сохранению конфигурации.



Первый этап настройки маршрутизатора Cisco – использование утилиты установки (setup). Эта утилита позволяет создать базовую начальную конфигурацию. Для создания более сложной специальной конфигурации можно использовать интерфейс командной строки, войдя в конфигурационный режим терминальной сессии.

Из привилегированного режима EXEC можно перейти в режим глобальной конфигурации с помощью команды **configure terminal**. Из режима глобальной конфигурации можно получить доступ к следующим специальным режимам конфигурации.

- **Интерфейс:** Поддерживает команды конфигурации отдельного интерфейса
- **Субинтерфейс:** Поддерживает команды конфигурации нескольких виртуальных интерфейсов функционирующих на базе одного физического интерфейса
- **Контроллер:** Поддерживает команды конфигурации контроллеров (например, контроллеров E1 и T1)
- **Линия:** Поддерживает команды конфигурации линии терминала, например, консольных портов и портов VTY
- **Протокол динамической маршрутизации:** Поддерживает команды конфигурации протокола динамической маршрутизации

С помощью команды **exit** можно вернуться в режим конфигурации более высокого уровня и в итоге выйти из системы. Как правило, команда **exit** вводится в специальных режимах конфигурации для возвращения в режим глобальной конфигурации. Нажмите **Ctrl-Z**, чтобы полностью выйти из режима конфигурации и вернуться в привилегированный режим EXEC.

В режиме конфигурации терминала вызывается пошаговый компилятор. Сразу после нажатия клавиши Enter выполняется синтаксический анализ каждой введенной команды конфигурации.

Если ошибок синтаксиса не обнаружено, команда выполняется, сохраняется в текущей конфигурации и вступает в действие немедленно.

Команды, которые влияют на маршрутизатор в целом, называются глобальными командами. Примеры глобальных команд – **hostname** и **enable password**.

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

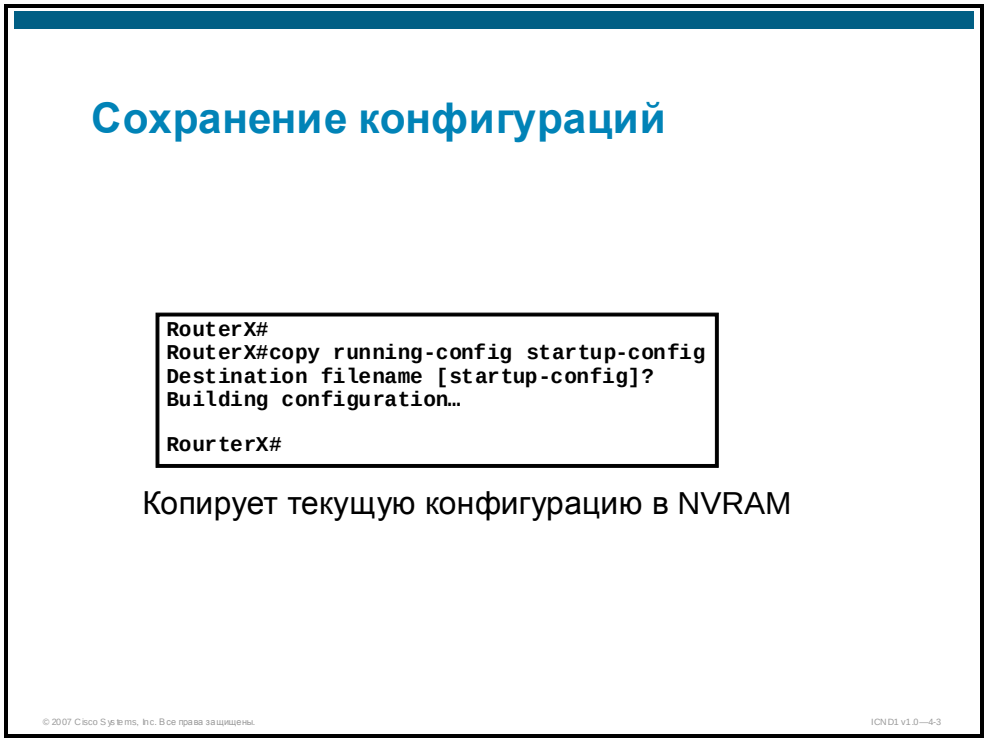
Ниже приведены примеры основных команд и соответствующих подкоманд.

```
Router(config)#interface serial 0 (основная команда)
Router(config-if)#shutdown (подкоманда)

Router(config-if)#line console 0 (основная команда)
Router(config-line)#password cisco (подкоманда)

Router(config-line)#router rip (основная команда)
Router(config-router)#network 10.0.0.0 (подкоманда)
```

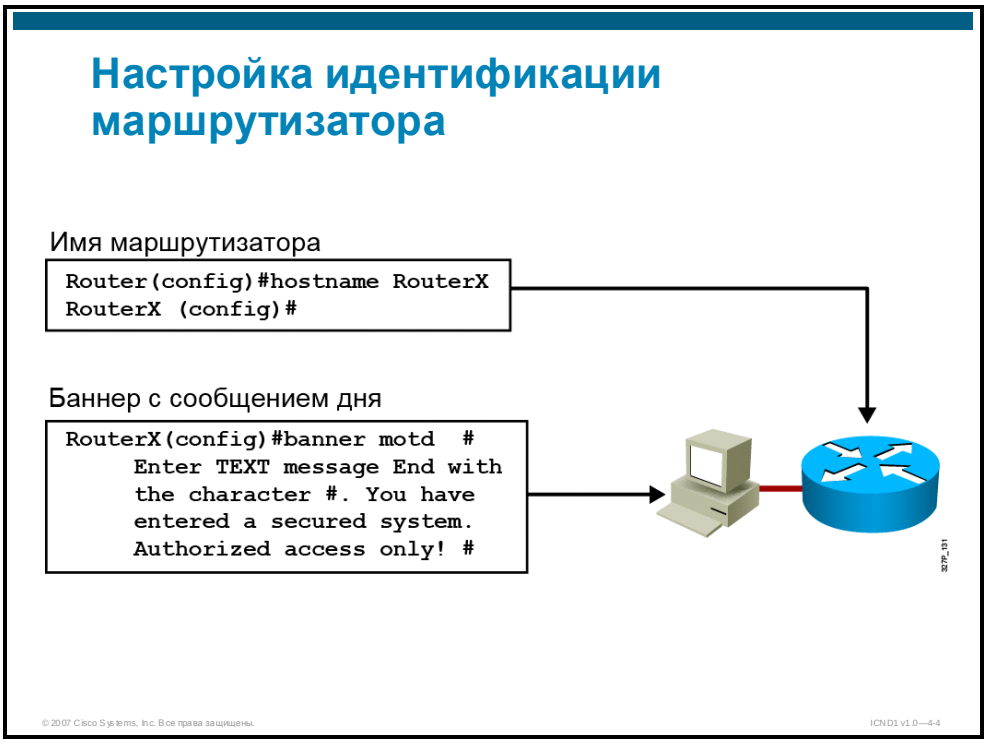
Обратите внимание, что при вводе основной команды выполняется переход из одного режима конфигурации в другой. Перед переходом в другой режим конфигурации не нужно возвращаться в режим глобальной конфигурации.



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

Настройка маршрутизатора Cisco с помощью интерфейса командной строки

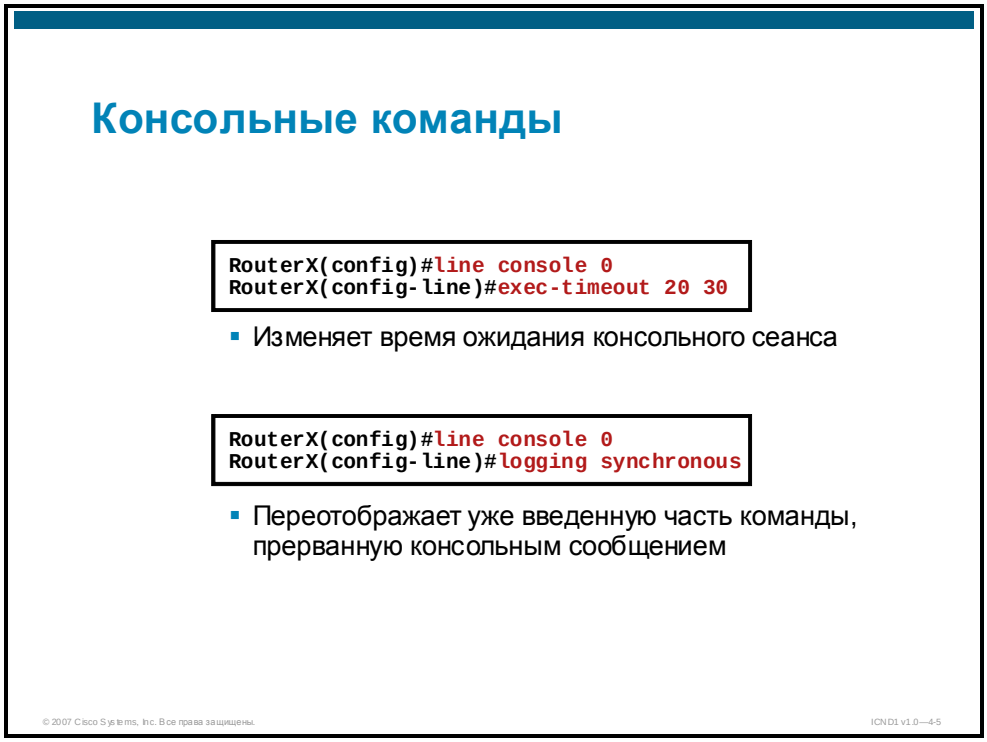
Интерфейс командной строки используется для настройки имени маршрутизатора, пароля и других консольных команд. В этом разделе описаны некоторые важные задачи конфигурации, включая настройку имени хоста и паролей.



Одна из первых задач конфигурации маршрутизатора заключается в назначении имени. Назначение имен маршрутизаторам помогает улучшить управление сетью, так как они позволяют однозначно определить каждый маршрутизатор в сети. Имя маршрутизатора считается именем хоста. Это имя отображается в приглашении системы. Если имя не задано, по умолчанию используется имя Router. Имя маршрутизатора задается в режиме глобальной конфигурации. В приведенном ниже примере для маршрутизатора задается имя RouterX.

Можно настроить баннер с сообщением дня (MOTD), который будет отображаться на всех подключенных терминалах. Баннер отображается при входе и позволяет выводить сообщения о таких событиях, как запланированные отключения системы, которые могут затронуть пользователей сети. После ввода команды **banner motd** поставьте за ней один или несколько пробелов и символ-разделитель по выбору. В этом примере в качестве символа-разделителя используется знак решетки (#). После ввода текста баннера завершите сообщение тем же символом-разделителем.

Кроме того, можно добавить описание интерфейса, которое поможет вспомнить сведения об интерфейсе, например сеть, обслуживаемую этим интерфейсом. Описание используется исключительно в качестве комментария по использованию данного интерфейса. Описание будет появляться в выводе данных конфигурации, сохраненной в памяти маршрутизатора, и в выводе команды **show interfaces**.

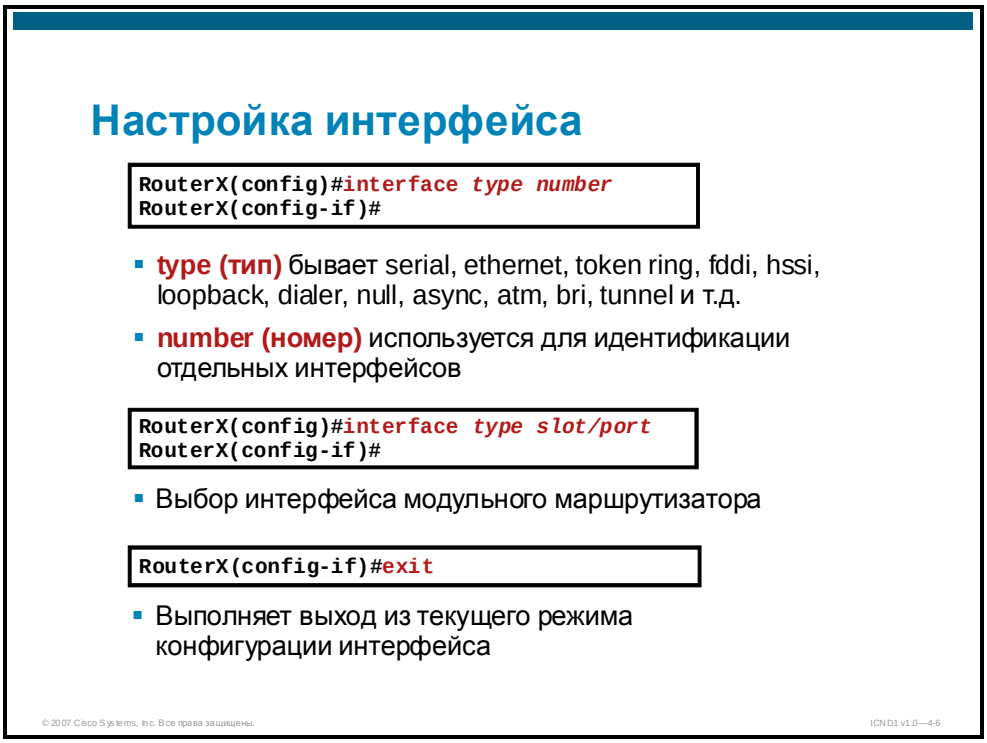


Другая полезная консольная команда – **exec-timeout**. На рисунке команда **exec-timeout** задает значение 20 минут и 30 секунд для времени ожидания перед выходом из сеанса EXEC консоли, которое переопределяет используемое по умолчанию значение 10 минут.

Команда консольного режима **logging synchronous** полезна в случае, если консольные сообщения отображаются, когда пользователь пытается ввести команды конфигурации или режима EXEC. В этом случае вывод на консоли перемешивается. После того, как данная команда сконфигурирована, после каждого выведенного консольного сообщения маршрутизатор будет заново выводить часть команды, уже введенной оператором к моменту появления сообщения. Это значительно упрощает чтение вводимых команд и сообщений.

Настройка интерфейсов маршрутизатора Cisco

Основная функция маршрутизатора – пересылка пакетов с одного сетевого устройства на другое. Для этого необходимо определить характеристики интерфейсов, через которые отправляются и принимаются пакеты. В этом разделе описаны команды, используемые для настройки интерфейсов на маршрутизаторе Cisco.



К характеристикам интерфейса маршрутизатора относится IP-адрес интерфейса, метод инкапсуляции канального уровня, тип среды передачи, полоса пропускания, частота синхронизации и т. д.

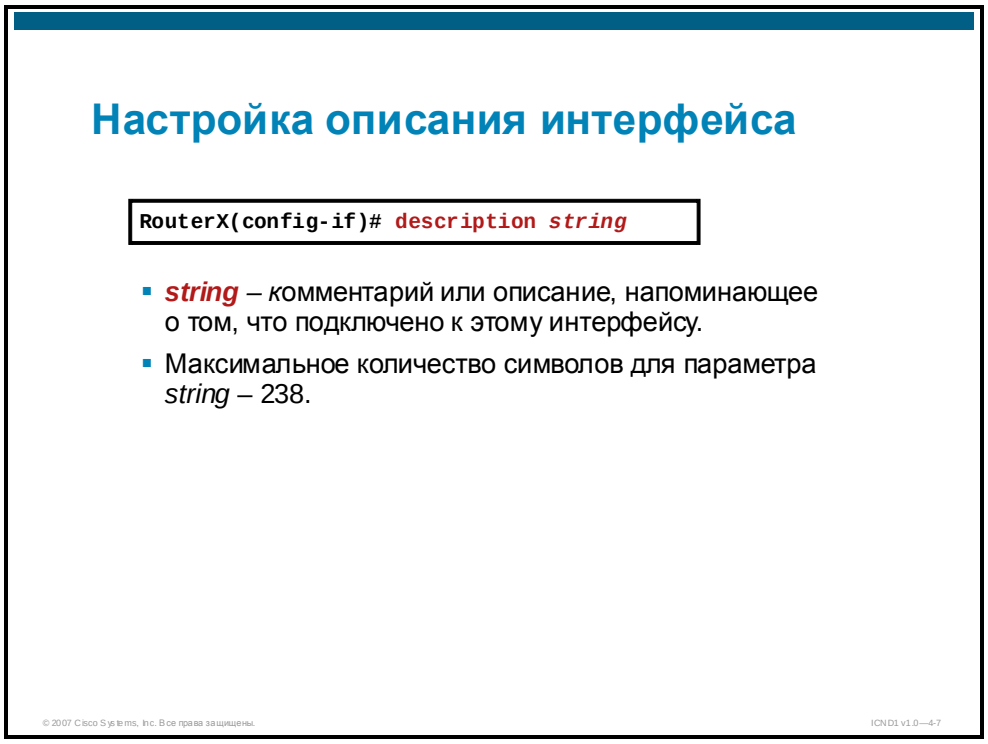
Многие функции можно включить на уровне интерфейса. Команды режима конфигурации интерфейса меняют режим работы Ethernet-интерфейса, последовательного интерфейса и многих других типов интерфейсов.
При вводе команды **interface** необходимо задать тип и номер интерфейса. Номер назначается каждому интерфейсу на основе физического расположения аппаратной части интерфейса на маршрутизаторе. Этот номер используется для идентификации каждого интерфейса. Эта идентификация важна, когда на одном маршрутизаторе работает несколько интерфейсов одинакового типа. Ниже приводятся примеры типа и номера интерфейса:

```
Router(config)#interface serial 0
Router(config)#interface fa 0/0
```

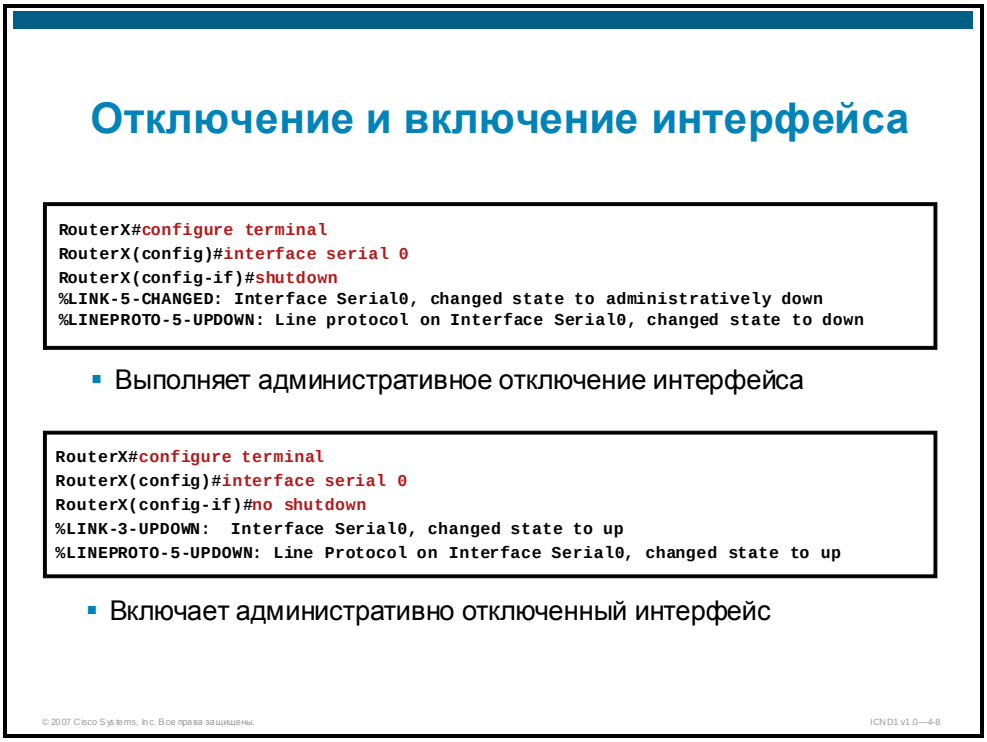
Интерфейсы маршрутизаторов Cisco с интегрированными службами серий 2800 и 3800 и других модульных маршрутизаторов указываются посредством номера физического слота на маршрутизаторе и номера порта в модуле этого слота следующим образом:

```
Router(config)#interface fa 1/0
```

Чтобы выйти из режима конфигурации интерфейса, введите команду **exit** в приглашении Router(config-if)#.



Чтобы добавить описание к конфигурации интерфейса, используйте команду **description** в режиме конфигурации интерфейса. Чтобы удалить описание, используйте версию «**no**» этой команды.



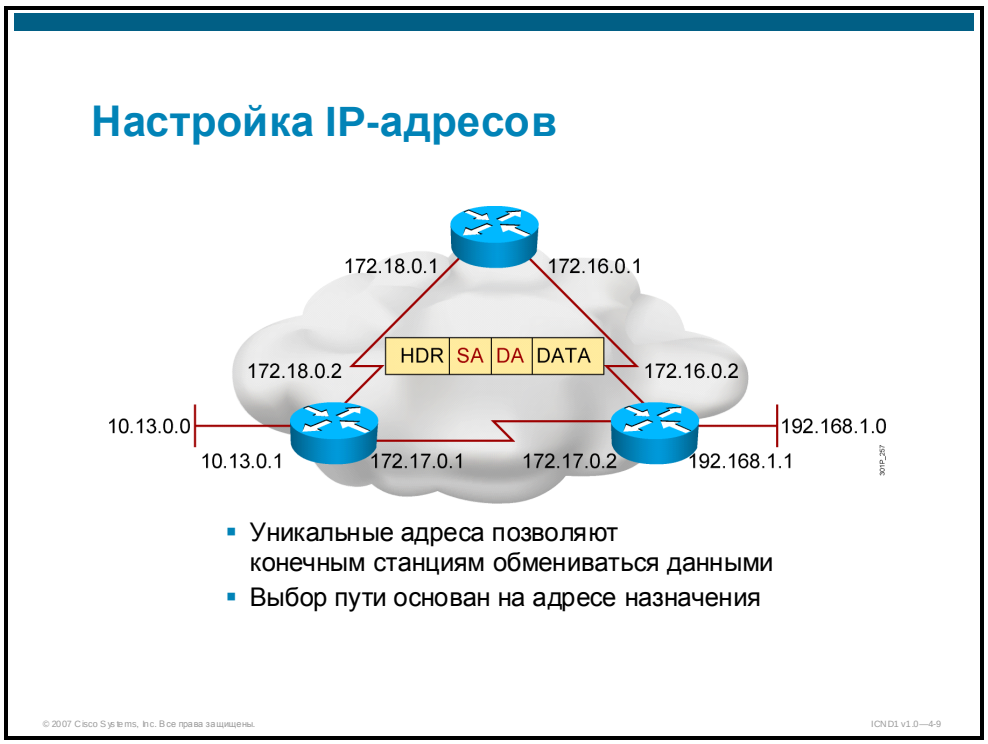
Для обслуживания определенного интерфейса или сегмента сети может потребоваться отключение интерфейса. Кроме того, если возникли проблемы в определенном сегменте сети или необходимо изолировать этот сегмент от остальной части сети, интерфейс также следует отключить.

Подкоманда **shutdown** выполняет административное отключение интерфейса. Для восстановления работы интерфейса используется подкоманда **no shutdown**.

Если интерфейс настраивается впервые и не в режиме установки (setup), перед использованием этого интерфейса для передачи и получения пакетов его необходимо включить административно. Используйте подкоманду **no shutdown**, чтобы разрешить ПО Cisco IOS использовать интерфейс.

Настройка IP-адреса маршрутизатора Cisco

У каждого маршрутизатора Cisco должен быть собственный IP-адрес для однозначной идентификации этого маршрутизатора в сети. В этом разделе приводятся инструкции по настройке IP-адреса для всех интерфейсах маршрутизатора Cisco.

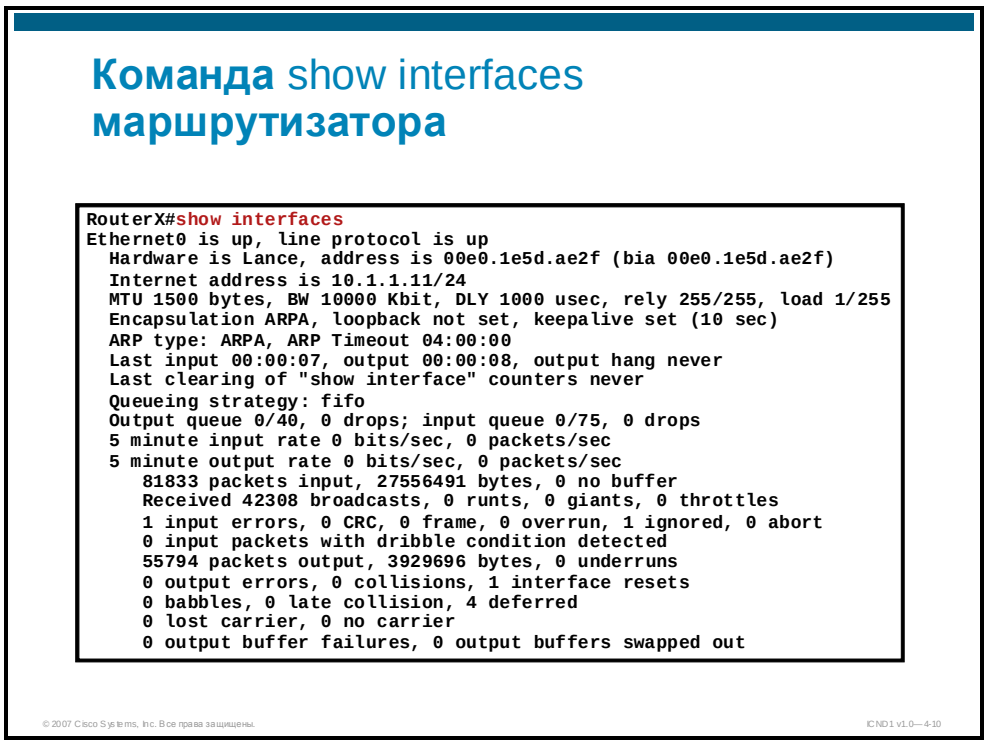


Чтобы настроить интерфейс на маршрутизаторе Cisco, выполните следующие действия.

№	Действие	Результаты и примечания
1.	Войдите в режим глобальной конфигурации с помощью команды **configure terminal**. `Router#`**`configure terminal`**	Эта команда выводит новое приглашение: `Router(config)#`
2.	Укажите интерфейс, которому необходим IP-адрес, с помощью команды **interface** *тип слот/порт*. `Router(config)#`**`interface fa 0/0`**	Эта команда выводит новое приглашение, например: `Router(config-if)#`
3.	Задайте IP-адрес и маску подсети для интерфейса с помощью команды **ip address** *ip-адрес маска*. `Router(config-if)#`**`ip address 192.168.1.1 255.255.255.0`**	Эта команда настраивает IP-адрес и маску подсети для выбранного интерфейса.
4.	Включите интерфейс, изменив состояние «administratively down» на состояние «up» с помощью команды **no shutdown**. `Router(config–if)#`**`no shutdown`**	Эта команда включает текущий интерфейс.
5.	Выйдите из режима конфигурации интерфейса с помощью команды **exit**. `Router(config–if)#`**`exit`**	Эта команда выводит приглашение режима глобальной конфигурации. `Router(config)#`

Проверка конфигурации интерфейса

После завершения настройки интерфейса маршрутизатора можно проверить конфигурацию с помощью команды **show interfaces**. В этом разделе описаны команды **show** и их вывод, который можно использовать для проверки конфигурации.



В выводе команды **show interfaces** отображаются сведения о состоянии и статистические данные для всех сетевых интерфейсов маршрутизатора. Кроме того, для получения сведений о состоянии определенного интерфейса можно использовать команду **show interfaces тип номер**. В следующей таблице описываются поля вывода для интерфейса Ethernet и их расшифровка.

Вывод	Описание
`Ethernet...is {up | down | administratively down}`	Указывает текущее состояние аппаратной части интерфейса. Интерфейс может быть активен, отключен или отключен администратором.
`line protocol is {up | down}`	Указывает, рассматривается ли данный интерфейс программными процессами, обслуживающими канальный протокол, как пригодный к использованию (то есть успешно ли приняты сообщения «keepalive»). Если интерфейс пропускает три сообщения «keepalive» подряд, канальный протокол помечается как отключенный.
`Hardware`	Адрес и тип оборудования (например, MCI Ethernet, интерфейс последовательных соединений [SCI], cBus Ethernet).
`Internet address`	IP-адрес и длина префикса (маска подсети).
`MTU`	Максимальный размер блока (MTU) для интерфейса.

Вывод	Описание
BW	Полоса пропускания интерфейса в килобайтах в секунду. Параметр полосы пропускания используется для расчета метрик протоколов маршрутизации и других вычислений.
DLY	Задержка интерфейса в микросекундах.
rely	Надежность интерфейса в долях 255 (255/255 соответствует стопроцентной надежности), рассчитываемая как экспоненциальное среднее за 5 минут.
load	Загрузка интерфейса в долях 255 (255/255 соответствует полной загрузке), рассчитываемая как экспоненциальное среднее за 5 минут.
Encapsulation	Метод инкапсуляции, назначенный интерфейсу.
keepalive	Указывает, настроены ли сообщения «keepalive».
ARP type:	Тип назначенного протокола ARP.
loopback	Указывает, настроен ли интерфейс обратной связи.
Last input	Количество часов, минут и секунд с момента успешного получения последнего пакета интерфейсом. Это значение позволяет определить момент прекращения работы интерфейса.
output	Количество часов, минут и секунд с момента успешной передачи последнего пакета интерфейсом. Это значение позволяет определить момент прекращения работы интерфейса.
output hang	Количество часов, минут и секунд (или никогда) с момента последнего сброса интерфейса из-за слишком большого времени передачи. Если количество часов в любом из предыдущих полей превысит 24 часа, печатается количество дней и часов. Если это поле переполнено, печатаются звездочки.
Last clearing	Время последнего сброса значений счетчиков в 0, определяющих совокупные статистические данные, отображаемые в этом отчете (например, количество переданных и полученных байт). Обратите внимание, что переменные, которые могут влиять на маршрутизацию (например, загрузка и надежность) не удаляются при сбросе значений счетчиков. Звездочки указывают, что истекшее время слишком велико для отображения.
Output queue, input queue, drops	Количество пакетов в очередях ввода и вывода. После каждого числа вводится косая черта (/), максимальный размер очереди и число отброшенных пакетов из-за переполнения очереди.
Five minute input rate, Five minute output rate	Среднее количество переданных бит и пакетов в секунду за последние 5 минут. Если для интерфейса не используется promiscuous (доверенный) режим, он отображает только отправляемый и получаемый сетевой трафик (а не весь сетевой трафик). Скорости входящего и исходящего потока за пятиминутный интервал должны пониматься только как приблизительные значения в течение данного пятиминутного интервала. Эти скорости являются экспоненциально средневзвешенными значениями с константой времени, равной 5 минутам. До того момента, как среднее значение будет находиться в пределах 2 процентов от текущей скорости равномерного потока трафика за этот период, должен пройти период времени, равный четырем таким пятиминутным интервалам.
packets input	Общее количество безошибочных пакетов, полученных системой.
bytes input	Общее количество байт, включая инкапсуляцию MAC-адресов и данных, в безошибочных пакетах, полученных системой.

Вывод	Описание
`no buffers`	Количество полученных пакетов, которые были отброшены из-за недостатка места в буфере в основной системе. Сравнивается со значением «ignored count». Недостаток места в буфере входящих пакетов часто связан с широковещательными штормами Ethernet.
`Received...broadcasts`	Общее количество широковещательных или групповых пакетов, полученных интерфейсом. Количество широковещательных пакетов должно быть по возможности минимальным. Приблизительное пороговое значение – менее 20 процентов от общего количества входящих пакетов.
`runts`	Количество кадров Ethernet, отброшенных из-за того, что их размер меньше минимально допустимого размера кадра Ethernet. Все кадры Ethernet с размером менее 64 байт считаются слишком маленькими (runt). Обычно слишком маленькие кадры вызваны коллизиями. Если на миллион полученных байт приходится более одного слишком маленького кадра, следует выяснить причину этой проблемы.
`giants`	Количество кадров Ethernet, которые отброшены из-за превышения максимально допустимого размера кадра Ethernet. Все кадры Ethernet с размером более 1 518 байт считаются слишком большими (giant).
`input error`	Содержит количество слишком маленьких и слишком больших кадров, кадров, отброшенных из-за отсутствия места в буфере, несоответствия циклического контроля избыточности (CRC), превышения установленных пределов, и проигнорированных пакетов. Другие ошибки, относящиеся к вводу, также могут увеличивать количество ошибок ввода, а в некоторых датаграммах может быть несколько ошибок. Поэтому эта сумма может не совпадать со значениями счетчиков ошибок ввода.
`CRC`	CRC, созданная станцией-источником в ЛВС или удаленном конечным устройстве, не совпадает с контрольной суммой, рассчитанной для полученных данных. В ЛВС это обычно указывает на шум или проблемы передачи в интерфейсе или шине ЛВС. Большое значение CRC обычно является результатом коллизий или передачи станцией неправильных данных.
`frame`	Количество полученных пакетов с ошибкой CRC и дробным числом октетов. В ЛВС это обычно обусловлено коллизиями или неисправностью устройства Ethernet.
`overrun`	Число неудачных попыток обработки получаемых данных приемником из-за слишком большой скорости передачи выходных данных, превышающей возможности обработки данных приемником.
`ignored`	Количество полученных пакетов, проигнорированных интерфейсом из-за недостатка места во внутренних буферах аппаратного интерфейса. Эти буферы отличаются от системных буферов, указанных в описании буфера. Широковещательные штормы и шумовые всплески могут приводить к увеличению количества проигнорированных пакетов.
`input packets with dribble condition detected`	Битовая ошибка указывает, что кадр слишком длинный. Значение счетчика ошибок кадров увеличивается только для информационных целей; маршрутизатор принимает этот кадр.
`packets output`	Общее количество сообщений, переданных системой.
`bytes`	Общее количество байт, включая инкапсуляцию MAC-адресов и данных, переданных системой.
`underruns`	Количество раз, когда скорость приемопередатчика превышала скорость обработки данных маршрутизатором. Для некоторых интерфейсов эти данные могут не выводиться.

Вывод	Описание
`output errors`	Сумма всех ошибок, которые мешали окончательной передаче датаграмм из анализируемого интерфейса. Обратите внимание, что эта сумма может не совпадать с суммой перечисленных ошибок в выводе, поскольку в некоторых датаграммах может быть несколько ошибок, а в других могут быть ошибки, которые не относятся к перечисленным в таблице категориям.
`collisions`	Количество сообщений, передаваемых повторно из-за коллизии Ethernet. Обычно это связано со слишком обширной ЛВС (слишком длинный кабель приемопередатчика или Ethernet, более двух повторителей между станциями или слишком много каскадных многопортовых приемопередатчиков). Пакет, вызвавший коллизию, учитывается только один раз в выходных пакетах.
`interface resets`	Количество полных сбросов интерфейса. Это может происходить в случае, если пакеты из очереди для передачи не были отправлены в течение нескольких секунд. В последовательной линии это может происходить при неисправности модема, который не подает сигнал синхронизации передачи, или проблем с кабелем. Если система обнаруживает, что линия обнаружения несущей (CD) последовательного интерфейса работает, но канальный протокол отключен, она периодически сбрасывает интерфейс, чтобы перезапустить его. Сброс интерфейса также может происходить, если интерфейс зациклен на себя или отключен.

Один из наиболее важных элементов вывода команды **show interfaces** – состояние линии и протокола канального уровня. На рисунке показана ключевая сводная строка для проверки и расшифровки состояния последовательного интерфейса. Для других типов интерфейсов содержание строки состояния может несколько отличаться.

Первый параметр относится к аппаратному уровню и, по сути, указывает, получен ли интерфейсом сигнал обнаружения несущей от устройства на другой стороне канала (DCE). Второй параметр относится к канальному уровню. Он указывает, принимаются ли сообщения «keepalive» протокола канального уровня.

Используя вывод команды **show interfaces**, можно устранить возможные проблемы следующим образом:

- Если интерфейс включен, а канальный протокол не функционирует, возникает проблема. Возможные причины проблемы:
  - отсутствие сообщений «keepalive»;
  - несоответствие типа инкапсуляции.
- Если не работает ни канальный протокол, ни интерфейс, наиболее вероятная причина – неподключенный кабель, однако возможны и другие проблемы с интерфейсом. Например, может быть административно отключена другая сторона подключения.
- Если интерфейс отключен административно, он был отключен вручную (с помощью команды **shutdown**) в текущей конфигурации.

Проверка конфигурации последовательного интерфейса

```
RouterX#show interface serial s0/0/0
Serial0/0 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Internet address is 10.140.4.2/24
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input 00:00:09, output 00:00:04, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
(дальше выходные данные опущены)
```


После настройки последовательного интерфейса используйте команду **show interface serial** для проверки изменений. Обратите внимание, что теперь этот канал включен, а полоса пропускания имеет значение 64 Кбит/с.

Резюме

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

Резюме

- Из привилегированного режима EXEC можно перейти в режим глобальной конфигурации, предоставляющий доступ к другим режимам конфигурации, таким как режим конфигурации интерфейса или режим конфигурации линии.
- Основная функция маршрутизатора – передача пакетов с одного сетевого устройства на другое. Для этого необходимо определить характеристики интерфейсов, через которые должны отправляться и приниматься пакеты. Характеристики интерфейсов, такие как IP-адрес и полоса пропускания, задаются в режиме конфигурации интерфейса.

Резюме (прод.)

- В среде TCP/IP конечные станции эффективно обмениваются данными с серверами и другими конечными станциями. Этот обмен данными возможен благодаря наличию уникальных 32-разрядных логических IP-адресов у всех узлов, использующих пакет протоколов TCP/IP.
- После завершения настройки интерфейса маршрутизатора используйте команды **show** для ее проверки

Занятие 6

Изучение процесса доставки пакетов данных

Обзор

Чтобы понять принцип работы сетевых устройств Cisco, необходимо изучить процесс доставки пакетов данных. Для администрирования сети необходимо понимание процесса обмена данными между хостами с использованием маршрутизаторов. На этом занятии описывает обмен данными между хостами через маршрутизатор в графическом представлении.

Задачи

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

- описывать адресацию второго уровня;
- описывать адресацию третьего уровня;
- описывать процесс доставки пакетов данных между хостами;
- объяснять использование команды **show ip arp**;
- описывать использование стандартных средств ПО Cisco IOS для проверки связи.

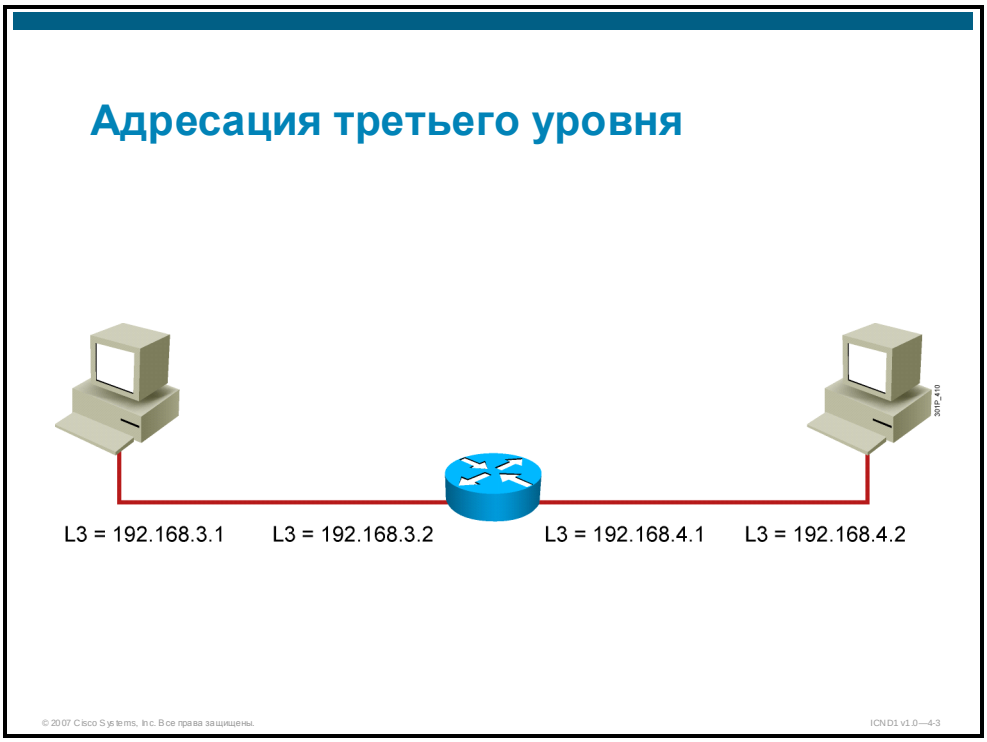
Адресация второго уровня

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

MAC-адреса присваиваются таким конечным устройствам, как хосты. Физические интерфейсы маршрутизатора обеспечивают функции второго уровня, поэтому им назначается MAC-адрес.

Адресация третьего уровня

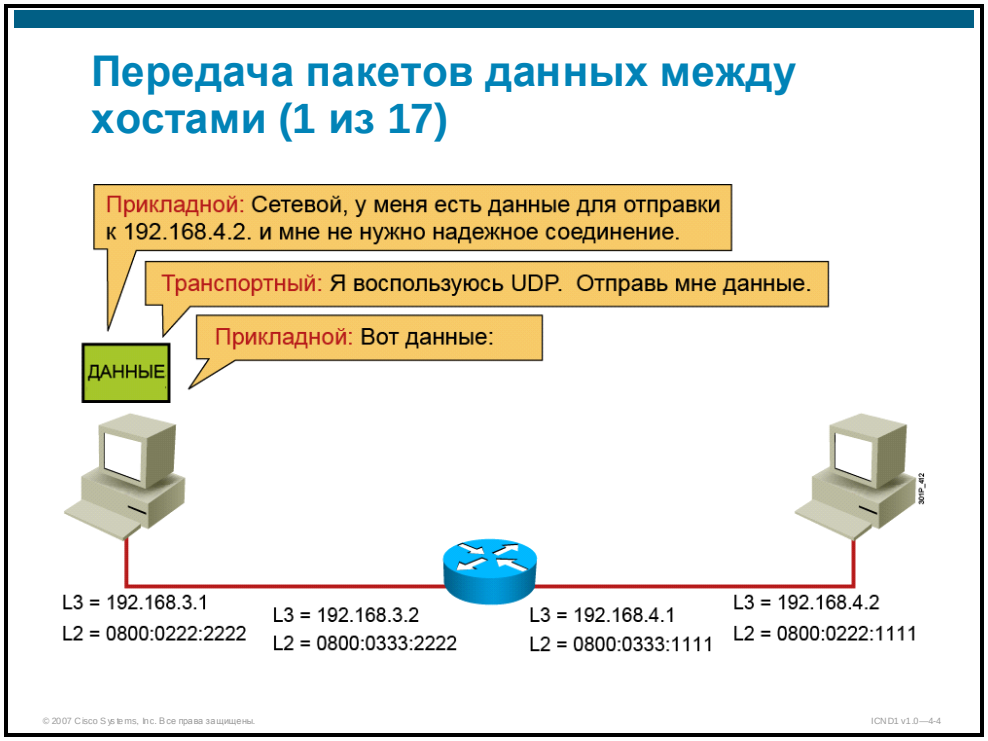
В этом разделе рассматривается роль адресации третьего уровня в модели обмена данными между хостами.



Маршрутизатор имеет отдельный адрес третьего уровня для каждого интерфейса.

Доставка пакетов между хостами

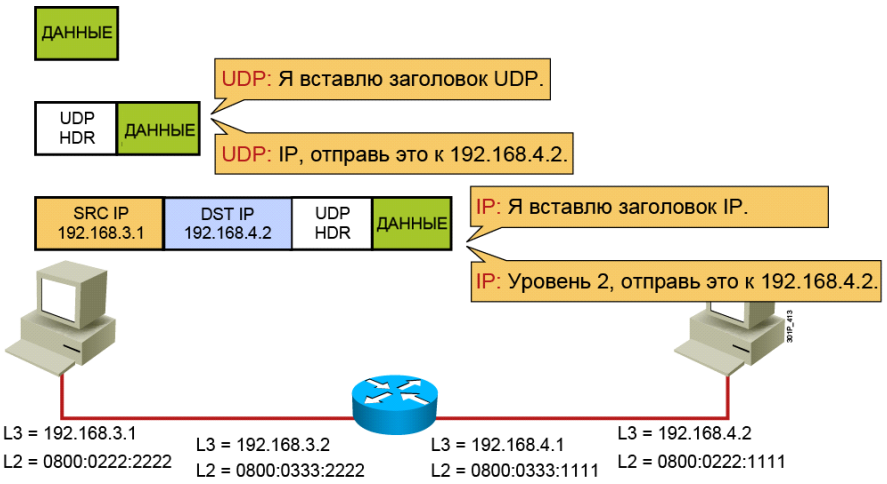
Процесс доставки IP-пакета в маршрутизируемой сети похож на процесс доставки письма по почте. В этом разделе рассматривается процесс доставки IP-пакета.



Процесс доставки IP-пакета в маршрутизируемой сети содержит несколько этапов.

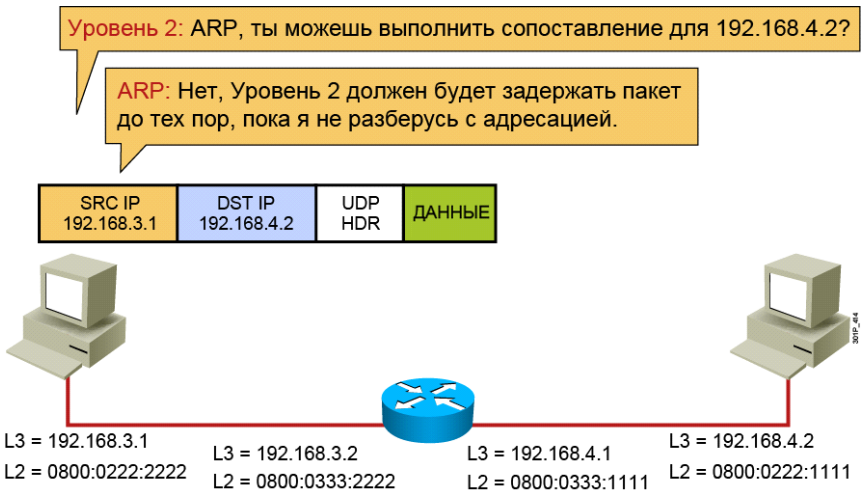
Хост отправляет пакет, не предназначенный для локальной IP-сети, шлюзу по умолчанию. Шлюз по умолчанию – адрес локального маршрутизатора, который должен настраиваться на хостах (ПК, серверах и т. д.).

Передача пакетов данных между хостами (2 из 17)



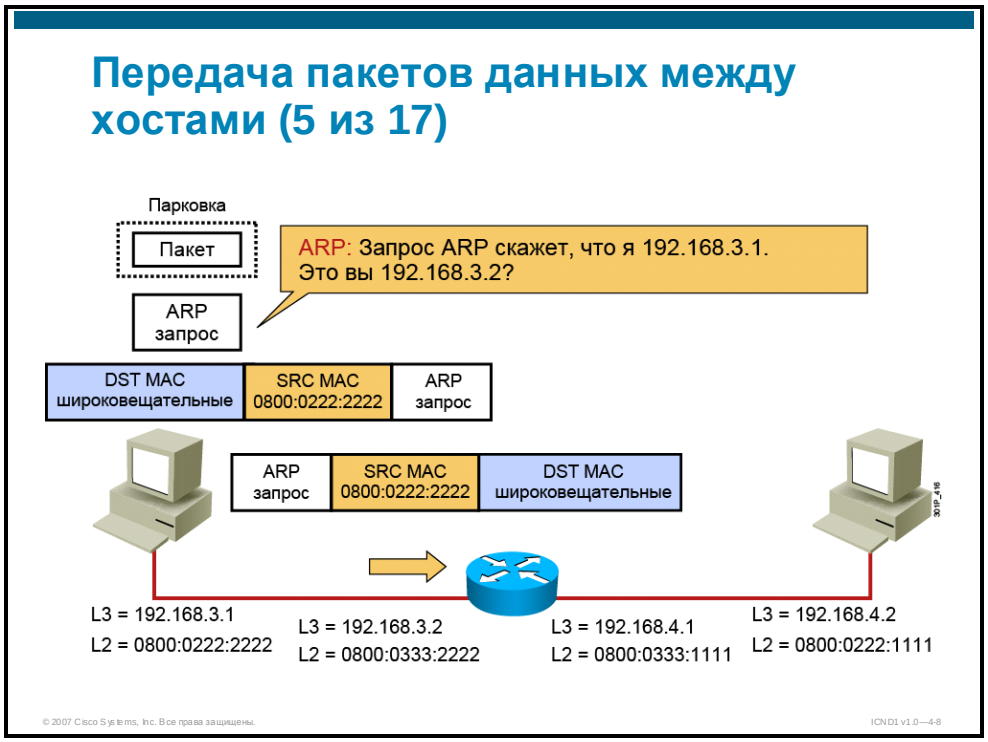
В этом примере хосту 192.168.3.1 необходимо передать данные хосту 192.168.4.2. При этом приложение не нуждается в надежном соединении, поскольку выбран протокол UDP (User Datagram Protocol).

Передача пакетов данных между хостами (3 из 17)

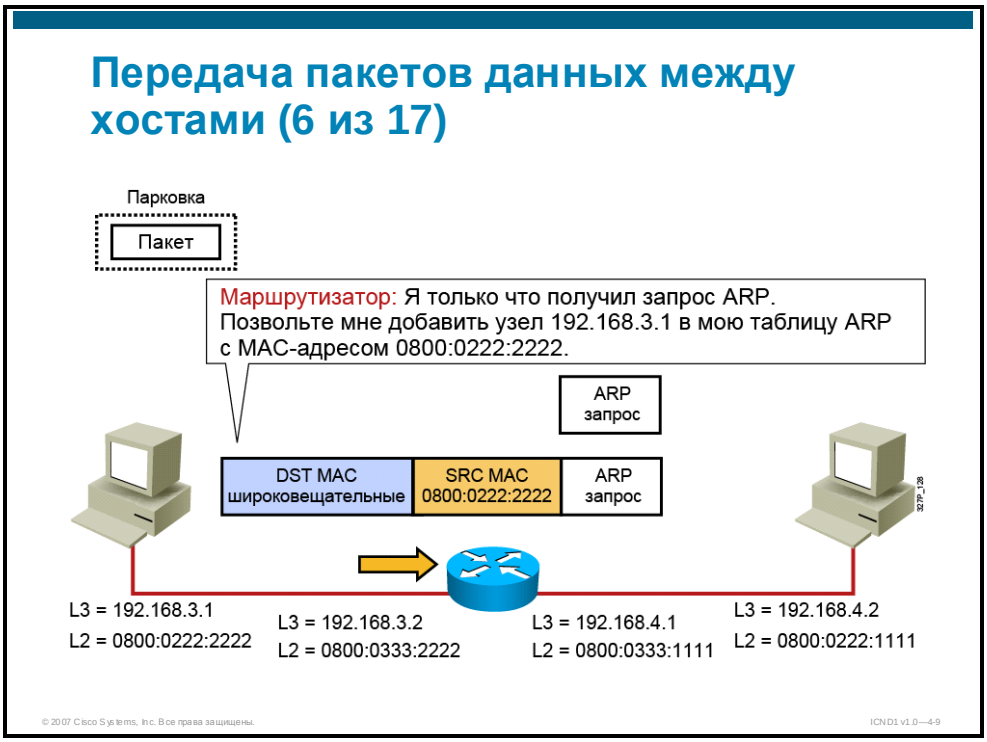


Поскольку установление сеанса связи не требуется, приложение может начать передачу данных. Протокол UDP добавляет в начало пакета заголовок UDP и передает элемент информации протокола (PDU) на уровень IP (третий уровень) с инструкцией отправить этот PDU хосту 192.168.4.2. IP инкапсулирует PDU в пакет третьего уровня и передает его на второй уровень.

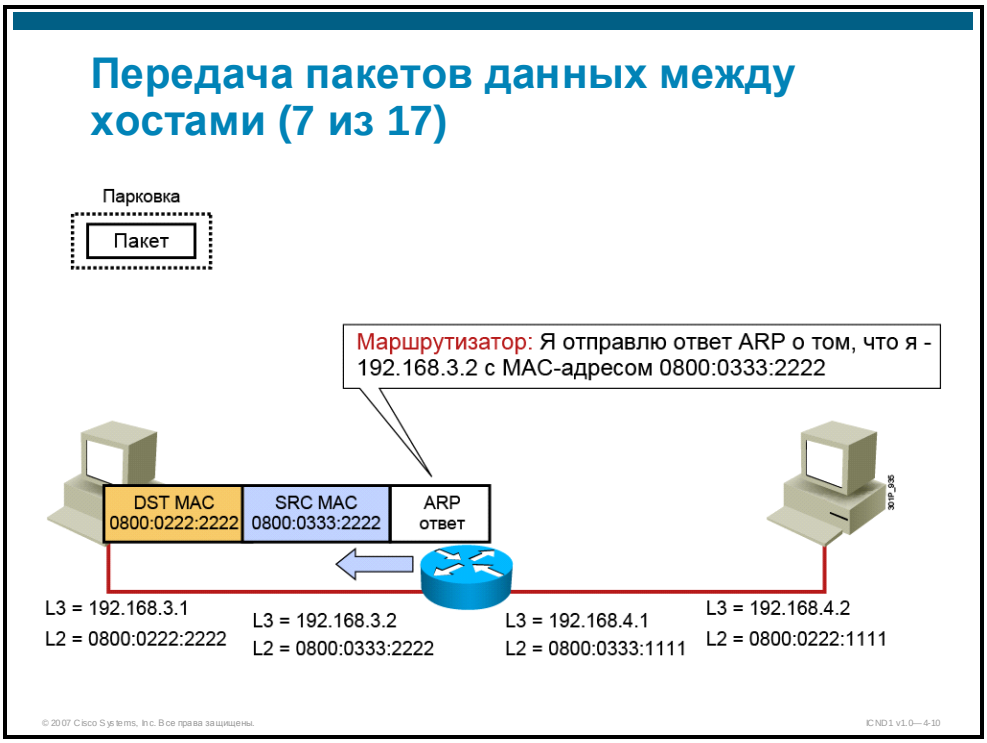
В таблице ARP (Address Resolution Protocol) нет записи.



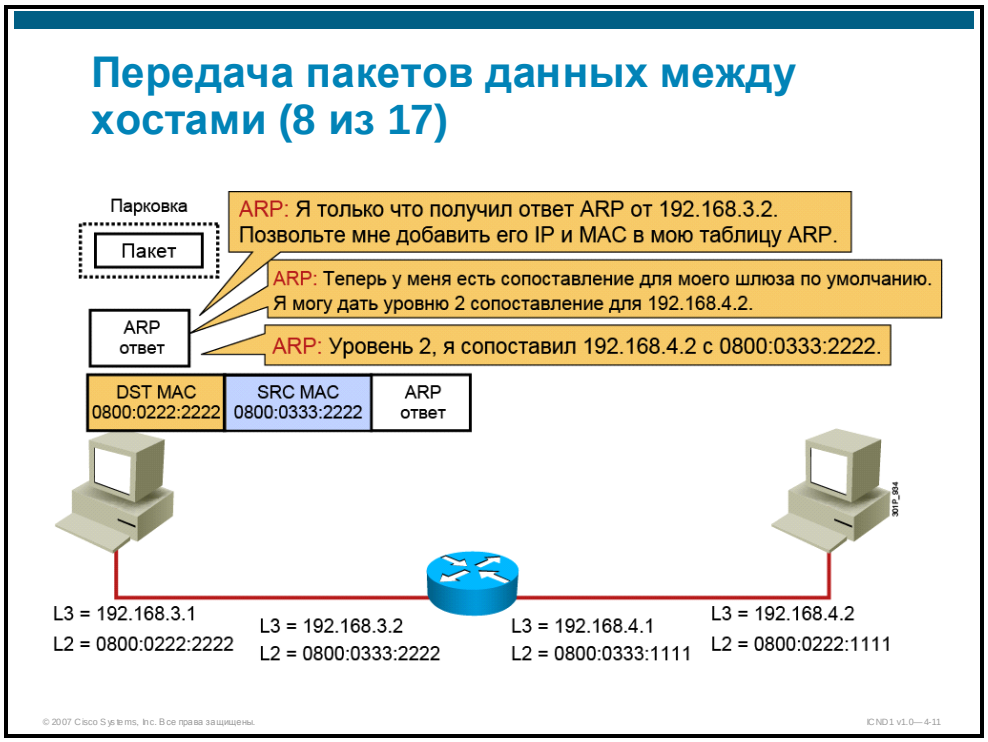
Этот пример отличается от предыдущих. Два хоста относятся к разным сегментам: 192.168.3.0/24 и 192.168.4.0/24. Поскольку на этом хосте не выполняется протокол маршрутизации, он не знает, как достичь другого сегмента. Он должен отправить кадр шлюзу по умолчанию, который может переслать этот кадр. Если у хоста нет привязки к шлюзу по умолчанию, он использует стандартный процесс ARP для получения этой привязки.



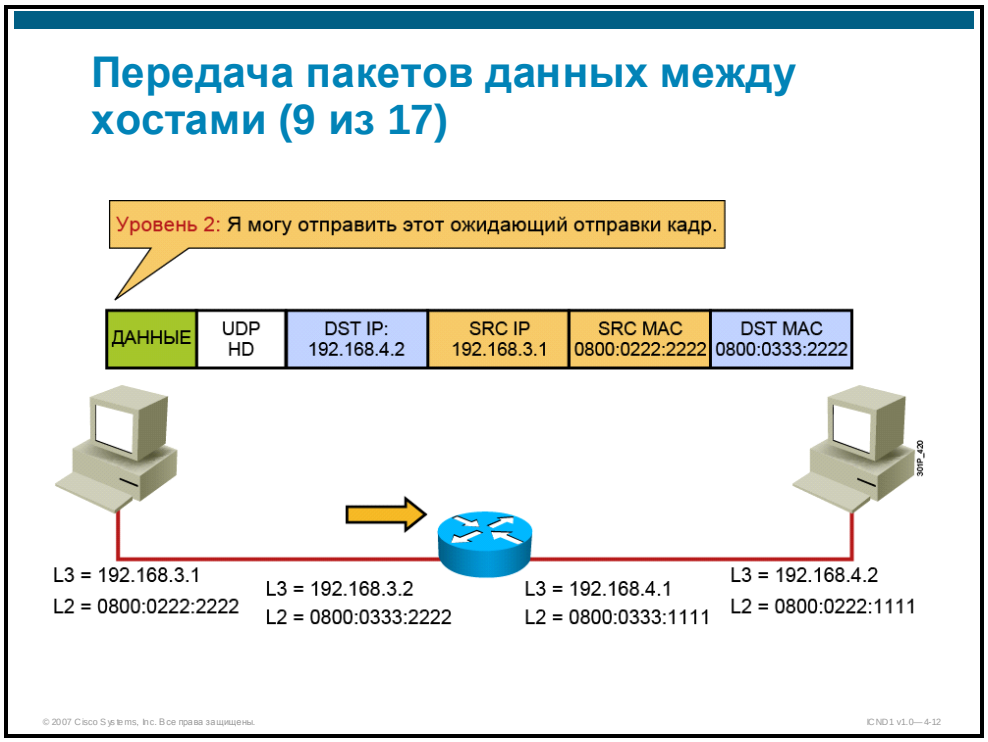
Пользователь программно задал IP-адрес 192.168.3.2 для шлюза по умолчанию. Хост 192.168.3.1 отправляет запрос ARP, который получает маршрутизатор.



Маршрутизатор обрабатывает запрос ARP так же, как любой другой хост.

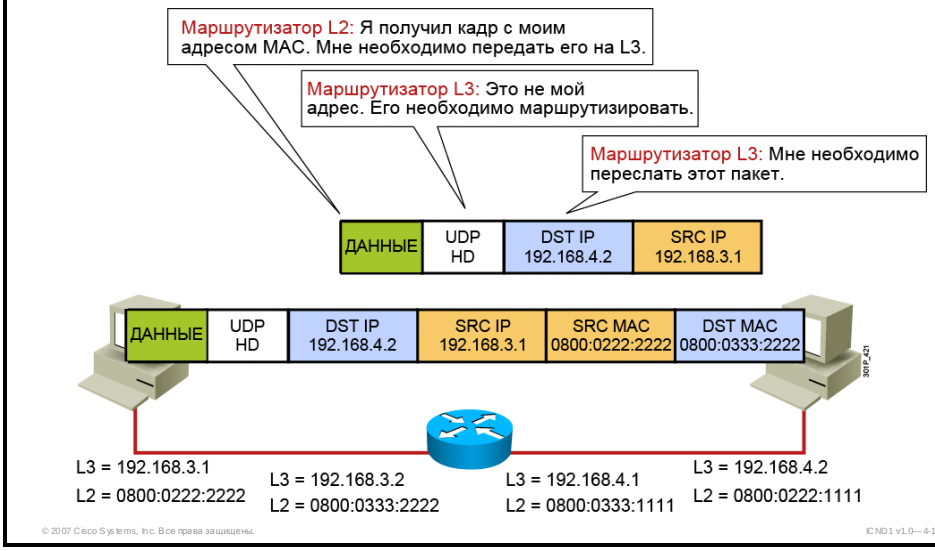


На запрос ARP отправляется ответ.



Хост назначения получает запрос ARP. Теперь второй уровень может передать ответ. Обратите внимание, что ARP сообщает о привязке IP-адреса назначения (192.168.4.2) к MAC-адресу шлюза по умолчанию, а не фактическому MAC-адресу назначения.

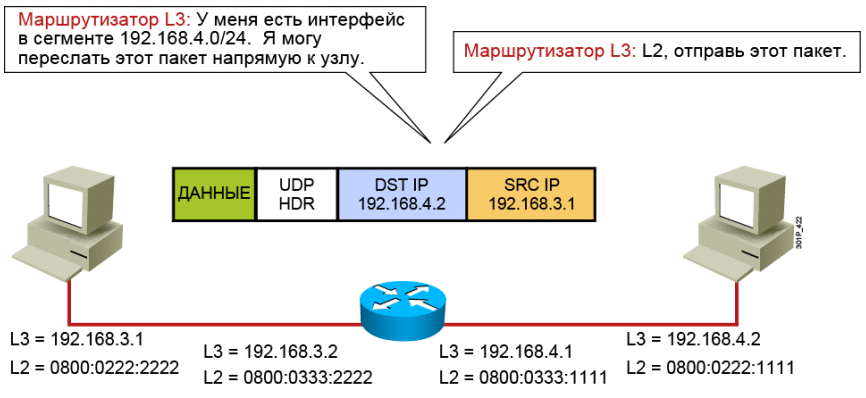
Передача пакетов данных между хостами (10 из 17)



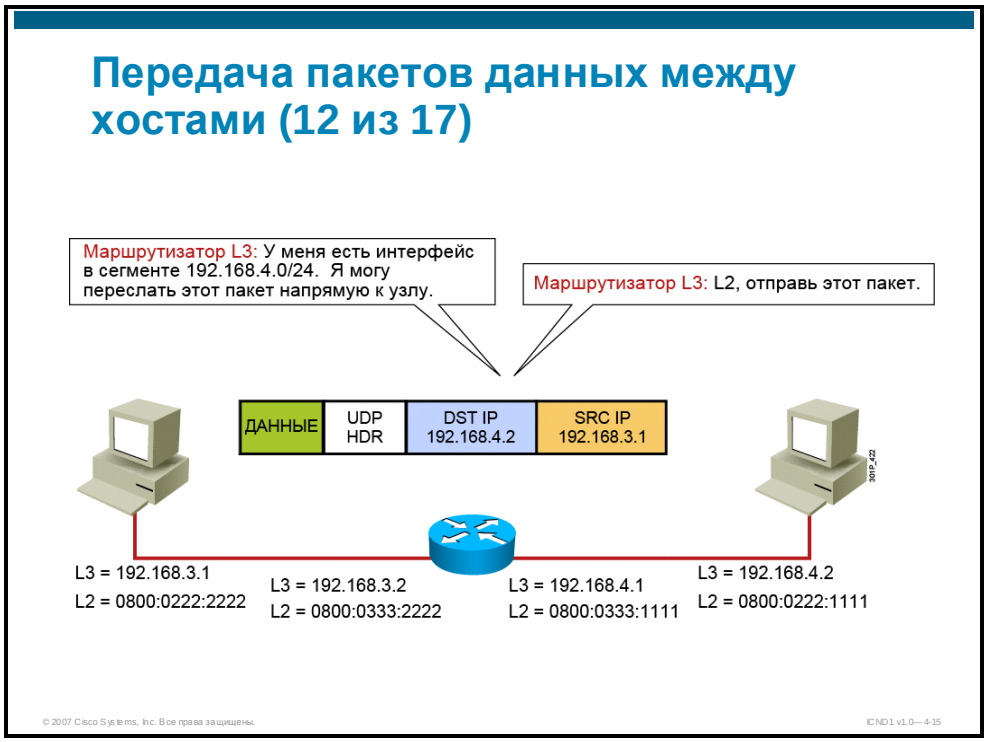
Ожидающий кадр отправляется с использованием IP-адреса и MAC-адреса локального хоста в качестве источника. Однако IP-адрес назначения соответствует удаленному хосту, а MAC-адрес назначения – шлюзу по умолчанию.

Передача пакетов данных между хостами (11 из 17)

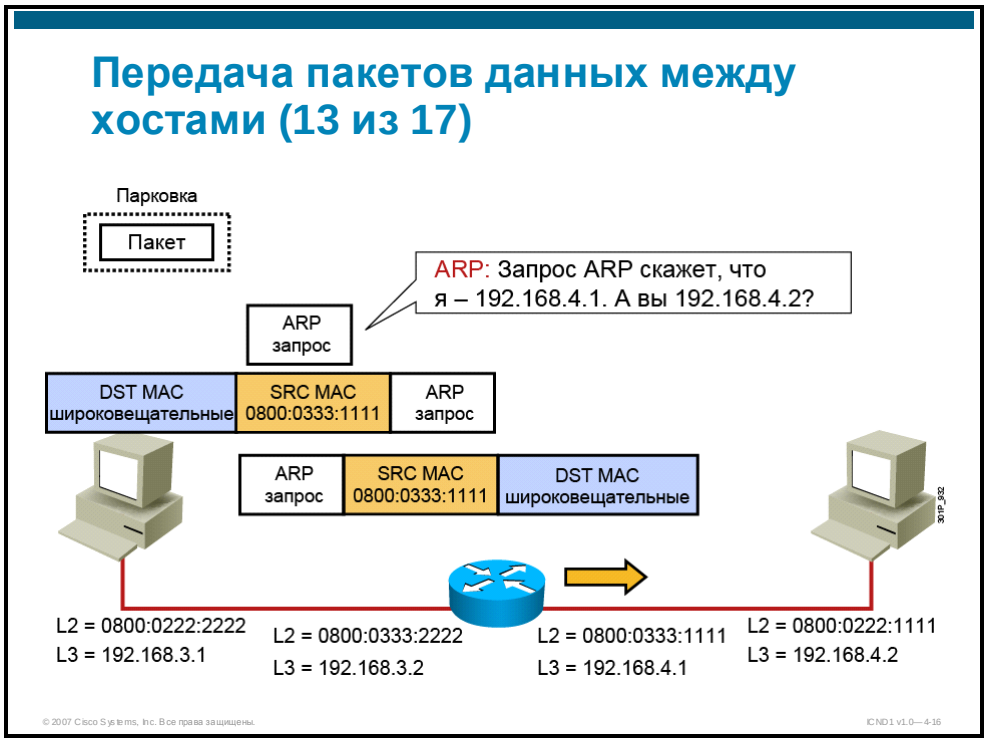
Назначение	Следующий переход	Интерфейс
192.168.3.0/24	Подключено	fa 0/0
192.168.4.0/24	Подключено	fa 0/1



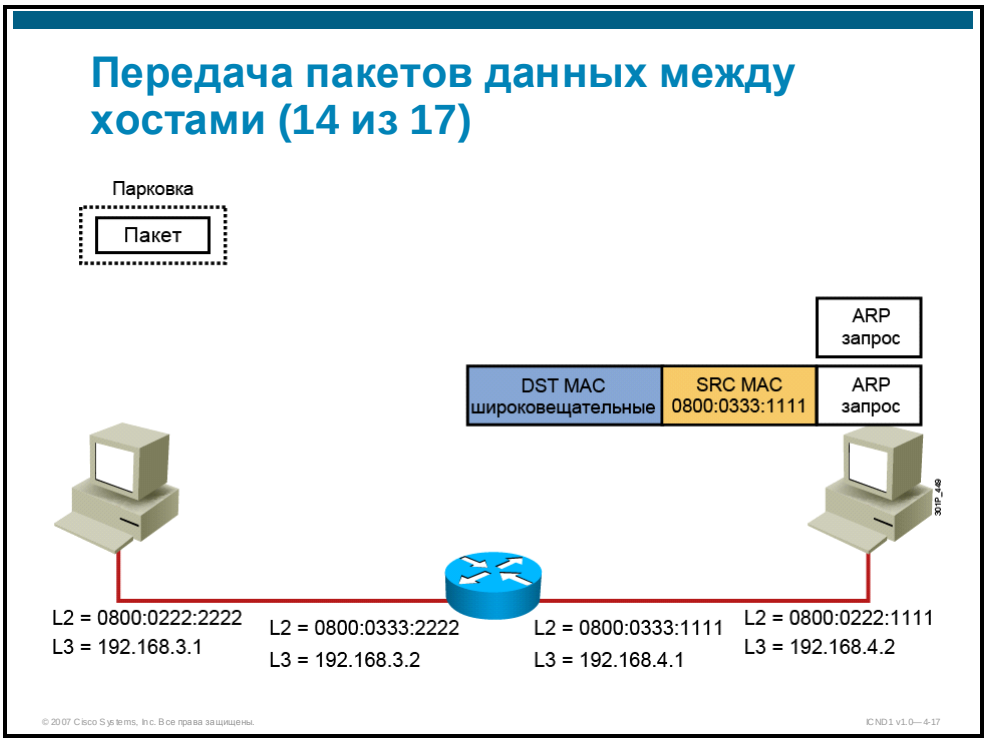
Когда маршрутизатор получает этот кадр, он распознает MAC-адрес и обрабатывает его. На третьем уровне маршрутизатор видит, что IP-адрес назначения не совпадает с его адресом. Хосты третьего уровня отбрасывают такие кадры. Однако поскольку это маршрутизатор, он передает все пакеты, которые относятся к неизвестным местам назначения, процессу маршрутизации.



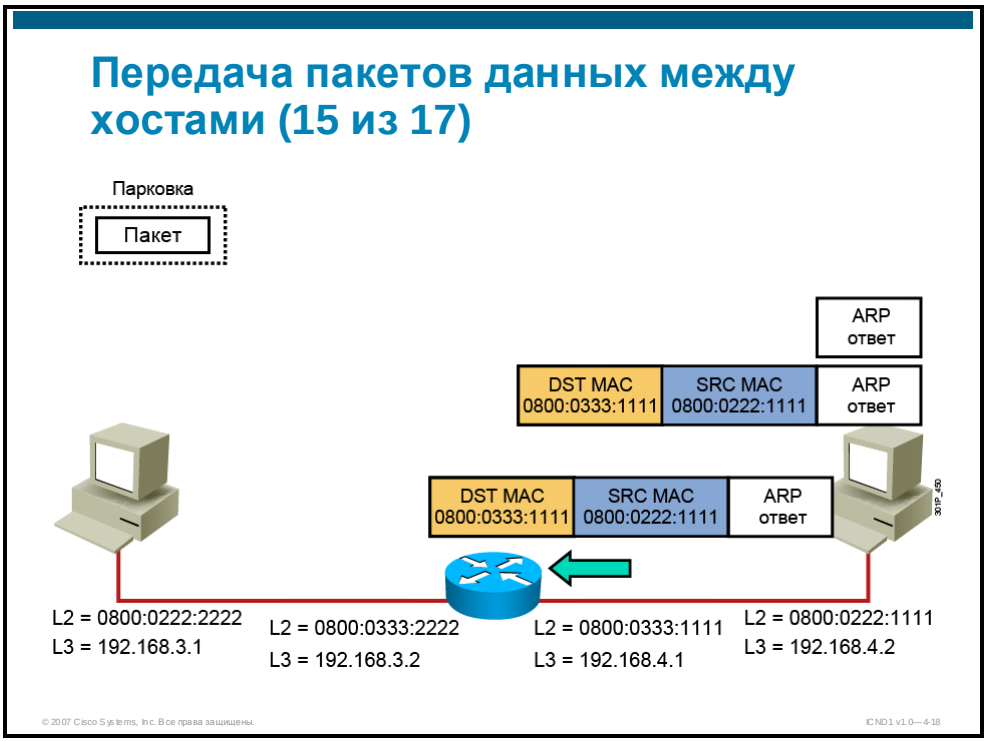
Процесс маршрутизации ищет IP-адрес назначения в своей таблице маршрутизации. В этом примере сегмент назначения подключен непосредственно. Поэтому процесс маршрутизации передает этот пакет прямо на второй уровень для соответствующего интерфейса.



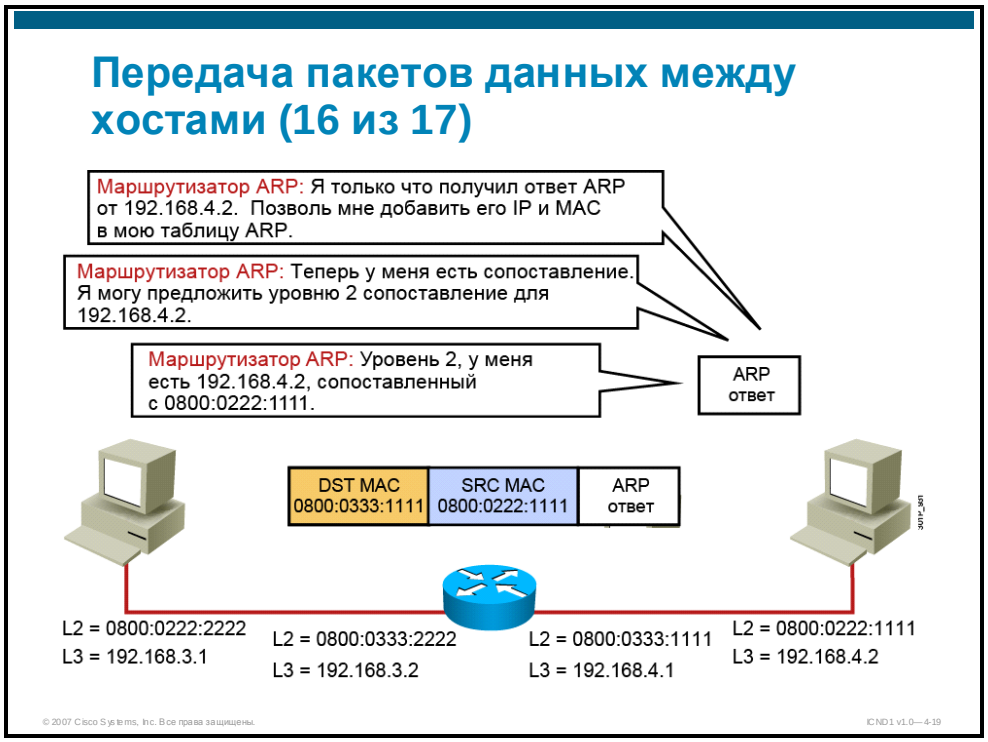
Чтобы получить привязку IP-адреса к MAC-адресу, второй уровень будет использовать процесс ARP.



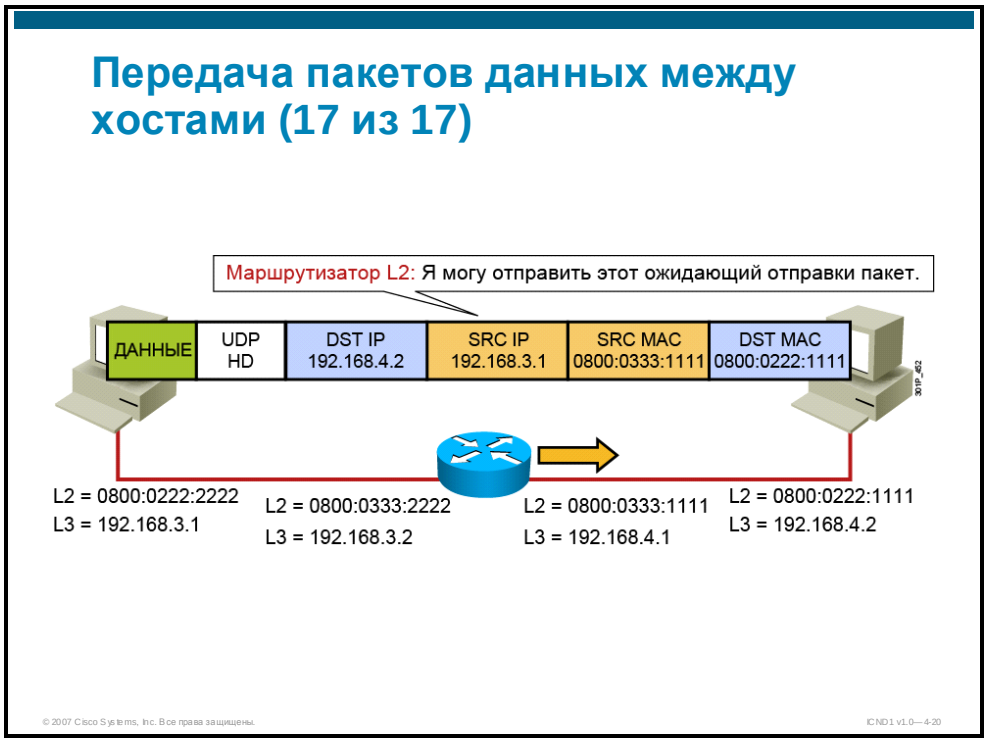
Устройство назначения получает и обрабатывает запрос ARP.



Этот хост получает кадр, включающий запрос ARP, и передает этот запрос процессу ARP.



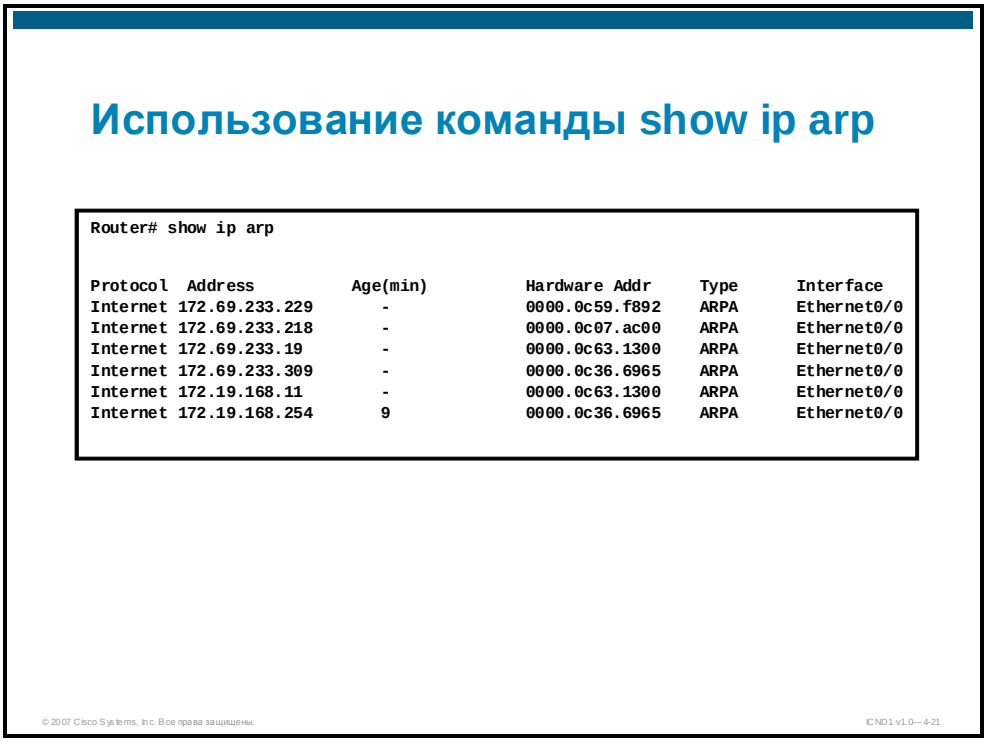
Хост отвечает на запрос ARP.



Кадр пересылается по месту назначения.

Использование команды show ip arp

В этом разделе описывается использование команды **show ip arp**.



Чтобы вывести кэш ARP, используйте команду **show ip arp** режима EXEC.

show ip arp [*ip-address*] [*host-name*] [*mac-address*] [*interface type number*]

Описание синтаксиса

ip-address	(Необязательно) Отображаются записи ARP, соответствующие этому IP-адресу.
host-name	(Необязательно) Имя хоста.
mac-address	(Необязательно) 48-битный MAC-адрес.
interface type number	(Необязательно) Отображаются записи ARP, полученные с помощью интерфейса с этим типом и номером.

Указания по использованию

ARP устанавливает соответствие между сетевыми адресами (например, IP-адресом) и аппаратными адресами устройств ЛВС (адреса Ethernet). Запись каждого соответствия хранится в кэше в течение заданного интервала времени, а затем удаляется.

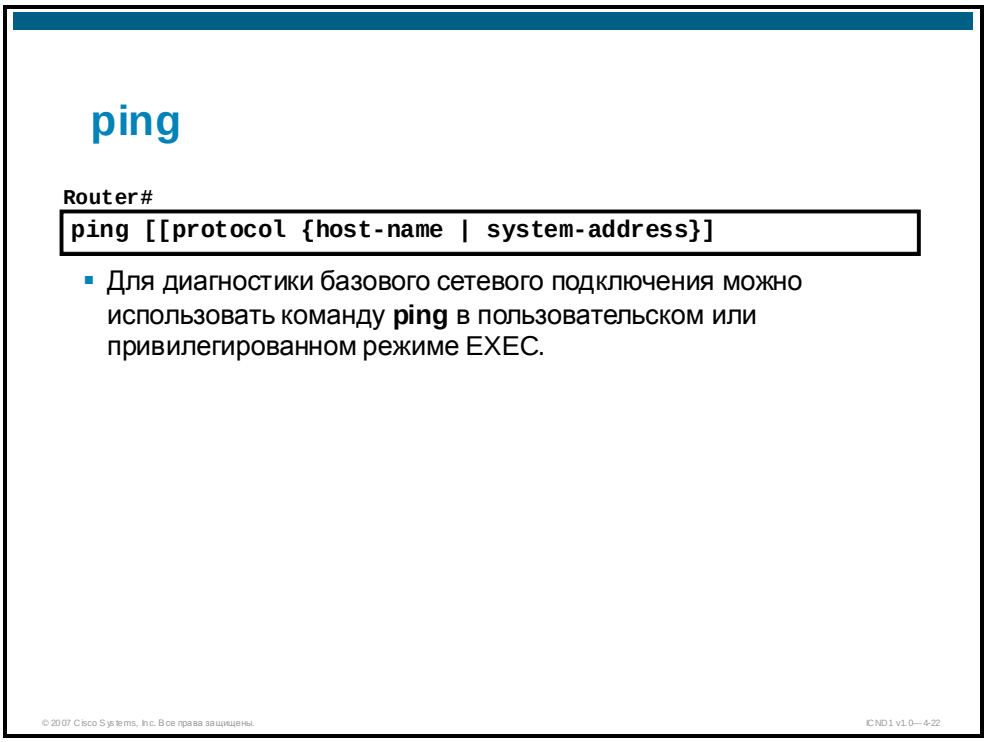
В таблице описан следующий пример вывода команды **show ip arp**:

```
Router# show ip arp
Protocol Address          Age(min)   Hardware Addr    Type      Interface
Internet  172.69.233.229     –        0000.0c59.f892   ARPA      Ethernet0/0
Internet  172.69.233.218     –        0000.0c07.ac00   ARPA      Ethernet0/0
Internet  172.69.233.19      –        0000.0c63.1300   ARPA      Ethernet0/0
Internet  172.69.233.309     –        0000.0c36.6965   ARPA      Ethernet0/0
Internet  172.19.168.11      –        0000.0c63.1300   ARPA      Ethernet0/0
Internet  172.19.168.254     9        0000.0c36.6965   ARPA      Ethernet0/0
```

Поле	**Описание**
Protocol	Протокол для сетевого адреса, указанного в поле адреса.
Address	Сетевой адрес, соответствующий аппаратному адресу.
Age (min)	Возраст записи кэша в минутах. Дефис (–) означает, что адрес является локальным.
Hardware Addr	Аппаратный адрес устройства ЛВС для MAC-адреса, который соответствует сетевому адресу.
Type	Указывает тип инкапсуляции, который используется ПО Cisco IOS в сетевом адресе в этой записи. Возможны следующие варианты: ■ ARPA (Advanced Research Projects Agency); ■ протокол SNAP (Subnetwork Access Protocol); ■ протокол SAP (Session Announcement Protocol).
Interface	Указывает интерфейс, связанный с этим сетевым адресом.

Использование стандартных средств Cisco IOS

В этом разделе описывается использование стандартных средств ПО Cisco IOS для проверки связи.

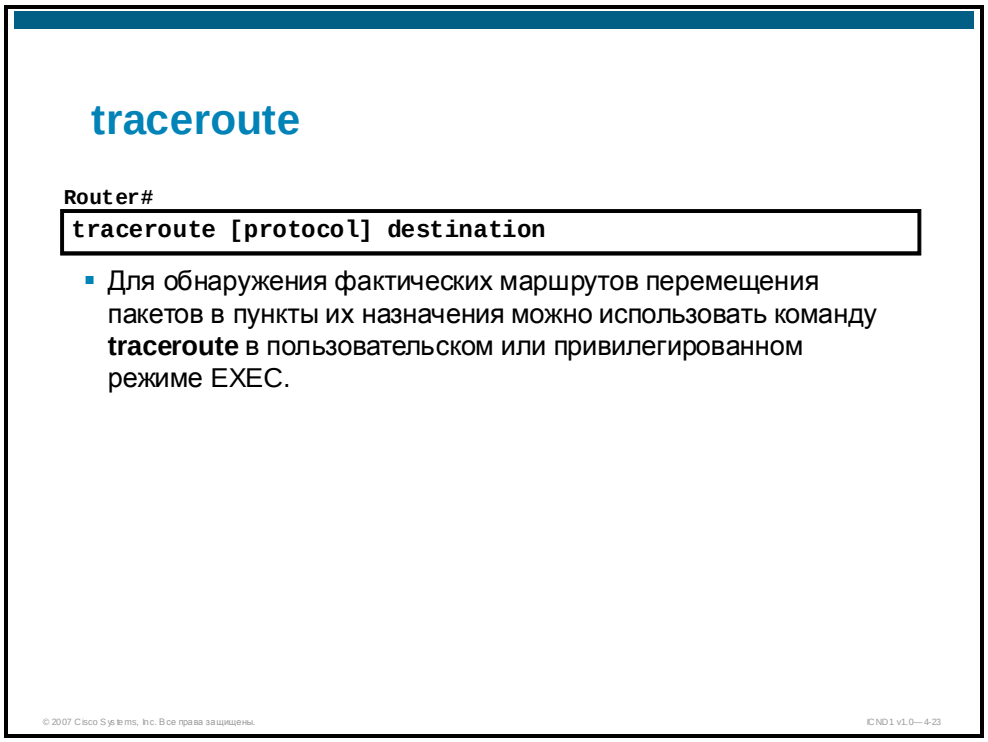


Для диагностики базового сетевого подключения можно использовать команду **ping** в пользовательском или привилегированном режиме EXEC.

ping [[*protocol* {*host-name* | *system-address*}]

Описание синтаксиса

protocol	(Необязательно) Ключевое слово протокола: **appletalk**, **atm**, **clns**, **decnet**, **ipx** или **srb**. Если конкретный протокол не указан, основные эхо-запросы будут отправляться с помощью IP (IPv4). Расширенные параметры отправки эхо-запросов поверх IP см. в документации для команды **ping ip**.
host-name	Имя хоста для отправки эхо-запросов. Если в командной строке не указан параметр *host-name* или *system-address*, он будет запрашиваться в системном диалоге **ping**.
system-address	Адрес системы для отправки эхо-запросов. Если в командной строке не указан параметр *host-name* или *system-address*, он будет запрашиваться в системном диалоге **ping**.



Для изучения фактических маршрутов перемещения пакетов в пункты их назначения можно использовать команду **traceroute** в пользовательском или привилегированном режимах EXEC.

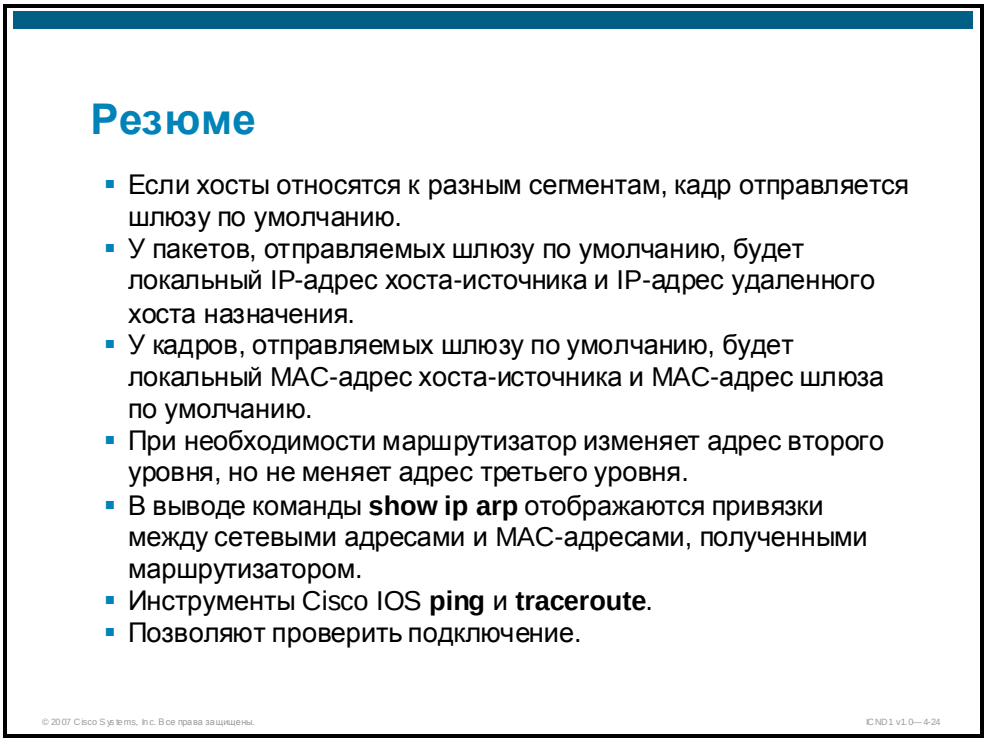
traceroute [**vrf** *vrf-name*] [*protocol*] *destination*

Описание синтаксиса

protocol	(Необязательно) Ключевое слово протокола: **appletalk**, **clns**, **ip**, **ipv6**, **ipx**, **oldvines** или **vines**. Если параметр *protocol* не указан, он вычисляется на основе анализа параметра *destination*.
destination	(необязательный в привилегированном режиме EXEC; обязательный в пользовательском режиме EXEC) Адрес или имя хоста назначения, для которого необходима трассировка маршрута. Программное обеспечение определяет параметры по умолчанию для соответствующего протокола и начинает трассировку.

Резюме

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



Занятие 7

Общие сведения о безопасности маршрутизатора Cisco

Обзор

После того, как вы защитили физический доступ к сети, необходимо обеспечить защиту доступа к маршрутизатору Cisco по консольному порту и портам VTY. Кроме того, необходимо исключить риски нарушения безопасности через неиспользуемые порты маршрутизатора. На этом занятии описывается обеспечение безопасности маршрутизатора.

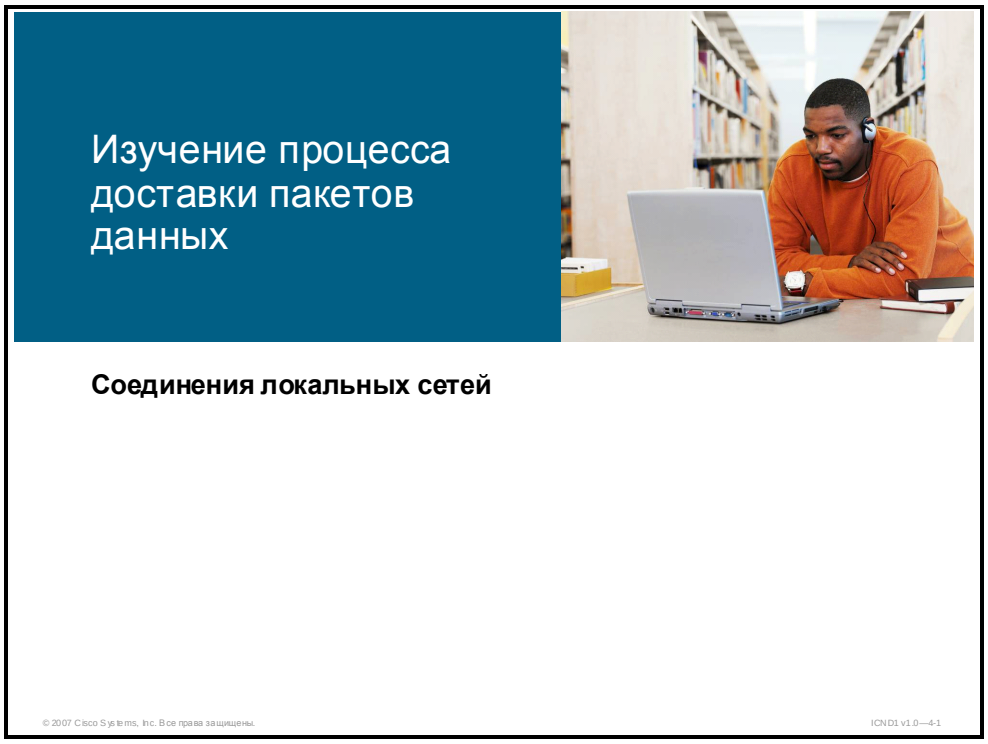
Задачи

По окончании этого занятия вы сможете создавать базовую конфигурацию безопасности на маршрутизаторе Cisco. Это значит, что вы сможете выполнять следующие задачи:

- описывать, как минимизировать аппаратные и электрические угрозы, угрозы, связанные с обслуживанием, а также угрозы со стороны окружающей среды, способные повредить безопасности маршрутизаторов Cisco;
- настраивать защиту на базе паролей;
- настраивать баннер входа в систему;
- описывать использование протоколов Telnet и SSH для удаленного доступа.

Физические угрозы и угрозы со стороны окружающей среды

Часто угрозу безопасности сети представляет неверная или неполная установка сетевых устройств, причем эта угроза часто оставляется без внимания. Невозможно предотвратить повреждение сети в результате плохо проведенной установки только программными средствами обеспечения безопасности. В этом разделе описывается, как минимизировать аппаратные и электрические угрозы, угрозы, связанные с обслуживанием, а также угрозы со стороны окружающей среды, способные повредить безопасности маршрутизаторов Cisco.

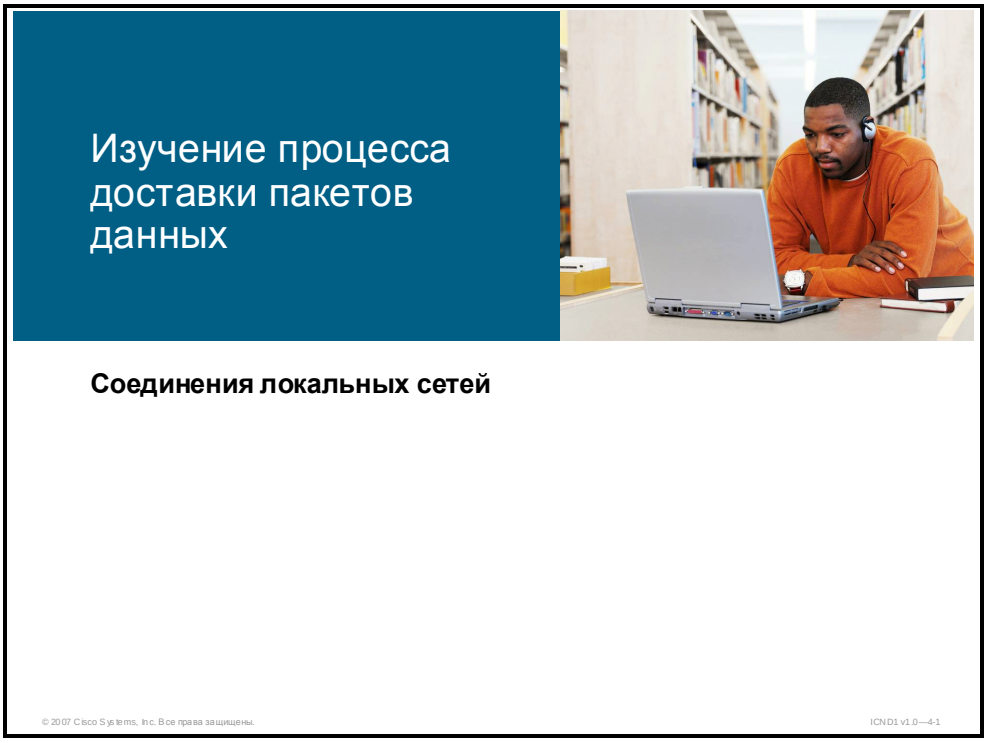


Существуют четыре класса угроз, связанных с небезопасной установкой или физическим доступом.

- **Угрозы для аппаратного обеспечения:** Это угрозы физического повреждения маршрутизатора или его компонентов.
- **Угрозы со стороны окружающей среды:** К ним относятся такие угрозы, как предельные температуры (слишком высокие или слишком низкие) или крайние 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 электрическими компонентами (электростатический разряд), отсутствие важных запасных частей, плохая прокладка кабеля, небрежная маркировка и т.д.

Настройка защиты паролем

Для настройки пароля и других консольных команд можно использовать интерфейс командной строки (CLI). В этом разделе описывается настройка паролей и другие важные задачи настройки.



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

Вы можете обеспечит безопасность маршрутизатора с помощью пароля для ограничения доступа. 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 в привилегированный режим EXEC. Пароли задаются с учетом регистра символов.

Порты Telnet маршрутизатора называется терминалами VTY. На маршрутизаторе может работать до шестнадцати портов VTY, обеспечивающих до шестнадцати одновременных сеансов Telnet. На маршрутизаторе портам VTY присваиваются номера с 0 по 15.

Используйте команду **line console 0** с подкомандами **password** и **login**, чтобы включить запрос пароля при входе в систему и установить пароль на консольном терминале или порте VTY. По умолчанию запрос пароля для порта VTY или консоли не применяется.

Команда **line vty 0 4** с подкомандами **password** и **login** включает запрос пароля при входе в систему и устанавливает пароль для входящих сеансов Telnet.

Команду **login local** можно использовать для включения проверки пароля каждого пользователя с использованием 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 назначить зашифрованную форму пароля доступа, которая называется «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 пароля **enable password**, а не вместе с ним.

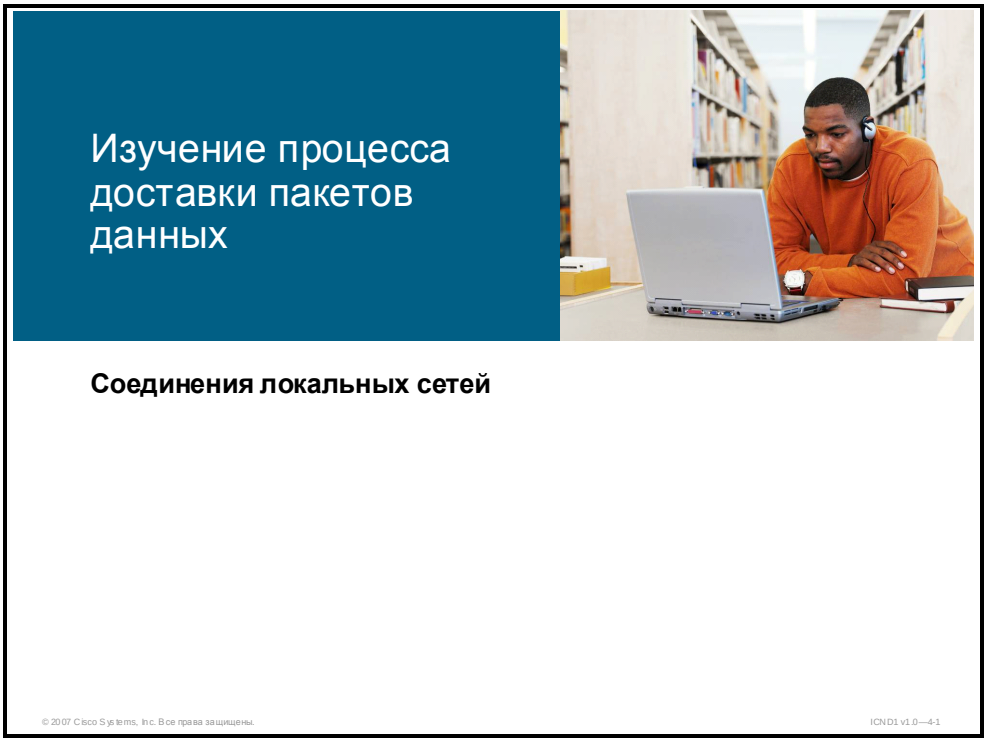
Можно также добавить еще один уровень безопасности, который будет особенно полезен для паролей, передаваемых по сети или хранящихся на TFTP-сервере. Cisco предоставляет средство, которое позволяет использовать зашифрованные пароли. Чтобы установить шифрование пароля, введите команду **service password-encryption** в режиме глобальной конфигурации.

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

Чтобы отключить команду, введите **no** перед этой командой. Например, используйте команду **no service password-encryption**, чтобы отключить шифрование пароля.

Настройка баннера входа

С помощью интерфейса командной строки можно настроить сообщение дня и другие консольные команды. В этом разделе описываются некоторые задачи конфигурации, необходимые для включения баннера входа.



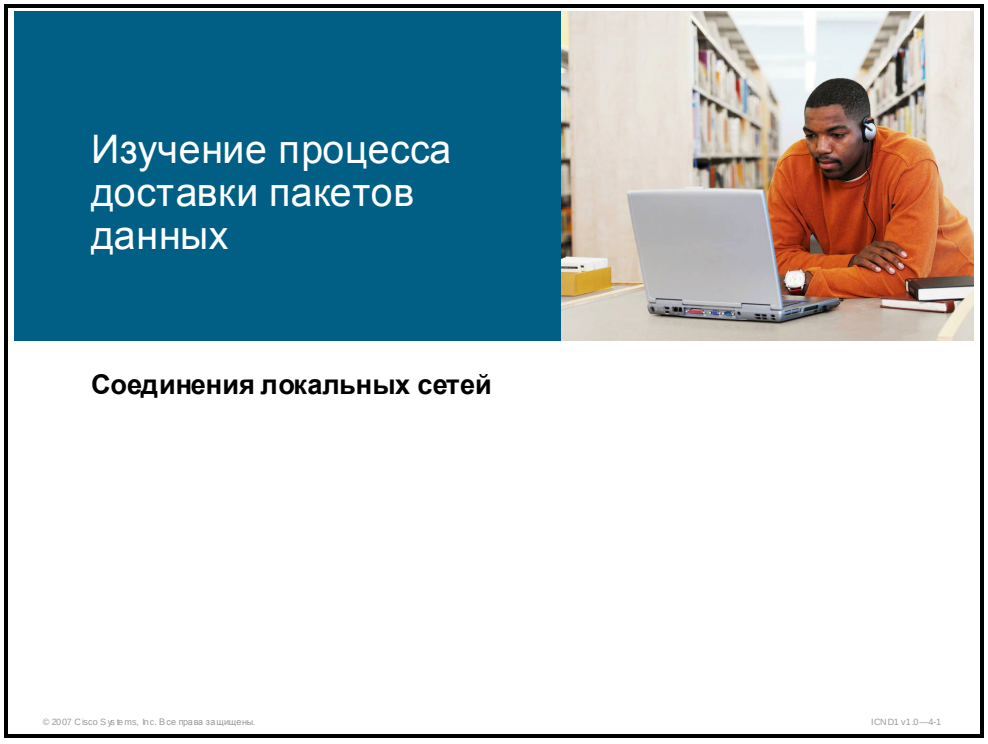
С помощью команды **banner login** в режиме глобальной конфигурации можно настроить баннер, который будет отображаться перед запросом имени пользователя и пароля. Для отключения баннера входа можно использовать команду **no banner login**.

После ввода команды **banner motd** поставьте за ней один или несколько пробелов и символ-разделитель. 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 не ограничен, что позволит хакерам оправдать свои действия.

Доступ по протоколам Telnet и SSH

В этом разделе описаны методы Telnet и SSH, которые можно выбрать в качестве средства удаленного доступа.



Telnet – это самый распространенный метод доступа к сетевому устройству. Однако протокол Telnet не может обеспечить безопасный доступ в сети. SSH является защищенным аналогом протокола Telnet. Взаимодействие между клиентом и сервером шифруется как в протоколе SSH версии 1 (SSHv1), так и в SSH версии 2 (SSHv2). По возможности используйте SSHv2, так как в этом протоколе используется сложный алгоритм шифрования. Если включено шифрование, на маршрутизаторе должен быть сгенерирован ключ шифрования RSA (Rivest, Shamir, and Adleman). Кроме того, маршрутизатору должен быть присвоен домен IP.

Перед внедрением SSH необходимо выполнить проверку аутентификации на маршрутизаторе без использования SSH. В следующем примере показана локальная аутентификация, позволяющая использовать протокол Telnet для подключения к маршрутизатору с именем пользователя «cisco» и паролем «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 ssh
```


Чтобы протестировать аутентификацию с протоколом SSH, необходимо добавить к предыдущему сценарию инструкции для включения SSH. Затем следует проверить работу SSH на ПК и станциях UNIX.

Если необходимо запретить подключение по всем протоколам, кроме SSH, добавьте команду **transport input ssh**, чтобы ограничить средства подключения к маршрутизатору протоколом SSH. Прямые (не SSH) подключения по протоколу Telnet будут отклоняться.

```
line vty 0 4

!--- Prevent non-SSH Telnets.

transport input ssh
```

Убедитесь, что пользователи, не применяющие протокол SSH, не могут подключиться к маршрутизатору по протоколу Telnet.

Резюме

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

Изучение процесса доставки пакетов данных

Соединения локальных сетей

Занятие 8

Использование Cisco SDM

Обзор

Cisco Router and Security Device Manager (SDM) – это простой в использовании инструмент для управления устройствами на базе Java, предназначенный для настройки локальных и глобальных сетей и функций безопасности на маршрутизаторе. В этом занятии приводятся инструкции по использованию Cisco SDM.

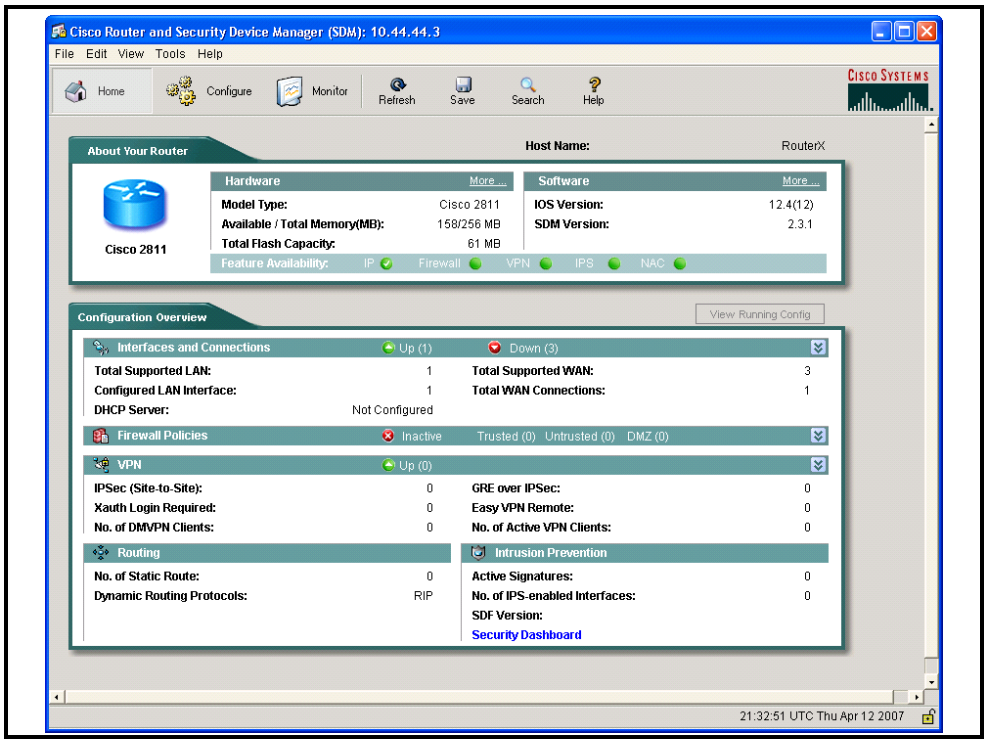
Задачи

По окончании этого занятия вы сможете описывать функции Cisco SDM. Это значит, что вы сможете выполнять следующие задачи:

- описывать функции Cisco SDM;
- объяснять методы использования элементов интерфейса SDM;
- объяснять функции каждого из пяти мастеров Cisco SDM.

Обзор Cisco SDM

В этом разделе приведены общие сведения о Cisco SDM.



Cisco SDM – это простой, интуитивно понятный инструмент на основе веб-интерфейса, предназначенный для управления маршрутизаторами на базе ПО Cisco IOS. Cisco SDM упрощает настройку функций безопасности маршрутизаторов с помощью мастеров, которые помогают клиентам и партнерам Cisco быстро и легко развертывать, настраивать и контролировать маршрутизатор Cisco, при этом знание интерфейса командной строки (CLI) не требуется. Cisco SDM поддерживается маршрутизаторами Cisco серий 830, 1700, 1800, 2600XM, 2800, 3600, 3700, 3800 и некоторыми маршрутизаторами Cisco серий 7200 и 7301.

Что такое Cisco SDM?

- Встроенный инструмент для управления на основе веб-интерфейса
- Интеллектуальные мастеры Cisco SDM помогают быстро и легко развертывать маршрутизаторы, при этом знания интерфейса командной строки Cisco IOS и средств безопасности не требуются.
- Инструменты для опытных пользователей:
  - редактор ACL;
  - редактор схемы шифрования VPN;
  - режим предварительного просмотра CLI Cisco IOS.

Cisco SDM позволяет пользователям легко настраивать службы маршрутизации, коммутации, безопасности и качества обслуживания (QoS) на маршрутизаторах Cisco, обеспечивая при этом упреждающее управление благодаря мониторингу производительности. При развертывании нового маршрутизатора или установке Cisco SDM на существующем маршрутизаторе у пользователей есть возможность дистанционной настройки и мониторинга маршрутизаторов Cisco без использования интерфейса командной строки Cisco IOS. Графический интерфейс Cisco SDM помогает неопытным пользователям программного обеспечения Cisco IOS в повседневных операциях, предлагает простые в использовании интеллектуальные мастера, автоматизирует управление функциями безопасности на маршрутизаторах и предоставляет пользователям комплексную интерактивную справочную систему и средства обучения.

Интеллектуальные мастера Cisco SDM предоставляют пользователям пошаговые инструкции по задачам конфигурации маршрутизаторов и функций безопасности путем упорядоченной настройки интерфейсов ЛВС и РВС (WAN), брандмауэров, систем предотвращения вторжений (IPS) и виртуальных частных сетей (VPN) IPSec. Мастера Cisco SDM могут определить некорректную конфигурацию и предложить изменения, например, разрешить прохождение трафика DHCP через брандмауэр, если в интерфейсе РВС действует адресация DHCP. В интерактивной справке, встроенной в Cisco SDM, приведена необходимая базовая информация, а также описаны пошаговые процедуры, помогающие пользователям ввести корректные данные в Cisco SDM. Термины и определения по сетевым технологиям и безопасности, с которыми может столкнуться пользователь, включены в интерактивный глоссарий.

Для специалистов по сетям, знакомых с программным обеспечением Cisco IOS и его функциями безопасности, Cisco SDM предлагает расширенные средства конфигурации для быстрой настройки и тонкого управления функциями безопасности маршрутизаторов, позволяя им анализировать команды, сгенерированные Cisco SDM, перед применением изменений конфигурации на маршрутизаторе.

Cisco SDM помогает настраивать маршрутизаторы и выполнять их мониторинг дистанционно, используя безопасные соединения SSL и SSHv2. Эта технология помогает сформировать защищенное соединение через Интернет между обозревателем пользователя и маршрутизатором. При развертывании маршрутизатора в филиальном офисе его настройку и мониторинг можно осуществлять из центрального офиса корпорации с помощью Cisco SDM. Это сокращает потребность филиалов в опытных сетевых администраторах.

Cisco SDM поддерживается многими маршрутизаторами Cisco и соответствующими версиями программного обеспечения Cisco IOS.

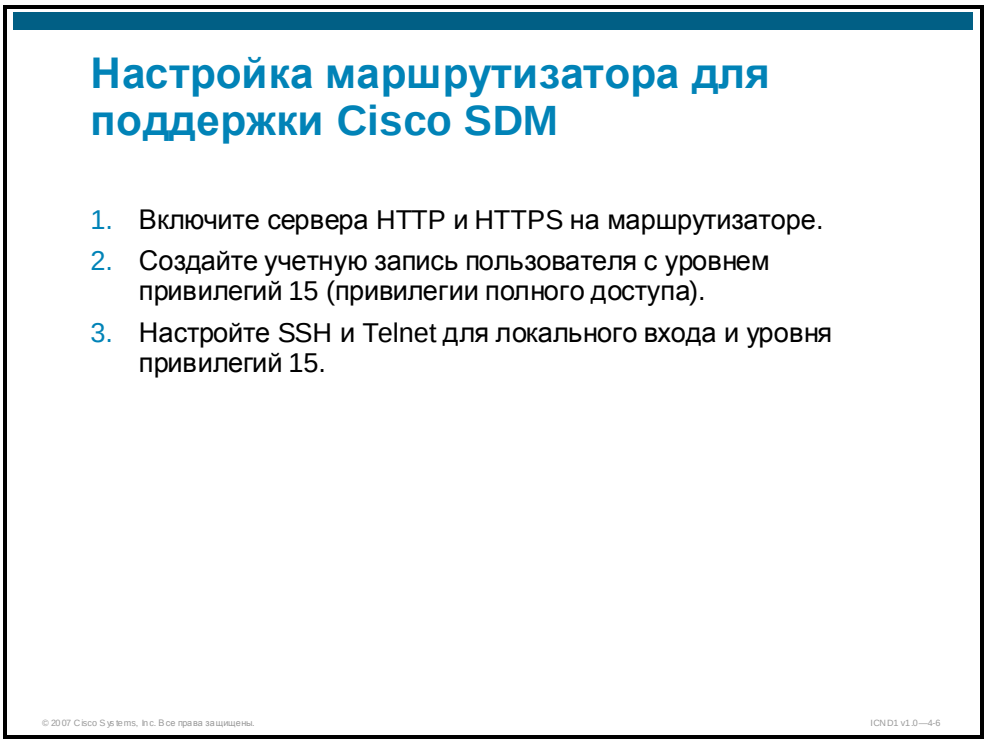
Новейшую информацию о поддержке версий ПО Cisco IOS и маршрутизаторов в Cisco SDM см. на странице http://www.cisco.com/go/sdm.

Cisco SDM устанавливается на предприятии-изготовителе на различных моделях новых маршрутизаторов (начиная с июня 2003 г.), приобретаемых вместе с пакетом VPN.

Если на вашем маршрутизаторе не установлена система Cisco SDM, ее можно загрузить с сайта Cisco.com и установить на маршрутизаторе. На маршрутизаторе должно быть достаточно флэш-памяти для поддержки существующей файловой структуры и файлов Cisco SDM. Сведения по установке Cisco SDM на маршрутизаторе Cisco не включены в этот курс.

Пользовательский интерфейс Cisco SDM

В этом разделе описаны различные элементы пользовательского интерфейса Cisco SDM.



Настройка маршрутизатора для поддержки Cisco SDM

Можно установить и запустить Cisco SDM на маршрутизаторе, который уже используется, не прерывая передачу сетевого трафика, но в файле конфигурации маршрутизатора должен присутствовать ряд параметров.

Получите доступ к интерфейсу командной строки, используя консольное подключение или подключение по протоколу Telnet, для изменения существующей конфигурации перед установкой Cisco SDM на маршрутизаторе.

Шаг 1 Введите следующие команды в режиме глобальной конфигурации, чтобы включить серверы HTTP и HTTPS на маршрутизаторе:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip http server
Router(config)# ip http secure-server
Router(config)# ip http authentication local
Router(config)# ip http timeout-policy idle 600 life 86400
requests 10000
```

Примечание Если маршрутизатор поддерживает протокол HTTPS, будет включен сервер HTTPS. В противном случае будет включен сервер HTTP. HTTPS поддерживается во всех образах, которые поддерживают набор криптографических функций IPsec, начиная с Cisco IOS версии 12.25(T).

Шаг 2 Создайте учетную запись пользователя с уровнем привилегий 15 (привилегии полного доступа). Введите в режиме глобальной конфигурации следующую команду, заменив параметры **username** и **password** нужными данными:

```
Router(config)# username username privilege 15 secret 0 password
```

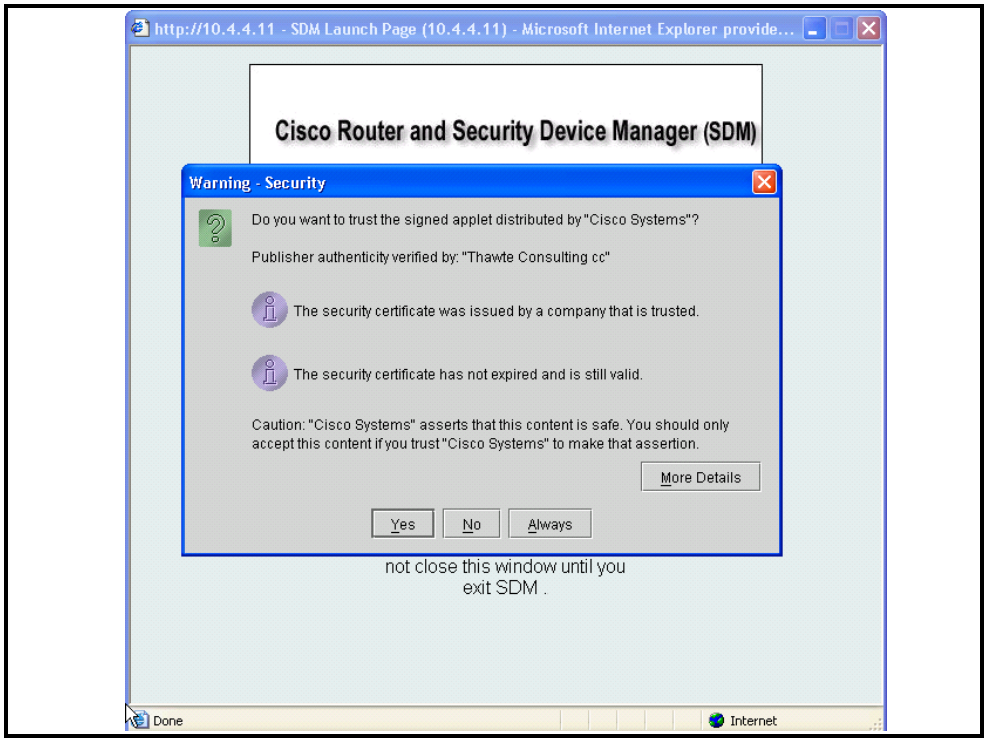
Например, если выбрано имя пользователя «tomato» и пароль «vegetable», необходимо ввести:

```
Router(config)# username tomato privilege 15 secret 0 vegetable
```

Это имя пользователя и пароль будут использоваться для входа в систему Cisco SDM.

Шаг 3 Настройте SSH и Telnet на локальную аутентификацию при входе и уровень привилегий 15 с помощью следующих команд:

```
Router(config)# line vty 0 4
Router(config-line)# privilege level 15
Router(config-line)# login local
Router(config-line)# transport input telnet ssh
Router(config-line)# exit
```



Запуск Cisco SDM

ПО Cisco SDM хранится во флэш-памяти маршрутизатора. Для его вызова выполняется HTML-файл из архива маршрутизатора, который затем загружает подписанный Java-апплет Cisco SDM. Для загрузки Cisco SDM выполните следующие действия:

Шаг 1 В обозревателе введите следующий URL:

https://*router IP address*

Обозначение https:// указывает, что для защищенного соединения используется протокол SSL.

Если протокол SSL недоступен, может использоваться обозначение http://.

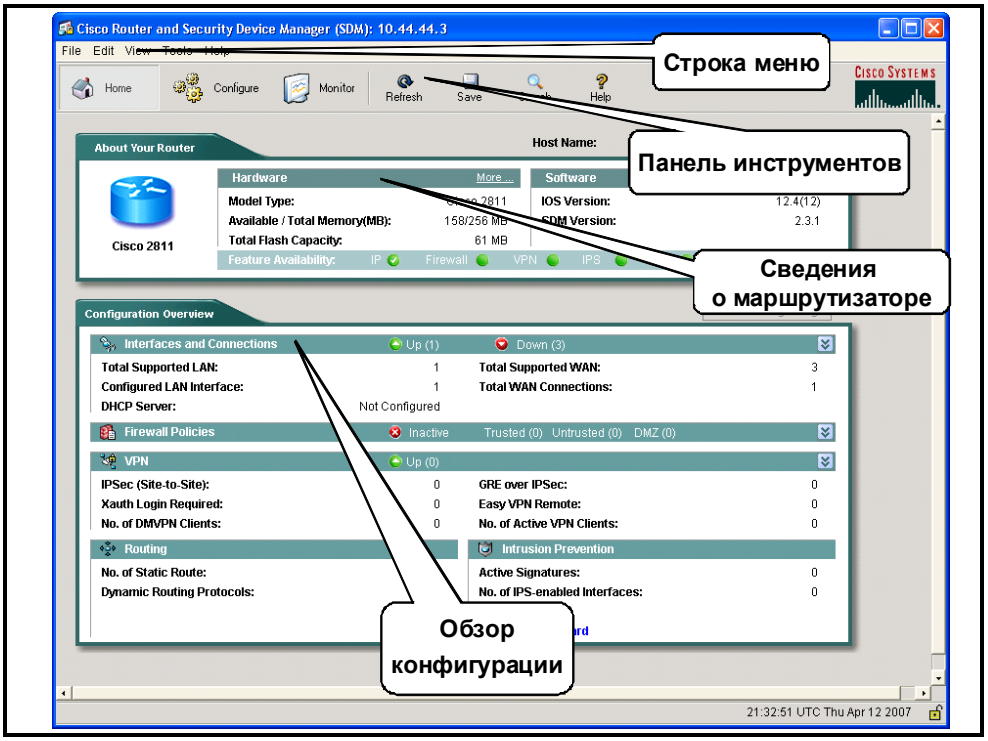
Шаг 2 В окне обозревателя появится домашняя страница Cisco SDM. Откроется диалоговое окно с запросом имени пользователя и пароля. Тип и форма этого диалогового окна будут зависеть от типа используемого обозревателя. Введите имя пользователя и пароль для привилегированной (уровень привилегий 15) учетной записи на маршрутизаторе.

На ПК начнет загружаться Java-апплет Cisco SDM.

Шаг 3 Cisco SDM является подписанным Java-апплетом. В окне обозревателя может появиться предупреждение системы безопасности. Примите сертификат.

Шаг 4 Появится страница запуска Cisco SDM.

При появлении окна запуска Cisco SDM выводит домашнюю страницу Cisco SDM. На домашней странице приводится сводка о конфигурации маршрутизатора и функциях, поддерживаемых образом Cisco IOS. Cisco SDM запускается в режиме мастера, который позволяет выполнить настройку, используя последовательность окон, разбивающих задачу настройки на контролируемые шаги.



На домашней странице приводятся основные сведения об аппаратном и программном обеспечении маршрутизатора и конфигурации, которые разделены на следующие разделы:

- **Host Name (Имя хоста).** Это заданное имя маршрутизатора.
- **About Your Router (Информация о маршрутизаторе).** В этой области приводятся основные сведения об аппаратном и программном обеспечении маршрутизатора и поля, показанные в таблице.

Hardware	
Model Type	Номер модели маршрутизатора.
Available/Total Memory	Объем доступной памяти ОЗУ и общей памяти ОЗУ.
Total Flash Capacity	Флэш-память и флэш-вебпамять (если применимо.)
Software	
IOS Version	Текущая версия ПО Cisco IOS, выполняемая на маршрутизаторе.
Cisco SDM Version	Текущая версия ПО Cisco SDM, выполняемая на маршрутизаторе.
Feature Availability	Доступные функции образа Cisco IOS, которые используются маршрутизатором, обозначаются флажком. Функции, которые проверяются Cisco SDM, включают IP, брандмауэр, VPN и IPS.

Ссылка More (Дополнительные сведения)

Ссылка "More" отображает всплывающее окно со следующими дополнительными сведениями об аппаратном и программном обеспечении:

- **Hardware Details (Сведения об аппаратном обеспечении).** Помимо информации, показанной в окне «About Your Router (Информация о маршрутизаторе)», на этой вкладке отображаются следующие данные:
  - источник для загрузки маршрутизатора – флэш-память или файл конфигурации;
  - используются ли ускорители, например ускорители VPN;
  - диаграмма конфигурации аппаратного обеспечения.
- **Software Details (Сведения о программном обеспечении).** Помимо информации, приведенной в разделе «About Your Router (Информация о маршрутизаторе)», на этой вкладке отображаются сведения о наборах функций, включенных в образ Cisco IOS.

Configuration Overview (Обзор конфигурации)

В этом разделе домашней страницы сведены все параметры конфигурации. Для просмотра текущей конфигурации нажмите **View Running Config (Просмотр текущей конфигурации)**.

Interfaces and Connections (Интерфейсы и подключения)

В этой области приводятся следующие сведения:

- **Up (Активные).** Количество активных подключений.
- **Down (Неактивные).** Количество неактивных подключений.
- **Double arrow (Двойная стрелка).** Щелкните, чтобы показать или скрыть подробные сведения.

- **Total Supported LAN (Общее количество поддерживаемых ЛВС).** Показывает общее количество интерфейсов ЛВС на маршрутизаторе.
- **Total Supported WAN (Общее количество поддерживаемых РВС).** Количество поддерживаемых системой Cisco SDM интерфейсов РВС, присутствующих на маршрутизаторе.
- **Configured LAN Interface (Количество настроенных интерфейсов ЛВС).** Количество поддерживаемых интерфейсов ЛВС, настроенных на маршрутизаторе.
- **Total WAN Connections (Общее количество подключений РВС).** Общее количество подключений РВС, поддерживаемых Cisco SDM на маршрутизаторе.
- **DHCP Server (DHCP-сервер).** Настроен или ненастроен.
- **DHCP Pool (Detail View) (Пул DHCP (подробное представление)).** Если настроен один пул, в данной области показаны начальный и конечный адреса пула DHCP. Если настроено несколько пулов, отображается список имен настроенных пулов.
- **Number of DHCP Clients (Detail View) (Количество DHCP-клиентов (подробное представление)).** Текущее количество клиентов, арендующих адреса.
- **Interface (Интерфейс).** Имя настроенного интерфейса.
  - **Type (Тип).** Тип интерфейса.
  - **IP Mask (Маска IP).** IP-адрес и маска подсети.
  - **Description (Описание).** Описание интерфейса.

Firewall Policies (Политики брандмауэра)

В этой области приводятся следующие сведения:

- **Active (Активен).** Брандмауэр используется.
- **Inactive (Неактивен).** Брандмауэр не используется.
- **Trusted (Доверенные).** Количество доверенных (внутренних) интерфейсов.
- **Untrusted (Недоверенные).** Количество недоверенных (внешних) интерфейсов.
- **DMZ (ДМЗ).** Количество интерфейсов демилитаризованной зоны (ДМЗ).
- **Double arrow (Двойная стрелка).** Щелкните, чтобы показать или скрыть подробные сведения.
- **Interface (Интерфейс).** Имя интерфейса, к которому применяется брандмауэр.
- **Firewall icon (Значок брандмауэра).** Указывает, является ли интерфейс внутренним или внешним.
- **NAT.** Имя или номер правила преобразования сетевых адресов (NAT), применяемого к этому интерфейсу.
- **Inspection Rule (Правило проверки).** Имена или номера правил входящей и исходящей проверки.
- **Access Rule (Правило доступа).** Имена или номера правил доступа к входящим и исходящим данным.

VPN

В этой области приводятся следующие сведения:

- **Up (Активные).** Количество активных VPN-соединений.
- **Double arrow (Двойная стрелка).** Щелкните, чтобы показать или скрыть подробные сведения.
- **IPsec (Site-to-Site) (соединение площадок).** Количество настроенных VPN-соединений между площадками.
- **GRE over IPsec (GRE поверх IPsec).** Количество настроенных соединений по протокол GRE (Generic Routing Encapsulation) поверх IPsec.
- **XAUTH Login Required (Требуется вход для аутентификации XAUTH).** Количество соединений Cisco Easy VPN, ожидающих ввода учетных данных для дополнительной аутентификации (XAUTH).

Примечание На некоторых серверах или концентраторах VPN для клиентов используется аутентификация XAUTH. Отображается количество туннелей VPN, ожидающих ввода учетных данных для аутентификации XAUTH. Если туннель Cisco Easy VPN ожидает ввода данных для аутентификации XAUTH, отображается отдельная панель сообщения с кнопкой Login (Вход). Нажмите кнопку **Login (Вход)** для ввода реквизитов туннеля.

Примечание Если для туннеля настроена аутентификация XAUTH, он начнет работу только после ввода учетной записи и пароля. Время ожидания ввода этих данных неограниченно.

- **Easy VPN Remote.** Количество настроенных соединений Cisco Easy VPN Remote.
- **No. of DMVPN Clients (Количество клиентов DMVPN).** Если маршрутизатор настроен как концентратор Dynamic Multipoint VPN (DMVPN), количество клиентов DMVPN.
- **No. of Active VPN Clients (Количество активных клиентов VPN).** Если данный маршрутизатор работает как сервер Cisco Easy VPN, количество клиентов Cisco Easy VPN с активными соединениями.
- **Interface (Интерфейс).** Имя интерфейса с настроенными VPN-соединениями.
- **IPsec Policy (Политика IPsec).** Имя политики IPsec, связанной с VPN-соединениями.

Routing (Маршрутизация)

В этой области приводятся следующие сведения:

- **No. of Static Routes (Количество статических маршрутов).** Количество статических маршрутов, настроенных на маршрутизаторе.
- **Dynamic Routing Protocols (Динамические протоколы маршрутизации).** Список динамических протоколов маршрутизации, настроенных на маршрутизаторе.

Intrusion Prevention (Защита от вторжений)

В этой области приводятся следующие сведения:

- **Active Signatures (Активные сигнатуры).** Количество активных сигнатур, используемых маршрутизатором. Они могут быть встроены или загружены из удаленного узла.
- **No. of IPS-Enabled Interfaces (Количество интерфейсов, на которых включена система IPS).** Количество интерфейсов, на которых включена система IPS.

Мастеры Cisco SDM

В этом разделе описаны некоторые мастера Cisco SDM.

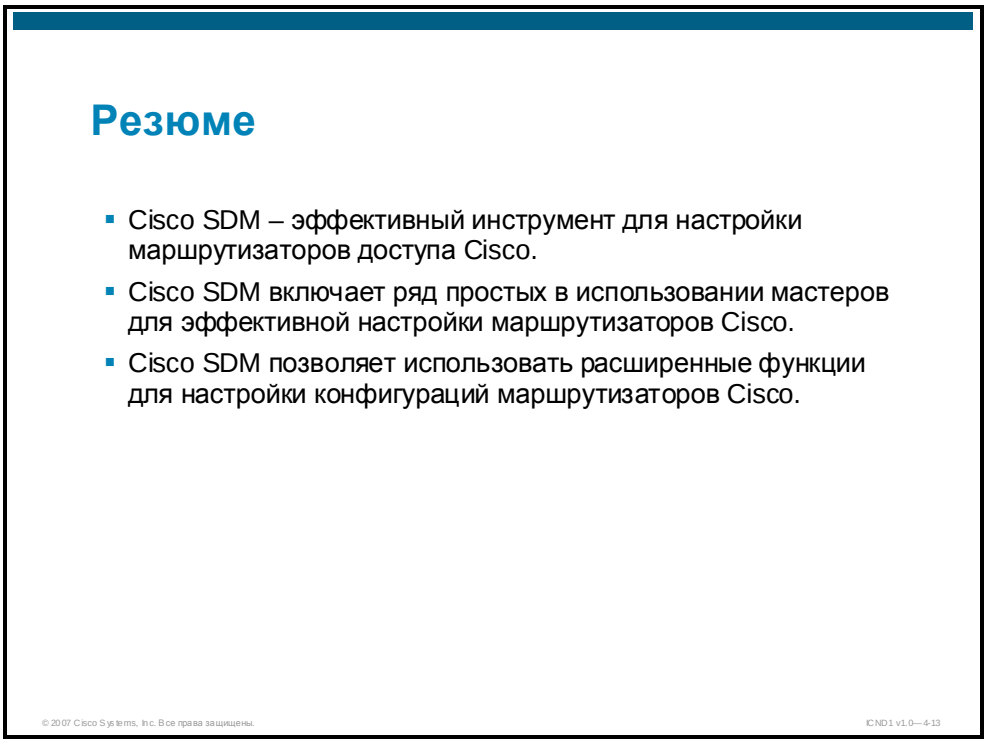
Cisco SDM включает различные мастера, показанные на рисунке:

- **LAN wizard (Мастер ЛВС).** Используется для настройки интерфейсов ЛВС и DHCP.
- **WAN wizard (Мастер РВС).** Используется для настройки интерфейсов РВС: PPP, Frame Relay, High-Level Data Link Control (HDLC). Последние сведения о мастерах и поддерживаемых ими интерфейсах см. на странице http://www.cisco.com/go/sdm.
- **Firewall wizards (Мастеры брандмауэров)**
- **VPN wizards (Мастеры VPN)**
- **Security Audit wizards (Мастеры аудита безопасности).** Доступны два мастера:
  - мастер аудита безопасности маршрутизатора и
  - мастер простой одношаговой блокировки для защиты маршрутизатора.
- **QoS (Качество обслуживания).** Мастер качества обслуживания.

Примечание В конце процедуры каждого мастера все изменения автоматически отправляются на маршрутизатор с помощью команд интерфейса командной строки, генерируемых Cisco SDM. Можно включить или выключить предварительный просмотр этих команд перед отправкой. По умолчанию предварительный просмотр команд отключен.

Резюме

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



Занятие 9

Использование маршрутизатора Cisco в качестве DHCP-сервера

Обзор

Первоначально сетевые администраторы должны были вручную задавать адрес хоста, шлюз по умолчанию и другие сетевые параметры на каждом хосте. Однако протокол DHCP (Dynamic Host Configuration Protocol) предоставляет параметры конфигурации для хостов. DHCP состоит из двух компонентов:

- протокол доставки параметров конфигурации хостов с DHCP-сервера;
- механизм выделения хостам сетевых адресов.

В этом занятии описывается использование маршрутизатора Cisco в качестве DHCP-сервера.

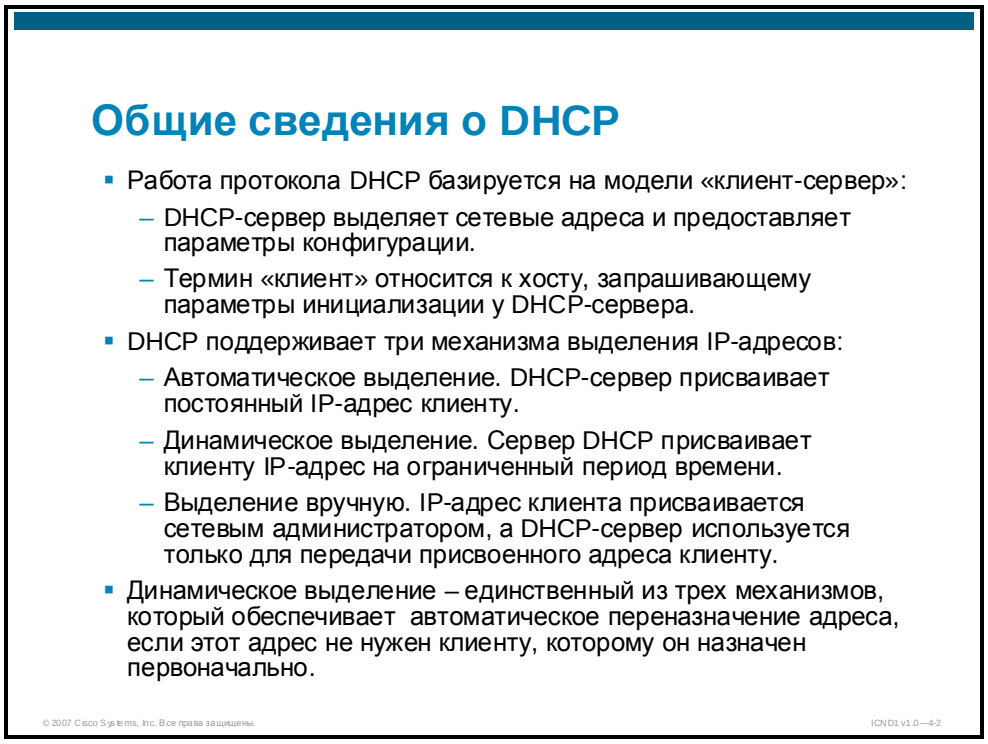
Задачи

По окончании этого занятия вы сможете настраивать DHCP-сервер Cisco IOS с помощью Cisco SDM. Это значит, что вы сможете выполнять следующие задачи:

- описывать функции протокола DHCP;
- описывать использование маршрутизатора в качестве DHCP-сервера;
- описывать использование Cisco SDM для включения функций DHCP-сервера на маршрутизаторе;
- описывать мониторинг функций DHCP-сервера.

Общие сведения о DHCP

В этом разделе рассматриваются функции DHCP.

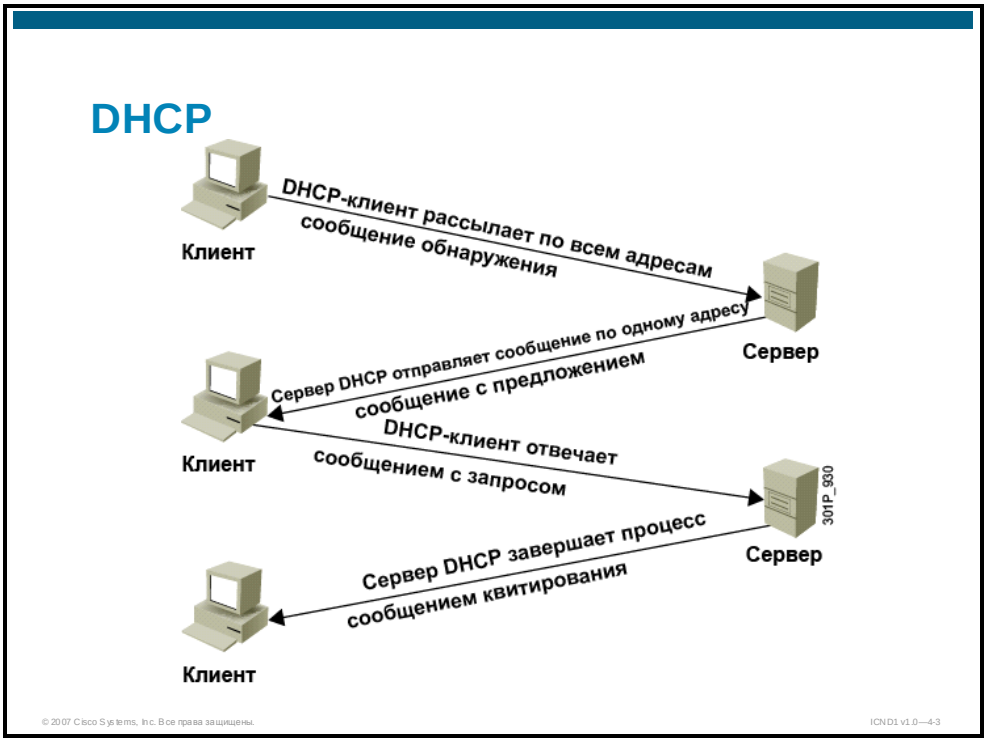


Работа протокола DHCP базируется на модели "клиент-сервер". DHCP-сервер выделяет сетевые адреса и передает параметры конфигурации динамически настраиваемым хостам. Термин «клиент» относится к хосту, запрашивающему параметры инициализации у DHCP-сервера.

DHCP поддерживает три механизма выделения IP-адресов:

- **Автоматическое выделение.** DHCP-сервер присваивает постоянный IP-адрес клиенту.
- **Динамическое выделение.** DHCP-сервер присваивает клиенту IP-адрес на ограниченный период времени (или пока клиент не освободит адрес в явной форме).
- **Выделение вручную.** IP-адрес клиента присваивается сетевым администратором, а DHCP используется только для передачи присвоенного адреса клиенту.

Динамическое выделение – единственный из трех механизмов, который обеспечивает автоматическое переназначение адреса, если этот адрес не нужен клиенту, которому он назначен первоначально. Динамическое выделение особенно эффективно для назначения адреса клиенту, подключаемому к сети временно, или для совместного использования ограниченного пула IP-адресов группой клиентов, которым не нужны постоянные IP-адреса. Кроме того, динамическое выделение рекомендуется использовать для присвоения IP-адреса новому клиенту с постоянным подключением к сети с ограниченным числом IP-адресов, где важно переназначение адресов при отключении старых клиентов.



DHCPDISCOVER

При первой загрузке клиента он передает сообщение DHCPDISCOVER в локальную физическую подсеть. Поскольку клиент не может знать, к какой подсети он относится, сообщение DHCPDISCOVER рассылается во все подсети (IP-адрес назначения 255.255.255.255). У клиента нет настроенного IP-адреса, поэтому используется IP-адрес источника 0.0.0.0.

DHCPOFFER

DHCP-сервер, который получил сообщение DHCPDISCOVER, может ответить сообщением DHCPOFFER, содержащем данные начальной конфигурации клиента. Например, DHCP-сервер предоставляет запрашиваемый IP-адрес. Маска подсети и шлюз по умолчанию задаются в соответствующем поле параметров маски подсети и шлюза. Другие общие параметры в сообщении DHCPOFFER содержат время аренды IP-адреса, срок возобновления, сервер доменных имен и службу именования NetBIOS (Microsoft Windows Internet Name Service [Microsoft WINS]).

DHCPREQUEST

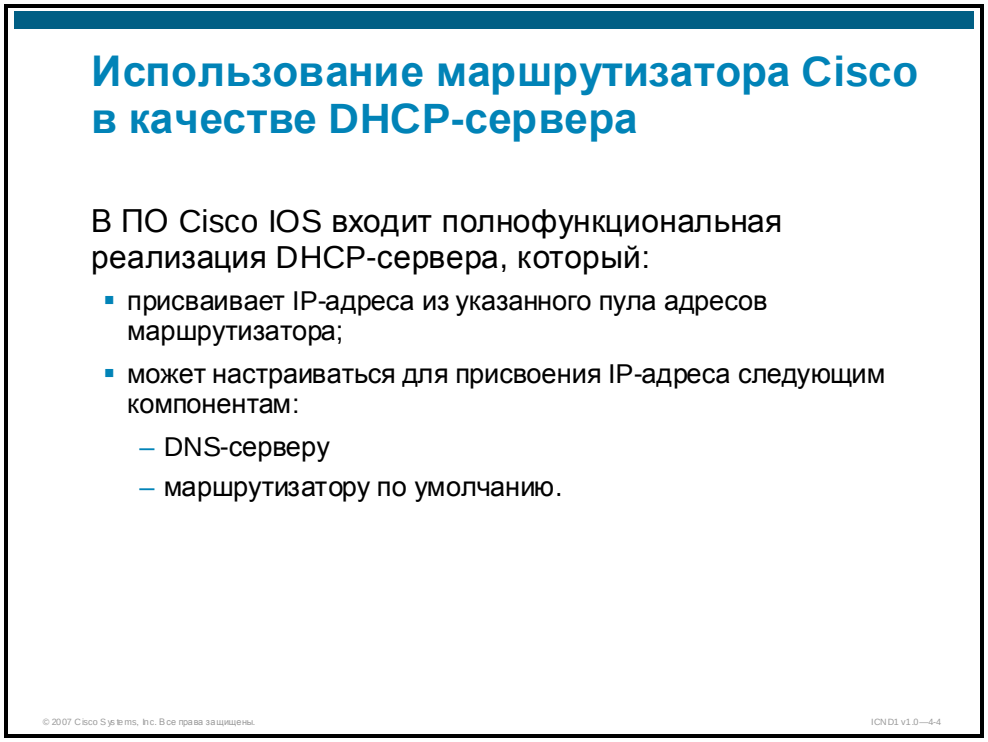
После получения клиентом сообщения DHCPOFFER он отправляет ответное сообщение DHCPREQUEST о намерении принять параметры из сообщения DHCPOFFER.

DHCPACK

После того, как DHCP-сервер получает сообщение DHCPREQUEST, он подтверждает запрос в сообщении DHCPACK, завершая таким образом процесс инициализации.

Использование маршрутизатора Cisco в качестве DHCP-сервера

В этом разделе описывается поддержка DHCP-сервера маршрутизатор Cisco.

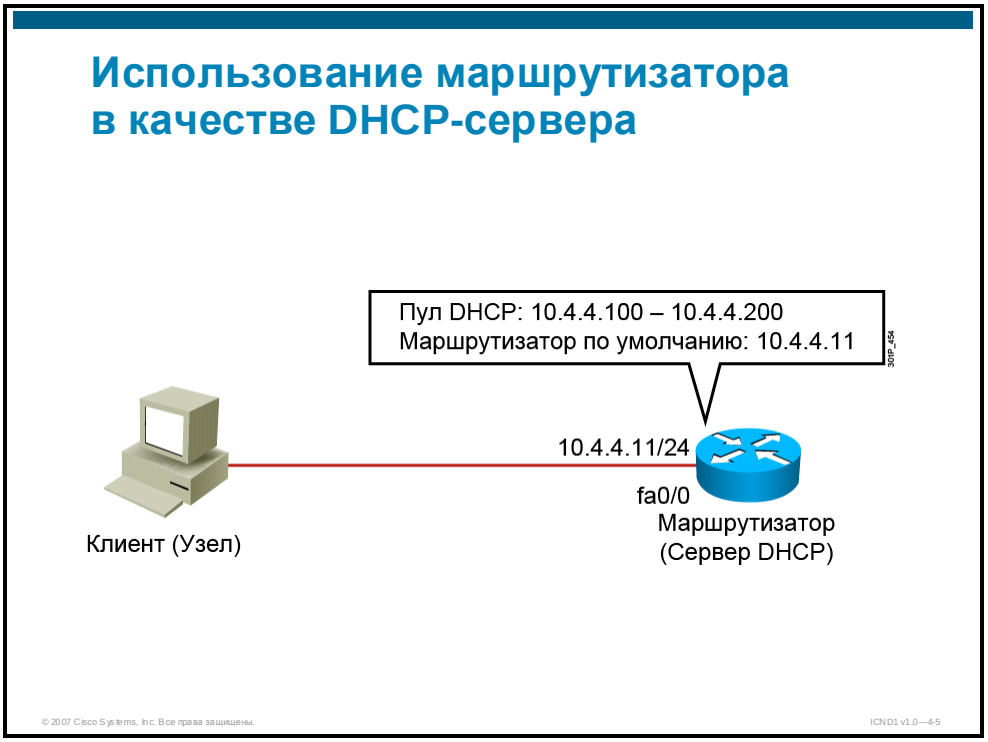


Маршрутизаторы Cisco, работающие под управлением программного обеспечения Cisco IOS, обеспечивают полную поддержку функций DHCP-сервера на маршрутизаторе. DHCP-сервер Cisco IOS является полнофункциональной реализацией DHCP-сервера, который управляет IP-адресами из заданных пулов адресов маршрутизатора и присваивает эти адреса DHCP-клиентам. Можно настроить DHCP-сервер для присвоения дополнительных параметров, таких как IP-адрес DNS-сервера и маршрутизатора по умолчанию.

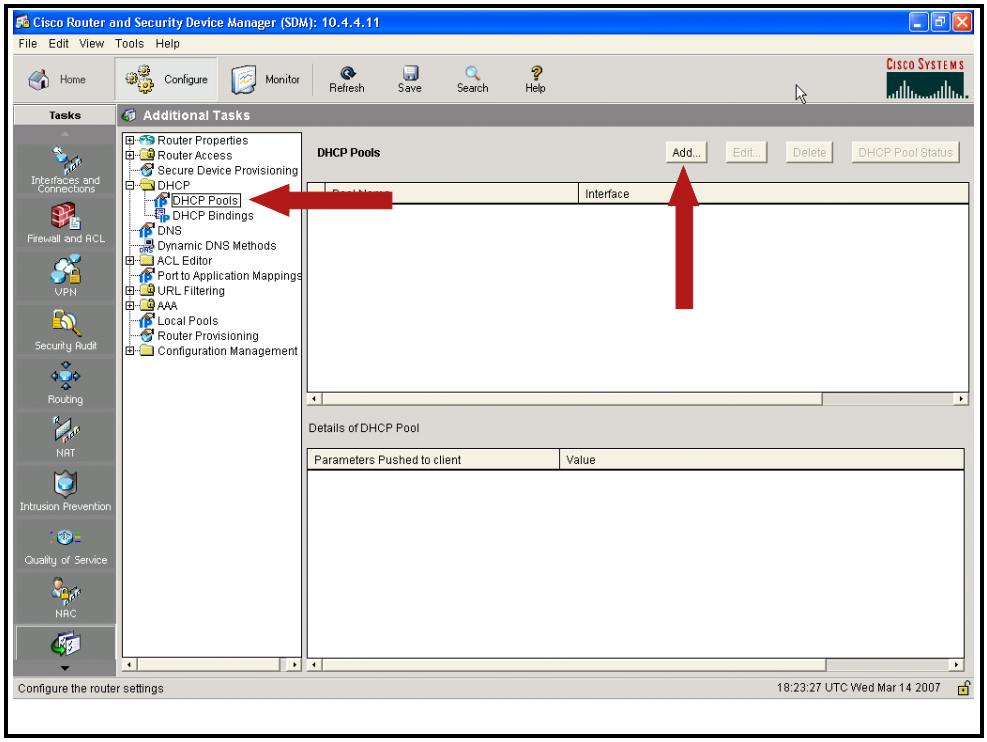
DHCP-сервер Cisco IOS принимает запросы на присвоение и возобновление адресов и присваивает адреса из предварительно заданных групп адресов в пулах DHCP. Кроме того, эти пулы адресов можно настроить на предоставление дополнительных данных запрашивающему клиенту, таких как IP-адрес DNS-сервера, маршрутизатора по умолчанию и другие параметры конфигурации. DHCP-сервер Cisco IOS может принимать широковещательные рассылки из подключенных локально сегментов ЛВС или из запросов DHCP, которые переданы другими агентами передачи DHCP в сети.

Использование Cisco SDM для включения функций DHCP-сервера

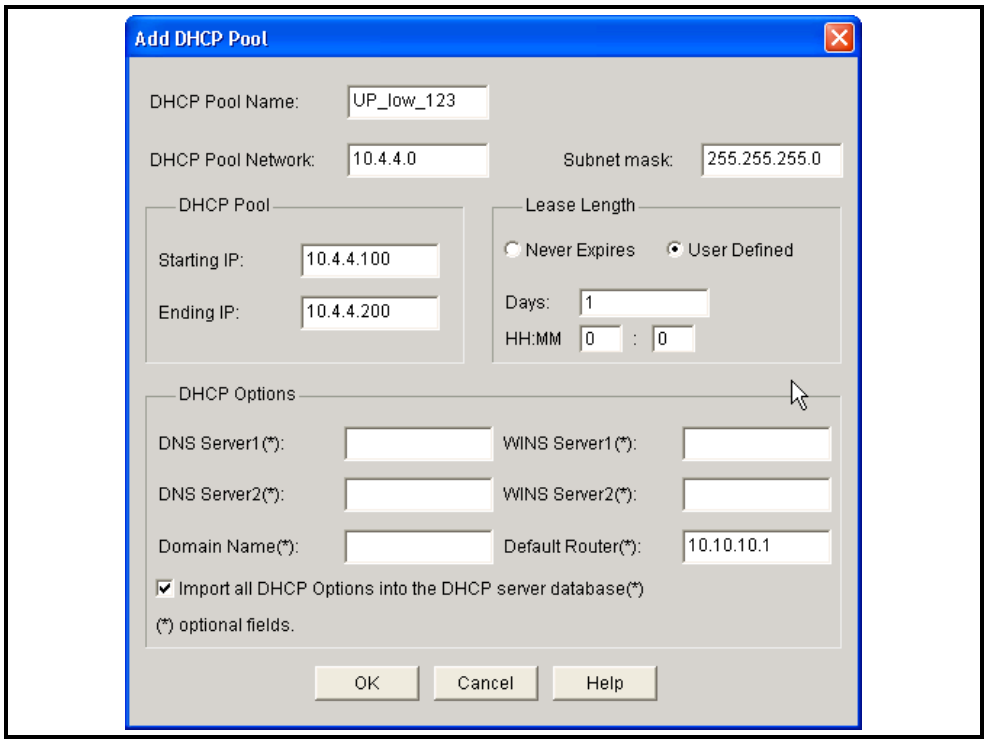
В этом разделе рассматривается использование менеджера Cisco Router and Security Device Manager (SDM) для включения функций DHCP-сервера на маршрутизаторе.



В этом примере DHCP-серверу разрешено использование пула адресов с 10.4.4.100 по 10.4.4.200 для интерфейса 10.4.4.11/24. Этот маршрутизатор будет объявляться маршрутизатором по умолчанию (шлюзом по умолчанию для клиентов).



Функция DHCP-сервера включается на вкладке «Additional Task (Дополнительная задача)». Выберите в каталоге элемент **DHCP Pools (Пулы DHCP)**. Затем нажмите кнопку **Add (Добавить)** для создания нового пула DHCP.



В окне «Add DHCP Pool (Добавить пул DHCP)» можно настраивать пул IP-адресов DHCP. DHCP-сервер присваивает IP-адреса из общего пула, для определения которого задаются начальный и конечный IP-адреса диапазона. В окне «Add DHCP Pool (Добавить пул DHCP)» отображаются следующие поля:

- **DHCP Pool Name (Имя пула DHCP).** Последовательность символов, которая идентифицирует пул DHCP.
- **DHCP Pool Network (Сеть пула DHCP)** и **Subnet Mask (Маска подсети).** DHCP-сервер присваивает IP-адреса из общего пула, для определения которого задаются начальный и конечный IP-адреса диапазона.

  Указанный диапазон адресов должен относиться к следующим диапазонам частных адресов:

  — с 10.1.1.1 по 10.255.255.255;

  — с 172.16.1.1 по 172.31.255.255;

  — с 192.168.0.0 по 192.168.255.255.

  Кроме того, указанный диапазон адресов должен относиться к той же подсети, что и IP-адрес интерфейса ЛВС. Этот диапазон должен включать не более 254 адресов. Ниже приводятся примеры допустимых диапазонов:

  — с 10.1.1.1 по 10.1.1.254 (предполагается, что IP-адрес ЛВС относится к подсети 10.1.1.0);

  — с 172.16.1.1 по 172.16.1.254 (предполагается, что IP-адрес ЛВС относится к подсети 172.16.1.0).

  Система Cisco SDM настраивает маршрутизатор на автоматическое исключение IP-адреса интерфейса ЛВС в данном пуле.

  Нельзя использовать следующие зарезервированные адреса из указываемого диапазона адресов:

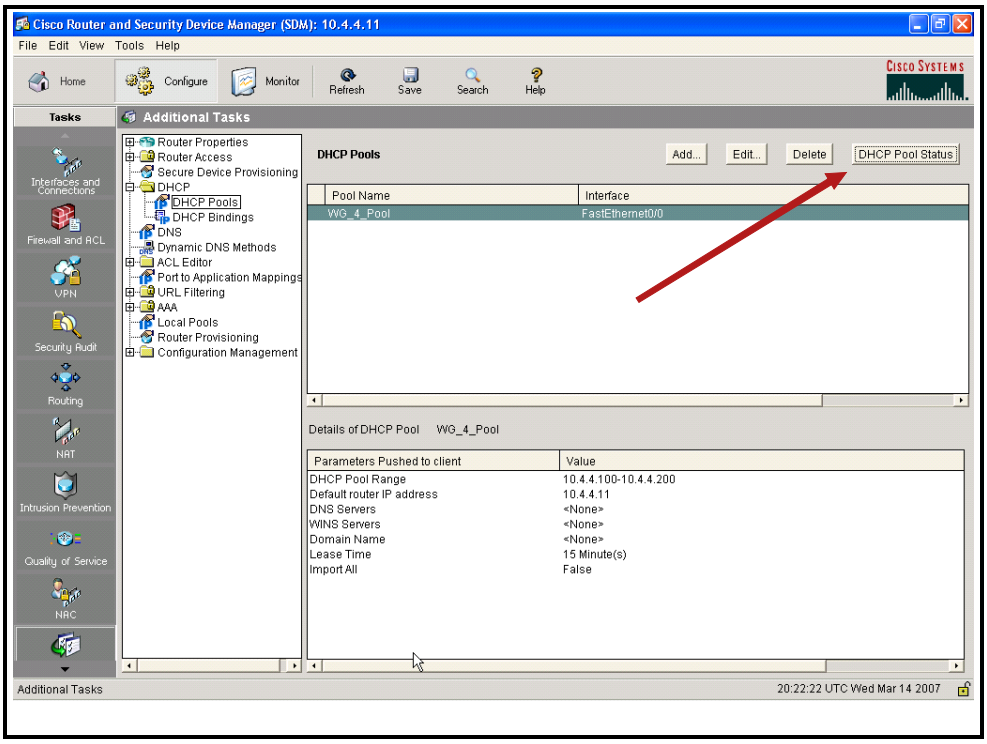
  — IP-адрес сети или подсети;

  — широковещательный адрес сети.
- **Starting IP (Начальный IP-адрес).** Введите начальный IP-адрес диапазона, который будет использоваться DHCP-сервером для присвоения адресов устройствам в ЛВС. Это наименьший IP-адрес диапазона.
- **Ending IP (Конечный IP-адрес).** Введите последний (наибольший) IP-адрес в диапазоне IP-адресов.
- **Lease Length (Время аренды).** Интервал времени, в течение которого клиент может использовать присвоенный адрес перед возобновлением.
- **DHCP Options (Параметры DHCP).** В этой области настраиваются параметры DHCP, которые будут отправляться хостам ЛВС, запрашивающим IP-адреса у маршрутизатора. Эти параметры задаются не для маршрутизатора, а для отправки запрашивающим хостам в ЛВС. Чтобы задать эти свойства для маршрутизатора, выберите **Additional Tasks (Дополнительные задачи)** на панели категорий Cisco SDM, щелкните **DHCP** и настройте эти параметры в окне пула DHCP.
- **DNS Server1 (1-й сервер DNS).** DNS-сервером обычно является сервер, который сопоставляет известное имя устройства с его IP-адресом. Если для сети настроен DNS-сервер, укажите в поле IP-адрес этого сервера.
- **DNS Server2 (2-й сервер DNS).** Если в сети есть дополнительный DNS-сервер, в данном поле можно указать IP-адрес этого сервера.

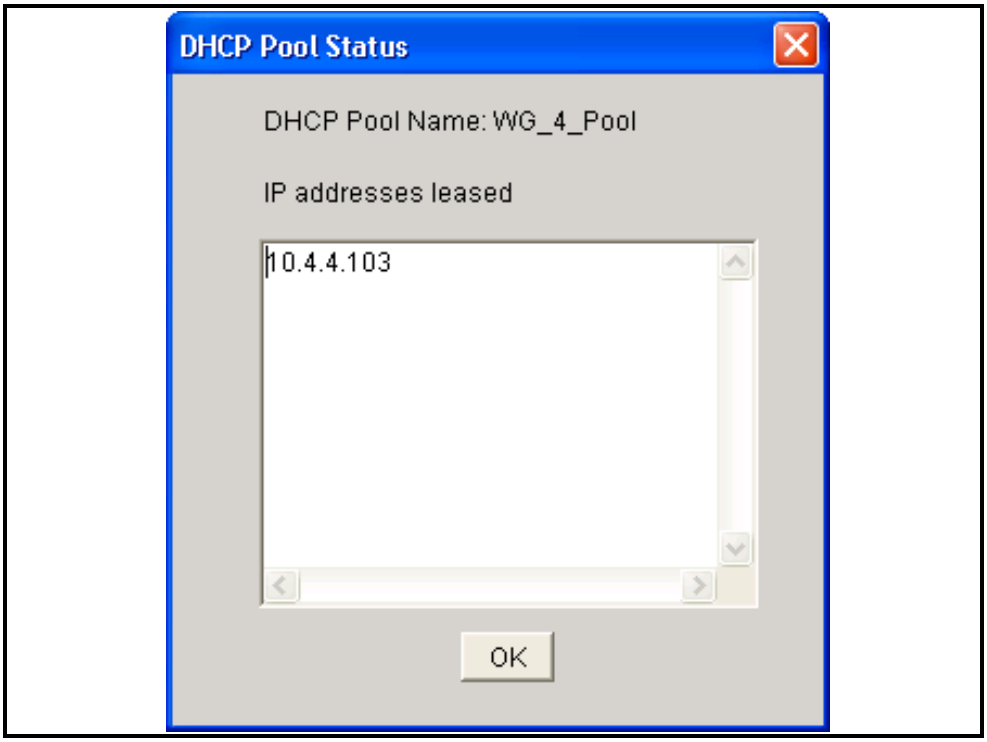
- **Domain Name (Имя домена).** DHCP-сервер, который настраивается на этом маршрутизаторе, будет обслуживать другие устройства в этом домене. Введите имя домена.
- **WINS Server1 (1-й сервер WINS).** Некоторым клиентам для подключения к устройствам в сети Интернет может требоваться сервер Microsoft WINS. Если в сети есть сервер Microsoft WINS, в этом поле можно указать IP-адрес данного сервера.
- **WINS Server2 (2-й сервер WINS).** Если в сети есть дополнительный сервер Microsoft WINS, в этом поле можно указать IP-адрес данного сервера.
- **Default Router (Маршрутизатор по умолчанию).** IP-адрес, который будет предоставляться клиентам для использования в качестве шлюза по умолчанию.
- **Import All DHCP Options into the DHCP Server Database (Импорт всех параметров DHCP в базу данных DHCP-сервера).** Этот флажок позволяет импортировать параметры DHCP с сервера более высокого уровня. Он обычно используется совместно с DHCP-сервером в Интернете.

Мониторинг функций DHCP-сервера

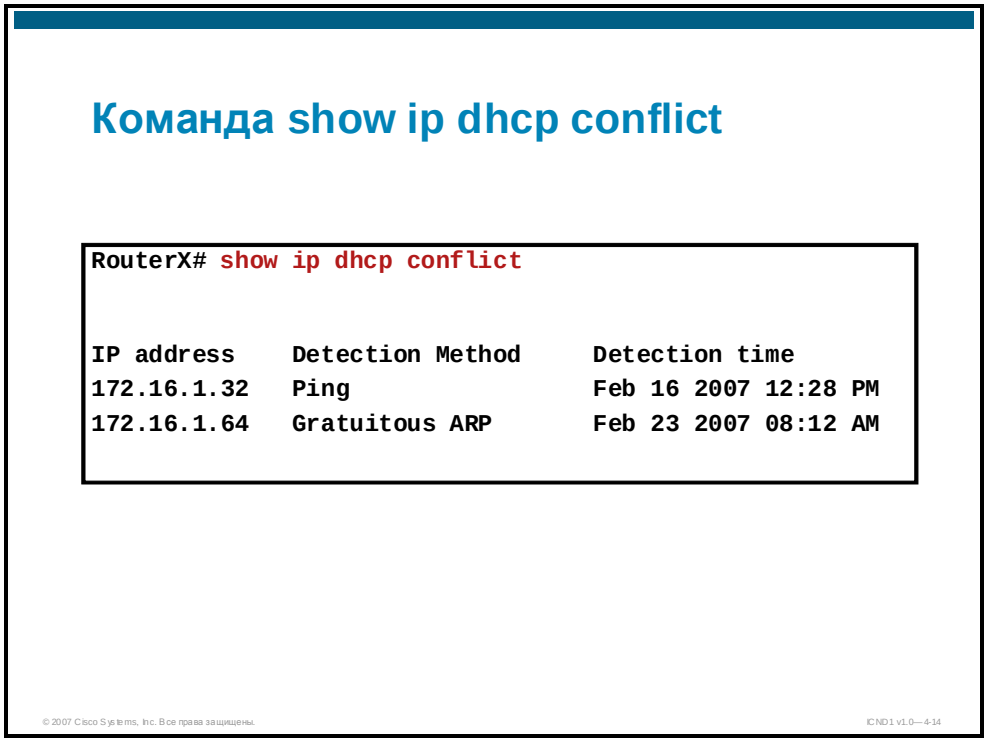
В этом разделе описывается мониторинг функций DHCP-сервера.



Параметры конфигурации DHCP можно проверить на вкладке «DHCP Pools (Пулы DHCP)». Кроме того, с помощью кнопки **DHCP Pool Status (Состояние пула DHCP)** можно вывести дополнительную информацию об арендуемых адресах.



В окне состояния пула DHCP отображается список адресов, арендуемых в данный момент.



Чтобы вывести конфликты адресов, обнаруженные DHCP-сервером при предоставлении адресов клиентам, используйте команду **show ip dhcp conflict** в пользовательском или привилегированном режимах EXEC.

show ip dhcp conflict [*ip-address*]

Для обнаружения конфликтов сервер использует эхо-запросы. Для обнаружения конфликтов клиент использует свободный запрос протокола ARP. Если обнаружен конфликт адресов, соответствующий адрес удаляется из пула и не присваивается до устранения конфликта администратором.

В следующем примере показан метод и время обнаружения для всех IP-адресов, выданных DHCP-сервером и конфликтующих с другими устройствами.

```
Router# show ip dhcp conflict

IP address    Detection Method     Detection time
172.16.1.32   Ping                 Feb 16 1998 12:28 PM
172.16.1.64   Gratuitous ARP       Feb 23 1998 08:12 AM
```

Описания полей вывода команды show ip dhcp conflict

Поле	Описание
IP address	IP-адрес хоста, зарегистрированный на DHCP-сервере
Detection Method	Способ обнаружения IP-адресов хостов на DHCP-сервере: использование эхо-запросов или свободный запрос (gratuitous ARP)
Detection time	Дата и время обнаружения конфликта

Резюме

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

Резюме

- Работа протокола DHCP базируется на модели «клиент-сервер».
- DHCP-сервер выделяет сетевые адреса и предоставляет параметры конфигурации.
- В ПО Cisco IOS входит DHCP-сервер.
- ПО Cisco SDM можно использовать для настройки DHCP-сервера на маршрутизаторе.
- Следующие элементы конфигурации являются обязательными:
  - Имя пула
  - Сеть и подсеть пула
  - Начальный и конечный адреса
- ПО Cisco SDM можно использовать для мониторинга DHCP-сервера на маршрутизаторе.
- Команду **show ip dhcp conflict** можно использовать для поиска конфликтов.

Занятие 10

Доступ к удаленным устройствам

Обзор

Во время текущего технического обслуживания часто бывает необходимо получить доступ к устройству с другого устройства. В программном обеспечении Cisco IOS предусмотрен набор средств для выполнения этой задачи. На этом занятии рассматриваются методы доступа к удаленным устройствам.

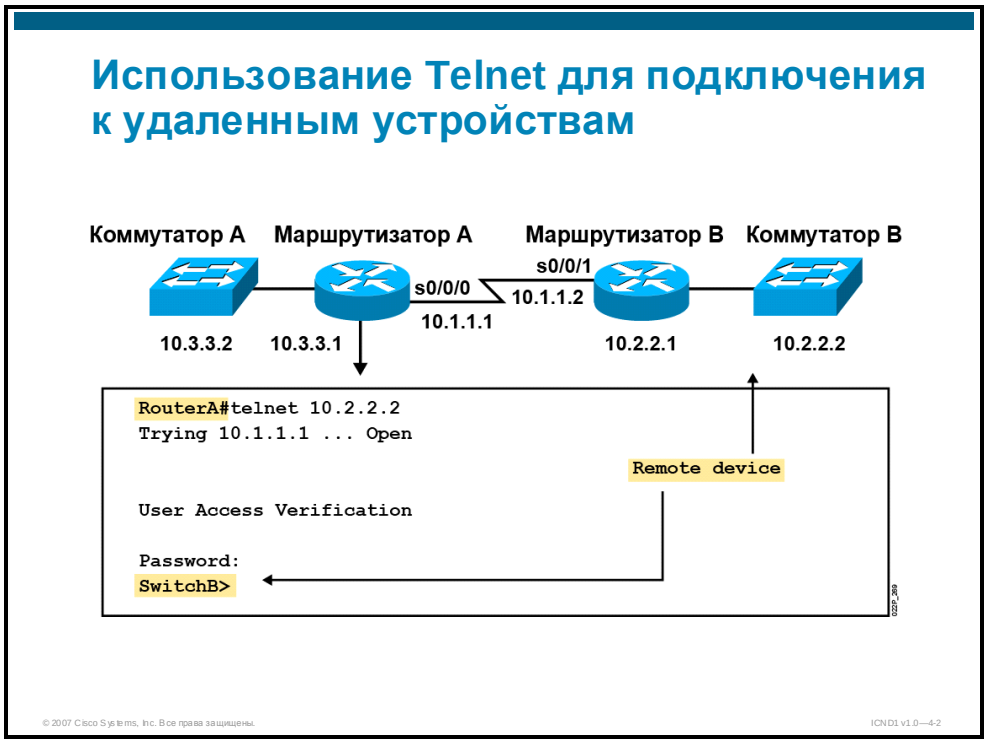
Задачи

По окончании этого занятия вы сможете использовать средства программного обеспечения Cisco IOS для доступа к удаленному устройству. Это значит, что вы сможете выполнять следующие задачи:

- использовать Telnet и SSH для подключения к удаленным сетевым устройствам;
- приостанавливать и возобновлять сеанс Telnet;
- закрывать сеанс Telnet;
- использовать команды программного обеспечения Cisco IOS для проверки подключения.

Установление соединения Telnet или SSH

Приложения Telnet и Secure Shell (SSH) обеспечивают удобный способ подключения к удаленным устройствам. В этом разделе описываются протоколы Telnet и SSH и создание удаленного подключения.



Одним из способов получения информации об удаленном устройстве является подключение к нему с помощью приложений Telnet или SSH. Telnet и SSH являются протоколами виртуального терминала, входящими в стек TCP/IP. Протоколы обеспечивают подключения и сеансы удаленной консоли с одного сетевого устройства к одному или нескольким другим удаленным устройствам.

Протокол Telnet на маршрутизаторах Cisco несколько отличается от протокола Telnet на большинстве коммутаторов Cisco Catalyst.

Telnet

Чтобы войти в систему хоста, поддерживающего протокол Telnet, воспользуйтесь командой **telnet в режиме** EXEC.

telnet *host*

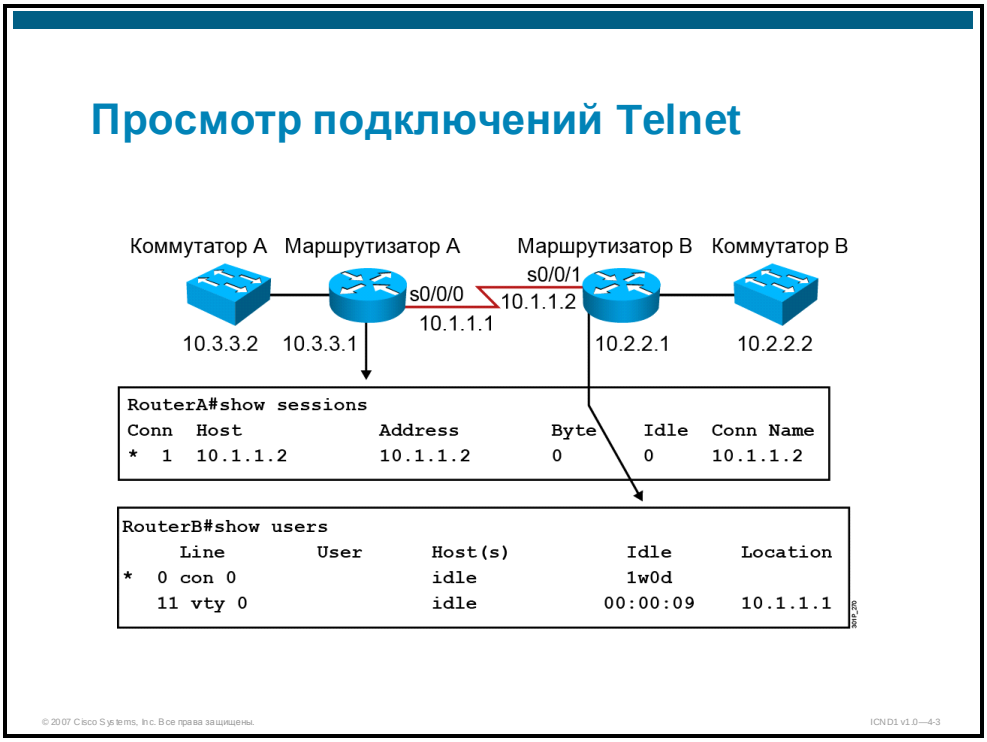
Синтаксис	Описание
host	Имя хоста или IP-адрес

Приложение SSH

Чтобы начать шифрованный сеанс с удаленным сетевым устройством, воспользуйтесь командой **ssh** в пользовательском режиме EXEC.

ssh {*ipaddr* | *hostname*} [*command*]

Синтаксис	Описание
ipaddr | *hostname*	IP-адрес или имя хоста удаленного сетевого устройства



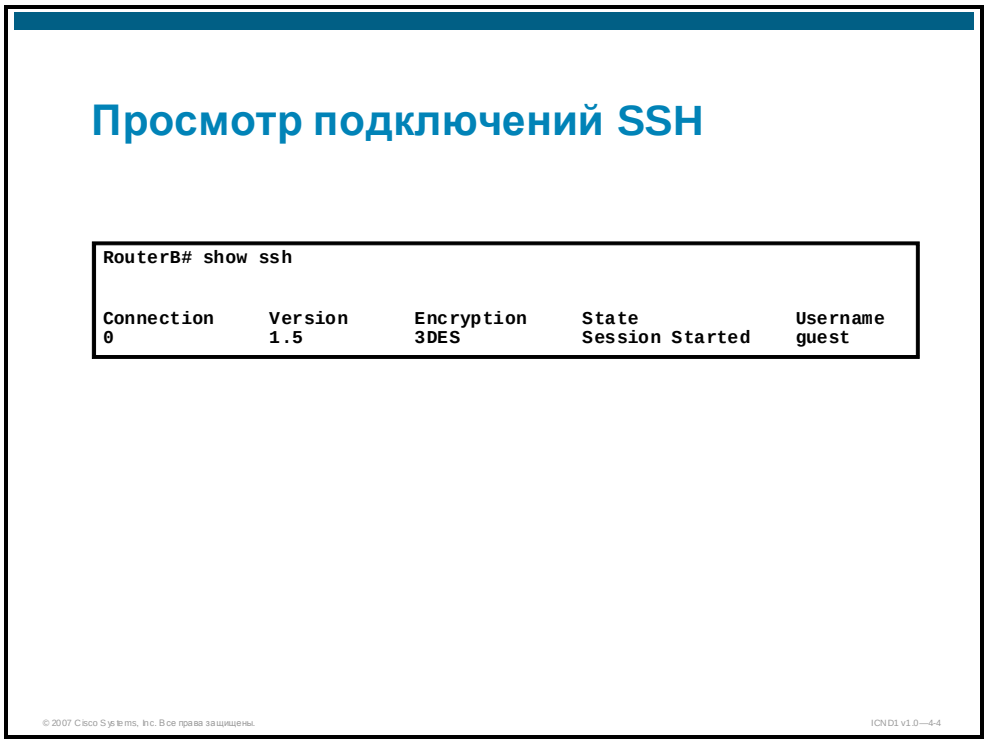
Если на маршрутизаторе установлено программное обеспечение Cisco IOS, для создания Telnet-подключения необходим только IP-адрес или имя хоста конечного устройства. Для создания соединения Telnet с коммутатора Cisco Catalyst используется команда **telnet**, введенная перед IP-адресом или именем хоста конечного устройства.

Появление приглашения при входе в консоль и для маршрутизаторов, и для коммутаторов означает успешное соединение Telnet, если вход в систему включен на портах VTY удаленного устройства. После входа в систему удаленного устройства в строке приглашения консоли указывается активное устройство консоли. В строке приглашения консоли используется имя хоста устройства.

Для проверки Telnet-подключения или вывода списка хостов, с которыми установлено соединение, используйте команду **show sessions** на исходном маршрутизаторе или коммутаторе. Эта команда выводит имя хоста, IP-адрес, число байт, количество времени, в течение которого устройство было неактивно, и имя подключения, присвоенное сеансу. Если выполняется несколько сеансов, знак звездочки (*****) указывает, какой сеанс был последним и к какому сеансу вернется пользователь при нажатии клавиши **Enter**.

На рисунке приводится вывод команды **show sessions** на маршрутизаторе A, который показывает, что маршрутизатор A приостановил сеанс Telnet с маршрутизатором B. Выполнение команды **show users** на маршрутизаторе B позволяет определить последний активный сеанс. Вывод показывает, что последний активный сеанс принадлежал пользователю, подключенному через консольный порт.

Команда **show users** определяет, активен ли консольный порт, и перечисляет все активные сеансы Telnet с IP-адресом или IP-псевдонимом хоста-источника на локальном устройстве. В выводе команды **show users** строка «con» представляет локальную консоль, а строка «VTY» – удаленное соединение. Число «11» рядом со значением VTY в данном примере означают номер линии VTY, а не номер порта. Если пользователей несколько, символ звездочки (*****) обозначает текущего пользователя терминального сеанса.



Команда **show ssh** в привилегированном режиме EXEC отображает состояние подключений к SSH-серверу.

Приостановка и возобновление сеанса Telnet

После подключения к удаленному устройству может возникнуть необходимость в получении доступа к локальному устройству без завершения сеанса Telnet. Приложение Telnet позволяет временно приостановить и затем возобновить удаленный сеанс. В этом разделе описывается приостановка и возобновление сеанса Telnet.

На рисунке показан сеанс Telnet с маршрутизаторе A к маршрутизатору B. Для приостановки сеанса необходимо нажать указанную последовательность клавиш. Приглашение локальной системы свидетельствует о том, что сеанс Telnet приостановлен.

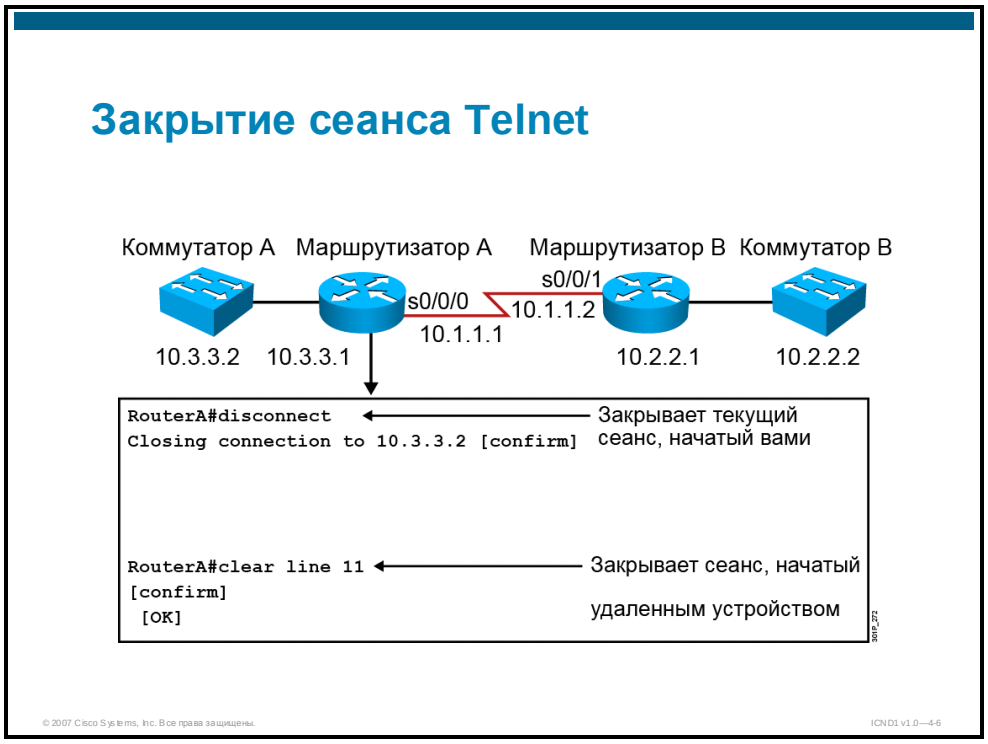
Для приостановки сеанса Telnet и перехода от удаленной конечной системы к локальному коммутатору или маршрутизатору следует воспользоваться командой **Ctrl-Shift-6** или **Ctrl-^** (в зависимости от клавиатуры) а затем отдельно нажать клавишу **x**.

Чтобы возобновить приостановленный сеанс Telnet, выполните следующие действия:

- Нажмите клавишу **Enter**.
- Если существует только один сеанс, введите команду **resume**. (Ввод команды **resume** без указания *номера сеанса* приведет к возобновлению последнего активного сеанса.)
- Введите команду **resume** *номер сеанса*, чтобы возобновить конкретный сеанс Telnet. (Номер сеанса можно узнать с помощью команды **show sessions**.)

Закрытие сеанса Telnet

Сеанс Telnet на устройстве Cisco можно завершить с помощью команд **exit**, **logout**, **disconnect** или **clear**. В этом разделе обсуждаются различные способы закрытия сеанса Telnet.



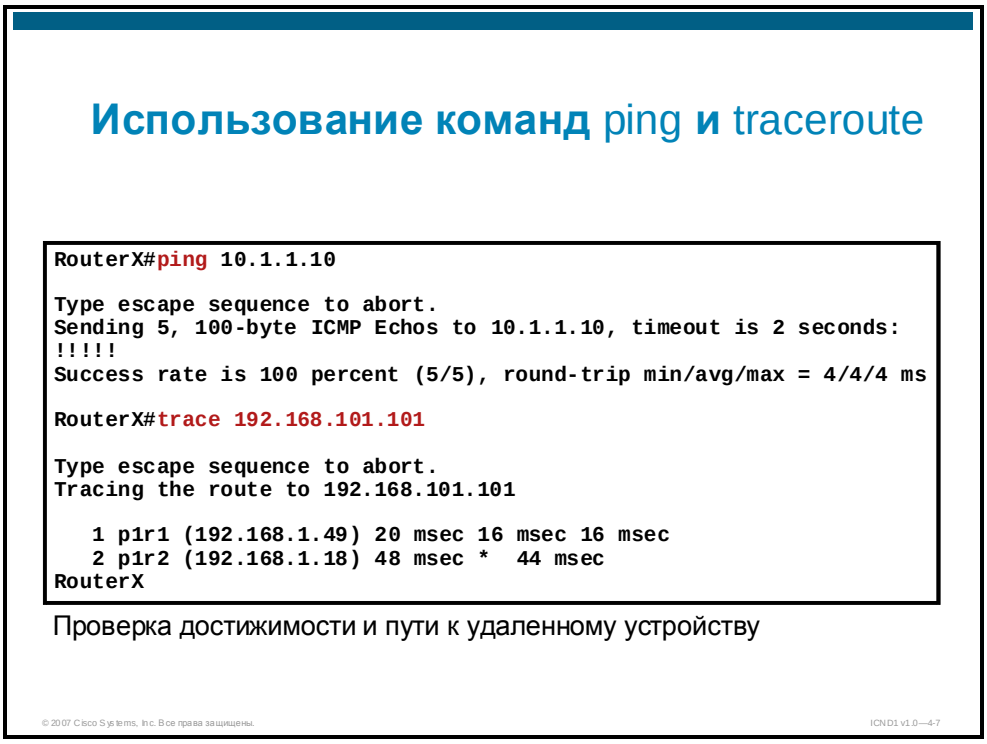
Закрыть сеанс Telnet на сетевом устройстве Cisco можно одним из следующих способов:

- с удаленного устройства, с помощью команды **exit** или **logout**, для выхода из сеанса консоли и возвращения к сеансу с локальным устройством;
- с локального устройства, с помощью команды **disconnect** (если установлено несколько сеансов) или **disconnect session** *номер сеанса* для отключения отдельного сеанса.

Если сеанс Telnet, установленный удаленным пользователем, вызывает проблемы, например, с полосой пропускания, необходимо закрыть сеанс. Кроме того, сеанс может быть завершен персоналом, обслуживающим сеть, со своей консоли. Чтобы закрыть сеанс Telnet с внешнего хоста, используйте команду **clear line** *номер линии*. Параметр *номер линии* соответствует порту VTY входящего сеанса Telnet. Команда **show sessions** позволяет определить параметр *номер линии*. Пользователь на другом конце соединения получает уведомление о том, что соединение закрыто внешним хостом.

Другие способы проверки подключения

Команды **ping** и **traceroute** предоставляют информацию о достижимости удаленного устройства и пути к нему. В этом разделе описывается использование команд **ping** и **traceroute**.



Службы SSH, Telnet и CDP позволяют собирать важную информацию об устройствах локальных и удаленных сетей. Эта информация используется для создания и ведения топологической карты сети.

Кроме того, при тестировании, поиске и устранении неполадок топологии сети могут помочь следующие средства.

- Команда **ping** позволяет проверить сетевые подключения. Она выводит минимальное, среднее и максимальное время, которое требуется пакетам эхо-запроса для поиска указанной системы и возвращения в локальную систему. Это позволяет проверить надежность пути к заданной системе.

В таблице перечислены возможные символы вывода команды **ping**.

Символ	Описание
!	Ответ получен
.	Время ожидания ответа на сетевом сервере истекло
U	Получен элемент информации протокола «destination unreachable»
Q	Переполнение очереди источника (получатель слишком занят)
M	Фрагментация невозможна
?	Неизвестный тип пакета
&	Время жизни пакета истекло

- Команда **traceroute** показывает фактический маршрут пакетов между сетевыми устройствами. Устройство, например маршрутизатор или коммутатор, отправляет последовательность датаграмм UDP на несуществующий адрес порта на удаленном хосте. Посылается три датаграммы, в каждой из которых поле времени жизни (TTL) имеет значение 1. Значение TTL = 1 вызывает истечение времени жизни датаграммы при достижении ею первого маршрутизатора на пути. Маршрутизатор посылает сообщение ICMP «Time Exceeded Message», означающее, что срок жизни датаграммы истек.

  После этого посылаются три следующих сообщения UDP с TTL = 2, которые заставляют второй маршрутизатор возвращать сообщения ICMP «Time Exceeded Message». Этот процесс продолжается до тех пор, пока пакеты не достигнут места назначения. Поскольку эти датаграммы пытаются получить доступ к недействительному порту на узле-получателе, будут получены сообщения ICMP «Port Unreachable». Цель состоит в регистрации источника каждого сообщения ICMP TEM, что позволяет проследить путь пакета к месту назначения.

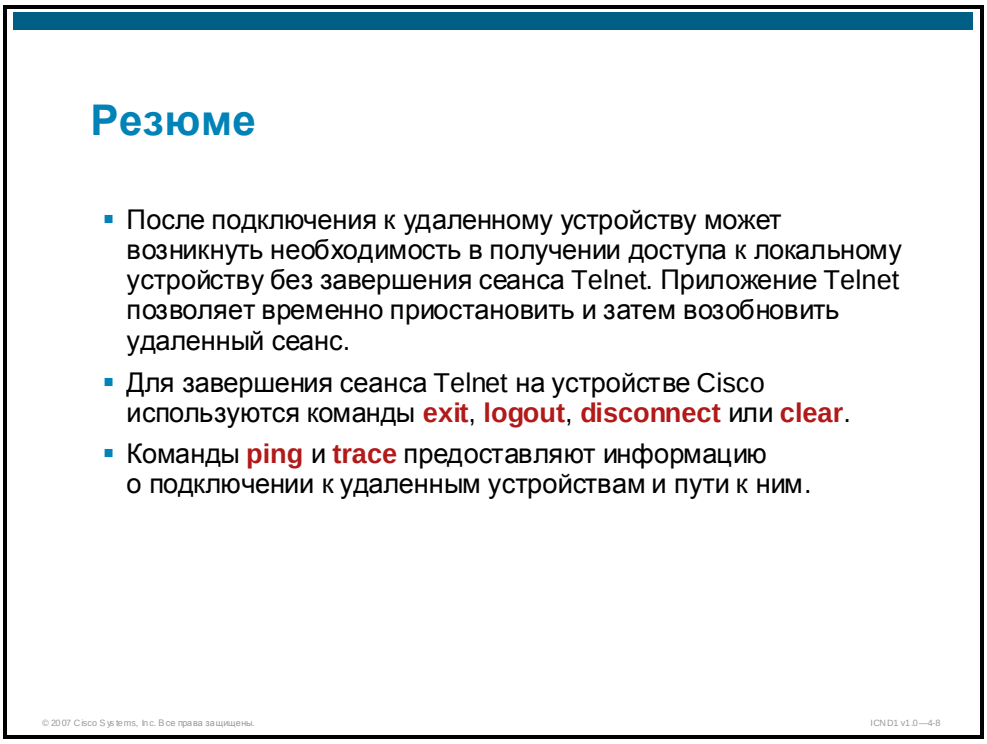
В таблице перечислены символы, которые могут появиться в выводе команды **traceroute**.

Символ	Описание
nn msec	Время прохождения сигнала в прямом и обратном направлении (RTT) в миллисекундах для каждого узла для заданного числа проб
*	Время ожидания ответа истекло
A	Административно запрещено (например, список доступа)
Q	Переполнение очереди источника (получатель слишком занят)
I	Прервано пользователем
U	Порт недостижим
H	Хост недостижим
N	Сеть недостижима
P	Протокол недостижим
T	Истечение времени ожидания
?	Неизвестный тип пакета

Примечание Если включено разрешение доменного имени по IP, маршрутизатор будет пытаться получить для каждого IP-адреса имя, что приведет к замедлению выполнения команды **traceroute**.

Резюме

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



Резюме модуля

В этом разделе приводится резюме вопросов, рассмотренных в модуле.

Резюме модуля

- Маршрутизаторы Cisco функционируют на уровне 3, и их задача заключается в определении пути.
- Двоичные числа основаны на степенях двойки.
- IP-адресация:
  - представление двоичной строки в десятичном формате с точками;
  - определяет сеть, подсеть и хост.
- В процессе запуска маршрутизаторов проверяется аппаратное обеспечение, загружается операционная система и конфигурация.

Резюме модуля (прод.)

- Базовая конфигурация маршрутизатора обычно осуществляется через консольный порт с помощью интерфейса командной строки и требует назначения адреса хоста и IP-адресов интерфейсов.
- Маршрутизаторы подвержены тем же угрозам со стороны окружающей среды, опасностям повреждения аппаратного обеспечения, электрическим и эксплуатационным угрозам, что и коммутаторы.
- Базовые средства безопасности маршрутизатора включают баннерное сообщение, а также настройку Telnet и SSH.

Резюме модуля (прод.)

- DHCP-сервер Cisco IOS является полнофункциональным DHCP-сервером, который можно настроить с помощью Cisco SDM.
- Команды Cisco IOS обеспечивают набор инструментов для удаленного доступа и тестирования, в том числе:
  - Telnet
  - SSH
  - **ping**
  - **traceroute**

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 компонента из перечисленных ниже являются общими для маршрутизаторов, коммутаторов и компьютеров? (Выберите три варианта.) (Источник: изучение функций маршрутизации)

А. ОЗУ;
Б. ЦП;
В. материнская плата;
Г. клавиатура.

В2) Укажите два типа портов маршрутизаторов. (Выберите два варианта.) (Источник: изучение функций маршрутизации)

А. принтерный;
Б. консольный;
В. сетевой;
Г. порт CD-ROM;
Д. USB.

В3) Какие два утверждения лучше всего описывают функции маршрутизатора в сети? (Выберите два варианта.) (Источник: изучение функций маршрутизации)

А. Маршрутизаторы ведут таблицы маршрутизации и обмениваются данными об изменениях в сети с другими маршрутизаторами.
Б. Маршрутизаторы используют таблицу маршрутизации, чтобы определить место назначения пересылки пакетов.
В. Маршрутизаторы усиливают сигнал на больших расстояниях в сети.
Г. Маршрутизаторы создают домены коллизий большего размера.
Д. Маршрутизаторы используют протокол ICMP для обмена сетевой информацией из своей таблицы маршрутизации с другими маршрутизаторами.

В4) Какие три из следующих утверждений о процессе определения пути являются верными? (Выберите три варианта.) (Источник: изучение функций маршрутизации)

А. Маршрутизаторы оценивают доступные пути к месту назначения.
Б. Процесс маршрутизации использует метрики и административные расстояния при оценке сетевых путей.
В. Динамическая маршрутизация выполняется при настройке администратором информации на каждом маршрутизаторе.
Г. Динамическая маршрутизация выполняется при получении данных маршрутизации по протоколам маршрутизации.
Д. Маршрут по умолчанию представляет явный маршрут к каждой сети.
Е. В таблице маршрутизации сохраняется несколько записей для каждой сети.

В5) Расположите шаги процесса маршрутизации в правильном порядке. (Источник: изучение функций маршрутизации)

_____ 1. Шаг 1.

_____ 2. Шаг 2.

_____ 3. Шаг 3.

_____ 4. Шаг 4.

_____ 5. Шаг 5.

А. Маршрутизатор деинкапсулирует кадр и, используя информацию протокола кадра, определяет, что пакет сетевого уровня будет передан в процесс IP.

Б. Если целевая сеть напрямую связана с сетью-источником, маршрутизатор использует процесс ARP для получения MAC-адреса хоста и направляет его в сегмент сети. Если доступ к сети осуществляется через другой маршрутизатор, первый маршрутизатор использует MAC-адрес маршрутизатора следующего перехода и пересылает пакет через интерфейс, указанный в таблице маршрутизации.

В. Маршрутизатор проверяет адрес назначения в заголовке IP и определяет, является ли он сам получателем пакета, или необходимо переслать его далее. Если необходимо переслать пакет, маршрутизатор ищет в таблице маршрутизации путь для отправки пакета.

Г. Исходящий интерфейс инкапсулирует пакет в соответствии со средой и передает пакет в сегмент сети.

Д. Маршрутизатор получает пакет на одном из интерфейсов.

В6) В каком из элементов содержатся данные маршрутизации, которые позволяют маршрутизатору определить путь маршрутизации? (Источник: изучение функций маршрутизации)

А. IP-адрес;

Б. MAC-адрес;

В. таблица маршрутизации;

Г. протокол маршрутизации.

В7) Какие три утверждения описывают функцию таблиц маршрутизации? (Выберите три варианта.) (Источник: изучение функций маршрутизации)

А. Таблицы маршрутизации включает упорядоченный список известных сетевых адресов.

Б. Таблицы маршрутизации ведутся путем передачи MAC-адресов.

В. Таблицы маршрутизации содержат метрики, используемые для определения целесообразности маршрута.

Г. С помощью привязок в таблице маршрутизации маршрутизатор узнает о том, можно ли достичь определенного пункта назначения напрямую или через другой маршрутизатор (маршрутизатор следующего перехода).

Д. Когда маршрутизатор получает входящий пакет, он использует адрес источника и ищет в таблице маршрутизации оптимальный путь от этого источника.

Е. Протоколы маршрутизации могут быть разными, но не метрики маршрутизации.

В8) Сопоставьте каждый метод заполнения таблицы маршрутизации с его определением. (Источник: изучение функций маршрутизации)

_____ 1. Эта запись создается на основе интерфейсов, подключенных к сегментам сети напрямую. Эта запись наиболее достоверна; в случае сбоя или административного отключения интерфейса запись для этой сети удаляется из таблицы маршрутизации.

_____ 2. Это необязательная запись, которая используется, если в таблице маршрутизации не найден явно заданный путь к месту назначения. Эта запись может вводиться вручную или с помощью протокола динамической маршрутизации.

_____ 3. Эти маршруты вводятся системным администратором вручную непосредственно в конфигурацию маршрутизатора.

_____ 4. Эти маршруты изучаются маршрутизатором. Такая информация постоянно меняется в соответствии с изменениями в сети.

А. Статическая маршрутизация.
Б. Динамическая маршрутизация.
В. Маршрут по умолчанию.
Г. Напрямую подключенные сети.

В9) Какие три метрики используются протоколами маршрутизации в большинстве случаев для определения сетевого пути? (Выберите три варианта.) (Источник: изучение функций маршрутизации)

А. Число переходов.
Б. Полоса пропускания.
В. Задержка.
Г. Длина пакета.
Д. Расстояние.
Е. Количество.

В10) Какие три утверждения точно описывают протокол на базе векторов расстояния? (Выберите три варианта.) (Источник: изучение функций маршрутизации)

А. Протокол IGRP был разработан компанией Cisco для маршрутизации в локальных сетях среднего размера.
Б. Примерами этого протокола могут служить протоколы RIP и IGRP.
В. Этот протокол определяет направление (вектор) и расстояние (число переходов) до любой сети в интерсети.
Г. При использовании этого протокола маршрутизатор не должен знать весь путь к каждому сегменту сети.
Д. Этот процесс также называется «маршрутизацией по слухам»
Е. Маршрутизатор, на котором выполняется протокол маршрутизации на базе векторов расстояния, отправляет периодические обновления только при наличии изменений в сети.

В11) Какие три утверждения точно описывают протокол состояния канала? (Выберите три варианта.) (Источник: изучение функций маршрутизации)

База данных состояния каналов используется для расчета путей с максимальной полосой пропускания в сети.
Протоколы состояния канала быстро реагируют на изменения в сети.
В протоколах состояния канала каждый маршрутизатор отправляет в сеть сообщения со списком маршрутизаторов, с которыми он непосредственно связан, и информацией о состоянии канала с каждым маршрутизатором.
Протоколы состояния канала отправляют периодические обновления (обновления состояния канала) через продолжительные интервалы времени, примерно каждые 30 минут.
В протоколах состояния канала каждый маршрутизатор пытается создать собственную внутреннюю схему топологии сети.
Протоколы состояния канала периодически отправляют обновления даже при отсутствии изменений в сети.

В12) Во всех компьютерах используется _____. (Источник: общие сведения о двоичной системы счисления)

Система с основанием 10
Десятичная система
Численная система
Двоичная система

В13) Десятичное число 10 преобразуется в двоичное число _____. (Источник: общие сведения о двоичной системы счисления)

А. 10
Б. 1010
В. 110
Г. 1000

В14) Какие из приведенных ниже двоичных октетов имеют нулевой младший бит (LSB)? (Источник: общие сведения о двоичной системы счисления)

А. 01100011
Б. 10100101
В. 10011010
Г. 10011001

В15) IP-адреса представляются в виде _____. (Источник: общие сведения о двоичной системы счисления)

А. 32-битные двоичные числа
Б. 16-битные десятичные числа
В. 8-битные двоичные числа
Г. 8 наборов 4-битных десятичных чисел

В16) 2 в степени 5 это _____. (Источник: общие сведения о двоичной системы счисления)

А. 2 * 5
Б. 128
В. число 2, умноженное на себя 5 раз
Г. ничего из вышеперечисленного

B17) Десятичное число 205 преобразуется в двоичное число _____. (Источник: общие сведения о двоичной системы счисления)

А. 11011101
Б. 11001001
В. 110001019
Г. 11001101

B18) Десятичное число 452, преобразованное в двоичное число путем последовательного деления на 2, равно _____. (Источник: общие сведения о двоичной системы счисления)

А. 111000100
Б. 110000100
В. 111001100
Г. 101000100

B19) Какому десятичному числу соответствует двоичное число 11000111? (Источник: общие сведения о двоичной системы счисления)

А. 218
Б. 199
В. 179
Г. 208

B20) Двоичное число 11101000111, преобразованное в десятичное число путем возведения в степень числа 2, равно _____. (Источник: общие сведения о двоичной системы счисления)

А. 1183
Б. 1873
В. 1638
Г. 1863

B21) Сколько октетов содержится в поле хоста сети класса А? (Источник: построение схемы сетевой адресации)

А. 3
Б. 2
В. 1
Г. 4

B22) Какое минимальное количество бит можно использовать для создания подсети? (Источник: построение схемы сетевой адресации)

А. 1
Б. 2
В. 3
Г. 4

B23) Сколько доступных подсетей можно создать с помощью 6 бит подсети? (Источник: построение схемы сетевой адресации)

А. 58
Б. 60
В. 62
Г. 66

В24) Сколько адресов хостов можно использовать в сети класса C? (Источник: построение схемы сетевой адресации)

А. 253
Б. 254
В. 255
Г. 256

В25) Какое максимальное количество бит можно использовать для создания подсети для сети класса C? (Источник: построение схемы сетевой адресации)

А. 2
Б. 4
В. 6
Г. 8

В26) На анализ какой части IP-адреса маска подсети настраивает маршрутизатор? (Источник: построение схемы сетевой адресации)

А. Биты маски и хоста
Б. Биты хоста и сети
В. Биты хоста и подсети
Г. Биты сети и подсети

В27) Если маршрутизатору не удается сопоставить соответствующую часть адреса с номером в таблице маршрутизации, он _____. (Источник: построение схемы сетевой адресации)

А. возвращает пакет отправителю;
Б. передает пакет следующему маршрутизатору в иерархии;
В. добавляет этот номер в таблицу;
Г. отбрасывает пакет.

В28) Какая из перечисленных ниже масок подсети приходится на границы октета? (Источник: построение схемы сетевой адресации)

А. 255.0.0.0
Б. 255.255.0.0
В. 255.255.255.0
Г. все вышеперечисленное

В29) Какие два номера являются двоичными масками подсети по умолчанию? (Выберите два варианта.) (Источник: построение схемы сетевой адресации)

А. 11111111.00000000.00000000.00000000
Б. 11111111.11111111.01000000.00000000
В. 11111111.11111111.11111111.00000000
Г. 255.255.224.0

В30) Какую часть IP-адреса 172.17.128.47 будет искать маршрутизатор для маски подсети 255.255.0.0? (Источник: построение схемы сетевой адресации)

А. 172.17.128.47
Б. 172.17.128
В. 172.17
Г. 10.172.47

В31) 255.255.224.0 преобразуется в двоичное число _____.(Источник: построение схемы сетевой адресации)

А. 11111111.00000000.11100000.00000000
Б. 11111111.11100000.00000000.00000000
В. 11111111.11111111.11100000.00000000
Г. 11111111.11111111.11110000.00000000

В32) Чтобы определить количество бит, которое необходимо заимствовать из идентификатора хоста в адресе сети для создания необходимого числа подсетей, нужно _____. (Источник: построение схемы сетевой адресации)

А. вычесть необходимое количество подсетей из идентификатора хоста;
Б. добавлять значения бит справа налево, пока итог (десятичное значение) не превысит необходимое количество сетей;
В. добавлять значения бит слева налево, пока итог (десятичное значение) не превысит необходимое количество сетей;
Г. ничего из вышеперечисленного.

В33) Как включить маршрутизатор Cisco? (Источник: запуск маршрутизатора Cisco)

А. Нажать клавишу **Reset (Сброс)**.
Б. Нажать кнопку включения питания маршрутизатора.
В. Подключить волоконно-оптический кабель к другому маршрутизатору.
Г. Вставить вилку кабеля питания в штепсельную розетку питания маршрутизатора.

В34) Что отображается на консоли при запуске маршрутизатора Cisco? (Источник: запуск маршрутизатора Cisco)

А. Сообщения отладки Cisco IOS.
Б. Меню диагностики консоли.
В. Вывод программного обеспечения Cisco IOS.
Г. Изображение текущего состояния светодиодного индикатора.

В35) Каково основное назначение режима установки маршрутизатора Cisco? (Источник: запуск маршрутизатора Cisco)

А. Отображение текущей конфигурации маршрутизатора.
Б. Проверка оборудования и интерфейса.
В. Создание минимальной конфигурации.
Г. Полная настройка маршрутизатора Cisco для IP-маршрутизации.

В36) Какое утверждение лучше описывает команды пользовательского режима EXEC, позволяющие настраивать маршрутизатор Cisco? (Источник: запуск маршрутизатора Cisco)

А. Настройка невозможна, команды пользовательского режима используются для вывода информации.
Б. Пользовательский режим EXEC позволяет выполнять задачи глобальной конфигурации, затрагивающие весь маршрутизатор.
В. Команды пользовательского режима EXEC позволяют ввести секретный пароль, позволяющий настроить маршрутизатор.
Г. Команды пользовательского режима EXEC позволяют настраивать интерфейсы, субинтерфейсы, каналы и маршрутизаторы.

B37) Какая команда Cisco IOS используется для возвращения в пользовательский режим EXEC из привилегированного режима EXEC? (Источник: запуск маршрутизатора Cisco)

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

B38) Сопоставьте каждый тип справки, доступный в интерфейсе командной строки Cisco IOS, с его описанием. (Источник: запуск маршрутизатора Cisco)

_____ 1. Контекстная справка.

_____ 2. Сообщения об ошибках консоли.

_____ 3. Буфер журнала команд.

А. Выдает список команд и параметров, связанных с конкретной командой.
Б. Позволяет повторно вызывать длинные или сложные команды или записи для повторного ввода, просмотра или исправления.
В. Определяет неправильно введенные команды маршрутизатора, позволяя изменить или исправить эти команды.

B39) Какую информацию о маршрутизаторе Cisco выводит команда **show running-config**? (Источник: запуск маршрутизатора Cisco)

А. Текущая (выполняемая) конфигурация в ОЗУ.
Б. Системное оборудование и имена файлов конфигурации.
В. Объем памяти NVRAM, используемый для хранения конфигурации.
Г. Версия программного обеспечения Cisco IOS, выполняемого на маршрутизаторе.

B40) Какие команды Cisco IOS выводят конфигурацию системного оборудования и информацию о версии программного обеспечения? (Источник: запуск маршрутизатора Cisco)

А. **show version**
Б. **show interfaces**
В. **show startup-config**
Г. **show running-config**

B41) Сопоставьте каждое приглашение маршрутизатора с соответствующим режимом конфигурации. (Источник: настройка маршрутизатора Cisco)

_____ 1. Канал.

_____ 2. Протокол динамической маршрутизации.

_____ 3. Интерфейс.

_____ 4. Контроллер.

_____ 5. Подинтерфейс.

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

В42) Что происходит при вводе основной команды на маршрутизаторе Cisco? (Источник: настройка маршрутизатора Cisco)

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

В43) Какая команда Cisco IOS позволяет создать сообщение, отображаемое при входе в систему маршрутизатора? (Источник: настройка маршрутизатора Cisco)

А. **hostname** *имя_хоста*
Б. **banner motd** *сообщение*
В. **hostname interface description**
Г. **description interface description**

В44) Если на маршрутизаторе настроены обе команды, **enable secret** и **enable password**, как вызвать приглашение #? (Источник: настройка маршрутизатора Cisco)

А. Ввести команду **enable** и затем ввести пароль **enable secret**.
Б. Ввести команду **enable password**.
В. Ввести команду **enable secret** или **enable password**.
Г. Ввести обе команды **enable secret** и **enable password**.

В45) Какую команду Cisco IOS следует использовать для задания времени ожидания сеанса консоли 15 минут 30 секунд? (Источник: настройка маршрутизатора Cisco)

А. **set exec timeout 15 30**
Б. **console timeout 15 30**
В. **timeout 15 30**
Г. **exec-timeout 15 30**

В46) Какие команды Cisco IOS настраивают последовательный порт в слоте 0, порт 1, на модульном маршрутизаторе? (Источник: настройка маршрутизатора Cisco)

А. **interface serial 0-0-1**
Б. **interface serial 001**
В. **interface serial 0/0/1**
Г. **interface serial 0/0-1**

В47) Какую команду Cisco IOS следует использовать для настройки тактовой скорости 64 Кбит/с на последовательном интерфейсе маршрутизатора Cisco? (Источник: настройка маршрутизатора Cisco)

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

В48) Последовательный интерфейс выводит «Serial1 is up, line protocol is down». Какие две ситуации могут вызвать эту ошибку? (Выберите два варианта.) (Источник: настройка маршрутизатора Cisco)

А. Не задана тактовая частота.
Б. Интерфейс отключен вручную.
В. К последовательному интерфейсу не подключен кабель.
Г. Отсутствуют сообщения "keepalives".
Д. Несоответствие типа инкапсуляции.

В49) Что из нижеперечисленного может считаться физической угрозой? (Выберите два варианта.) (Источник: общие сведения о безопасности маршрутизатора Cisco)

А. Пользователь оставляет пароль без присмотра на столе.
Б. Отключение кем-либо питания коммутатора для блокировки доступа к сети.
В. Отключение кем-либо системы вентиляции в сетевом отсеке.
Г. Проникновение постороннего в стол, в котором хранится сетевая документация.

В50) Какие четыре элемента из перечисленных ниже можно защитить паролем? (Выберите четыре ответа.) (Источник: общие сведения о безопасности маршрутизатора Cisco)

А. Доступ к консоли.
Б. Доступ к vty.
В. Доступ к tty.
Г. Доступ на уровне пользователя.
Д. Доступ на уровне EXEC.

В51) Что из нижеперечисленного является настраиваемым текстом, отображаемым перед запросом имени пользователя и пароля для входа в систему? (Источник: общие сведения о безопасности маршрутизатора Cisco)

А. Баннер «Сообщение дня».
Б. Баннер входа.
В. Предупреждение доступа.
Г. Пользовательский баннер.
Д. Предупреждающее сообщение.

В52) Что из нижеперечисленного является наиболее безопасным методом удаленного доступа к сетевому устройству? (Источник: общие сведения о безопасности маршрутизатора Cisco)

А. HTTP
Б. Telnet
В. SSH
Г. RMON
Д. SNMP

В53) Какое из следующих утверждений описывает Cisco Router and Security Device Manager? (Источник: использование Cisco SDM)

А. Это система управления на основе ПК, которая может использоваться для настройки таких функций, как DHCP-сервер.
Б. Это система управления на базе веб-интерфейса, которая может использоваться для настройки таких функций, как DHCP-сервер.
В. Это серверная система управления, которая может использоваться для настройки таких функций, как DHCP-сервер.
Г. Это система управления на основе клиента, которая может использоваться для настройки таких функций, как DHCP-сервер.

В54) Где хранятся файлы Cisco SDM? (Источник: использование Cisco SDM)

А. ПК
Б. Маршрутизатор
В. Локальный клиент
Г. Сетевой сервер

В55) Какие две функции являются функциями DHCP? (Выберите два варианта.) (Источник: использование маршрутизатора Cisco в качестве DHCP-сервера)

А. DHCP динамически назначает клиентским устройствам имена хостов.
Б. DHCP динамически назначает клиентским устройствам IP-адреса.
В. DHCP динамически назначает клиентским устройствам шлюз по умолчанию.
Г. DHCP динамически назначает клиентским устройствам уровни доступа системы безопасности.

В56) Какое из следующих утверждений описывает DHCP-сервер программного обеспечения Cisco IOS? (Источник: использование маршрутизатора Cisco в качестве DHCP-сервера)

А. Это полнофункциональный DHCP-сервер.
Б. Он поддерживает только назначение клиентам IP-адресов.
В. Его роль состоит в получении данных DHCP с главного сервера DHCP.
Г. Он поддерживает только назначение клиентам IP-адресов и шлюзов по умолчанию.

В57) Какие четыре элемента являются обязательными параметрами DHCP при настройке DHCP-сервера на маршрутизаторе Cisco? (Выберите четыре ответа.) (Источник: использование маршрутизатора Cisco в качестве DHCP-сервера)

А. Имя пула.
Б. Время аренды.
В. Имя домена.
Г. Маршрутизатор по умолчанию.
Д. Адреса DNS-сервера.
Е. Адреса WINS-сервера.
Ж. Сеть и подсеть DHCP.
З. Начальный и конечный адреса.

В58) Какую команду можно использовать, чтобы определить, используется ли данный адрес из пула DHCP? (Источник: использование маршрутизатора Cisco в качестве DHCP-сервера)

А. **sh ip dhcp bindings**
Б. **sh ip dhcp database**
В. **sh ip dhcp mapping**
Г. **sh ip dhcp conflicts**

В59) Что из нижеперечисленного относится к инструментам Cisco IOS, которые используются для безопасного удаленного доступа к другому устройству? (Источник: доступ к удаленным устройствам)

А. SSH.
Б. SDM.
В. ping
Г. Telnet
Д. traceroute

В60) Какая команда используется для просмотра сеансов связи Telnet с вашим маршрутизатором? (Источник: доступ к удаленным устройствам)

А. show user
Б. show telnet
В. show sessions
Г. show connections

В61) Что из нижеперечисленного используется для приостановки сеанса Telnet? (Источник: доступ к удаленным устройствам)

А. Ключевое слово end.
Б. Ключевое слово suspend.
В. Сочетание клавиш Ctrl-Shift-6.
Г. Сочетание клавиш Ctrl-Shift-Del.

Ответы на вопросы для самопроверки по модулю

В1) А, Б, В

В2) Б, В

В3) А, Б

В4) А, Б, Г

В5) 1 = Д, 2 = А, 3 = В, 4 = Б, 5 = Г

В6) В

В7) А, В, Г

В8) 1 = Г, 2 = В, 3 = А, 4 = Б

В9) А, Б, В

В10) Б, В, Д

В11) Б, Г, Д

В12) Г

В13) Б

В14) В

В15) А

В16) В

В17) Г

В18) А

В19) Б

В20) Г

В21) А

В22) Б

В23) В

В24) Б

В25) В

В26) Г

В27) Г

В28) Г

В29) А, В

В30) В

В31) В

В32) Г

В33) Б

В34) В

В35) В

B36) А

B37) В

B38) 1 = А, 2 = В, 3 = Б

B39) А

B40) А

B41) 1 = Б, 2 = Г, 3 = А, 4 = Д, 5 = В

B42) Г

B43) Б

B44) А

B45) Г

B46) В

B47) В

B48) Г, Д

B49) Б, В

B50) А, Б, В, Д

B51) Б

B52) В

B53) Б

B54) Б

B55) Б, В

B56) А

B57) А, Б, Ж, З

B58) Г

B59) А

B60) А

B61) В

Модуль 5

Соединения распределенных сетей

Обзор

Распределенная сеть обеспечивает соединение географически удаленных площадок. Распределенные сети обычно являются платными и обеспечивают доступ к ресурсам обширного географического региона. Существует несколько типов распределенных сетей, включая арендованные каналы «точка-точка», сети с коммутацией каналов и коммутацией пакетов. В распределенных сетях используется множество сетевых устройств и технологий доступа и инкапсуляции, например DSL, Frame Relay, ATM, PPP и HDLC. В этом модуле рассматриваются распределенные технологии на основе протоколов HDLC и PPP.

При соединении двух площадок необходим способ доставки информации на нужную площадку. Маршрутизация является процессом доставки информации от одного объекта к другому. Важно понимать, как различные протоколы маршрутизации определяют IP-маршруты. В этом модуле описываются функции и принцип работы статической маршрутизации, маршрутизации по умолчанию и протокола RIP.

При слиянии организаций могут возникать проблемы из-за ограниченного количества адресов или конфликтов между ними. Одна из наиболее распространенных проблем адресации возникает при подключении сети с частной адресацией к Интернету, в котором используются общие адреса. Для решения этой проблемы используются два протокола: преобразование сетевых адресов (NAT) и преобразование адресов и портов (PAT).

Связь между небольшими площадками все чаще осуществляется через Интернет. В подобных средах поставщик услуг Интернета часто динамически назначает адрес интерфейса с помощью протокола DHCP. Чтобы обеспечить совместимость с такими средами, маршрутизатор должен действовать как DHCP-клиент.

Задачи модуля

По окончании этого модуля вы сможете определять характеристики, функции и компоненты распределенной сети. Это значит, что вы сможете выполнять следующие задачи:

- описывать распределенные сети, их основные устройства и технологии;
- настраивать маршрутизатор в качестве интерфейса для подключения к Интернету с использованием DHCP-клиента и функций преобразования адресов портов маршрутизатора Cisco IOS;
- настраивать и проверять статическую и динамическую маршрутизацию;
- настраивать и проверять последовательные порты с инкапсуляцией HDLC и PPP;
- настраивать маршрутизацию RIP.

Занятие 1

Общие сведения о технологиях распределенных сетей

Обзор

Со временем предприятие растет, занимает дополнительные помещения, и перед ним встает необходимость объединить локальные сети различных офисов в распределенную сеть. Для функционирования распределенной сети существует ряд технологий, охватывающих оборудование и функции программного обеспечения. В этом занятии рассматриваются функции и характеристики распределенных сетей в сравнении с локальными сетями. Кроме того, здесь обсуждается связь архитектуры и функции распределенных сетей с эталонной моделью взаимодействия открытых систем (OSI), основные аппаратные компоненты которой обычно используются в средах распределенных сетей.

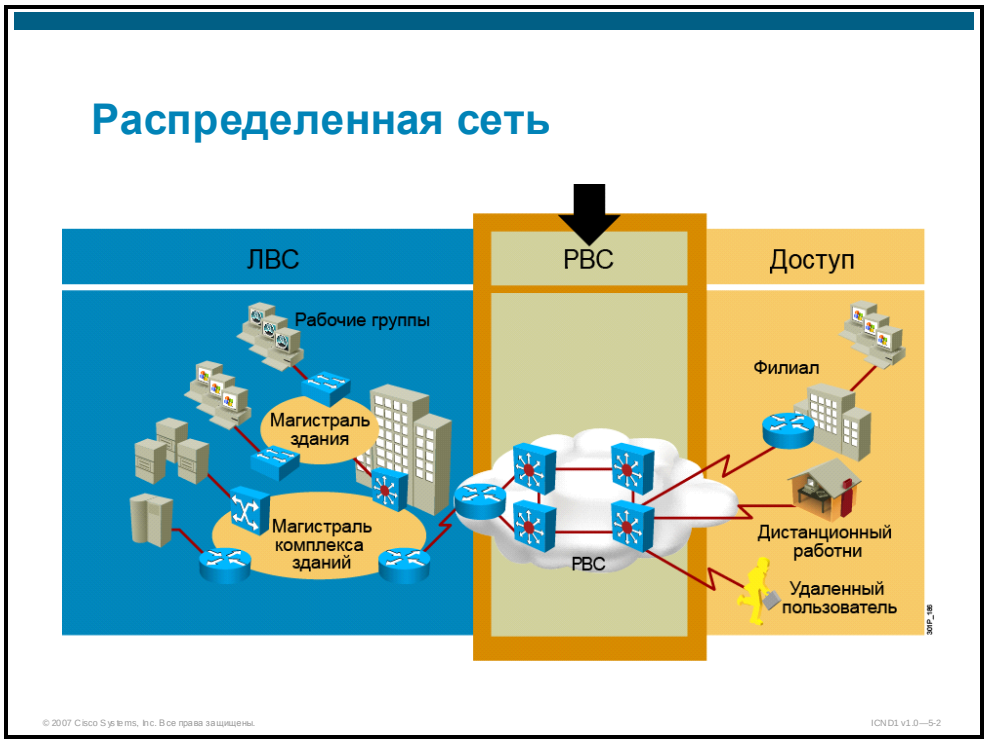
Задачи

По окончании этого занятия вы сможете описывать распределенные сети, а также их основные устройства и технологии. Это значит, что вы сможете выполнять следующие задачи:

- перечислять функции и характеристики распределенной сети;
- перечислять требования предприятий к распределенным сетям;
- сравнивать распределенные сети с локальными;
- описывать работу протоколов распределенных сетей по отношению к эталонной модели OSI;
- перечислять устройства, обычно применяемые при подключении к распределенной сети, и определять их функции;
- описывать кабельные соединения, применяемые для подключений к распределенной сети;
- определять роль маршрутизаторов для доступа к распределенной сети;
- перечислять основные протоколы, действующие в распределенных сетях;
- перечислять основные параметры канала доступа к распределенным сетям.

Что такое распределенная сеть?

Распределенная сеть – это коммуникационная сеть, функционирующая за пределами географической области локальной сети. В этом разделе рассматриваются характеристики распределеной сети.



В распределенных сетях используются средства, предоставляемые поставщиком услуг, или оператором, например, телефонной или кабельной компанией. Они соединяют офисы организации между собой, с офисами других организаций, с внешними службами и удаленными пользователями. Через распределенные сети проходят различные типы трафика, такие как голос, данные и видео.

Ниже представлены три основные характеристики распределенных сетей.

- Распределенные сети соединяют устройства, расположенные в различных географических областях.
- Распределенные сети используют услуги операторов, например телефонных и кабельных компаний, спутниковых систем и поставщиков сетевых услуг.
- В распределенных сетях используются различные типы последовательных подключений для предоставления доступа к полосе пропускания на обширных географических пространствах.

Почему необходимы распределенные сети?

Существуют несколько причин, по которым распределенные сети необходимы в коммуникационной среде. В этом разделе рассматриваются причины для внедрения распределенной сети.

Технологии локальной сети обеспечивают быструю и экономичную передачу данных в сравнительно небольших географических районах. Однако у предприятий существуют другие потребности, которые подразумевают взаимодействие с удаленными пользователями.

- Персоналу в региональных офисах и филиалах организации необходимо обмениваться данными и совместно использовать их.
- Организациям нередко приходится использовать данные совместно с другими предприятиями, расположенными на значительном расстоянии. Например, производители программного обеспечения регулярно обмениваются информацией о продукте и рекламными материалами с дистрибьюторами, поставляющими ее конечным пользователям.
- Сотрудники, путешествующие по делам предприятия, часто нуждаются в доступе к информации, хранящейся в корпоративных сетях.

Кроме того, пользователям домашних компьютеров требуется передавать (и получать) данные на постоянно увеличивающиеся расстояния. Можно привести несколько примеров.

- В настоящее время многие потребители связываются с банками, складами и различными поставщиками товаров и услуг с домашних компьютеров.
- Студенты выполняют учебные задания, изучая каталоги и публикации в библиотеках, расположенных в других частях света.

Очевидно, что соединить все компьютеры в стране или мире с помощью кабелей невозможно, поэтому были разработаны различные технологии, призванные удовлетворить эти потребности. Распределенные сети позволяют организациям и частным лицам удовлетворять свои потребности в обмене данными на большие географические расстояния.

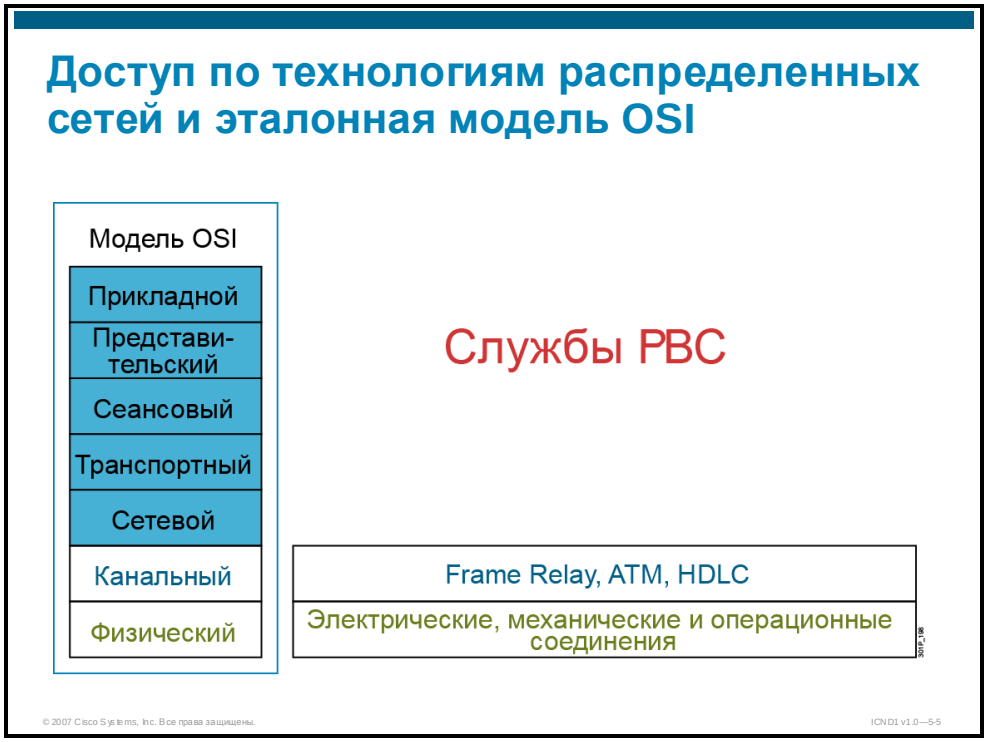
Чем распределенная сеть отличается от локальной сети?

Распределенные сети отличаются от локальных по целому ряду характеристик. В этом разделе описываются различия между этими двумя типами сетевых сред.

Если локальная сеть соединяет компьютеры, периферийные и другие устройства внутри одного здания или небольшой географической области, распределенная сеть обеспечивает передачу данных на значительные расстояния. Кроме того, чтобы пользоваться сетевыми услугами оператора распределенной сети, компания или организация должны стать абонентами внешнего поставщика услуг распределенной сети. Владельцами локальных сетей обычно является использующие их компании или организации.

Доступ по технологиям распределенных сетей и эталонная модель OSI

Стандарты распределенных сетей функционируют в тесной связи с эталонной моделью OSI. Их функции сосредоточены в основном на 1-ом и 2-ом уровнях. В этом разделе описывается связь уровня 1 и уровня 2 эталонной модели OSI с распределенными сетями.



Стандарты доступа по технологиям распределенных сетей описывают способы доставки физического уровня и требования к канальному уровню, включая физическую адресацию, управление потоком и инкапсуляцию. Определение этих стандартов и управление ими возложено на ряд признанных учреждений, таких как ISO, TIA и EIA.

Протоколы физического уровня (уровня 1 модели OSI) описывают способы обеспечения электрических, механических, процедурных и функциональных подключений к услугам поставщика услуг связи.

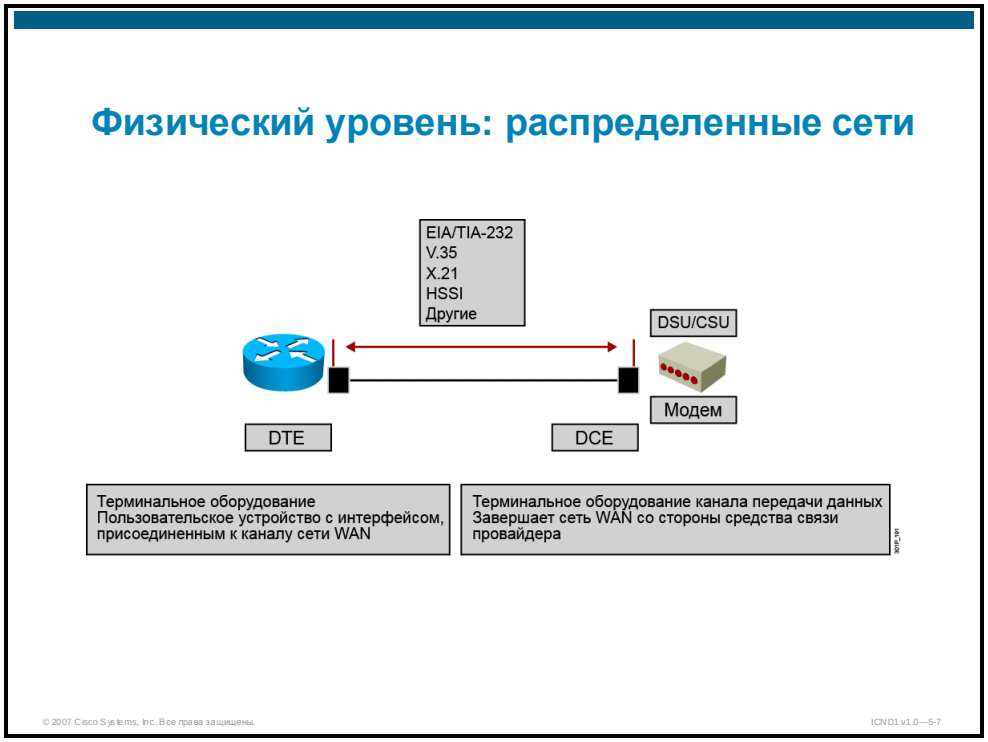
Протоколы канального уровня (уровня 2 модели OSI) определяют инкапсуляцию данных для передачи в удаленный объект и механизмы передачи кадров, полученных при инкапсуляции. Для этого используется множество различных технологий, в том числе Frame Relay и ATM. В некоторых из этих протоколов используется одинаковый механизм разделения на кадры – протокол HDLC, стандарт ISO, или один из его подмножеств или вариантов.

Устройства распределеных сетей

На физическом уровне в распределенной сети функционирует несколько устройств. В этом разделе рассматриваются такие устройства и их назначение в распределенной сети.

Для доступа по технологиям распределенных сетей используются следующие устройства.

- **Маршрутизаторы:** Маршрутизаторы обеспечивают объединение сетей и интерфейсные порты доступа к распределенным сетям.
- **Коммуникационные серверы:** Коммуникационные серверы выполняют обслуживание входящих и исходящих коммутируемых подключений пользователей.
- **Модемы или устройства DSU/CSU:** В аналоговых линиях модемы преобразуют цифровой сигнал устройства-отправителя в аналоговый формат для передачи по аналоговой линии, а затем обратно в цифровую форму, чтобы он мог быть получен и обработан принимающим устройством в сети. Для цифровых линий требуется блок обслуживания канала (CSU) и блок обслуживания данных (DSU). Эти два устройства часто объединяются в одном устройстве, которое называется DSU/CSU. Устройство DSU/CSU может быть встроено в интерфейсную плату маршрутизатора.
- **Сетевые устройства распределенной сети:** Кроме того, в распределенной сети для поддержки услуг доступа используются другие устройства, такие как коммутаторы ATM, коммутаторы Frame Relay, коммутаторы телефонных сетей общего пользования (ТфОП) и центральные маршрутизаторы.



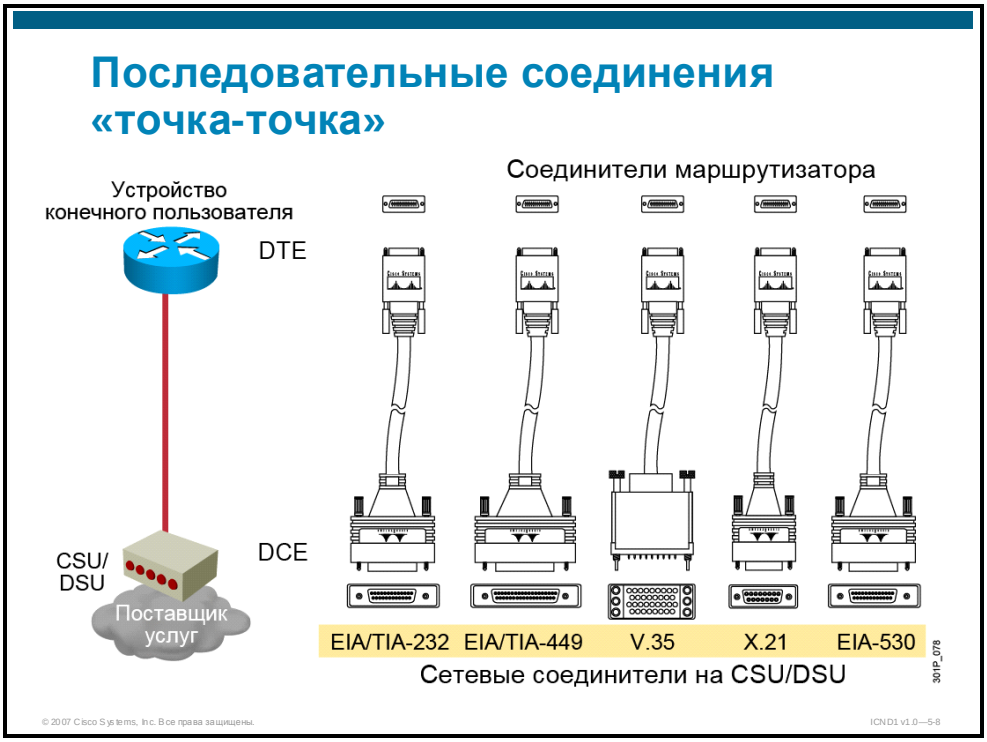
Устройства, расположенные в помещениях абонента, называются абонентским оборудованием (CPE). Абонент является собственником CPE или арендует его у поставщика услуг. Это оборудование соединяется медным или оптоволоконным кабелем с ближайшей станцией связи или центральным офисом поставщика услуг. Это кабельное соединение часто называется местной линией или «последней милей». Передаваемые аналоговые данные (например, телефонный вызов) локально соединяются с другими местными линиями или через магистраль с основным центром. Затем по мере поступления аналоговые данные передаются в местный, региональный или международный операторский центр.

Для передачи данных по последней миле требуется устройство, такое как модем или DSU/CSU, для подготовки данных. Устройства, передающие данные в местную линию, называются конечным оборудованием линии или оборудованием для передачи данных (DCE). Устройства абонента, передающие данные оборудованию для передачи данных, называются терминальным оборудованием (DTE). Оборудование DCE в первую очередь обеспечивает интерфейс для оборудования DTE с каналом связи распределенной сети.

Физический уровень доступа по технологиям распределенных сетей описывает интерфейс между этими двумя типами оборудования.

Кабельные соединения распределенных сетей

В этом разделе рассматриваются кабельные соединения, применяемые для подключений к распределенным сетям.



Маршрутизаторы Cisco поддерживают стандарты EIA/TIA-232, EIA/TIA-449, V.35, X.21 и EIA/TIA-530 для последовательных подключений.

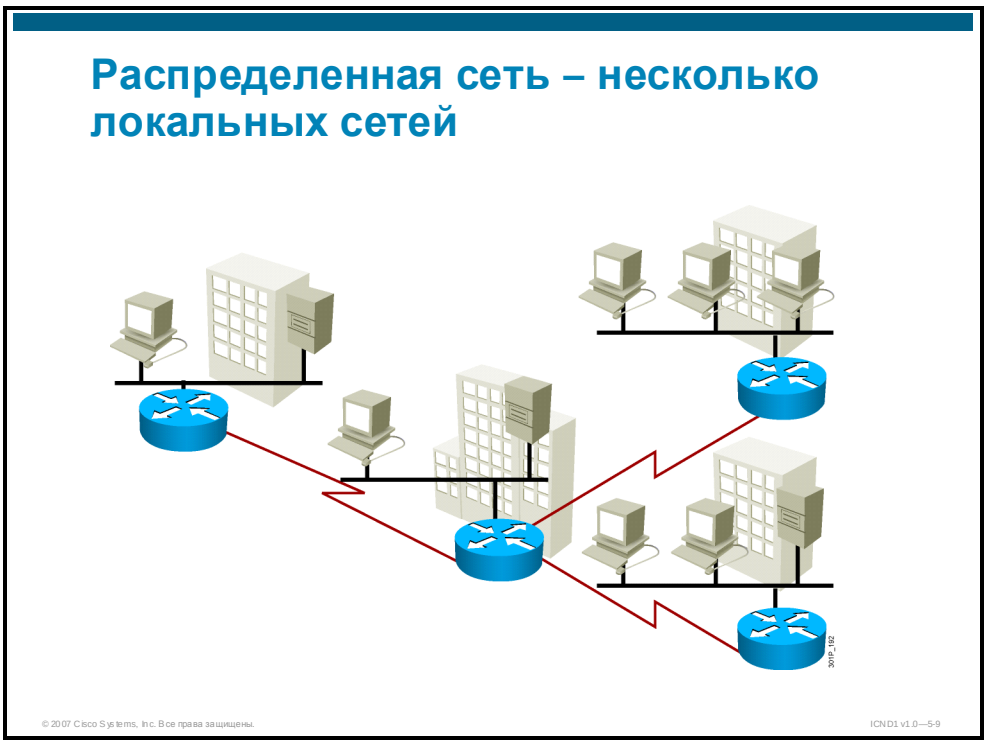
При заказе кабеля поставляется экранированный последовательный переходный кабель с разъемом, соответствующим выбранному стандарту. На конце экранированного последовательного переходного кабеля расположен разъем DB-60, подключаемый к порту DB-60 на последовательной интерфейсной плате PBC (WIC). Поскольку этот порт поддерживает пять различных типов кабелей, он иногда называется последовательным портом «пять-в-одном». На другом конце экранированного последовательного переходного кабеля находится разъем, соответствующий выбранному стандарту. Стандарт подключаемого устройства должен быть указан в документации по этому устройству.

Абонентское оборудование, в данном случае маршрутизатор, является терминальным оборудованием (DTE). Устройство DCE (обычно это модем или DSU/CSU) служит для преобразования данных оборудования DTE в форму, приемлемую для поставщика услуг глобальной сети. Синхронный последовательный порт маршрутизатора настраивается как DTE или DCE (за исключением EIA/TIA-530, который может быть только DTE) в зависимости от подключаемого кабеля, заказанного как DTE или DCE (определяется конфигурацией маршрутизатора). Если порт настроен как DTE (параметр по умолчанию), для него требуется внешняя синхронизация с устройством DCE.

Примечание	Для поддержки повышенной плотности портов в минимальном форм-факторе Cisco предлагает последовательный кабель Smart Serial. На последовательном конце смарт-кабеля находится разъем с 26 контактами. Он намного меньше разъема DB-60, который используется для подключения к последовательному порту «пять-в-одном». Эти переходные кабели поддерживают те же пять стандартов последовательной передачи данных, доступны в конфигурации DTE или DCE и используются для двухпортовых последовательных соединений, а также двухпортовых синхронных и асинхронных интерфейсных плат PBC.

Роль маршрутизаторов в распределенных сетях

Корпоративная глобальная сеть представляет собой набор отдельных, но связанных между собой локальных сетей, причем центральную роль в передаче данных по этой сети играют маршрутизаторы. В этом разделе рассматриваются функции и роль маршрутизатора в окружении распределенных сетей.



Маршрутизаторы оснащены интерфейсами ЛВС и РВС. Хотя маршрутизаторы используются для сегментации локальных сетей, они также служат коммутационным устройством для доступа к распределенной сети. Чтобы лучшеG понять функции и роль маршрутизатора в предоставлении доступа к распределенной сети, рассмотрим типы доступных соединений на маршрутизаторе.

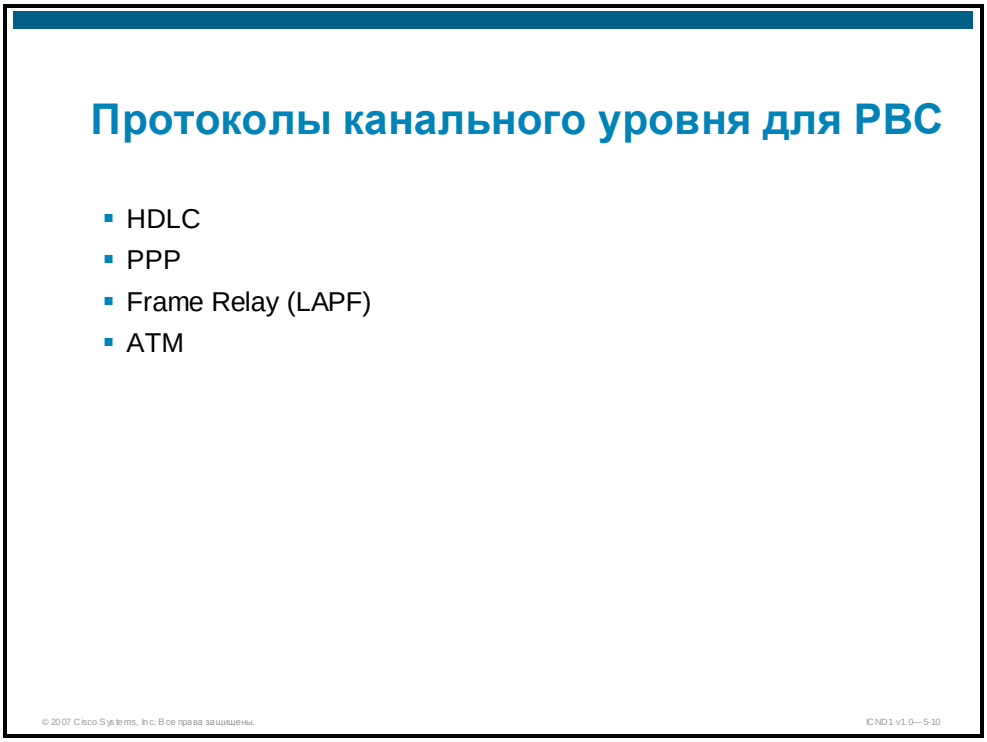
На маршрутизаторе используется три основных типа подключений: интерфейсы ЛВС, интерфейсы РВС и порты управления. Интерфейсы ЛВС позволяют маршрутизатору подключаться к среде локальной сети через Ethernet или другие технологии локальных сетей, например Token Ring или ATM.

Через интерфейс РВС осуществляются подключения к поставщику услуг, удаленному объекту или к Интернету. Это могут быть последовательные подключения или любое количество других интерфейсов РВС. Для подключения некоторых типов интерфейсов РВС к локальной точке присутствия (POP) поставщика услуг требуется внешнее устройство, DSU/CSU или модем (например, аналоговый, кабельный или DSL-модем). Физическая точка разграничения – это место, в котором ответственность за соединение переходит от пользователя к поставщику услуг. Это очень важно, поскольку при возникновении проблем обе стороны канала должны доказать, что проблема не связана с ними.

Порты управления обеспечивают передачу текстовых команд для настройки и устранения неполадок маршрутизатора. К распространенным интерфейсам управления относятся консольный и вспомогательные порты. Эти порты подключаются к коммуникационным портам компьютера. На компьютере должна быть запущена программа эмуляции терминала, которая устанавливает текстовый сеанс с маршрутизатором для управления устройством.

Протоколы PBC канального уровня

Кроме устройств физического уровня в распределенных сетях необходимы протоколы канального уровня для создания канала через линию связи между устройством-отправителем и устройством-получателем. В этом разделе рассматривается функция протоколов канального уровня в среде PBC.



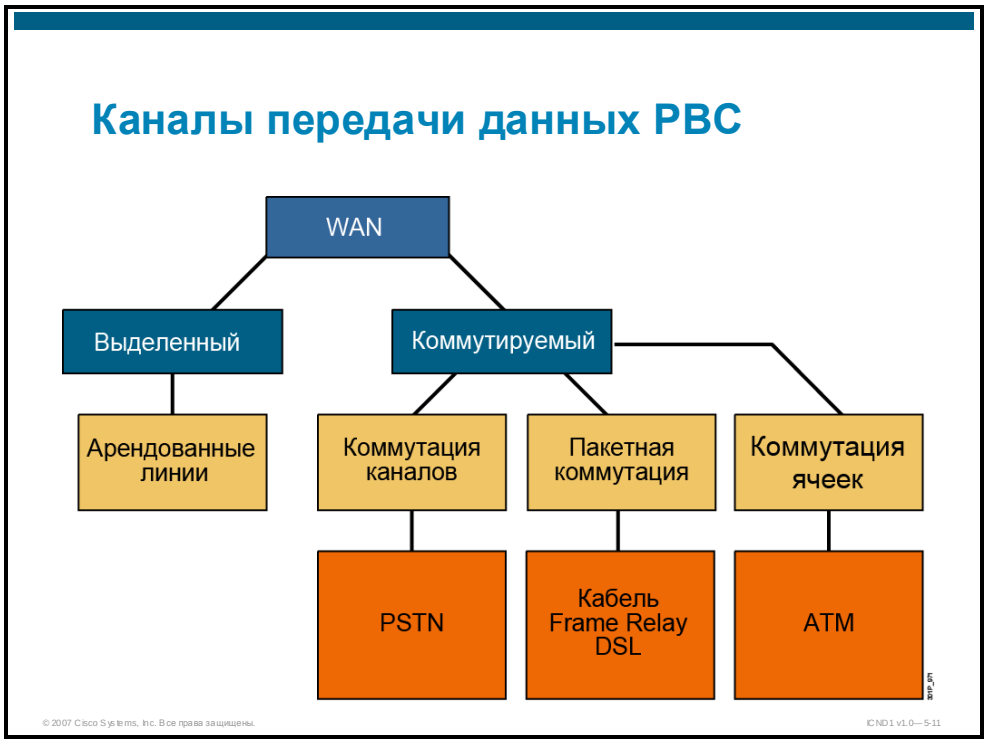
Протоколы канального уровня определяют инкапсуляцию данных для передачи на удаленные площадки и механизмы передачи кадров, полученных при инкапсуляции. Для этого используется множество различных технологий, в том числе ISDN, Frame Relay и ATM. Многие из этих протоколов используют одинаковый механизм разделения кадров, протокол HDLC, стандарт ISO, или один из его поднаборов или вариантов. Больше всего отличий имеет технология ATM, поскольку в ней используются небольшие ячейки фиксированного размера 53 байта (48 байтов для данных).

В глобальных сетях используются следующие протоколы канального уровня:

- HDLC
- PPP
- Frame Relay (Link Access Procedure for Frame Relay – процедура доступа к режиму кадровой передачи [LAPF])
- ATM

Варианты каналов связи PBC

Существует несколько способов доступа к рапспределенным сетям, которые определяются требованиями к передаче данных в распределенной сети. В этом разделе обсуждаются основные варианты каналов передачи данных PBC.



Существует две основные категории каналов передачи данных PBC: выделенные и коммутируемые. Каждая из этих категорий имеет свои типы каналов связи.

- **Выделенные каналы:** Для постоянных выделенных соединений используются каналы «точка-точка» с различной полосой пропускания, ограниченной только возможностями физических компонентов и готовностью пользователей оплачивать эти выделенные линии. Канал «точка-точка» обеспечивает установленные связи по распределенной сети от абонента через поставщика сетевых услуг к удаленному месту назначения. Каналы «точка-точка», как правило, арендуются у оператора и называются также арендуемыми линиями.
- **Коммутируемые каналы:** При коммутации каналов динамически устанавливается выделенное виртуальное соединение для передачи обычных или голосовых данных между отправителем и получателем. Перед началом обмена данными необходимо установить соединение через сеть поставщика услуг.
- **Каналы с коммутацией пакетов:** Многие пользователи распределенных сетей недостаточно эффективно используют фиксированную полосу пропускания выделенных, коммутируемых или постоянных линий, поскольку поток данных меняется. Поставщики услуг связи располагают сетями передачи данных, которые позволяют более эффективно обслуживать этих пользователей. В сетях с коммутацией пакетов данные передаются в помеченных ячейках, кадрах или пакетах.

Резюме

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

Резюме

- Существует три основные характеристики распределенных сетей: соединение устройств, расположенных в различных географических областях; использование услуг операторов, например телефонных и кабельных компаний, спутниковых систем и поставщиков сетевых услуг; и использование различных типов последовательных подключений для доступа к полосе пропускания на протяженных географических пространствах.
- Многим предприятиям и домашним пользователям требуется взаимодействие с удаленными пользователями, включая обмен данными между пользователями в удаленных офисах компании, совместный доступ к данным для разных организаций, доступ к корпоративной информации для мобильных пользователей и доступ к Интернету.

Резюме (прод.)

- Локальная сеть соединяет компьютеры, периферийные и другие устройства внутри одного здания или небольшой географической области, распределенная сеть обеспечивает передачу данных на значительные расстояния.
- Чтобы пользоваться сетевыми услугами распределенной сети, компания, организация или частное лицо должны стать абонентами внешнего поставщика услуг распределенной сети, тогда как владельцами локальных сетей обычно является использующие их компании, организации или частные лица.
- Распределенные сети функционируют в тесной связи с эталонной моделью OSI; их работа сосредоточена в основном на 1-ом и 2-ом уровнях.

Резюме (прод.)

- Основными типами устройств, используемых для доступа к распределенным сетям, являются маршрутизаторы, коммуникационные серверы, модемы (DSU/CSU) и другие сетевые устройства, такие как коммутаторы Frame Relay и ТфОП.
- Маршрутизаторы оснащены интерфейсами ЛВС и РВС. Хотя маршрутизаторы используются для сегментации локальных сетей, они также служат коммутационным устройством для доступа к распределенной сети.
- Протоколы канального уровня (уровня 2 модели OSI) определяют инкапсуляцию данных для передачи на удаленный объект и механизмы передачи кадров, полученных при инкапсуляции. Для этого используется множество технологий, в том числе ISDN, Frame Relay и ATM.

Занятие 2

Подключение к сети Интернет

Обзор

Связь между небольшими площадками часто осуществляется через Интернет. Эта услуга предоставляется поставщиком услуг Интернета (ISP). Физическое подключение обычно осуществляется с помощью цифровой абонентской линии (DSL) или кабельной технологии с коммутацией пакетов.

Иногда поставщик услуг Интернета предоставляет статический адрес для интерфейса, подключенного к сети Интернет. В других случаях этот адрес назначается с помощью протокола DHCP.

Существует две проблемы масштабируемости, связанные с использованием Интернета: истощение пространства зарегистрированных IP-адресов версии 4 (IPv4) и увеличение масштаба маршрутизации. В Cisco IOS используются два механизма экономии зарегистрированных IP-адресов, преобразование сетевых адресов (NAT) и преобразование адресов и портов (PAT), которые упрощают задачи IP-адресации. NAT и PAT преобразуют адреса IPv4 в частных внутренних сетях в зарегистрированные адреса IPv4 для передачи через сети общего доступа, такие как Интернет, без потребности в зарегистрированном адресе подсети. При доставке входящего трафика во внутреннюю сеть выполняется обратное преобразование.

Это преобразование IPv4 устраняет потребность в изменении адресов хостов и позволяет использовать один диапазон адресов IPv4 в нескольких интрасетях. В этом занятии описываются функции NAT и PAT и их настройка на маршрутизаторах Cisco.

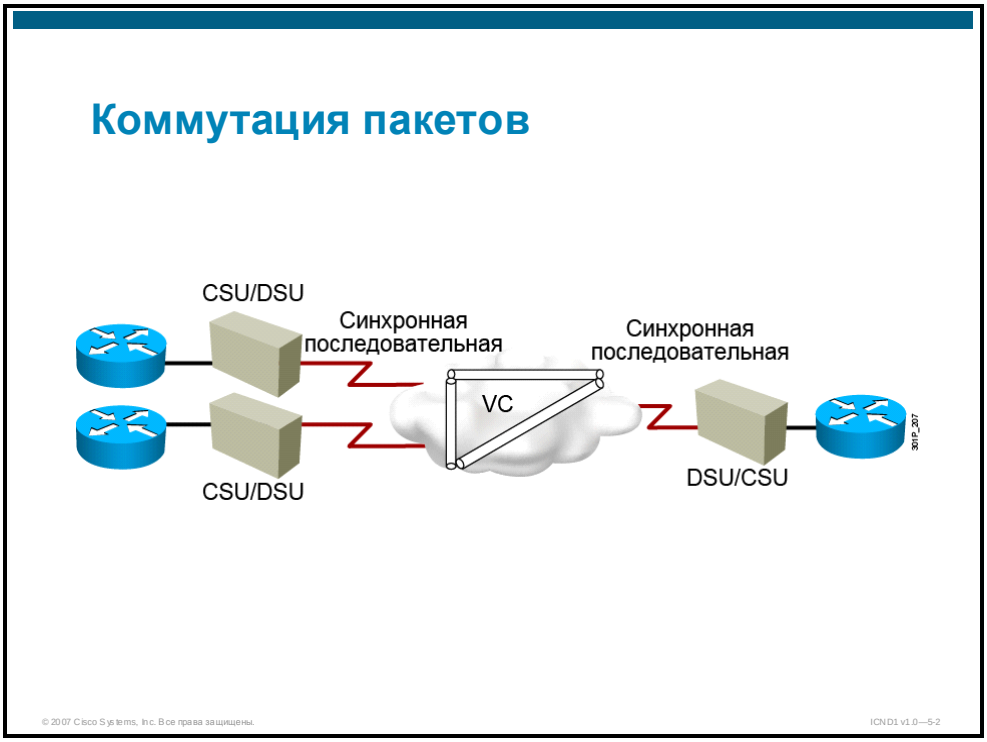
Задачи

По окончании этого занятия вы сможете настраивать доступ к Интернету с использованием DHCP-клиента, NAT и PAT на маршрутизаторах Cisco. Это значит, что вы сможете выполнять следующие задачи:

- определять функции канала PBC с коммутацией пакетов;
- перечислять функции и характеристики DSL;
- перечислять функции и характеристики кабельных PBC;
- описывать развитие и функцию глобальной сети Интернет;
- описывать процесс получения адреса интерфейса с DHCP-сервера;
- описывать функции NAT и PAT на маршрутизаторах Cisco;
- описывать использование статического и динамического преобразования внутренних адресов источника;
- использовать Cisco SDM для настройки DHCP-клиента и PAT с помощью перегрузки внутреннего глобального адреса;
- применять Cisco SDM для проверки правильности работы DHCP-клиента;
- использовать команды Cisco IOS для проверки работы NAT и PAT.

Каналы передачи данных с коммутацией пакетов

Коммутация пакетов представляет собой способ коммутации, при котором между устройством-источником и устройством назначения нет выделенного пути, и для передачи данных используются общие каналы связи и ресурсы оператора. В этом разделе рассматривается принцип коммутации пакетов.

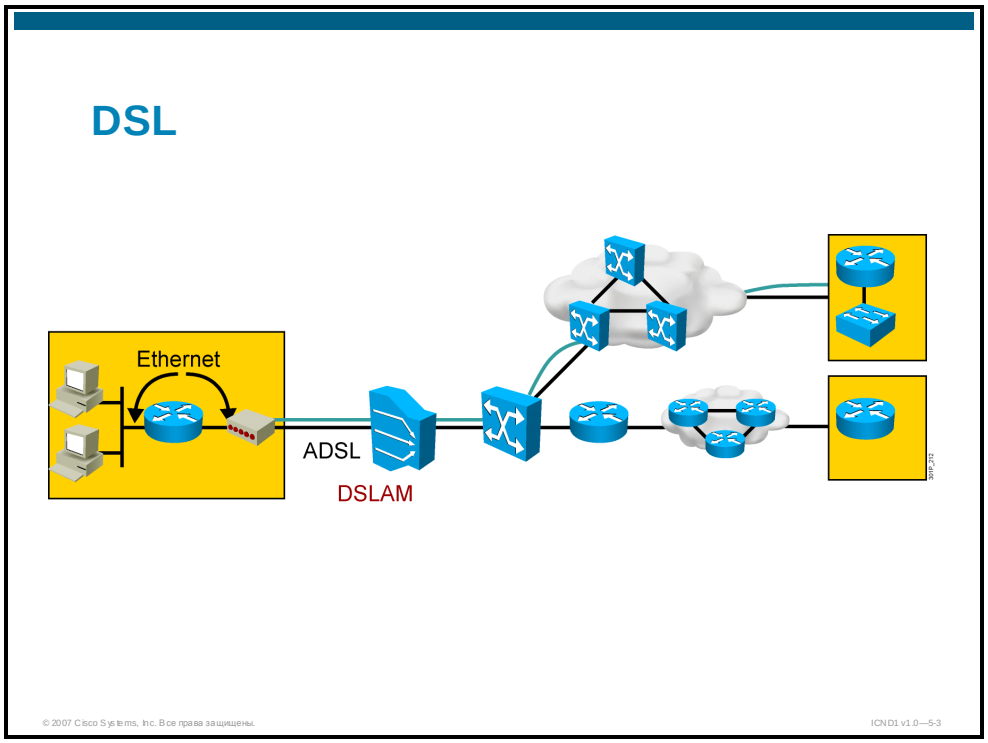


В сетях с коммутацией пакетов пакеты данных отправляются к одному месту назначения по различным маршрутам через сеть общего доступа. Вместо выделения пути оператор предоставляет своим абонентам сеть и гарантирует, что данные, полученные с одной площадки, будут переданы на другую площадку. Однако маршруты, по которым пакеты достигают места назначения, могут меняться. Когда пакеты прибывают к месту назначения, ответственность за их сборку в правильном порядке ложится на принимающий протокол.

Коммутация пакетов позволяет сократить число каналов в сети и дает оператору возможность повысить эффективность использования инфраструктуры, снизив общую стоимость по сравнению с отдельными арендуемыми линиями и линиями «точка-точка». В среде с коммутацией пакетов к сети оператора подключается большое число клиентских сетей. В зависимости от используемой технологии оператор может создавать виртуальные линии между площадками клиентов. Если клиент не использует полную полосу пропускания своей виртуальной линии, оператор может предоставить эту неиспользуемую полосу пропускания другому клиенту с помощью статистического мультиплексирования.

Цифровая абонентская линия (DSL)

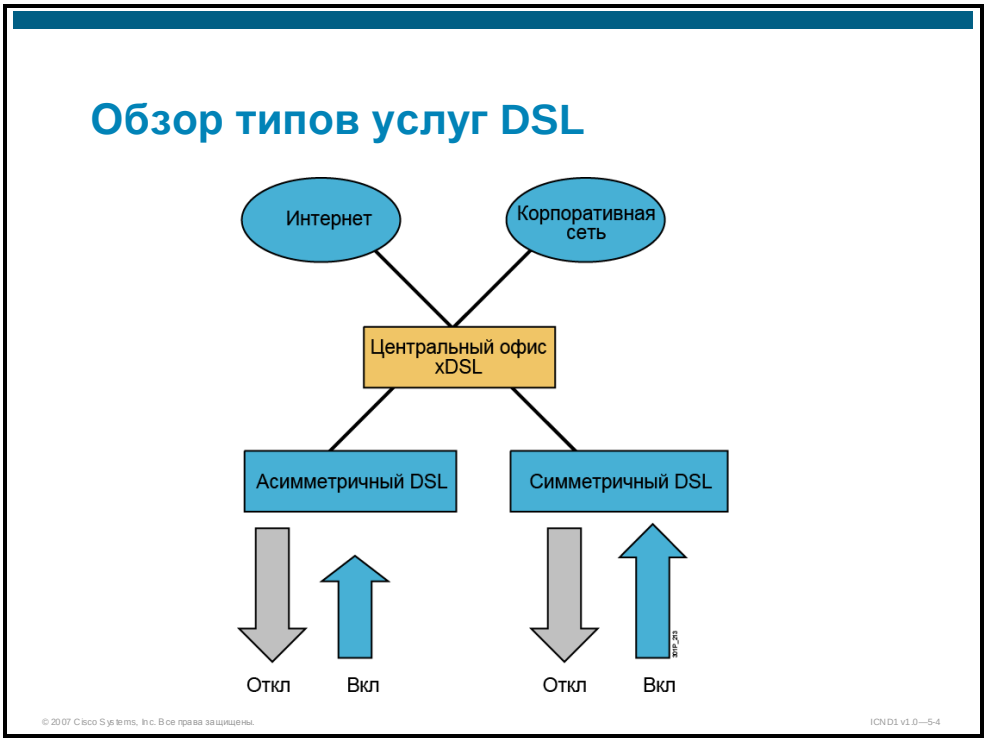
Технология DSL обеспечивает постоянное соединение, которое использует существующие телефонные линии на основе витой пары для широкополосной передачи данных и предоставляет абонентам IP-услуги. Для преобразования сигнала Ethernet от пользователей в сигнал DSL для центрального офиса используется модем DSL. В этом разделе описывается функционирование DSL.



Технология DSL позволяет поставщику услуг предлагать клиентам высокоскоростные сетевые услуги, сравнимые со скоростями T1-соединения и превышающие их, используя имеющиеся местные линии связи на основе медных проводов. Технология DSL позволяет использовать местные линии связи не только для обычных телефонных голосовых коммуникаций, но и для постоянного сетевого соединения. С помощью мультиплексора доступа DSL (DSLAM), установленного у поставщика, несколько абонентских линий DSL мультиплексируются в единый высокоскоростной канал. В устройствах DSLAM используется технология мультиплексирования с временным разделением каналов, позволяющая объединить несколько абонентских линий в более экономичную единую среду, как правило, в соединения T3 (DS3). В современных технологиях DSL применяются сложные методы кодирования и модуляции, обеспечивающие скорости передачи данных до 8,192 Мбит/с.

Канал тональной частоты обычного потребительского телефона охватывает диапазон частот от 330 Гц до 3,3 КГц. Диапазон частот 4 КГц, или окно, считается обязательным требованием для любой передачи голосовых данных по местной линии. Технологии DSL реализуют исходящую и входящую передачу данных на частотах, превышающих это окно в 4 КГц, что обеспечивает одновременную передачу голоса и данных в службе DSL.

Доступность DSL далека от универсальной. Существует множество типов, признанных и новых стандартов DSL. В настоящее время DSL является популярным решением среди ИТ-подразделений предприятий для поддержки своих сотрудников, работающих на дому. Обычно абонент не может напрямую подключаться к корпоративной сети. Он должен сначала подключиться к поставщику услуг Интернета, а затем установить соединение с предприятием через Интернет. Этот процесс сопряжен с рисками безопасности.



Типы и стандарты DSL

Существует два основных типа технологий DSL.

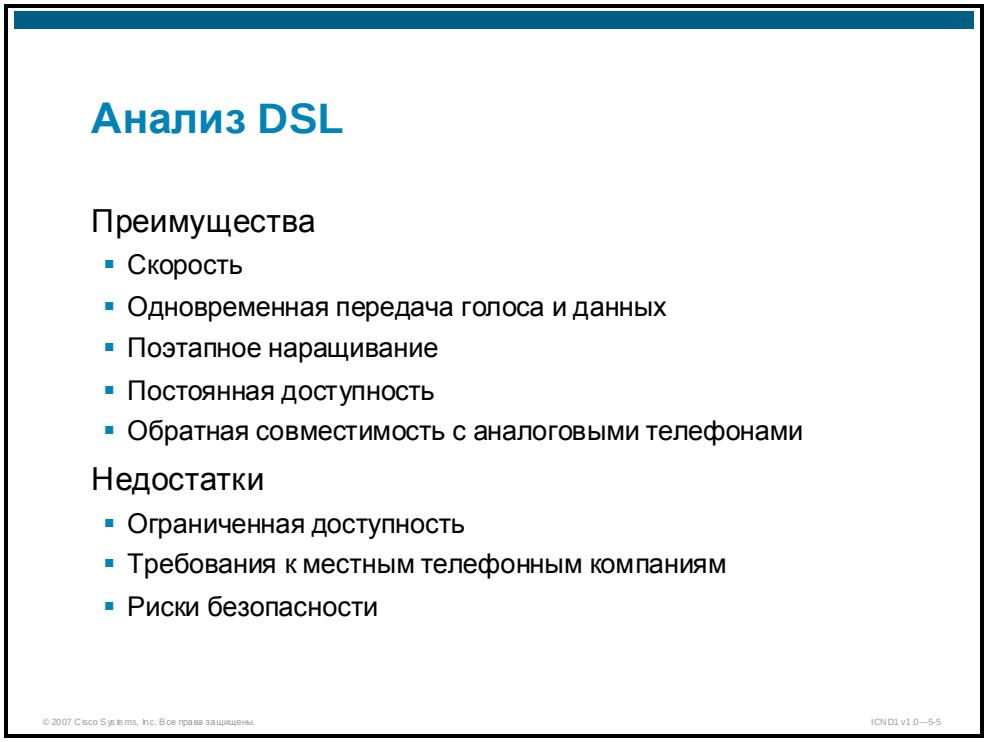
- **Асимметричная DSL (ADSL):** Обеспечивает большую полосу пропускания для входящего потока по сравнению с исходящим.
- **Симметричная DSL (SDSL):** Обеспечивает одинаковую пропускную способность в обоих направлениях.

Все виды услуг DSL делятся на асинхронные и синхронные, но каждый тип имеет несколько разновидностей. ADSL бывает следующих видов:

- ADSL
- Consumer (потребительская) DSL (CDSL), именуемая также G.Lite или G.992.2
- Very-high-data-rate (высокоскоростная) DSL (VDSL)

SDSL включает следующие виды:

- SDSL
- Very-high-data-rate (высокоскоростная) DSL (HDSL)
- ISDN DSL (IDSL).
- Symmetric high bit rate (симметричная высокоскоростная) DSL (G.shdsl)



Анализ DSL

Служба DSL может внедряться поэтапно в любом регионе. Поставщик услуг может модернизировать полосу пропускания в соответствии с ростом числа абонентов. DSL обратно совместима с аналоговой передачей голосовых данных и эффективно использует местные линии связи, что обеспечивает простоту использования службы DSL одновременно с сервисами телефонии.

Однако DSL имеет дистанционные ограничения. Радиус действия большинства предложений DSL в настоящее время не превышает 5,5 км от точки присутствия поставщика, и старые, более длинные местные линии представляют проблему. Кроме того, скорость исходящей передачи данных обычно существенно ниже скорости входящего потока. Использование технологии постоянного подключения DSL представляет также повышенный риск нарушения безопасности, поскольку потенциальные злоумышленники получают более широкие возможности доступа.

Кабельный доступ

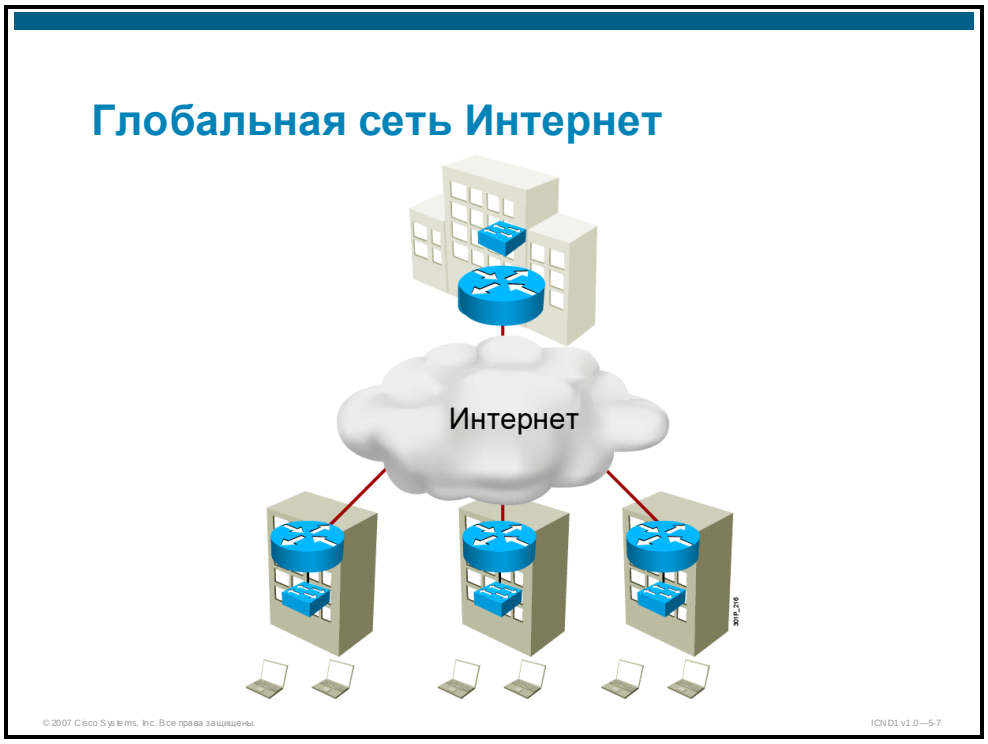
Другая технология доступа к распределенным сетям, популярность которой постоянно растет, – услуга доступа к сети Интернет по протоколу IP-over-Ethernet, использующая кабельные сети. В этом разделе описывается работа кабельной распределенной сети.

Изначально, кабели служили однонаправленными носителями, созданными для передачи аналоговых видеоканалов клиентам или абонентам. Однако в 1990-х годах с появлением спутников прямого вещания (DBS) и технологии DSL операторы столкнулись с серьезной угрозой со стороны конкурирующих технологий. Спутниковые операторы DBS предложили более разнообразные и качественные развлекательные продукты с использованием цифровых технологий, и существующие местные операторы связи предоставили целый набор услуг по передаче голоса, видео и данных посредством DSL.

Опасаясь потерять долю рынка и столкнувшись с необходимостью предложить потребителям дополнительные услуги, чтобы сохранить экономическую жизнеспособность, ведущие операторы универсальных кабельных систем (MSO) создали организацию Multimedia Cable Network System Partners Ltd. (MCNS), чтобы определить стандарт продуктов и систем, способных обеспечивать передачу данных и предоставлять новые услуги с помощью оборудования для кабельного телевидения (CATV). MCNS предложила решение на основе пакетов (IP) в отличие от решения на основе ячеек (ATM), поддерживаемого стандартом IEEE 802.14. Партнерами по MCNS являются такие ведущие операторы, как Comcast Cable Communications, Cox Communications, Tele-Communications, Time Warner Cable, MediaOne, Rogers Cablesystems и Cable Television Laboratories (CableLabs).

Глобальная сеть Интернет: крупнейшая из распределенных сетей

Интернет можно рассматривать как распределенную сеть, охватывающую весь мир. В этом разделе описываются истоки и функции Интернета как самой масштабной распределенной сети.



В 1960-х годах исследователи Министерства обороны США решили построить командно-административную сеть, связав несколько вычислительных систем, разбросанных по всей стране. Однако, эта ранняя распределенная сеть, была уязвимой для стихийных бедствий или нападения противника. Поэтому необходимо было обеспечить работоспособность оставшейся части сети при выходе из строя ее участка. Сеть не должна была иметь централизованного управления, чтобы работающие в ней компьютеры могли автоматически перенаправить поток информации в обход разрушенных каналов связи.

Исследователи Министерства обороны разработали способ разделения сообщения на части, отправляя каждую часть к месту назначения по отдельности. Достигнув места назначения сообщение должно собираться в исходную форму. Сегодня этот метод передачи данных известен как пакетная система.

Изучение этой пакетной системы, обнародованной военными в 1964, проводилось также в Массачусетском технологическом институте (MIT), Калифорнийском университете в Лос-Анжелесе (UCLA) и Национальной физической лаборатории в Великобритании. В конце 1969 года в Калифорнийском университете в Лос-Анжелесе был установлен первый компьютер этой сети. Несколько месяцев спустя, в этой сети, получившей название Advanced Research Projects Agency Network (ARPANET), было уже четыре компьютера.

В 1972 году было разработано первое программное обеспечение для электронной почты, позволившее разработчикам ARPANET свободно обмениваться данными и координировать проекты. Позже в этом же году была создана программа, позволившая пользователям читать сообщения, сохранять в виде файла, пересылать или отвечать на них.

На протяжении 70-х и 80-х годов прошлого века сеть значительно расширилась с совершенствованием технологий. В 1984 году была введена система доменных имен (DNS), давшая миру доменные суффиксы (такие как .edu, .com, .gov и .org) и ряд кодов стран. Эта система сделала Интернет значительно более управляемым. Без DNS пользователи должны были запоминать IP-адрес каждого интернет-сайта, который хотели посетить – длинные наборы цифр вместо строки слов.

В 1989 году Тимоти Джон Бернерс-Ли (Timothy John Berners-Lee) начал работу над средствами гипертекста, способными упростить обмен данными между физиками во всем мире, которые позволили бы напрямую связывать электронные документы между собой. Окончательным результатом связывания документов стала «Всемирная паутина» – World Wide Web. Стандартные языки форматирования, такие как Hypertext Markup Language (HTML) и его варианты, позволили отображать на веб-страницах форматированный текст, графику и мультимедиа. Веб-обозреватель может считывать и отображать документы в формате HTML, а также открывать и загружать связанные файлы и программное обеспечение.

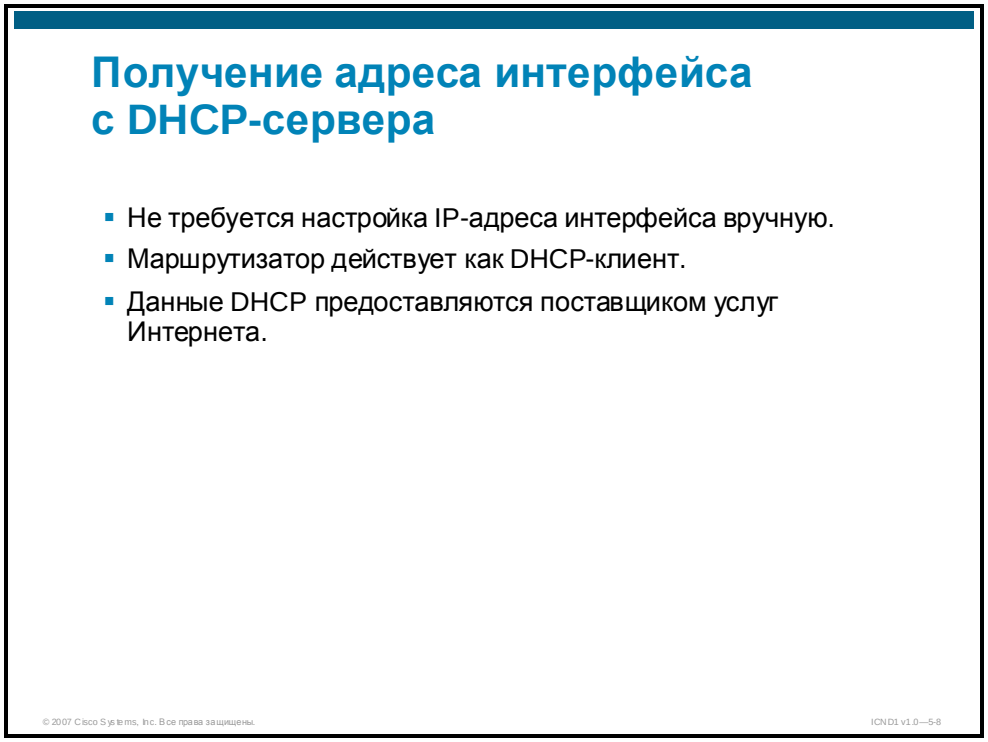
Популярность всемирной сети выросла после 1993 года благодаря разработке удобного графического обозревателя Mosaic. Таким образом, хотя всемирная паутина начиналась только как один из компонентов Интернета, она, безусловно, стала самой популярной, и теперь эти два понятия являются синонимами.

В течение 1990-х годов значительно увеличилась мощность и снизилась стоимость персональных компьютеров (ПК), и миллионы людей получили возможность приобрести их для своего дома или офиса. Поставщики услуг Интернета, такие как America Online (AOL), CompuServe, и множество местных операторов, стали предлагать доступное коммутируемое подключение к сети Интернет. Чтобы удовлетворить потребности в растущих скоростях передачи данных, поставщики кабельных услуг начали предоставлять доступ на базе кабельных сетей и их технологий.

Сегодня Интернет превратился в крупнейшую в мире сеть, обеспечивающую доступ к информации и обмен данными для сотрудников предприятий и пользователей домашних компьютеров. Интернет можно рассматривать как сеть сетей, состоящую из объединения сотен тысяч сетей, принадлежащих миллионам компаний и пользователей во всем мире, подключенных к тысячам поставщикам сетевых услуг.

Получение адреса интерфейса с DHCP-сервера

В этом разделе описывается процесс получения адреса интерфейса с DHCP-сервера.

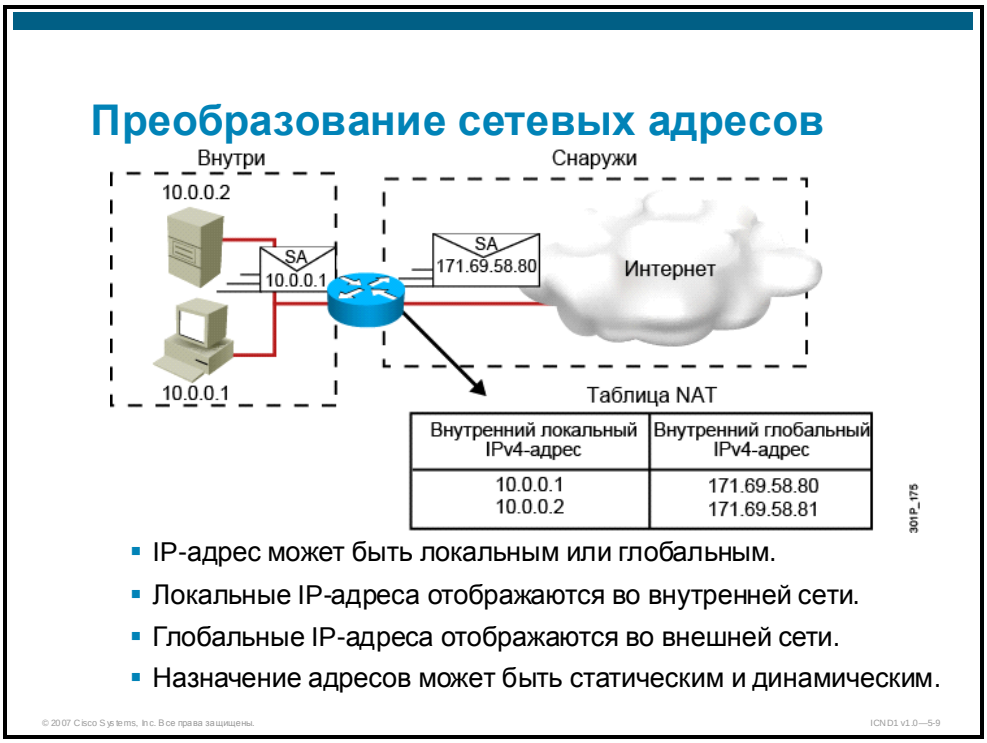


Иногда поставщик услуг Интернета предоставляет статический адрес для интерфейса, подключенного к сети Интернет. В других случаях этот адрес назначается с помощью протокола DHCP.

Если адрес интерфейса предоставляется поставщиком услуг Интернета с помощью DHCP, настройка адреса вручную не требуется. Вместо этого интерфейс настраивается для работы в качестве DHCP-клиента.

Общие сведения о NAT и PAT

В этом разделе описываются функции NAT и PAT.



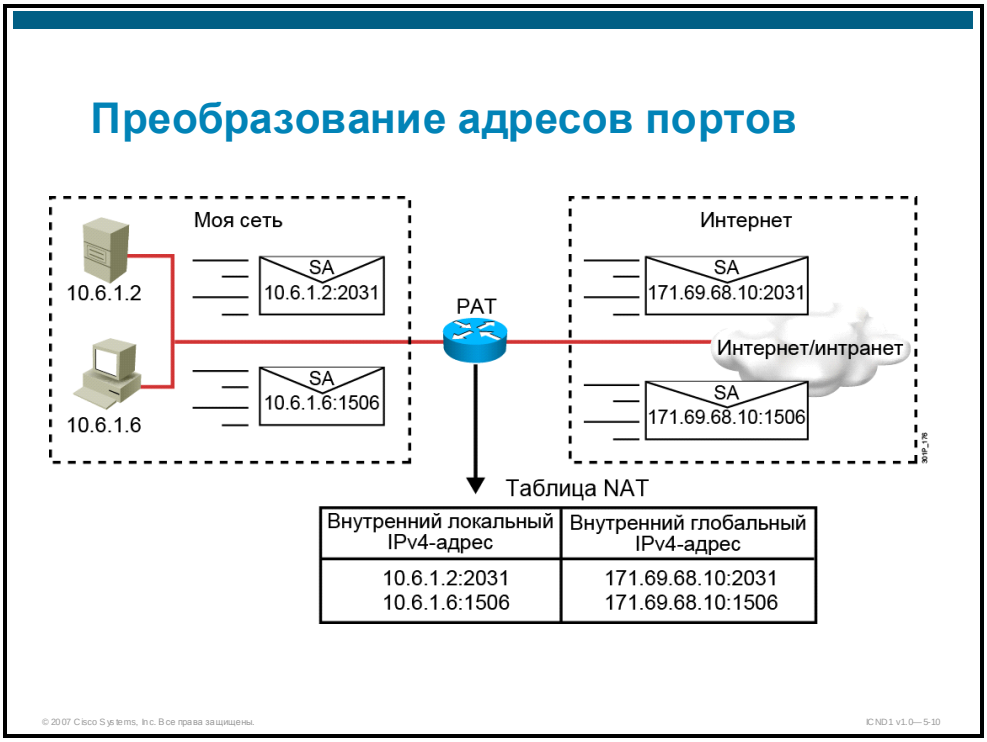
В небольших сетях, как правило, используется частная IP-адресация. При подключении сетей подобного типа к сетям общего доступа, например Интернету, требуется способ преобразования частных IP-адресов в общие. Преобразование NAT работает на маршрутизаторе Cisco и предназначено для экономии адресного пространства IPv4 и упрощения работы с ним. NAT позволяет внутренним сетям на основе протокола IP использовать незарегистрированные IP-адреса для подключения к сети Интернет. Как правило, NAT соединяет две сети и преобразует частные (внутренние локальные) адреса внутренней сети в общие (внутренние глобальные) адреса перед пересылкой пакетов в другую сеть. Можно настроить NAT для объявления внешнему миру только одного адреса. Объявление одного адреса скрывает внутреннюю сеть от внешнего мира, что обеспечивает дополнительную безопасность.

Любое устройство между внутренней сетью и сетью общего доступа, например брандмауэр, маршрутизатор или компьютер, использует преобразование NAT, описанное в стандарте RFC 1631.

В терминологии NAT под «внутренней сетью» подразумевается набор преобразуемых сетей. Термин «внешняя сеть» относится ко всем остальным адресам. Как правило, подразумеваются действующие адреса, расположенные в Интернете.

Cisco определяет следующие термины NAT.

- **Внутренний локальный адрес:** IP-адрес, назначенный хосту внутренней сети. Как правило, внутренний локальный адрес *не* является IP-адресом, назначенным сетевым информационным центром (NIC) или поставщиком услуг.
- **Внутренний глобальный адрес:** Зарегистрированный IP-адрес, назначенный центром NIC или поставщиком услуг. Представляет один или несколько внутренних локальных IP-адресов во внешних сетях.
- **Внешний локальный адрес:** IP-адрес внешнего хоста, под которым он отображается во внутренней сети. Внешний локальный адрес не обязательно должен быть зарегистрированным, он назначается из маршрутизируемого внутреннего адресного пространства.
- **Внешний глобальный адрес:** IP-адрес, назначенный хосту во внешней сети его владельцем. Внешний глобальный адрес выделяется из глобального маршрутизируемого адресного или сетевого пространства.

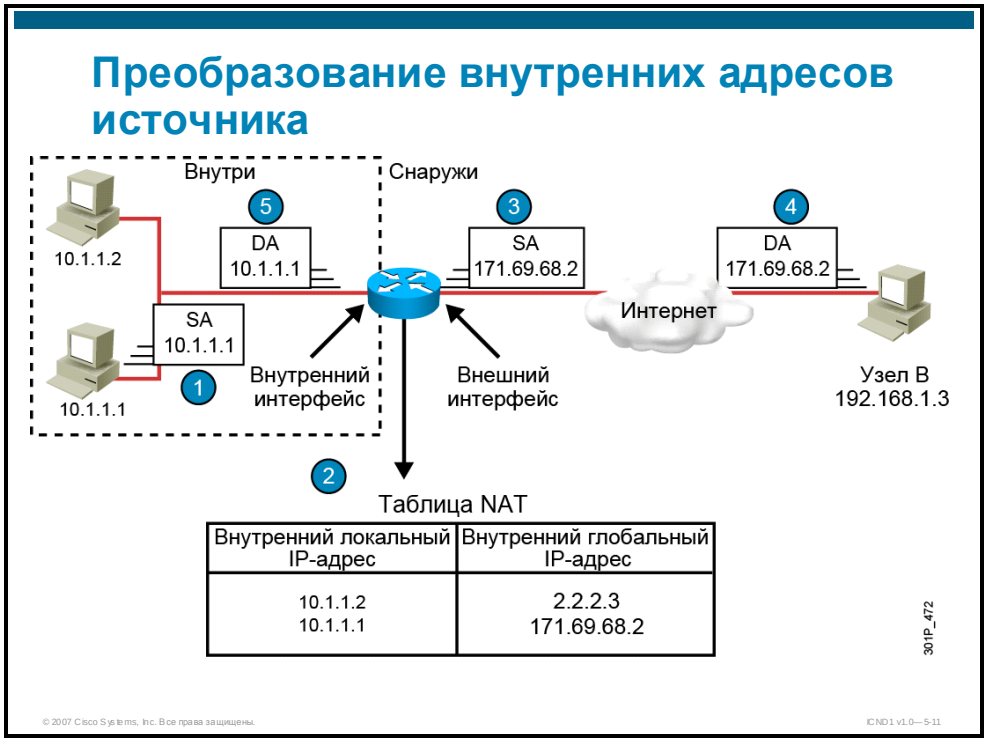


Одна из главных функций NAT – статическое преобразование PAT, которое также называется «перегрузкой» в конфигурации Cisco IOS. Несколько внутренних адресов могут быть преобразованы с помощью NAT в один внешний адрес или в небольшое их количество с использованием PAT.

Преобразование PAT использует уникальные номера портов источника, принадлежащих внутреннему глобальному IP-адресу, чтобы различать записи преобразования. Поскольку порт маршрутизатора кодируется 16 битами, общее число внутренних адресов, которое может быть преобразовано во внешний адрес, равняется 65 536. Преобразование PAT пытается сохранить оригинальный порт источника. Если порт источника уже выделен, преобразование PAT ищет первый доступный порт. Поиск выполняется с начала соответствующей группы портов – 0 – 511, 512 – 1023 или 1024 – 65535. Если преобразование PAT не обнаруживает доступный порт в соответствующей группе портов, и настроено несколько внешних IP-адресов, преобразование PAT переходит к следующему IP-адресу и пытается выделить исходный порт источника. Преобразование PAT продолжает попытки выделить оригинальный порт источника, пока не заканчиваются доступные порты и внешние IP-адреса.

Преобразование внутренних адресов источника

В этом разделе описывается статическое и динамическое преобразование внутренних адресов источника.



Вы можете преобразовать внутренние IP-адреса в IP-адреса, уникальные в глобальном масштабе, которые будут использоваться для связи с внешними сетями. Поддерживается статическое и динамическое преобразование внутренних адресов источника.

Пример: преобразование внутренних адресов источника

На рисунке изображен маршрутизатор, преобразующий адрес источника внутренней сети во внешний адрес источника. При преобразовании внутреннего адреса источника выполняются следующие действия.

Шаг 1 Пользователь хоста 10.1.1.1 создает подключение к хосту B.

Шаг 2 Первый пакет, полученный маршрутизатором от хоста 10.1.1.1 заставляет его проверить свою таблицу NAT.

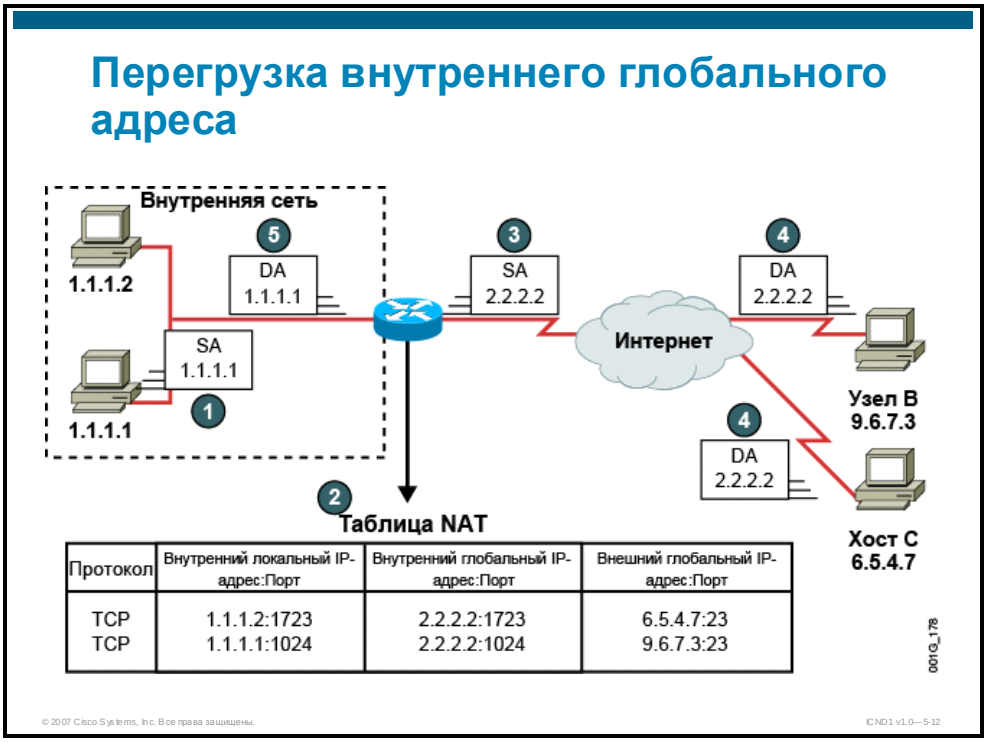
- Если в таблице настроена статическая запись, маршрутизатор переходит к действию 3.
- Если статических записей нет, маршрутизатор решает, что для адреса источника 10.1.1.1 (SA 10.1.1.1) необходимо выполнить динамическое преобразование. Затем маршрутизатор выбирает глобальный, зарегистрированный адрес из динамического пула и создает запись преобразования (в нашем примере 171.69.68.2). Такая запись называется простой.

Шаг 3 Маршрутизатор заменяет внутренний локальный адрес источника 10.1.1.1 глобальным адресом в записи преобразования и пересылает пакет.

Шаг 4 Хост B получает пакет и отвечает хосту 10.1.1.1, используя внутренний глобальный IP-адрес назначения 171.69.68.2 (DA 171.69.68.2).

Шаг 5 Когда маршрутизатор получает пакет с внутренним глобальным IP-адресом, он выполняет поиск по таблице NAT, используя внутренний глобальный адрес в качестве критерия. Затем маршрутизатор выполняет обратное преобразование адреса во внутренний локальный адрес хоста 10.1.1.1 и пересылает пакет хосту 10.1.1.1.

Шаг 6 Хост 10.1.1.1 получает пакет и продолжает преобразование. Маршрутизатор выполняет действия 2 – 5 для каждого пакета.



Вы можете сэкономить адреса в глобальном внутреннем пуле, разрешив маршрутизатору использовать один внутренний глобальный адрес для нескольких внутренних локальных адресов. Когда настроена перегрузка, маршрутизатор сохраняет достаточно информации протоколов верхнего уровня, например TCP и UDP, для обратного преобразования внутреннего глобального адреса в нужный внутренний локальный адрес. При привязке нескольких внутренних локальных адресов одному к внутреннему глобальному адресу для различения локальных адресов используются номера портов TCP или UDP.

Пример: перегрузка внутреннего глобального адреса

На рисунке описывается работа преобразования NAT в ситуации, когда один внутренний глобальный адрес представляет несколько внутренних локальных адресов. В качестве отличительных параметров используются номера портов TCP. Хосты B и C считают, что они работают с одним хостом по адресу 171.69.68.2. На самом деле они работают с разными хостами, отличительным

параметром служит номер порта. Фактически, несколько хостов могут использовать один глобальный IP-адрес с помощью нескольких номеров портов.

Маршрутизатор выполняет следующий процесс при перегрузке внутреннего глобального адреса.

Шаг 1 Пользователь хоста 10.1.1.1 создает подключение к хосту B.

Шаг 2 Первый пакет, полученный маршрутизатором от хоста 10.1.1.1 заставляет его проверить свою таблицу NAT.

Если запись преобразования не задана, маршрутизатор определяет, что адрес 10.1.1.1 должен быть преобразован и устанавливает преобразование адреса 10.1.1.1 в зарегистрированный глобальный внутренний адрес. Если включена перегрузка и активно другое преобразование, маршрутизатор использует глобальный адрес этого преобразования и сохраняет достаточно информации для обратного преобразования. Такая запись называется расширенной.

Шаг 3 Маршрутизатор заменяет внутренний локальный адрес источника 10.1.1.1 выбранным глобальным адресом в записи преобразования и пересылает пакет.

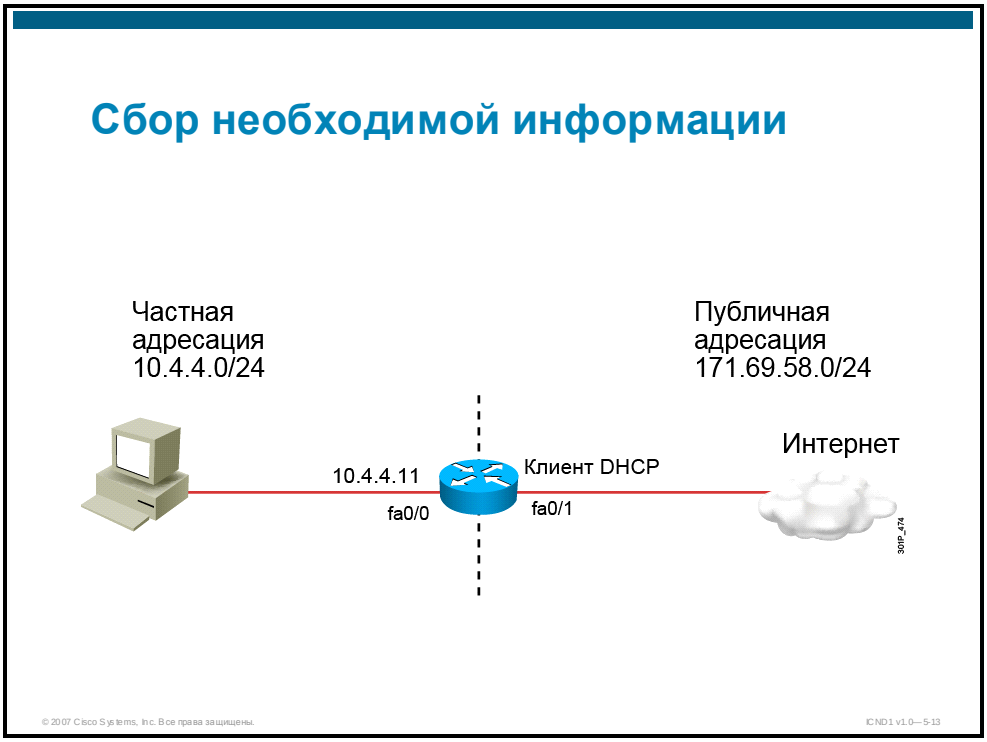
Шаг 4 Хост B получает пакет и отвечает хосту 10.1.1.1, используя внутренний глобальный IP-адрес назначения 171.69.68.2.

Шаг 5 Когда маршрутизатор получает пакет с внутренним глобальным IP-адресом, он выполняет поиск в таблице NAT. Используя внутренний глобальный адрес с портом и внешний глобальный адрес с портом в качестве ключа, маршрутизатор выполняет обратное преобразование адреса в локальный адрес 10.1.1.1 и пересылает пакет хосту 10.1.1.1.

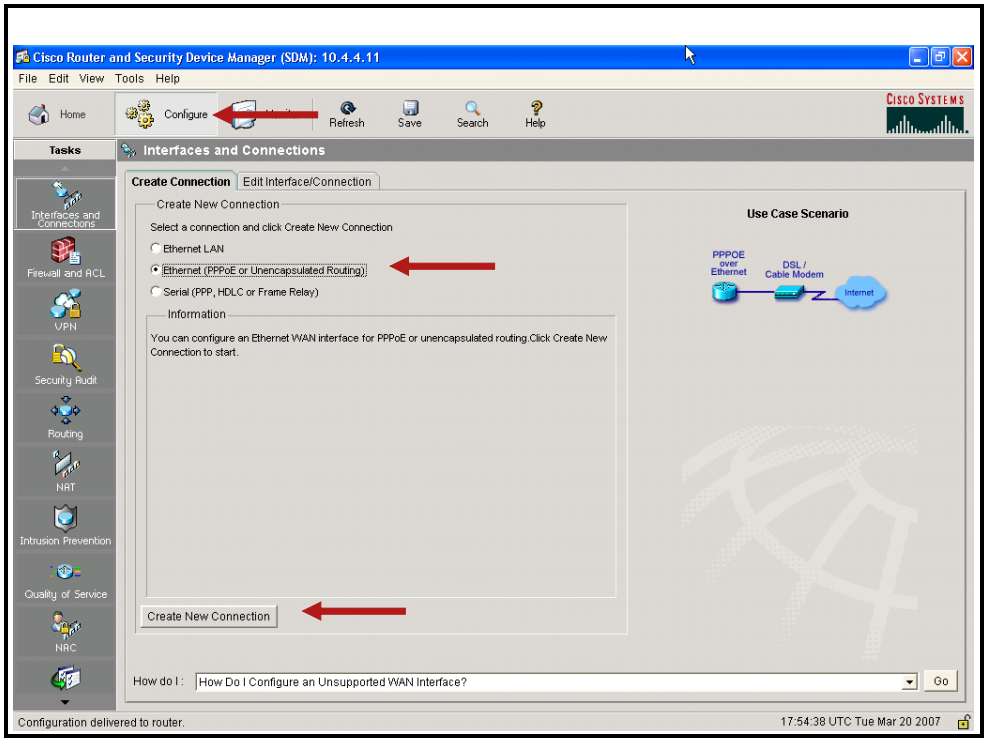
Шаг 6 Хост 10.1.1.1 получает пакет и продолжает преобразование. Маршрутизатор выполняет действия 2 – 5 для каждого пакета.

Настройка DHCP-клиента и преобразования PAT

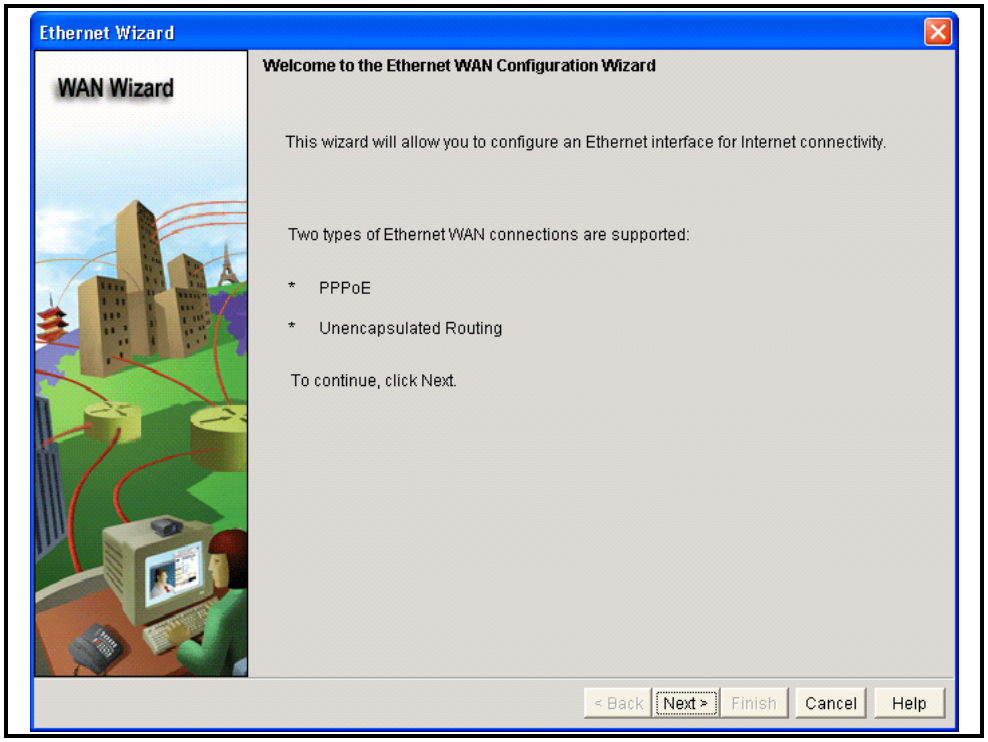
В этом разделе описывается настройка DHCP-клиента и преобразования PAT с использованием Cisco SDM.



В рассматриваемой среде будет выполнена настройка интерфейса глобальной сети (fa0/1) в качестве DHCP-клиента, ему будет назначен IP-адрес, шлюз по умолчанию и маршрутизация по умолчанию с DHCP-сервера Интернета. Кроме того, для преобразования внутренних частных адресов во внешние общие адреса будет включен механизм PAT.

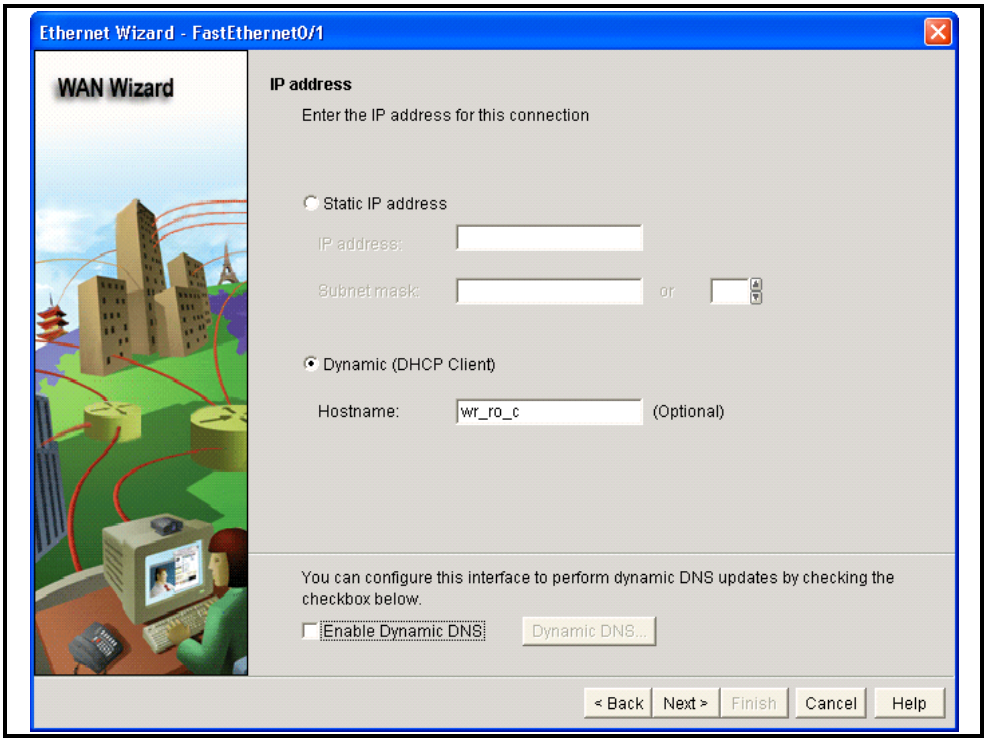


Чтобы начать настройку интерфейса DHCP-клиента, откройте вкладку **Interfaces and Connections (Интерфейсы и подключения)**. Установите переключатель **Ethernet (PPPoE or Unencapsulated Routing) (Ethernet или маршрутизация без инкапсуляции)** и нажмите кнопку **Create New Connection (Создать новое подключение)**.

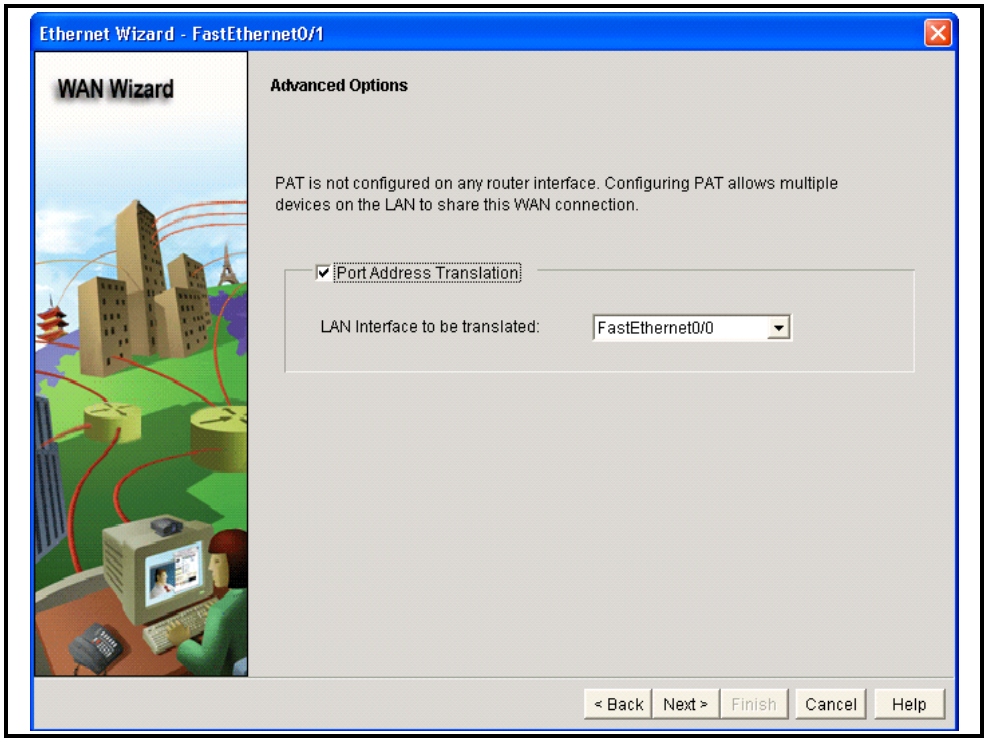


Это окно представляет мастер.

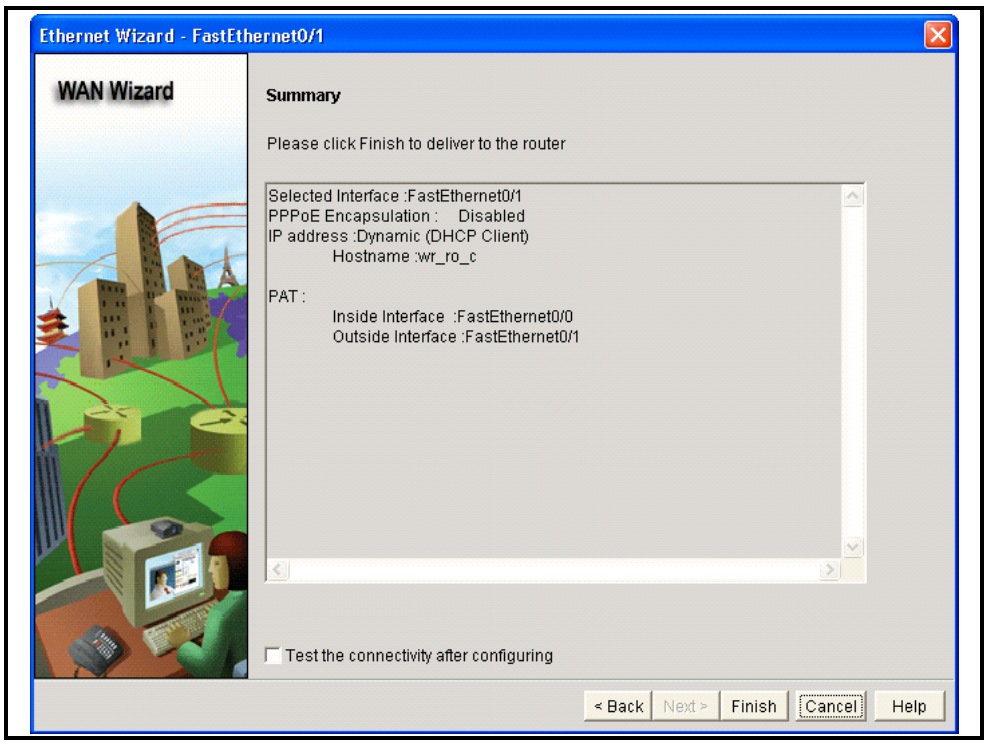
Если поставщик услуг Интернета использует протокол PPP over Ethernet (PPPoE), установите этот флажок и нажмите кнопку **Next (Далее)**.



Установите переключатель **Dynamic (DHCP Client) (Динамическая (DHCP-клиент))**.



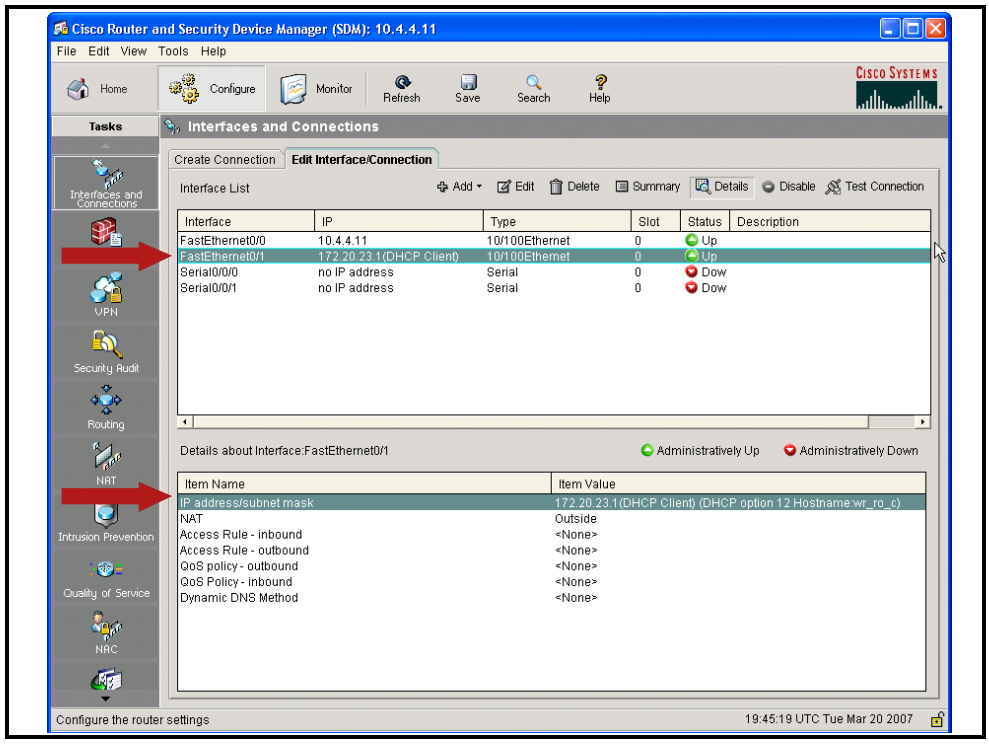
Установите флажок **Port Address Translation (Преобразование адресов портов)** и выберите внутренний интерфейс из раскрывающегося списка.



В этом окне отображается сводка по конфигурации.

Проверка конфигурации DHCP-клиента

В этом разделе описывается проверка конфигурации NAT и PAT.

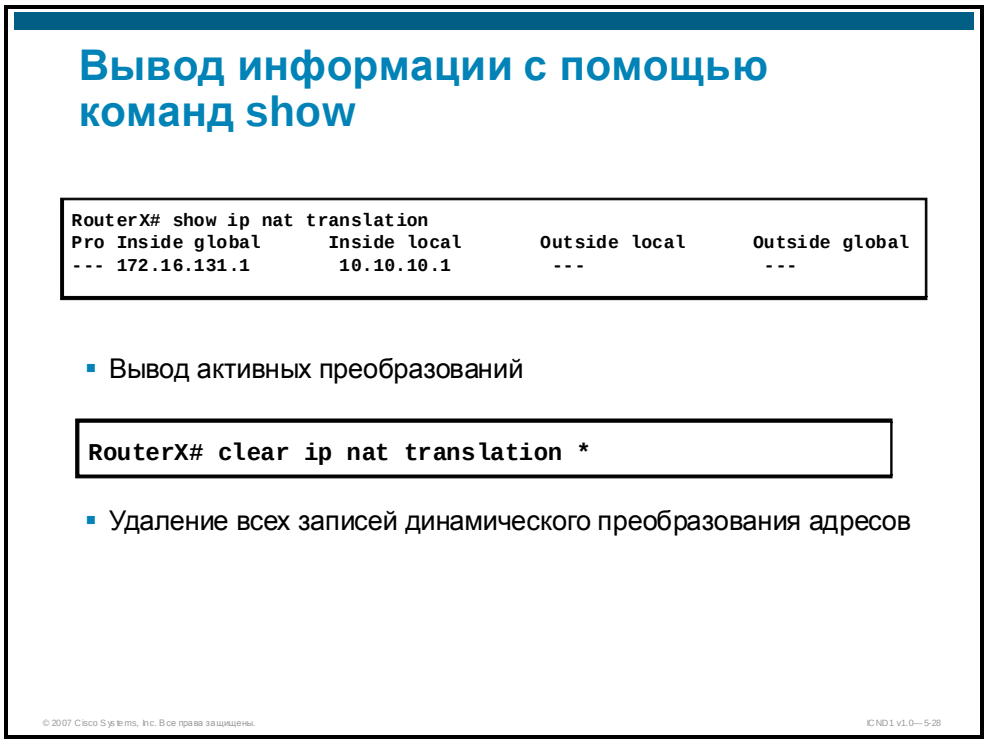


В окне Interfaces and Connections (Интерфейсы и подключения) убедитесь, что DHCP-клиент получает адрес с DHCP-сервера.

Примечание	Для отображения IP-адреса клиента может потребоваться обновление окна.

Проверка конфигурации NAT и PAT

В этом разделе описывается проверка конфигурации NAT и PAT.



В таблице приводятся команды, которые могут использоваться в режиме EXEC для отображения информации о преобразовании.

Команда	Описание
show ip nat translations	Выводит активные преобразования.
clear ip nat translation *	Удаляет все записи динамического преобразования из таблицы преобразования NAT.

После настройки NAT проверьте правильность работы механизма преобразования. Для этого можно воспользоваться командами **clear** и **show**.

По умолчанию для динамического преобразования NAT и PAT задается период бездействия (время ожидания). Если преобразование адресов портов не настроено, время ожидания записей преобразования истекает спустя 24 часа, если они не будут настроены повторно с помощью команды **ip nat translation**. Можно удалить записи до истечения времени ожидания с помощью одной из команд, перечисленных в таблице.

Или можно воспользоваться командой **show run** и найти команды NAT, ACL, интерфейса или пула с нужными значениями.

Резюме

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

Резюме

- В сетях с коммутацией пакетов пакеты данных отправляются к одному месту назначения по различным маршрутам через сеть общего доступа, принадлежащую оператору. Однако маршруты, по которым пакеты достигают места назначения, могут меняться.
- Существует несколько вариантов DSL, в том числе ADSL, SDSL, HDSL, IDSL и CDSL. Доступ по цифровой абонентской линии имеет ряд преимуществ (скорость, постоянный доступ к сети и т. д.) и недостатков (доступность).
- Кабельный доступ в Интернет стал высокоскоростной альтернативой DSL и последовательному подключению.
- Глобальная сеть Интернет возникла в результате планов министерства обороны США построить командно-административную сеть в 1960-х и выросла в крупнейшую в мире распределенную сеть с многочисленными методами доступа и вариантами использования для обмена данными, исследований и коммерции.
- Интерфейс может получить IP-адрес с DHCP-сервера.

Резюме (прод.)

- NAT позволяет внутренним интерсетям на основе протокола IP использовать незарегистрированные IP-адреса для подключения к сети Интернет. Механизм PAT является функцией NAT и позволяет преобразовать несколько внутренних адресов в один внешний адрес или небольшую группу внешних адресов.
- Для обмена данными с внешними сетями можно преобразовать внутренние IP-адреса в IP-адреса, уникальные в глобальном масштабе.
- Перегрузка — это форма динамического преобразования сетевых адресов, при которой несколько незарегистрированных IP-адресов сопоставляются с одним зарегистрированным IP-адресом (многие к одному) с использованием разных портов. Эта функция также известна как PAT.
- После настройки преобразования NAT для проверки правильности его работы можно использовать команды **clear** и **show**.

Занятие 3

Обеспечение статической маршрутизации

Обзор

Маршрутизация – это процесс определения места назначения для отправки пакетов данных, направленных за пределы локальной сети. Маршрутизаторы собирают и хранят данные маршрутизации, чтобы обеспечивать прием и передачу этих пакетов.

По сути данные маршрутизации обрабатываются в виде записей в таблице маршрутизации, при этом каждая запись соответствует идентифицированному маршруту. Можно статически (вручную) настраивать записи в таблице маршрутизации, или маршрутизатор может динамически создавать и вести таблицу маршрутизации с помощью протокола маршрутизации, который позволяет оперативно реагировать на изменения в сети.

Для эффективного управления IP-сетью необходимо понимать принцип работы статической и динамической маршрутизации и их воздействие на IP-сеть. На этом занятии рассматривается статическая IP-маршрутизация.

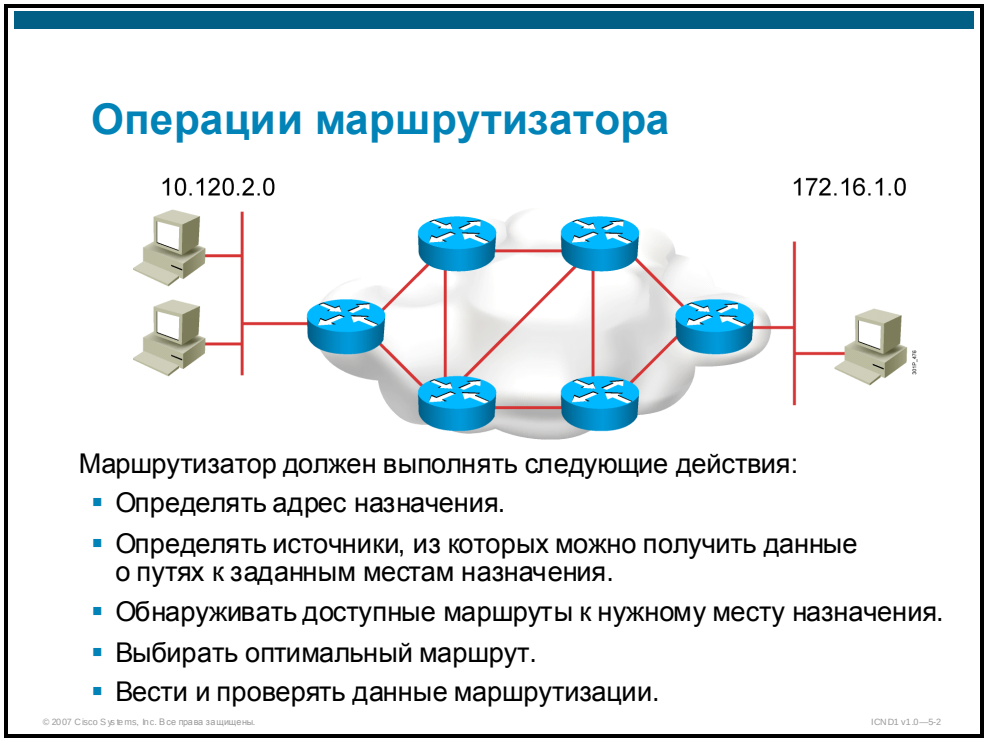
Задачи

По окончании этого занятия вы сможете описывать принцип работы, преимущества и ограничения статической и динамической маршрутизации. Это значит, что вы сможете выполнять следующие задачи:

- описывать основные характеристики статической и динамической IP-маршрутизации;
- объяснять различия между статической и динамической маршрутизацией;
- настраивать статические маршруты на маршрутизаторах Cisco;
- настраивать передачу по маршруту по умолчанию;
- проверять конфигурации статических маршрутов.

Обзор маршрутизации

В этом разделе обсуждаются основные характеристики операций статической и динамической маршрутизации.

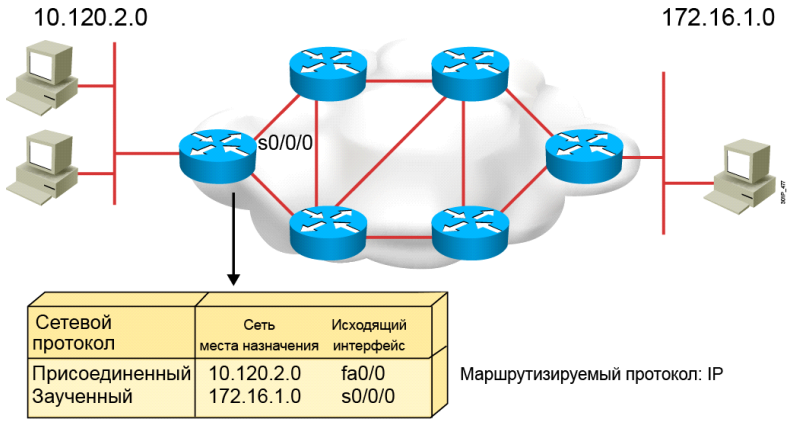


Маршрутизация является процессом доставки пакета от одного объекта к другому. Маршрутизатор служит устройством маршрутизации трафика в сетях.

Для маршрутизации данных маршрутизатор или любой другой объект, осуществляющий маршрутизацию, должен выполнить следующие операции.

- **Определить адрес назначения:** Определить место назначения (или адрес) элемента, который нуждается в маршрутизации.
- **Определить источники данных маршрутизации:** Определить источники (другие маршрутизаторы), от которых можно узнать о путях к местам назначения.
- **Определить маршруты:** Определить возможные маршруты, или пути, к нужному месту назначения.
- **Выбрать маршруты:** Выбрать оптимальный путь к нужному месту назначения.
- **Вести и проверять информацию маршрутизации:** Определять, не устарели ли известные пути к месту назначения.

Операции маршрутизатора (прод.)



Сетевой протокол	Сеть места назначения	Исходящий интерфейс
Присоединенный	10.120.2.0	fa0/0
Заученный	172.16.1.0	s0/0/0

Маршрутизируемый протокол: IP

- Маршрутизаторы могут собирать данные о местах назначения, к которым они не подключены напрямую.

Данные маршрутизации, получаемые маршрутизатором от других маршрутизаторов, хранятся в его таблице маршрутизации. Маршрутизатор узнает из этой таблицы, какие интерфейсы необходимо использовать при передаче адресованных пакетов.

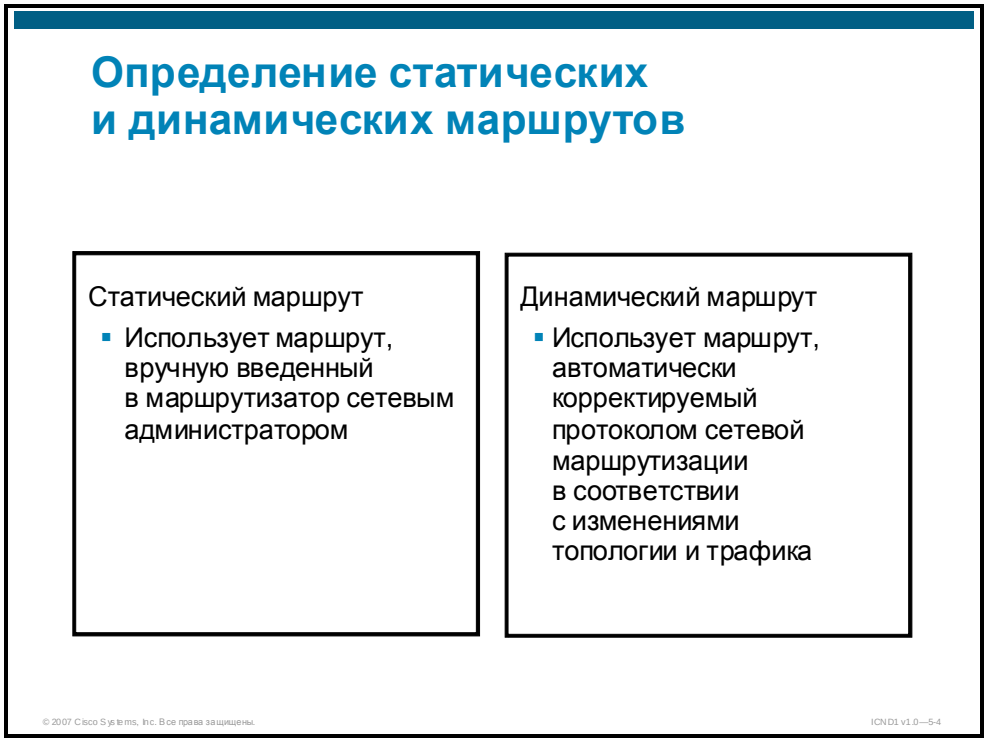
Если сеть назначения непосредственно подключена к сети-источнику, маршрутизатор уже знает интерфейсы, через которые следует переслать пакеты. Если сеть назначения не имеет непосредственного подключения к сети-источнику, маршрутизатор должен определить оптимальный маршрут передачи пакетов.

Существует два способа определения информации о месте назначения.

- Ввод информации маршрутизации вручную.
- Сбор данных маршрутизации через процесс динамической маршрутизации, выполняемый на маршрутизаторах.

Сравнение статического и динамического маршрутов

В этом разделе обсуждаются различия между статической и динамической маршрутизацией.

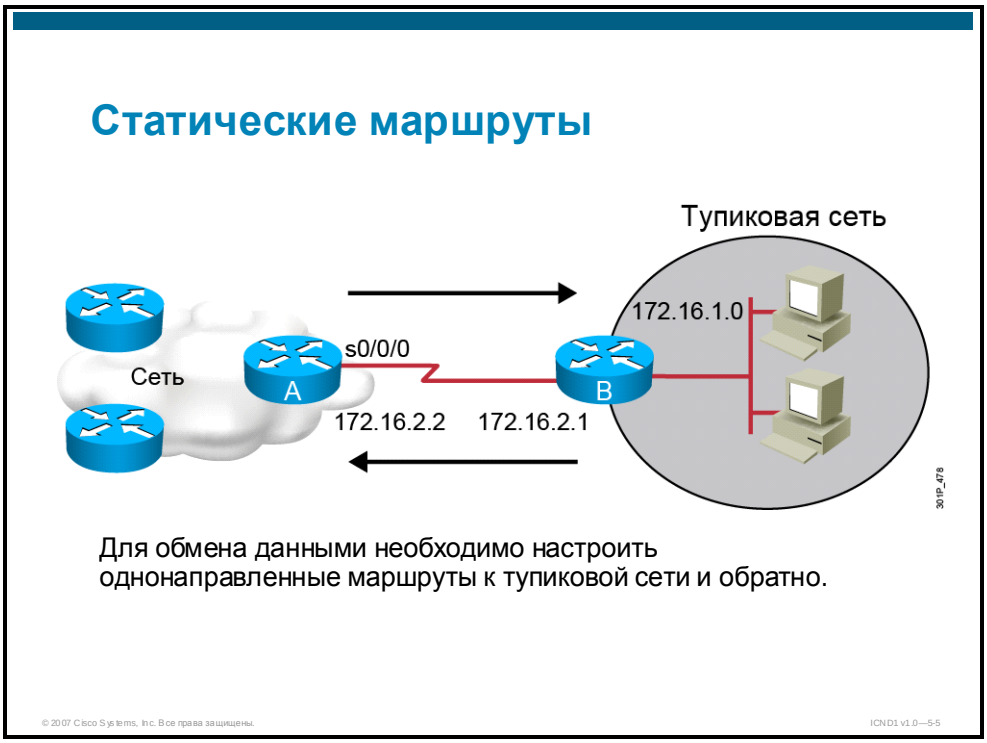


В зависимости от конфигурации маршрутизаторы передают пакеты по статическим или динамическим маршрутам. Существует два способа определения пути передачи пакетов, если сеть назначения не имеет непосредственного подключения к сети-источнику.

- **Статический маршрут:** Маршрутизатор узнает маршруты, когда администратор настраивает статический маршрут вручную. Администратор должен вручную обновлять этот статический маршрут при любом изменении топологии интерсети, требующей обновления. Статические маршруты определяются пользователем и задают путь передачи пакетов между источником и местом назначения. Эти определяемые администратором маршруты обеспечивают очень точный контроль над режимом маршрутизации в интерсети на основе протокола IP.
- **Динамический маршрут:** Маршрутизатор динамически получает маршруты, после того как администратор настраивает протокол маршрутизации, помогающий определить маршруты. В отличие от ситуации со статическими маршрутами после включения администратором динамической маршрутизации процесс маршрутизации автоматически обновляет сведения о маршруте при получении новых данных о топологии сети. Маршрутизатор получает и обновляет маршруты к удаленным местам назначения, обмениваясь обновлениями таблиц маршрутизации с другими маршрутизаторами в интерсети.

Настройка статического маршрута

В этом разделе обсуждается настройка статических маршрутов на маршрутизаторах Cisco.

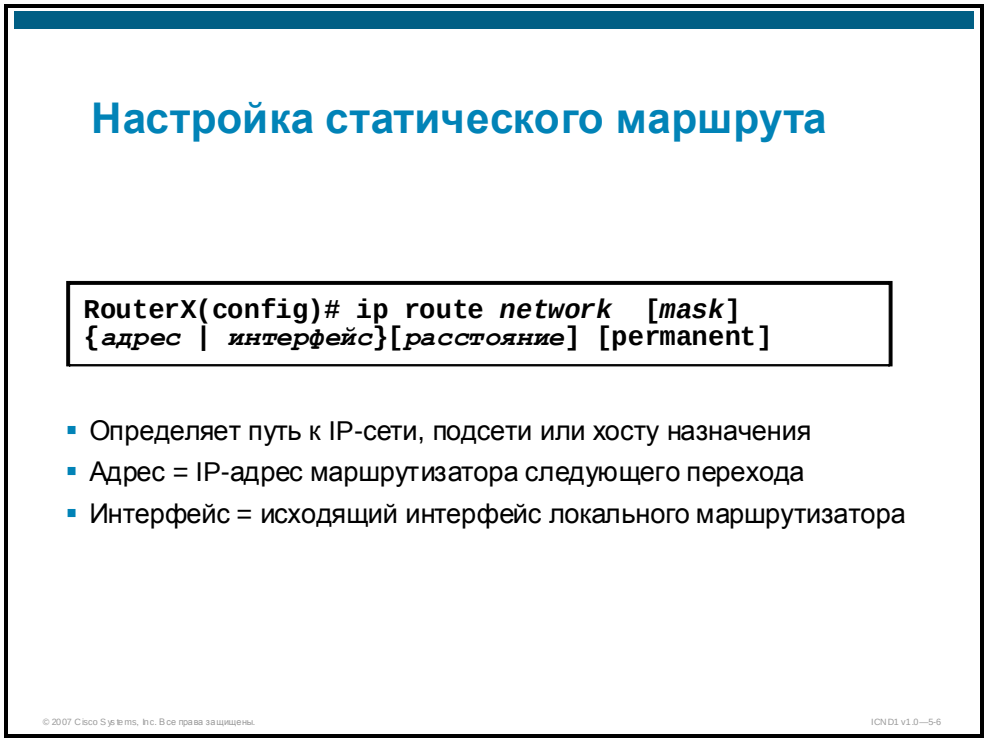


Статические маршруты часто используются при маршрутизации из сети в Тупиковую сеть. Тупиковая сеть (иногда называется конечным узлом) – это сеть, доступ к которой возможен по единственному маршруту. Статические маршруты могут также использоваться для определения «шлюза последней надежды» (gateway of last resort), на который будут отправляться все пакеты с неизвестным адресом назначения.

Пример: статические маршруты

На рисунке для маршрутизатора A настроен статический маршрут к подсети 172.16.1.0 через последовательный интерфейс маршрутизатора A. На маршрутизаторе B настроен статический маршрут или маршрут по умолчанию к сетям, находящимся после маршрутизатора A, через последовательный интерфейс маршрутизатора B.

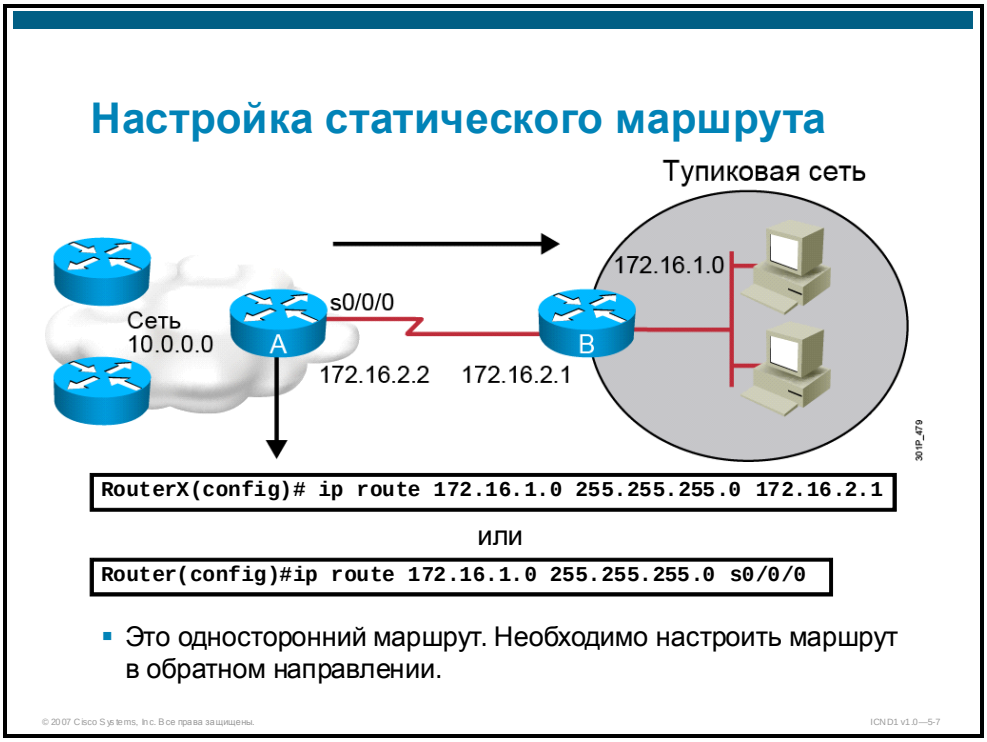
Примечание	Статический маршрут настраивается для подключения к удаленным сетям, не имеющим непосредственного подключения к данному маршрутизатору. Для обеспечения сквозного подключения необходимо настроить статический маршрут в обоих направлениях.



Чтобы настроить статический маршрут, введите команду **ip route** в режиме глобальной конфигурации. Параметры, указанные в таблице, описывают статический маршрут более подробно. Статический маршрут позволяет выполнять настройку таблицы маршрутизации вручную. Пока путь активен, динамические изменения записи в таблице маршрутизации не производятся.

В таблице перечислены параметры команды **ip route** и их описания.

Параметры команды ip route	**Описание**
network	Сеть, подсеть или хост назначения.
mask	Маска подсети.
address	IP-адрес маршрутизатора следующего перехода.
interface	Имя интерфейса, используемого для доступа к сети назначения. Это должен быть интерфейс «точка-точка». В случае интерфейса множественного доступа (например, интерфейс Ethernet общей среды) команда будет работать неправильно.
distance	(Необязательный) Определяет административное расстояние маршрута.
permanent	(Необязательный) Запрещает удаление маршрута при отключении интерфейса.



Пример: настройка статических маршрутов

В этом примере статический маршрут настроен следующим образом:

```
Router(config)#ip route 172.16.1.0 255.255.255.0 172.16.2.1
```

или

```
Router(config)#ip route 172.16.1.0 255.255.255.0 s0/0/0
```

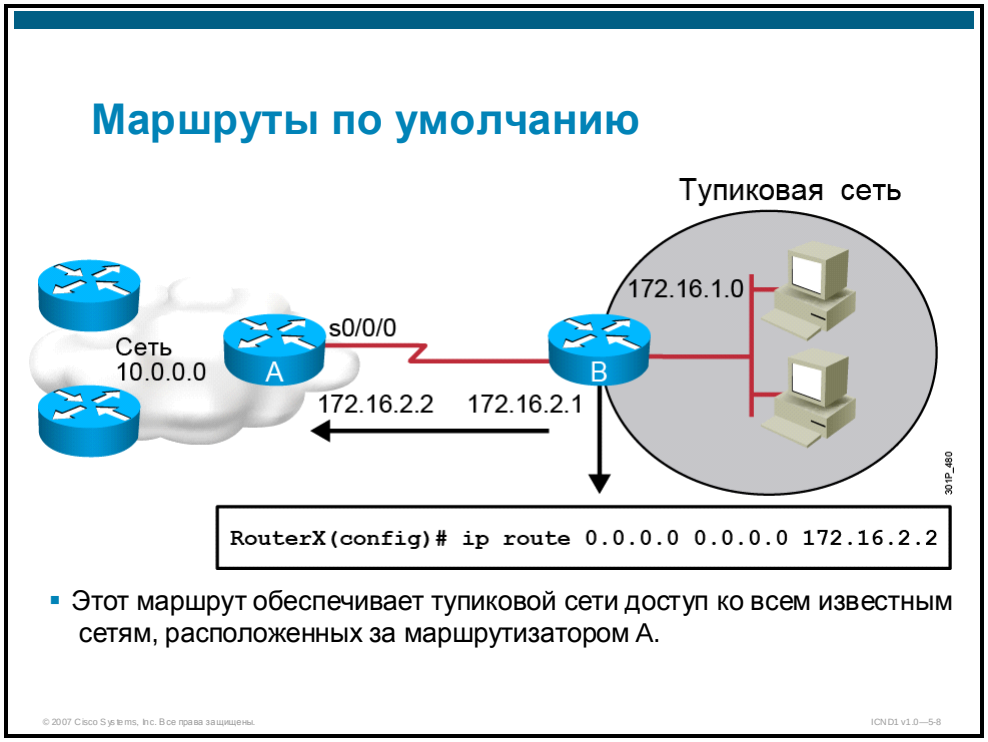
В таблице перечислены параметры команды **ip route** для этого примера.

Параметры команды ip route	**Описание**
ip route	Определяет статический маршрут.
172.16.1.0	IP-адрес статического маршрута к подсети назначения.
255.255.255.0	Определяет маску подсети. Для подсети отводится 8 бит.
172.16.2.1	IP-адрес маршрутизатора следующего перехода на пути к месту назначения.
s0/0/0	Определяет интерфейс, который будет использоваться для доступа к маршрутизатору следующего перехода.

Назначение статического маршрута для доступа к тупиковой подсети 172.16.1.0 для маршрутизатора A является правильным, поскольку существует только один путь для доступа к этой сети.

Настройка передачи данных с использованием маршрута по умолчанию

В этом разделе описывается настройка передачи пакетов с использованием маршрута по умолчанию.



Маршрут по умолчанию используется в случаях, когда маршрут от источника к месту назначения неизвестен или маршрутизатор не может поддерживать большое число маршрутов в своей таблице маршрутизации.

Команда **ip route** служит для настройки передачи пакетов с использованием маршрута по умолчанию. На рисунке для маршрутизатора B настроена передача всех пакетов с адресом назначения, не указанным в его таблице маршрутизации, маршрутизатору A.

В этом примере маршрут по умолчанию настроен следующим образом:

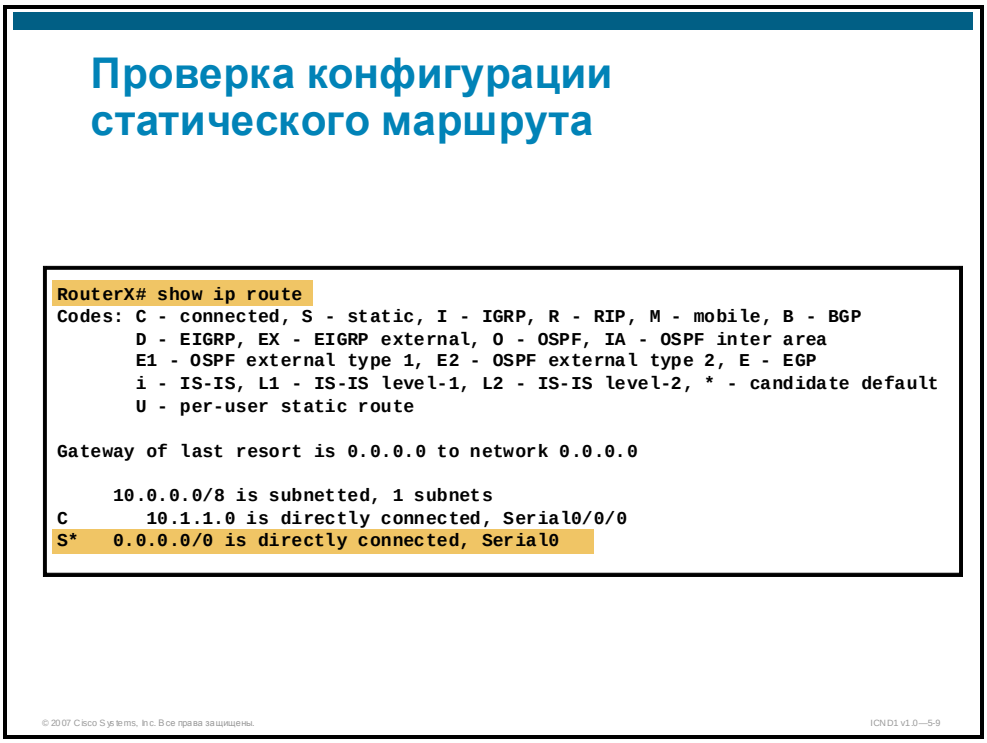
```
Router(config)# ip route 0.0.0.0 0.0.0.0 172.16.2.2
```

В таблице перечислены параметры команды **ip route** для этого примера.

Параметры команды ip route	**Описание**
ip route	Определяет статический маршрут.
0.0.0.0	Маршруты к сетям, не указанным в таблице маршрутизации.
0.0.0.0	Специальная маска, указывающая на маршрут по умолчанию.
172.16.2.2	IP-адрес маршрутизатора следующего перехода, который используется по умолчанию для передачи пакетов.

Проверка конфигурации статического маршрута

В этом разделе описывается проверка конфигурации статического маршрута.



Пример: проверка конфигурации статического маршрута

Чтобы убедиться в правильности настройки статической маршрутизации, введите команду **show ip route** и выполните поиск статических маршрутов, обозначенных буквой «S». Вывод команды показан на рисунке. Символ звездочки (*) маршрут, который будет использоваться в последнюю очередь для передачи маршрутов.

Резюме

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

Резюме

- Маршрутизация – это процесс доставки информации от одного объекта к другому. Маршрутизатор служит для маршрутизации трафика в сетях. В зависимости от конфигурации маршрутизаторы пересылают пакеты по статическим или динамическим маршрутам.
- Статические маршрутизаторы используют маршрут, вручную введенный в маршрутизатор администратором сети. Динамические маршрутизаторы используют маршрут, автоматически корректируемый протоколом сетевой маршрутизации в соответствии с изменениями топологии и трафика.
- Для обмена данными необходимо настроить однонаправленные маршруты к тупиковой сети и обратно.
- Команда **ip route** служит для настройки пересылки пакетов с использованием маршрута по умолчанию.
- Команда **show ip route** служит для проверки правильности настройки статической маршрутизации. Статические маршруты обозначены в выводе команды буквой «S».

Занятие 4

Настройка инкапсуляции последовательных интерфейсов

Обзор

Последовательные соединения «точка-точка» могут использоваться для соединения локальной сети с распределенной сетью поставщика услуг. Скорее всего, последовательные соединения «точка-точка» будут использоваться внутри локальной сети, между локальной сетью и поставщиком услуг или в обоих случаях. Необходимо знать, как настраиваются последовательные порты для таких соединений.

Наиболее распространенным способом соединения удаленных площадок является использование распределенных сетей с коммутацией каналов. Поскольку современные приложения предъявляют высокие требования к полосе пропускания, технология коммутации каналов применяется в основном в решениях для резервного копирования или в очень небольших домашних офисах. Поэтому на этом занятии будет дан только краткий обзор технологии коммутации каналов.

Соединение «точка-точка» является самым распространенным типом соединений распределенных сетей. Иногда соединение «точка-точка» называют последовательным соединением или соединением по арендуемой (выделенной) линии, поскольку каналы связи арендуются у оператора (обычно у телефонной компании) и выделяются для использования арендующей компанией. Компании оплачивают постоянное соединение между двумя удаленными площадками. Канал связи остается активным и доступным постоянно. Представление о том, как каналы связи «точка-точка» обеспечивают доступ к распределенной сети, необходимо для понимания принципа работы распределенных сетей в целом.

К технологиям коммутации пакетов, используемым для соединения площадок, можно отнести Frame Relay и ATM. Из-за сложности этих технологий на этом уроке будет дан только их общий обзор. Более подробно технологии с коммутацией пакетов обсуждаются в курсе *Interconnecting Cisco Network Devices Part 2* (ICND2).

Это занятие описывает протоколы, используемые для инкапсуляции данных канального и сетевого уровней по последовательным каналам, а также их настройка.

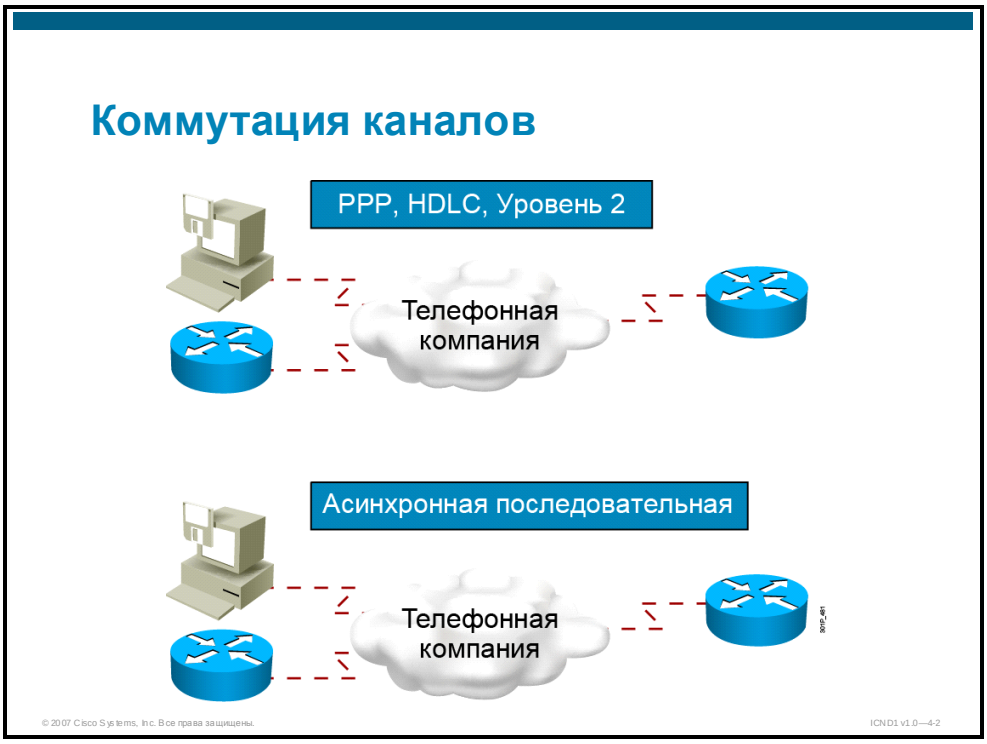
Задачи

По окончании этого занятия вы сможете настраивать последовательные порты для инкапсуляции PPP. Это значит, что вы сможете выполнять следующие задачи:

- определять функции и характеристики соединений распределенной сети с коммутацией каналов;
- перечислять характеристики и функции коммутируемых телефонных сетей общего пользования (ТфОП);
- определять функции и характеристики коммуникационных каналов «точка-точка»;
- определять характеристики протокола HDLC;
- выполнять настройку инкапсуляции HDLC на последовательном интерфейсе;
- определять характеристики протокола PPP и описывать его настройку на последовательном интерфейсе;
- проверять конфигурации HDLC и PPP;
- определять характеристики протокола Frame Relay;
- определять характеристики ATM.

Каналы передачи данных с коммутацией каналов

Коммутируемые каналы позволяют устанавливать соединения, если необходимо передать данные, и закрывать их после завершения передачи. В этом разделе рассматривается принцип действия коммутации каналов.



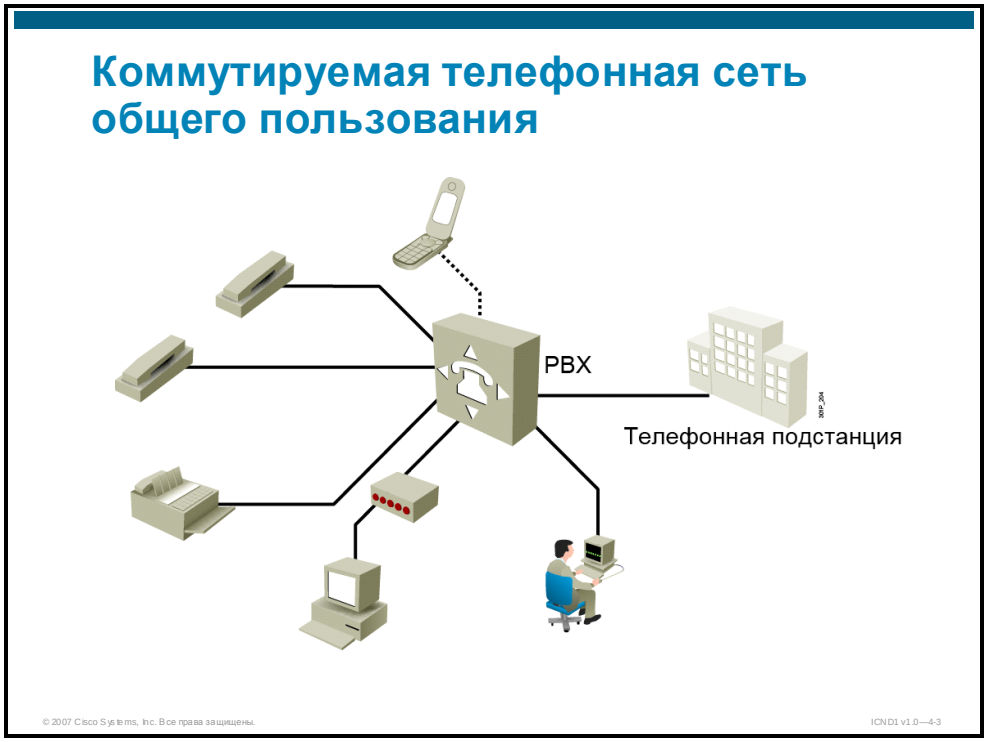
При коммутации каналов для каждого сеанса связи устанавливается, поддерживается и закрывается выделенный путь по сети оператора. Только путь доступа является выделенным физическим каналом, сеть использует те или иные технологии мультиплексирования внутри распределенной сети.

Принцип действия коммутации каналов очень похож на обычный коммутируемый телефонный вызов и широко используется в сетях телефонных компаний. При коммутации каналов устанавливается выделенное физическое соединение для передачи данных или голоса между отправителем и получателем. Перед началом обмена данными необходимо установить соединение путем настройки коммутаторов посредством выполнения дозвона. В то время как каналы «точка-точка» могут обеспечить соединение только двух площадок, коммутация каналов позволяет нескольким площадкам подключаться к коммутируемой сети оператора и обмениваться данными между собой.

Примером соединения с коммутацией каналов может служить коммутируемая телефонная сеть общего пользования (ТфОП).

Коммутируемая телефонная сеть общего пользования

Наиболее распространенным типом распределенной сети с коммутацией каналов является коммутируемая телефонная сеть общего пользования ТфОП (также известная как обычная аналоговая телефонная сеть). В этом разделе описывается принцип работы ТфОП.

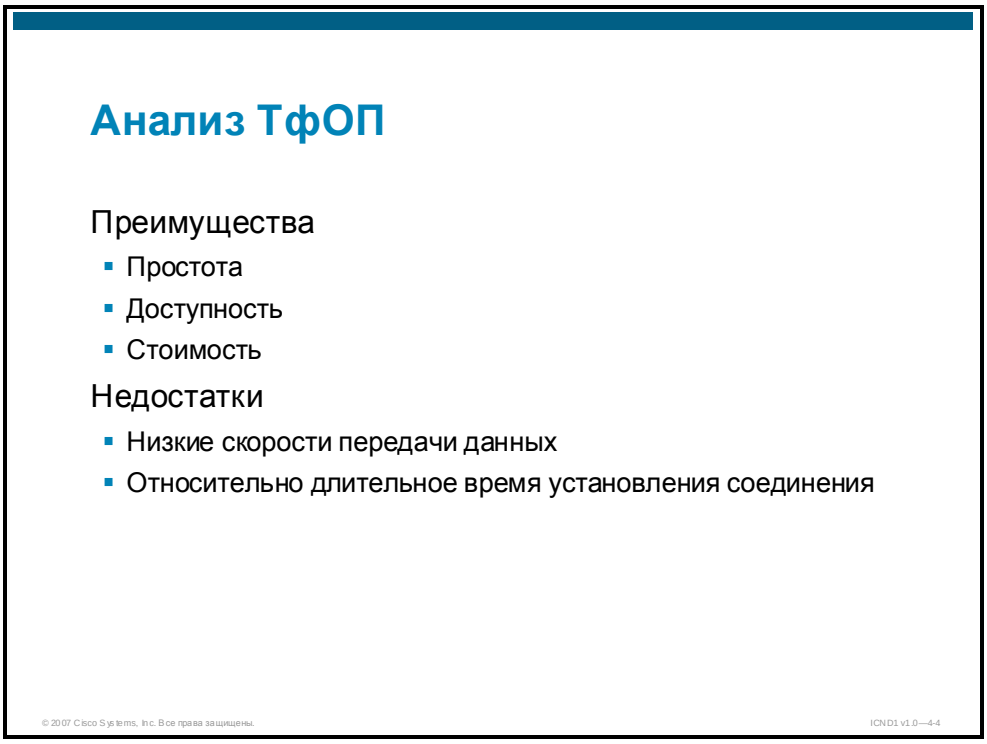


Если необходима кратковременная передача малых объемов данных, асинхронные модемы и аналоговые коммутируемые телефонные каналы обеспечивают выделенные коммутируемые соединения по требованию с низкой пропускной способностью. В традиционной телефонии для соединения телефона абонента с телефонной сетью применяется медный кабель, именуемый местной линией связи. Сигнал, передаваемый по местной линии связи во время вызова, является постоянно меняющимся электронным сигналом, в который преобразуется голос абонента.

Местная линия связи непригодна для непосредственной передачи двоичных компьютерных данных, однако модем может передавать компьютерные данные по голосовой телефонной сети. Модем модулирует двоичные данные в аналоговый сигнал на источнике и демодулирует его в двоичные данные в месте назначения.

Скорость передачи сигнала ограничена физическими характеристиками местной линии связи и ее подключения к ТфОП. Верхний предел составляет примерно 33 Кбит/с. Скорость передачи данных может быть увеличена до 56 Кбит/с, если сигнал поступает по цифровому соединению.

Для небольших предприятий ТфОП может быть вполне приемлемым решением для обмена данными продаж, ценами, стандартными отчетами и электронными сообщениями. Использование автоматического коммутируемого соединения в ночное время или по выходным для передачи крупных файлов и резервного копирования данных может оказаться выгодным за счет невысоких тарифов (платы за пользование линиями). Тарифы зависят от расстояния между конечными устройствами, времени суток и продолжительности вызова.



Использование ТфОП имеет ряд преимуществ, в том числе:

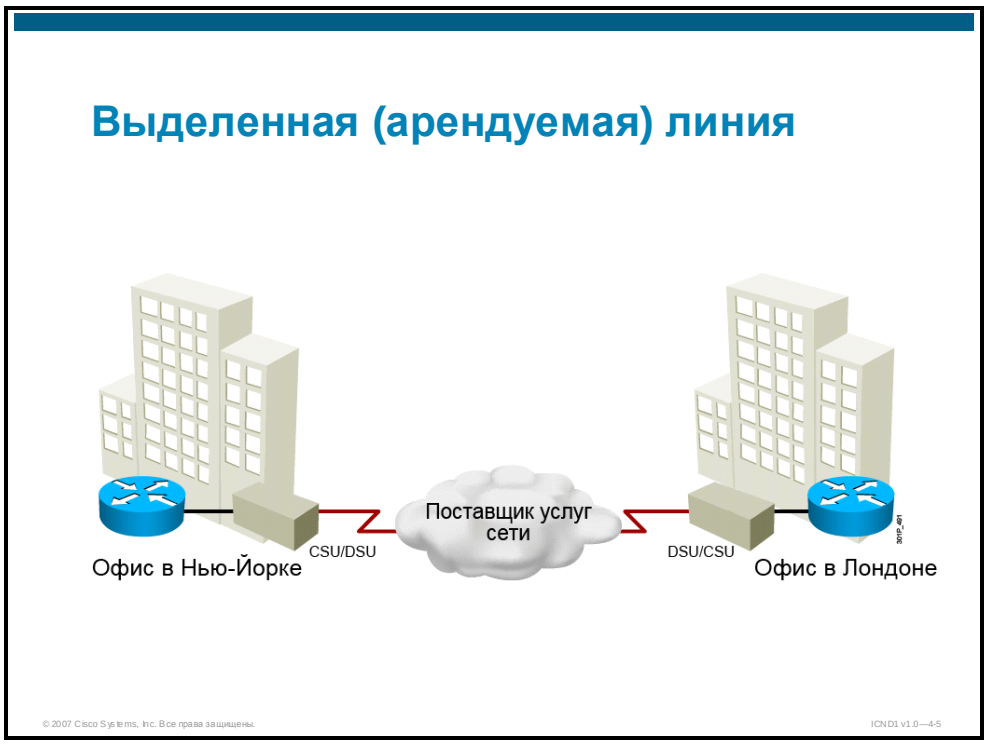
- **Простота:** Не требуется никакого дополнительного оборудования, кроме модема, причем аналоговые модемы легко настраиваются.
- **Доступность:** Поскольку телефонная сеть общего пользования доступна практически повсеместно, не составляет труда найти поставщика телефонных услуг с высоким качеством обслуживания телефонной системы. Ситуации, где линии недоступны, крайне редки.
- **Стоимость:** Затраты, связанные с реализацией канала ТфОП к распределенной сети, относительно низки и состоят преимущественно из платы за пользование каналом и стоимости модемов.

Использование ТфОП имеет и ряд недостатков:

- **Низкие скорости передачи данных:** Поскольку телефонная система предназначена для передачи голосовых данных, скорость передачи больших файлов данных весьма низка.
- **Относительно длительное время установления соединения:** Так как подключение к ТфОП требует коммутируемого доступа, время, требуемое для подключения к распределенной сети, существенно превышает это значение для других типов подключений.

Каналы связи «точка-точка»

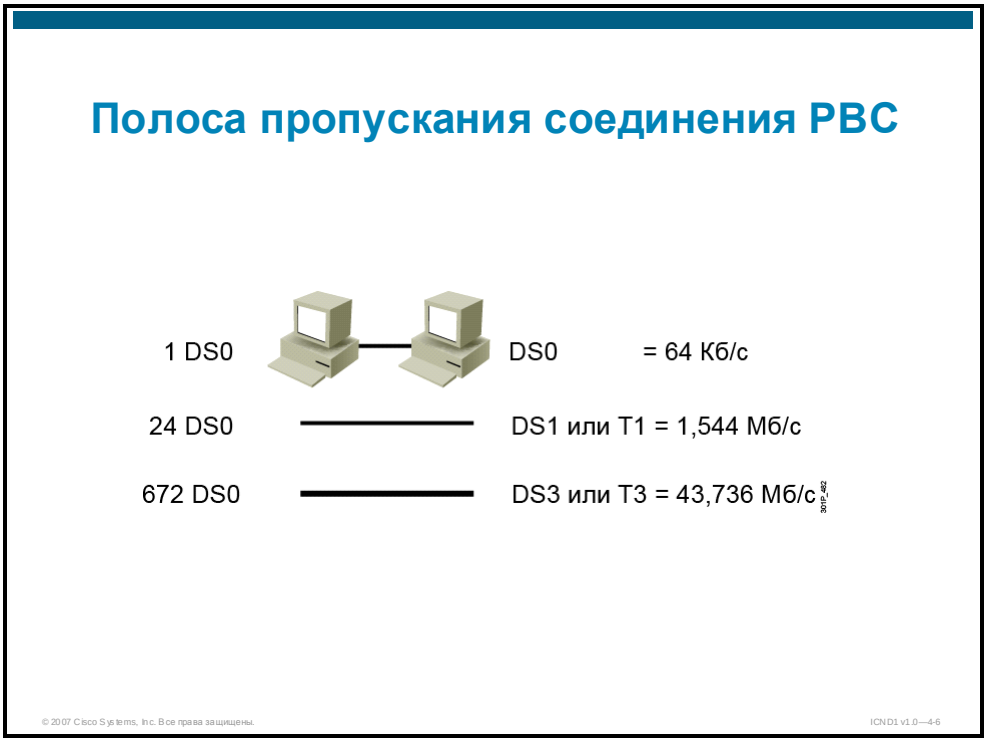
Канал связи «точка-точка» (последовательный канал) обеспечивает отдельный постоянный коммуникационный путь PBC от абонента к удаленной сети через сеть оператора, например телефонной компании. В этом разделе описываются функции технологии «точка-точка».



Канал "точка-точка" (последовательный канал) соединяет две географически удаленных площадки, например корпоративный офис в Москве и региональный офис в Волгограде. Каналы «точка-точка», как правило, арендуются у оператора и поэтому часто называются арендуемыми линиями. Для канала «точка-точка» оператор выделяет фиксированную полосу пропускания и вспомогательное оборудование для арендуемой линии. Однако оператор будет применять в сети технологии мультиплексирования.

Если базовая сеть основана на технологиях T-каналов или E-каналов, арендуемая линия соединяется через сетью оператора посредством DSU/CSU. Назначение DSU/CSU состоит в подаче синхронизированного сигнала на интерфейс клиентского оборудования с DSU и подключения транспортного носителя с разделением каналов к CSU. Кроме того, CSU выполняет диагностические функции, например тесты возвратной петли. Большая часть интерфейсов T1 или E1 с временным мультиплексированием (TDM) на современных маршрутизаторах поддерживает соответствующие функции DSU/CSU.

Выделенные каналы являются распространенным типом доступа к распределенной сети, стоимость которого определяется необходимой полосой пропускания и расстоянием между двумя соединяемыми точками.



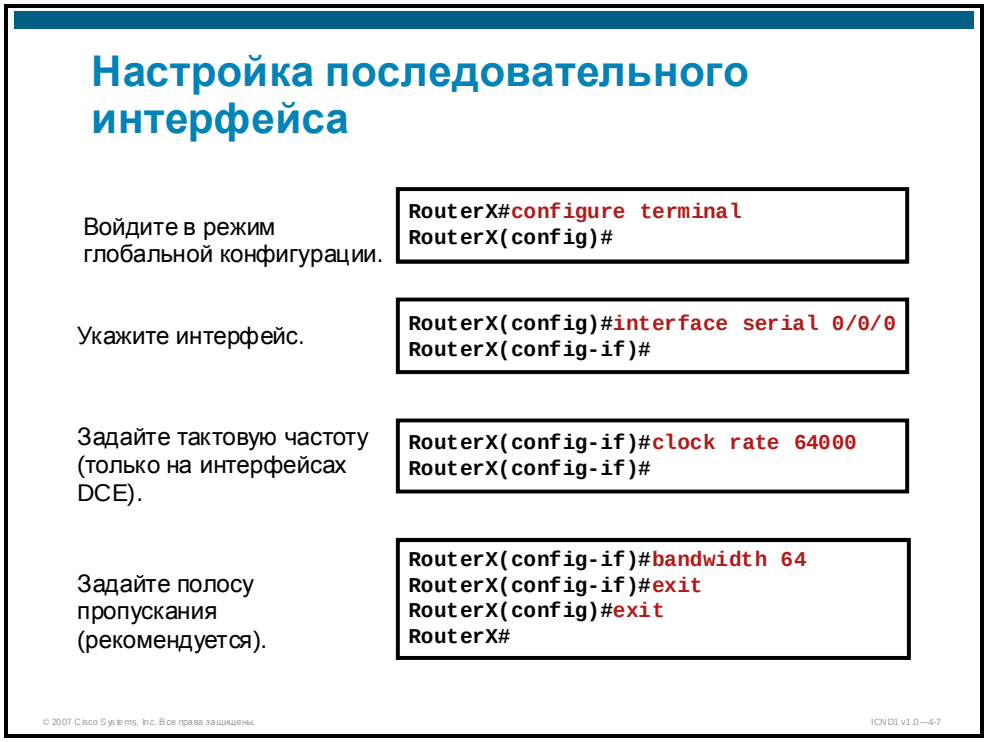
Полоса пропускания

Полосой пропускания называется скорость передачи данных по каналу связи. Доступные полосы пропускания зависят от базовой технологии оператора. Существуют различия в вариантах полосы пропускания, принятыми в Северной Америке (T-каналы) и в Европе (E-каналы). Обе системы основаны на плезиохронной цифровой иерархии (PDH), поддерживаемой в их сетях. В оптических сетях используется другая иерархия полосы пропускания, которая также различается в Северной Америке и Европе. В США варианты полосы пропускания определяются стандартом Optical Carrier (OC), в Европе – Synchronous Digital Hierarchy (SDH).

В Северной Америке полоса пропускания обычно выражается номером уровня цифрового сигнала (DS0, DS1 и т. д.), который с технической точки зрения отражает скорость передачи и формат сигнала. Скорость базового канала составляет 64 Кбит/с, или DS0, что соответствует полосе пропускания, необходимой для несжатого оцифрованного телефонного вызова.

Полосы пропускания последовательного соединения могут постепенно увеличиваться в соответствии с потребностью более быстрой передачи данных. Например, 24 канала DS0 могут быть объединены в канал DS1 (именуемый также каналом T1) со скоростью 1,544 Мбит/с. В свою очередь, 28 каналов DS1 могут быть объединены в канал DS3 (именуемый также каналом T3) со скоростью 43,736 Мбит/с.

Примечание	Каналы E1 (2,048 Мбит/с) и E3 (34,368 Мбит/с) являются европейскими стандартами, аналогичными T1 и T3, хотя они имеют другие полосы пропускания и структуры кадров.



В таблице перечислены действия по настройке последовательного интерфейса.

№	Действие
1.	Войдите в режим глобальной конфигурации (с помощью команды **configure terminal**).
2.	В режиме глобальной конфигурации перейдите в режим конфигурации интерфейса. В данном примере используется команда **interface serial 0/0/0**.
3.	Если подключен кабель DCE, воспользуйтесь командой **clock rate** *bps*, задав нужную скорость. Используйте команду конфигурации интерфейса **clock rate** для настройки тактовой частоты для подключений оборудования к последовательным интерфейсам, например сетевым интерфейсным модулям (NIM) и интерфейсным процессорам, на соответствующую скорость передачи. Необходимо задать полное значение тактовой частоты. Например, нельзя сократить тактовую частоту 64000 до 64. В последовательных каналах одна сторона канала действует как оборудование для передачи данных (DCE), а другая – как терминальное оборудование (DTE). По умолчанию маршрутизаторы Cisco являются устройствами DTE, но могут быть настроены как устройства DCE. В каскадной (back-to-back) конфигурации маршрутизатора, в которой модем не используется, один из интерфейсов должен быть настроен как устройство DTE, чтобы обеспечить тактовый сигнал. Необходимо указать тактовую частоту для каждого интерфейса DCE, настраиваемого в такой среде. Тактовые частоты, выраженные в битах в секунду, могут иметь следующие значения: 1200, 2400, 4800, 9600, 19200, 38400, 56000, 64000, 72000, 125000, 148000, 500000, 800000, 1000000, 1300000, 2000000 и 4000000.
4.	Введите указанную полосу пропускания для интерфейса. Командой **bandwidth** указывается минимальная гарантированная полоса пропускания при возникновении перегрузки сети. Команда **bandwidth** переопределяет полосу пропускания по умолчанию, отображаемую командой **show interfaces** и используемую несколькими протоколами маршрутизации, например протоколом Interior Gateway Routing Protocol (IGRP), для вычислений метрики маршрутизации. Маршрутизатор использует полосу пропускания и в других вычислениях, например, в расчетах для протокола Resource Reservation Protocol (RSVP). По умолчанию полоса пропускания последовательного канала равна скорости канала T1 (1,544 Мбит/с). Введенная полоса пропускания не влияет на фактическую скорость канала.

Примечание Режим DTE или DCE на маршрутизаторе Cisco определяется подключенным последовательным кабелем. Выбирайте кабель в соответствии с требованиями сети.

Пример конфигурации PPP

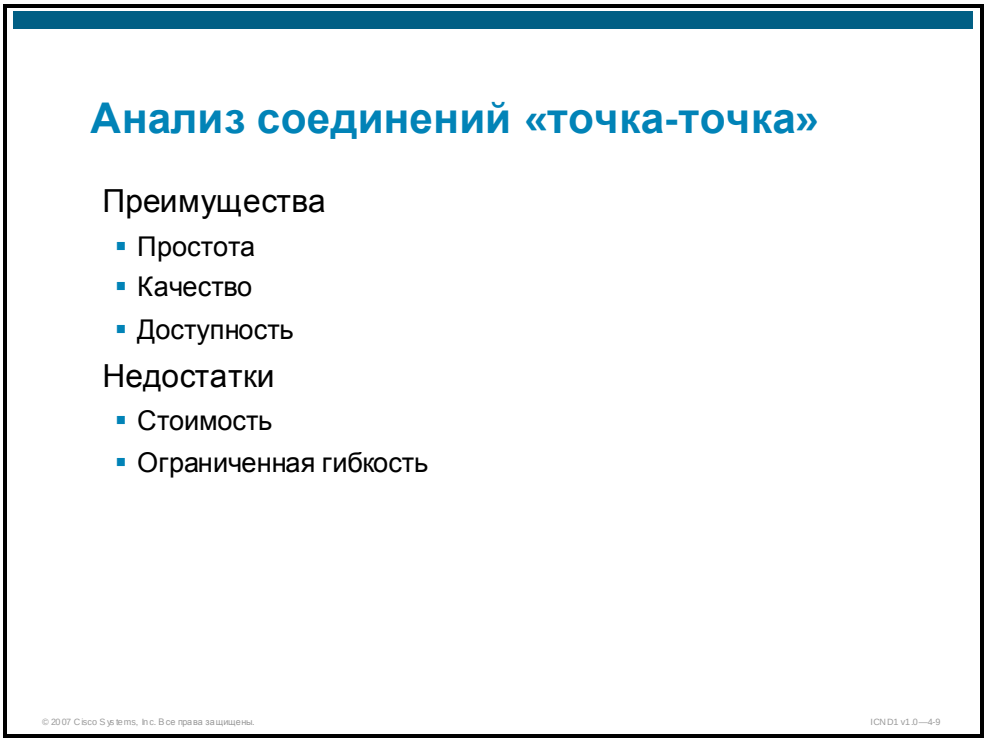

```
hostname left
!
int serial 0
 ip address 10.0.1.1 255.255.255.0
 encapsulation ppp
```

```
hostname right
!
int serial 0
 ip address 10.0.1.2 255.255.255.0
 encapsulation ppp
```


Команда **show controller** отображает информацию о физическом интерфейсе. Эта команда позволяет определить тип кабеля, подключенного к последовательному интерфейсу, без непосредственного осмотра кабеля.

На рисунке приводится конфигурация последовательного интерфейса с подключенным кабелем DTE.

Вывод определяется при первоначальном запуске маршрутизатора и включает только тип кабеля, подключенного при запуске. Если тип кабеля после запуска меняется, команда **show controller** не может отобразить тип нового кабеля.



Анализ соединений «точка-точка»

Каналы «точка-точка» являются традиционным типом соединений. Эта разновидность доступа к распределенной сети имеет ряд преимуществ.

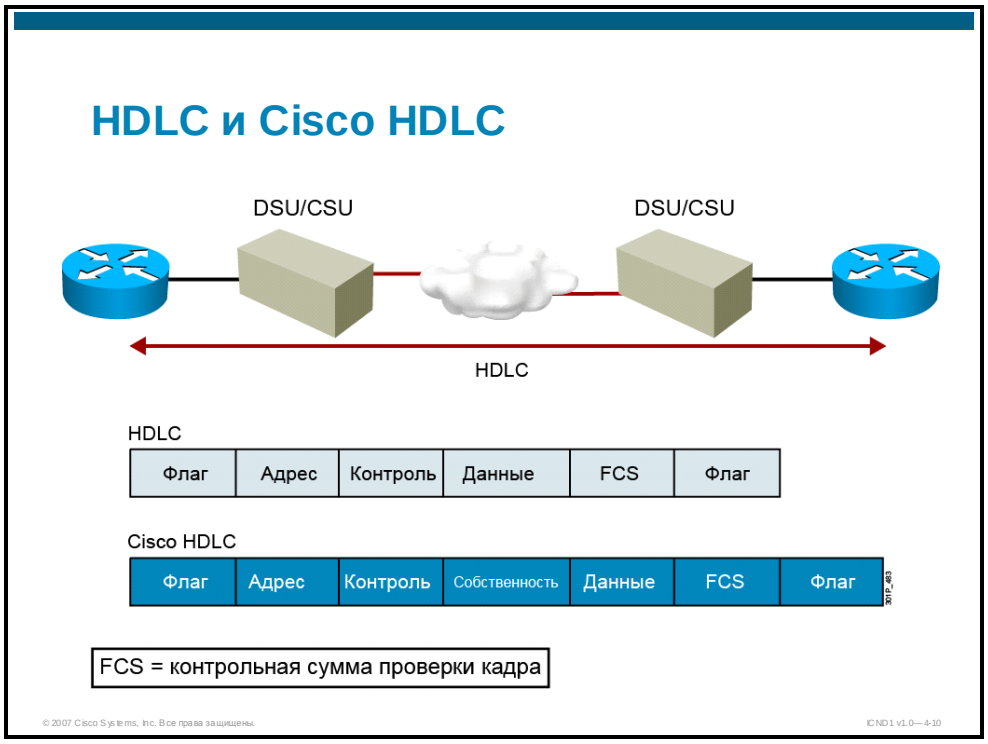
- **Простота:** Установка и обслуживание каналов «точка-точка» требует минимального опыта.
- **Качество:** Каналы «точка-точка», как правило, обеспечивают высокое качество услуг при условии достаточной полосы пропускания. Выделенная полоса пропускания не создает задержки или джиттера между конечными устройствами.
- **Доступность:** Постоянная доступность является обязательным требованием некоторых приложений, например, электронной коммерции, и каналы «точка-точка» обеспечивают непрерывно доступную выделенную полосу пропускания.

Использование этого типа доступа к распределенной сети имеет и ряд недостатков.

- **Стоимость:** Каналы «точка-точка» обычно являются самым дорогостоящим видом доступа к распределенной сети, и их стоимость становится значительной при использовании для соединения большого количества площадок. Кроме того, для каждого конечного устройства необходим интерфейс на маршрутизаторе, что увеличивает стоимость оборудования.
- **Ограниченная гибкость.** Трафик распределенной сети подвержен колебаниям, и фиксированная полоса пропускания выделенных линий приводит к тому, что линия часто не соответствует требованиям. Любые изменения выделенного канала требуют посещения площадки специалистами поставщика услуг Интернета или оператора для регулировки полосы пропускания.

Протокол HDLC (High-Level Data Link Control Protocol)

Протокол HDLC (High-Level Data Link Control) является одним из двух основных протоколов канального уровня, широко используемым в соединениях PBC типа «точка-точка». В этом разделе описывается протокол HDLC.

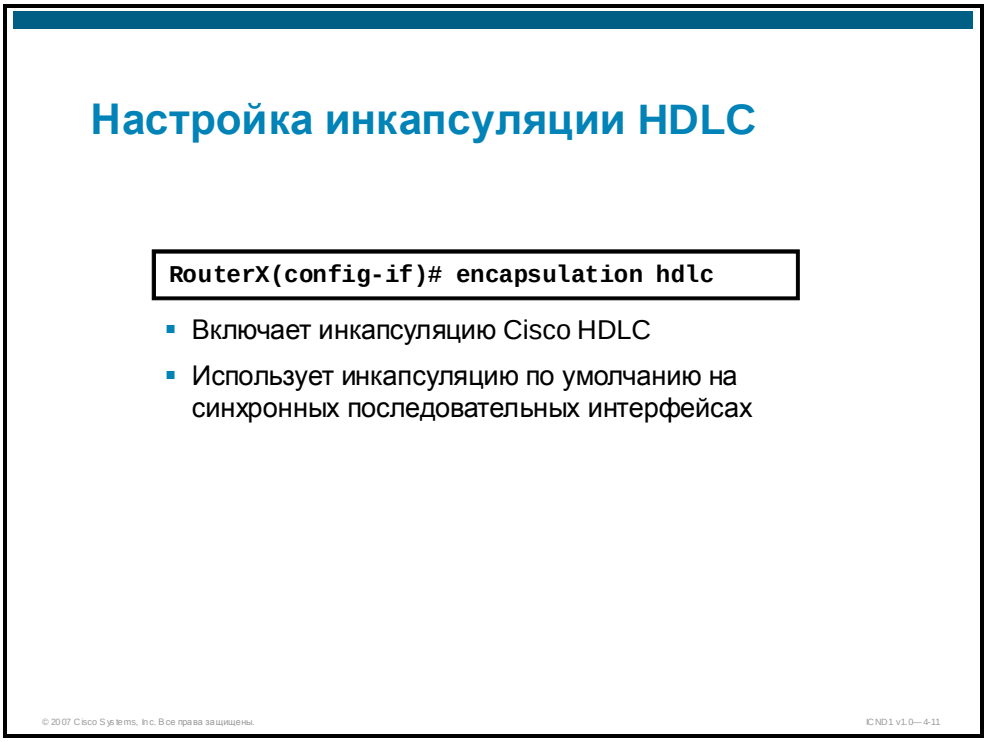


Протокол HDLC определяет метод инкапсуляции данных в каналах синхронной последовательной передачи с использованием кадров и контрольной суммы. Протокол HDLC поддерживает как конфигурацию «точка-точка», так и многоточечные конфигурации, а также аутентификацию. Однако протокол HDLC может стать причиной несовместимости двух устройств различных поставщиков из-за разных способов его реализации.

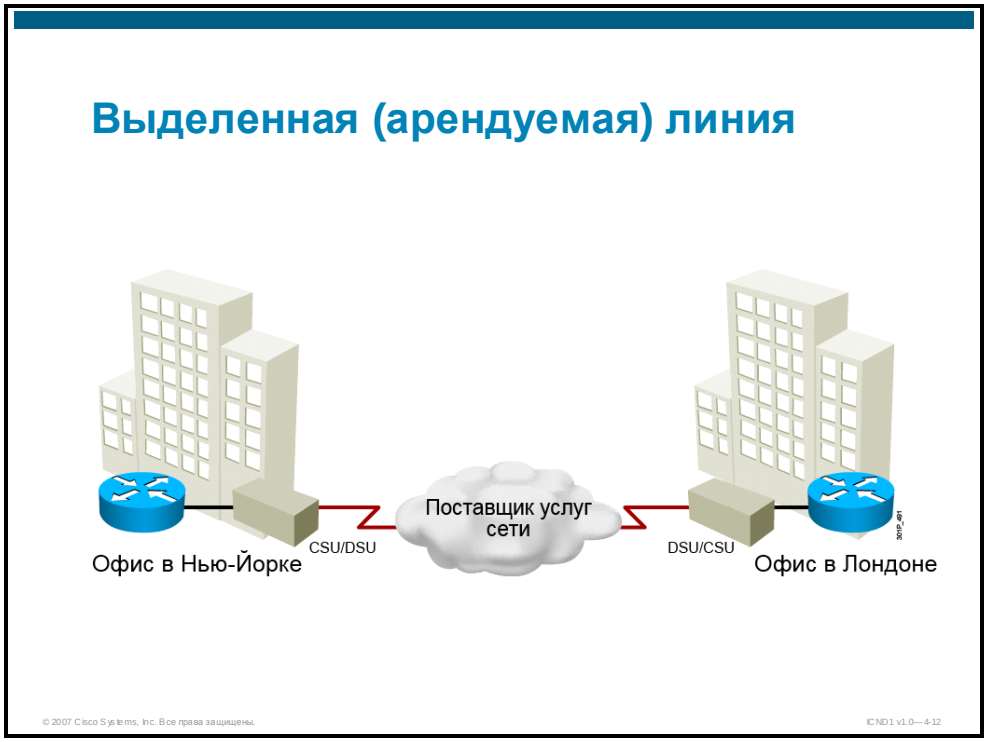
Существует реализация Cisco HDLC, которая применяется по умолчанию для инкапсуляции последовательных каналов. Протокол Cisco HDLC максимально упрощен; в нем не используется управление размером окна или потоком и допускаются только соединения «точка-точка». Реализация HDLC от Cisco включает частные расширения в поле данных, как показано на рисунке. Эти расширения допускали поддержку нескольких протоколов до появления протокола PPP. Эта модификация протокола HDLC делает невозможным взаимодействие с другими реализациями HDLC. Варианты инкапсуляции HDLC могут отличаться, если необходима совместимость, следует использовать протокол PPP.

Настройка инкапсуляции HDLC

В этом разделе описывается настройка инкапсуляции HDLC на последовательном интерфейсе.



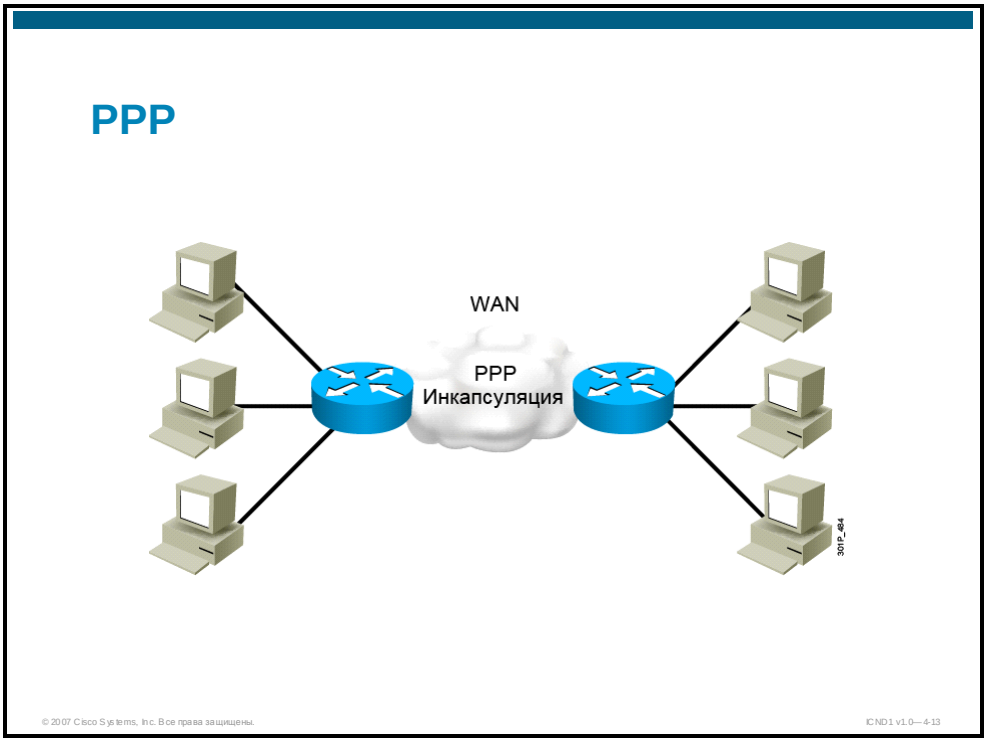
По умолчанию в синхронных последовательных каналах на устройствах Cisco используется метод последовательной инкапсуляции Cisco HDLC. Однако если на последовательном интерфейсе настроен другой протокол инкапсуляции, который необходимо изменить на HDLC, войдите в режим конфигурации настраиваемого интерфейса. Воспользуйтесь командой конфигурации интерфейса **encapsulation hdlc**, чтобы задать инкапсуляцию HDLC на этом интерфейсе.



Cisco HDLC – это протокол соединения «точка-точка», который используется на выделенных каналах между двумя устройствами Cisco. Для связи с устройством от другого поставщика синхронный протокол PPP является оптимальным вариантом.

Протокол PPP (Point-to-Point Protocol)

В этом разделе описываются характеристики протокола PPP и его активация на последовательном интерфейсе.



PPP был создан как протокол инкапсуляции, используемый для передачи IP-трафика через каналы «точка-точка». Протокол PPP также определяет стандарт назначения IP-адресов и управления ими, асинхронной (бит начала и остановки передачи) и побитовой синхронной инкапсуляции, мультиплексирования сетевых протоколов, конфигурации канала, проверки качества канала, обнаружения ошибок и согласования параметров для таких функций, как согласование адресов сетевого уровня и сжатия данных.

Протокол PPP обеспечивает соединения «маршрутизатор-маршрутизатор» и «хост-сеть» в синхронных и асинхронных каналах. Примером асинхронного соединения является коммутируемое подключение. Примером синхронного соединения является арендованная линия.

Протокол PPP предоставляет стандартный метод передачи многопротокольных датаграмм (пакетов) по каналам «точка-точка». Протокол PPP включает три основных компонента:

- метод инкапсуляции многопротокольных датаграмм;
- протокол управления каналом связи (LCP) для установления, настройки и проверки канального соединения;
- семейство программ управления сетью (NCP) для установки и настройки различных протоколов сетевого уровня.

Протокол PPP предполагает, что протокол управления каналом (LCP) является достаточно универсальным и доступным для широкого диапазона сред. Протокол LCP используется для автоматического определения формата инкапсуляции, управления различными ограничениями размеров пакетов, обнаружение петли канала и закрытия канала. Другие дополнительные средства обеспечивают аутентификацию узла на другой стороне канала и обнаружение возможных неполадок канала.

Этап аутентификации сеанса PPP не является обязательным. После создания канала связи и выбора протокола аутентификации возможна аутентификация узла на противоположной стороне канала. Если аутентификация выбрана, она выполняется до начала этапа конфигурации протокола сетевого уровня.

Параметры аутентификации требуют ввода вызывающей стороной данных аутентификации, чтобы гарантировать, что пользователь имеет разрешение сетевого администратора на выполнение вызова. Соседние маршрутизаторы обмениваются сообщениями аутентификации.

Многоуровневая архитектура протокола PPP

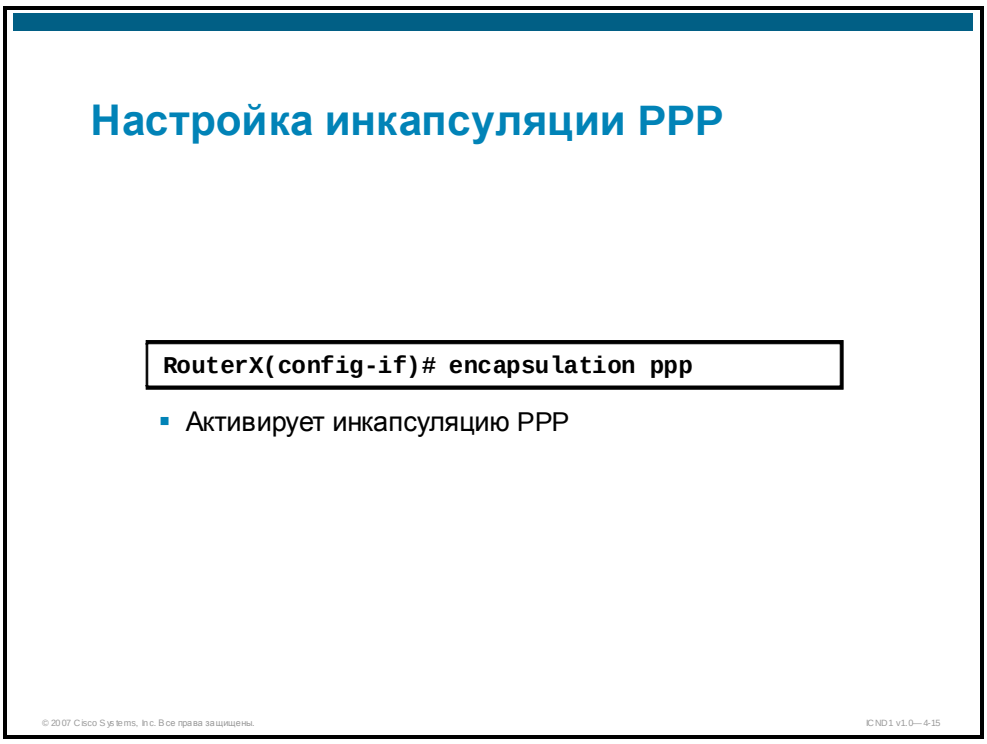
Протокол PPP предназначен для установления соединения по каналам «точка-точка». Протокол PPP, спецификации которого приводятся в стандартах RFC 1661 и 1332, инкапсулирует данные протокола сетевого уровня в каналах «точка-точка». RFC 1661 модифицирован в стандарте RFC 2153, *расширения PPP для производителей*.

Протокол PPP можно настроить на следующих типах физических интерфейсов.

- асинхронный последовательный;
- синхронный последовательный;
- высокоскоростной последовательный интерфейс (HSSI).

Компонент NCP протокола PPP используется для инкапсуляции и согласования параметров нескольких протоколов сетевого уровня.

LCP, другой основной компонент протокола PPP, служит для согласования и задания параметров управления канала PBC.



Чтобы активировать инкапсуляцию PPP, войдите в режим конфигурации интерфейса. Воспользуйтесь командой конфигурации интерфейса **encapsulation ppp**, чтобы задать инкапсуляцию PPP на этом интерфейсе.

Примечание	Для активации протокола PPP на асинхронном последовательном интерфейсе необходимо выполнить дополнительные действия по настройке. Эти действия не рассматриваются в данном курсе. Информацию о настройке протокола PPP на асинхронном последовательном интерфейсе см. в курсе *Implementing Secure Converged Wide Area Networks* (ISCW).

Пример: конфигурация PPP

На рисунке приводится пример конфигурации PPP.

Пример конфигурации PPP


```
hostname left
!
int serial 0
 ip address 10.0.1.1 255.255.255.0
 encapsulation ppp
```

```
hostname right
!
int serial 0
 ip address 10.0.1.2 255.255.255.0
 encapsulation ppp
```


Проверка конфигурации последовательного интерфейса

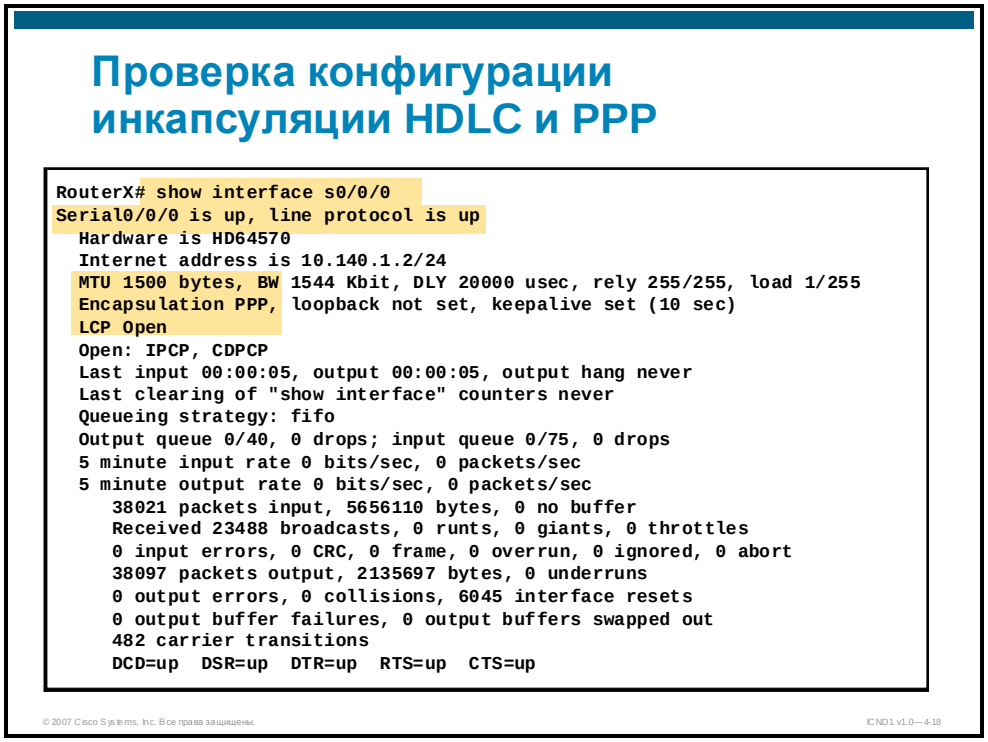
```
RouterX# show interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 10.140.1.2/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive set (10 sec)
  LCP Open
  Open: IPCP, CDPCP
  Last input 00:00:05, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     38021 packets input, 5656110 bytes, 0 no buffer
     Received 23488 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     38097 packets output, 2135697 bytes, 0 underruns
     0 output errors, 0 collisions, 6045 interface resets
     0 output buffer failures, 0 output buffers swapped out
     482 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```


После настройки последовательного интерфейса проверьте внесенные изменения с помощью команды **show interface serial**.

Примечание	Обратите внимание, что в данном примере канал теперь включен и полоса пропускания составляет 1 544 Кбит/с.

Проверка конфигурации последовательной инкапсуляции

В этом разделе описывается проверка конфигурации протоколов HDLC и PPP.

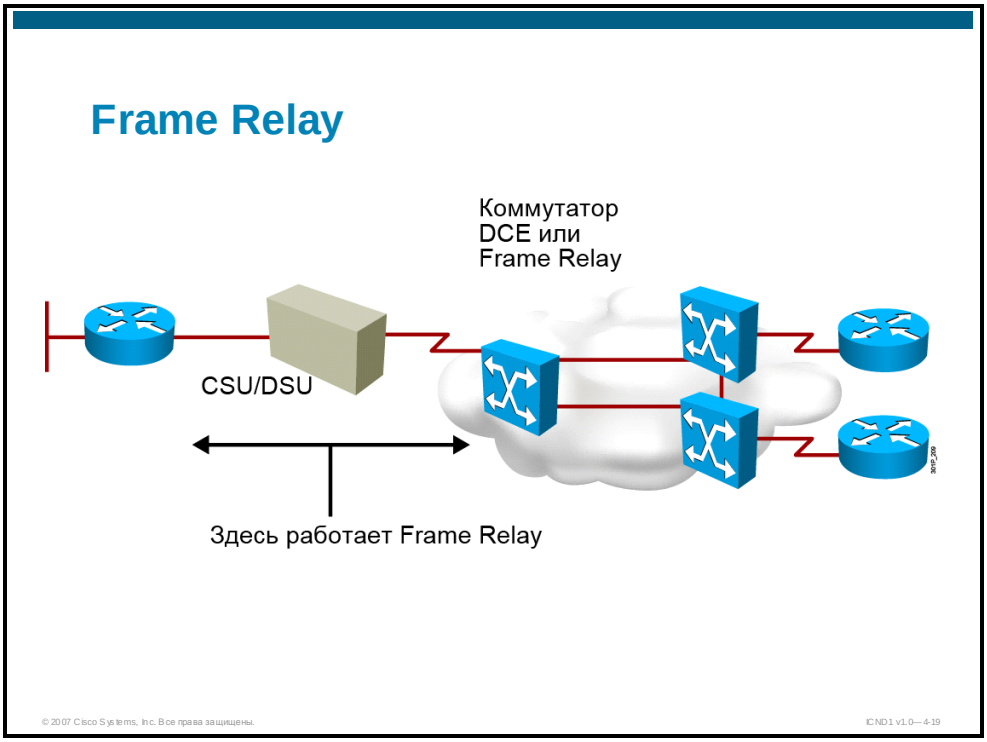


Пример: проверка конфигурации инкапсуляции HDLC и PPP

Команда **show interface** позволяет проверить правильность конфигурации. На рисунке приводится конфигурация протокола PPP. Если настроен протокол HDLC, в выводе команды **show interface** будет отображаться «Encapsulation HDLC» (Инкапсуляция HDLC). Если настроен протокол PPP, с помощью этой команды можно проверить также состояния протоколов LCP и NCP.

Frame Relay

Популярность протокола коммутацию пакетов Frame Relay сильно возросла за счет более высокой рентабельности по сравнению с вытесненными им старыми технологиями, такими как X.25 и арендованные линии. В этом разделе описывается работа протокола Frame Relay.

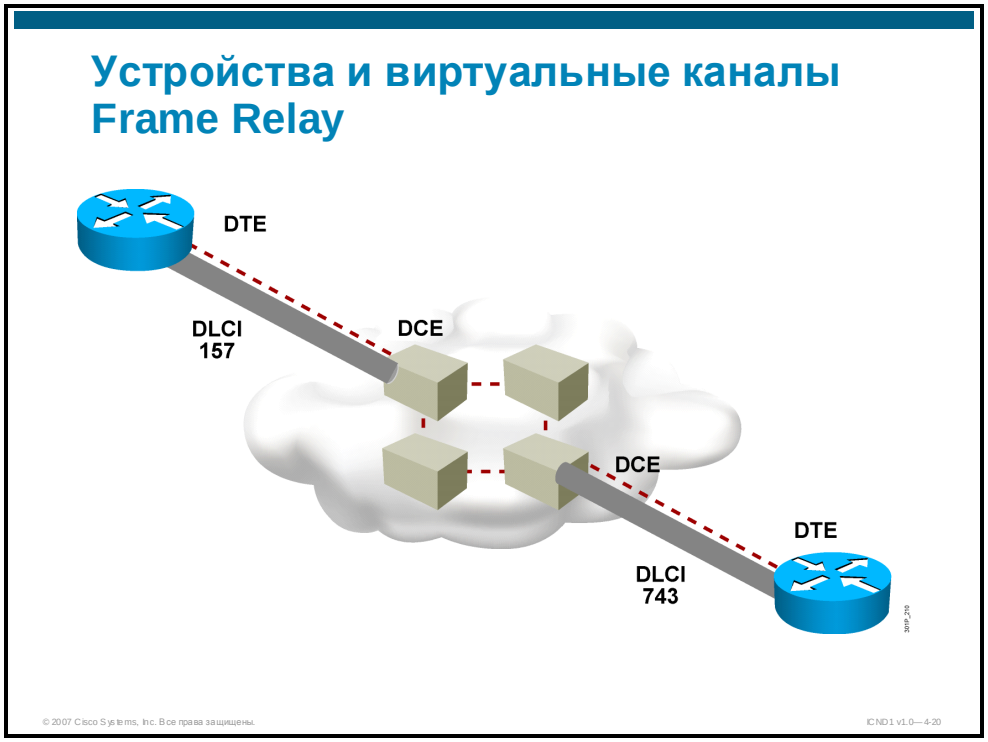


Протокол Frame Relay был представлен поставщиками сетевых услуг в ответ на возрастающую потребность в увеличении полосы пропускания и уменьшении задержки при коммутации пакетов. Протокол Frame Relay поддерживает постоянные (PVC) и коммутируемые (SVC) виртуальные каналы с использованием общей полосы пропускания для передачи голоса и данных. Доступные скорости передачи данных, как правило, не превышают 4 Мбит/с, хотя некоторые поставщики услуг предлагают и более высокие скорости. Кроме того, Frame Relay является более простым протоколом, работающим не на сетевом, а на канальном уровне.

В протоколе Frame Relay отсутствует исправление ошибок или управление потоком. Упрощенная обработка кадров ведет к уменьшению задержки, а меры, предпринимаемые для предотвращения накопления кадров на промежуточных коммутаторах, позволяют сократить джиттер.

Большинство соединений Frame Relay составляют каналы PVC, а не SVC. Для подключения к границе сети часто используется выделенная линия, однако некоторые поставщики услуг предоставляют коммутируемые подключения с использованием каналов ISDN или xDSL.

Протокол Frame Relay является оптимальным вариантом при соединении корпоративных локальных сетей, поскольку маршрутизатору в локальной сети даже при использовании нескольких виртуальных каналов требуется только один интерфейс распределенной сети. Выделенный канал до границы сети Frame Relay обеспечивает экономичные соединения между разрозненными локальными сетями.

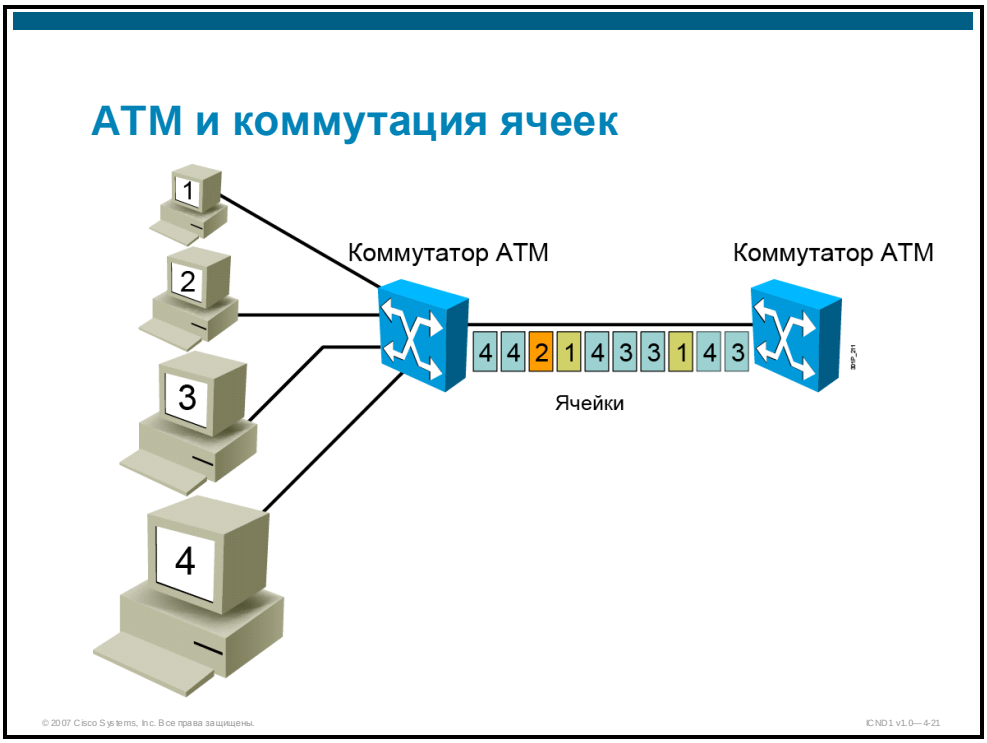


Виртуальные каналы Frame Relay

Frame Relay обеспечивает работу по виртуальным каналам, которые являются логическими соединениями, созданными для связи между двумя удаленными устройствами в сети. Виртуальные каналы обеспечивают двунаправленный путь связи от одного устройства DTE к другому. Виртуальный канал однозначно определяется идентификатором подключения к каналу передачи данных (DLCI) в заголовке адреса Frame Relay. Идентификатор DLCI применяется только на том маршрутизаторе, на котором он настроен. Виртуальный канал может проходить через любое количество промежуточных устройств DCE в сети. Несколько виртуальных каналов можно мультиплексировать в один физический канал для доступа к сети и передачи данных.

ATM и коммутация ячеек

ATM представляет собой технологию соединения на основе коммутации ячеек, способную обеспечить передачу голосовых и видеосигналов и данных через частные и общедоступные сети. ATM используется в основном в магистралях корпоративных локальных сетей или каналах распределенной сети. В этом разделе описывается принцип действия ATM.



Поставщики сетевых услуг давно нуждались в технологии общих сетей постоянного доступа с низкой задержкой и джиттером и высокой полосой пропускания. Решением стало использование технологии, которая применяется в центральных сетях – ATM. Технология ATM обеспечивает скорости передачи данных свыше 155 Мбит/с. Схемы топологии распределенных сетей ATM очень похожи на другие технологии общего доступа, такие как X.25 и Frame Relay.

В основе технологии ATM лежит архитектура ячеек, а не кадров. Ячейки ATM всегда имеют фиксированную длину 53 байта. 53-байтовая ячейка ATM состоит из 5-байтового заголовка ATM и 48-байтовой полезной части. Небольшие ячейки фиксированной длины удобны для переноса голосового и видеотрафика, чувствительных к задержке. Видео и голосовой трафик не должны ожидать передачи более крупных пакетов данных.

53-байтовая ячейка ATM менее эффективна, чем кадры и пакеты большего размера в Frame Relay и X.25. К тому же, в ячейке ATM на каждые 48 байтов полезной части приходится 5 байтов служебной информации. При передаче ячейкой сегментированных пакетов сетевого уровня эта неэффективная информация может занимать больший объем, поскольку 48-байтовое полезное пространство ячейки ATM может *не* соответствовать пакетам другого размера (например, 64-байтовым IP-пакетам). Полоса пропускания типичного канала ATM должна быть по крайней мере на 20% больше Frame Relay для переноса такого же объема данных сетевого уровня.

Как и протокол Frame Relay, технология ATM использует виртуальные каналы, которые могут быть постоянными или коммутируемыми. В технологии ATM перед передачей данные разделяются на небольшие ячейки размером 53 байта. Заголовок ячейки ATM содержит поле идентификатора виртуального пути/ идентификатора виртуального канала (VPI/VCI), который служит для определения виртуального канала, которому принадлежит ячейка ATM. На физическом уровне ATM может работать в различных физических средах, включая оптоволокно с использованием разделения на кадры SONET/SDH и коаксиальный кабель с использованием DS3.

Сеть ATM содержит коммутаторы ATM, отвечающие за пересылку ячеек. Коммутатор ATM получает входящую ячейку от конечного устройства ATM или другого коммутатора ATM. Затем коммутатор ATM использует входящий идентификатор VPI/VCI для сопоставления исходящего интерфейса и новый VPI/VCI, который будет использоваться в следующем соединении по пути к месту назначения. Процесс коммутации ячеек ATM осуществляется очень быстро и может быть запрограммирован в аппаратном обеспечении.

Виртуальный канал ATM является логическим соединением, созданным между двумя конечными устройствами ATM в сети ATM. Существует две категории виртуальных каналов ATM: постоянные и коммутируемые. Виртуальные каналы обеспечивают двунаправленный путь связи от одного конечного устройства ATM к другому. Идентификатор VPI/VCI в заголовке ячейки ATM однозначно определяет виртуальный канал.

Виртуальный канал может проходить через любое количество промежуточных коммутаторов ATM в сети ATM. Многочисленные виртуальные каналы могут быть мультиплексированы в один физический канал для передачи данных через сеть.

Резюме

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

Резюме

- Канал «точка-точка» или последовательный канал соединяет два географически удаленных объекта. Эти каналы, как правило, арендуются у оператора и поэтому часто называются арендуемыми линиями.
- Полосой пропускания называется скорость передачи данных по каналу связи. В Северной Америке полоса пропускания обычно выражается номером уровня цифрового сигнала (DS0, DS1 и т. д.), который с технической точки зрения отражает скорость передачи и формат сигнала.
- Протокол HDLC является одним из основных протоколов канального уровня и широко используется соединениях PBC «точка-точка». HDLC поддерживает конфигурации «точка-точка» и многоточечные конфигурации.
- Воспользуйтесь командой конфигурации интерфейса **encapsulation hdlc**, чтобы выбрать инкапсуляцию Cisco HDLC на этом интерфейсе.
- Функции нижнего уровня протокола PPP используют синхронные и асинхронные физические носители. Функции верхнего уровня PPP выполняют передачу пакетов различных сетевых протоколов с помощью NCP.

Резюме (прод.)

- Команда конфигурации интерфейса **encapsulation ppp** позволяет задать инкапсуляцию PPP на интерфейсе.
- Команда **show interface** служит для проверки правильности настройки инкапсуляции PPP.
- Скорости передачи данных Frame Relay, как правило, не превышают 4 Мбит/с, хотя некоторые поставщики услуг предлагают и более высокие скорости. Frame Relay является более простым протоколом, работающим не на сетевом, а на канальном уровне.
- ATM представляет собой технологию соединения на основе коммутации ячеек, способную обеспечить передачу голосовых и видеосигналов и данных через частные и общедоступные сети. ATM используется в основном в сетях поставщиков услуг и в магистралях корпоративных локальных сетей.
- Виртуальные каналы ATM могут быть постоянными (PVC) или коммутируемыми (SVC).

Занятие 5

Активация протокола RIP

Обзор

Фактически данные маршрутизации обрабатываются в виде записей в таблице маршрутизации, при этом каждая запись соответствует идентифицированному маршруту. Можно статически (вручную) настраивать записи в таблице маршрутизации, или маршрутизатор может динамически создавать и вести таблицу маршрутизации с помощью протокола маршрутизации, чтобы оперативно реагировать на изменения в сети.

Протокол RIP (Routing Information Protocol) является одним из наиболее распространенных протоколов маршрутизации на базе векторов расстояния. Давно существующий и по-прежнему широко используемый протокол внутреннего шлюза RIP был разработан для небольших однородных сетей. RIP является классическим протоколом вектора расстояния. На этом занятии описываются основные функции и принцип работы RIP и объясняется процесс активации протокола RIP в IP-сетях.

Задачи

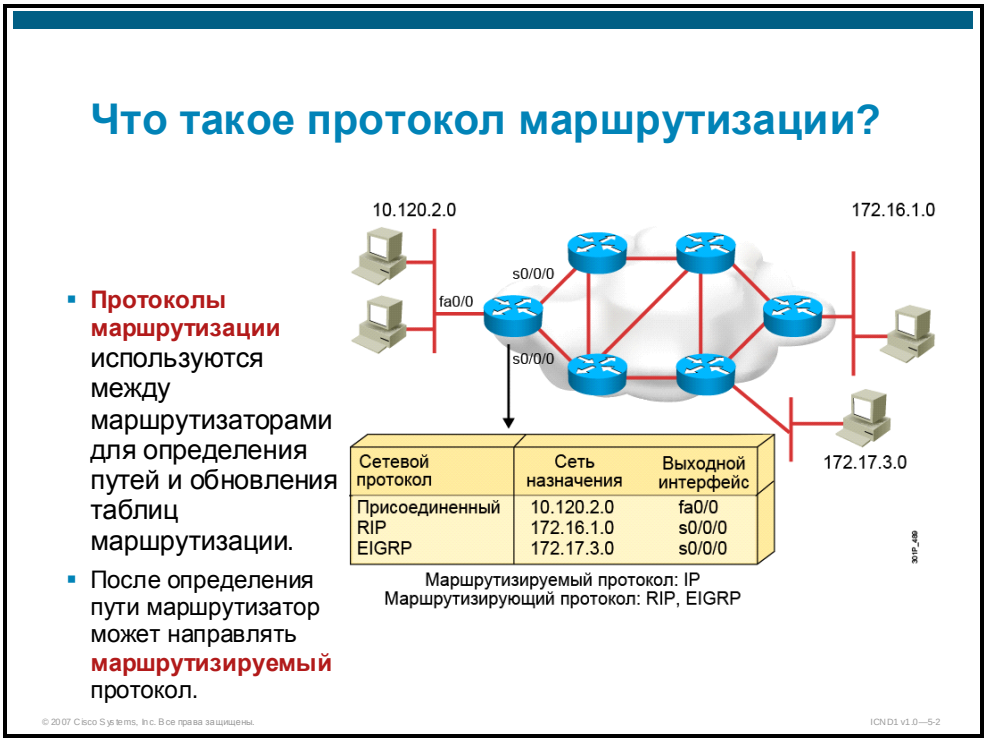
По окончании этого занятия вы сможете описывать принцип работы, преимущества и ограничения статической и динамической маршрутизации. Это значит, что вы сможете выполнять следующие задачи:

- описывать назначение, типы и классы протоколов динамической маршрутизации;
- описывать различные классы протоколов маршрутизации;
- объяснять механизмы выбора маршрутов и обновления информации протоколом маршрутизации на базе векторов расстояния;
- перечислять функции RIP;
- объяснять различия между RIPv1 и RIPv2;
- описывать задачи, необходимые для включения протокола динамической маршрутизации на маршрутизаторе Cisco;
- описывать задачи конфигурации, необходимые для включения базового протокола RIP на маршрутизаторе Cisco;

- использовать команду **show interface** для проверки правильности конфигурации RIP;
- объяснять использование команды **debug ip rip**.

Обзор протоколов динамической маршрутизации

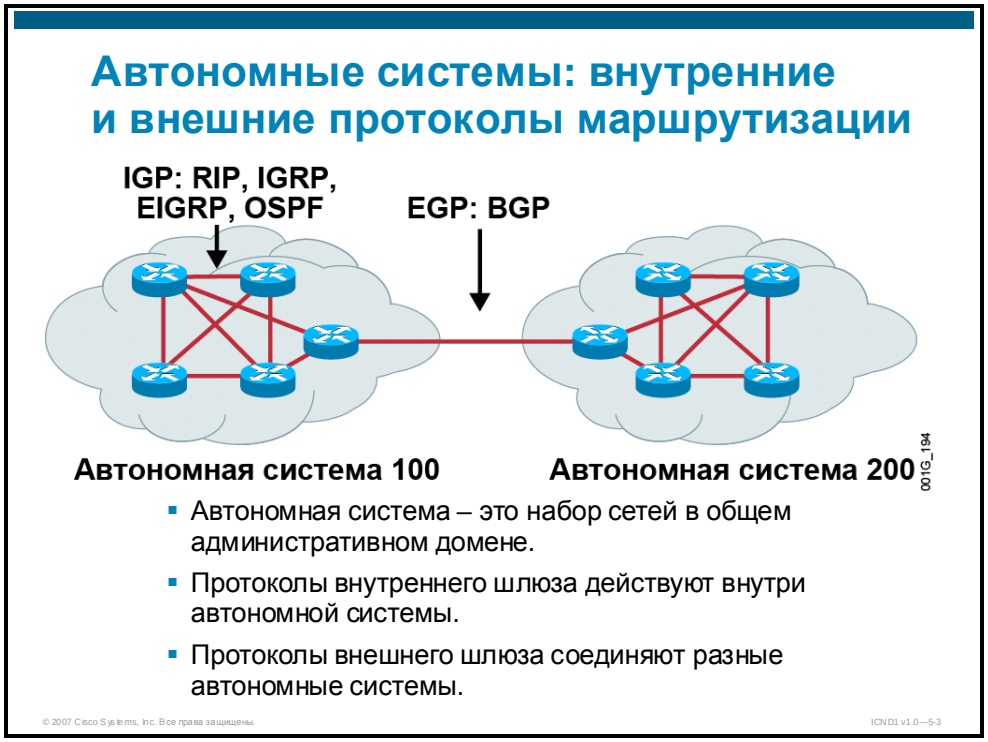
В этом разделе описывается назначение, типы и классы протоколов динамической маршрутизации.



Протокол маршрутизации определяет правила, используемые маршрутизатором при взаимодействии с соседними маршрутизаторами. В динамической маршрутизации обмен данными о топологии сети происходит с помощью протокола маршрутизации. В то же время статическая маршрутизация определяет формат и назначение полей в пакете. Пакеты, как правило, передаются от одной конечной системы к другой.

Протоколы маршрутизации также отражают следующую информацию:

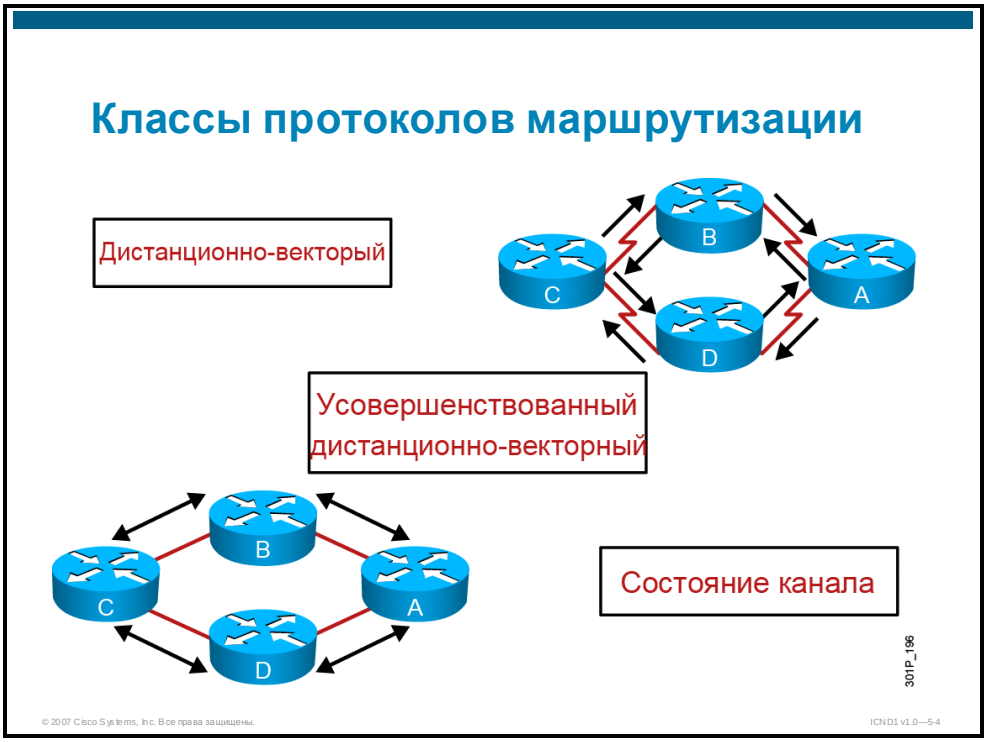
- способ передачи обновлений;
- передаваемые данные;
- время передачи данных;
- методы определения получателей обновлений.



Существует два основных типа протоколов маршрутизации.

- **Протоколы внутреннего шлюза (IGP):** Эти протоколы маршрутизации используются для обмена данными маршрутизации внутри автономной системы. примеры IGP: Routing Information Protocol version 1 (RIPv1), RIPv2, Enhanced Interior Gateway Routing Protocol (EIGRP) и Open Shortest Path First (OSPF).
- **Протоколы внешнего шлюза (EGP):** Эти протоколы используются для соединения автономных систем. Автономная система – это совокупность сетей с общим управлением, использующих общую стратегию маршрутизации. Примером протокола внешнего шлюза может служить протокол Border Gateway Protocol (BGP).

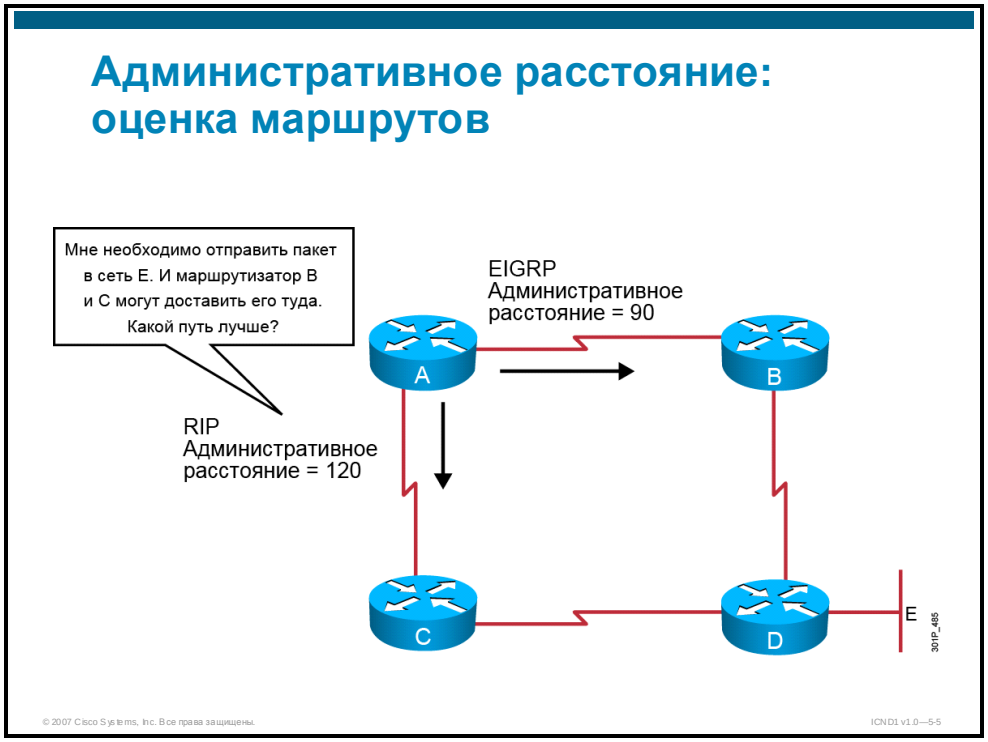
Примечание	Организация IANA (полномочный орган по цифровым адресами Интернета) назначает номера автономных систем во многих юрисдикциях. Нумерация IANA является обязательной, если ваша организация планирует использовать протокол внешнего шлюза, например BGP. Однако мы рекомендуем студентам ознакомиться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



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

- **Дистанционно-векторный:** Метод маршрутизации на основе векторов расстояния определяет направление (вектор) и расстояние (например, количество переходов) к любому каналу интерсети.
- **Состояние канала:** Маршрутизация на основе состояния канала, также известная как алгоритм определения кратчайших путей (SPF), подразумевает создание абстракции точной топологии полной интерсети или ее отдела, в котором работает маршрутизатор.
- **Сбалансированный гибридный алгоритм:** Сбалансированный гибридный подход сочетает в себе отдельные аспекты алгоритмов на основе состояния канала и вектора расстояния.

Не существует идеального алгоритма маршрутизации, подходящего для всех интерсетей. Каждый протокол маршрутизации предоставляет информацию по-своему.



Функции динамических протоколов маршрутизации

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

Пример: административное расстояние

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

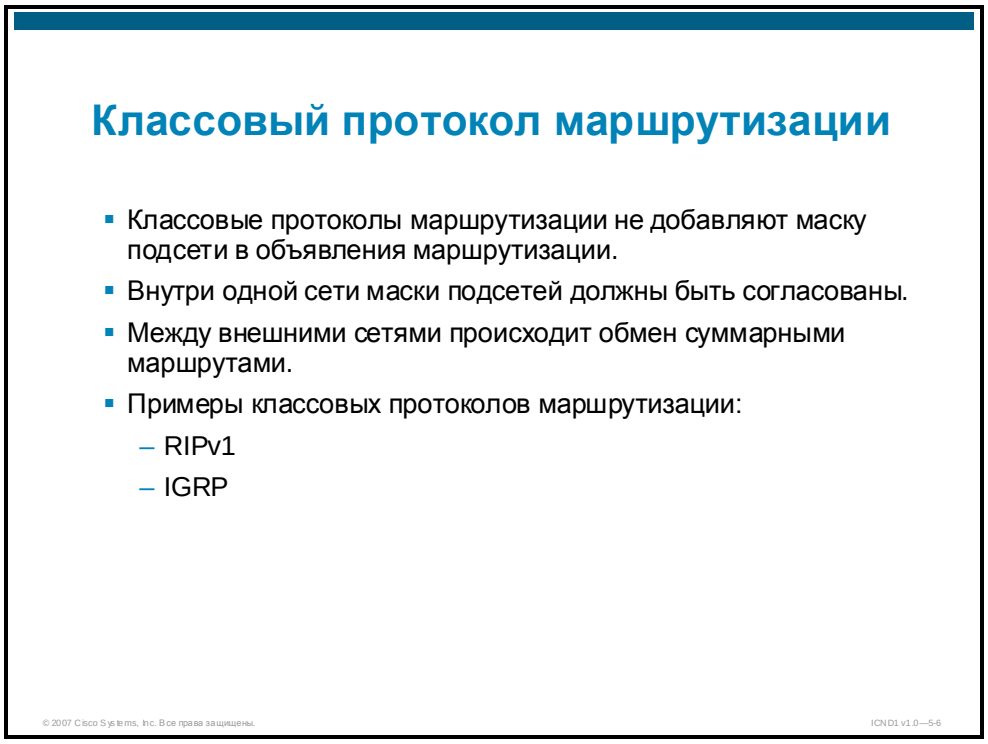
В таблице приводятся административные расстояния по умолчанию для некоторых источников данных маршрутизации.

Источник маршрутов	Расстояние по умолчанию
Подключенный интерфейс	0
Адрес статического маршрута	1
EIGRP	90
OSPF	110
RIPv1, RIPv2	120
Внешний EIGRP	170
Неизвестный или непредусмотренный	255 (не будет использоваться для передачи трафика)

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

Бесклассовая и классовая маршрутизация

В этом разделе описывается бесклассовая и классовая маршрутизация.

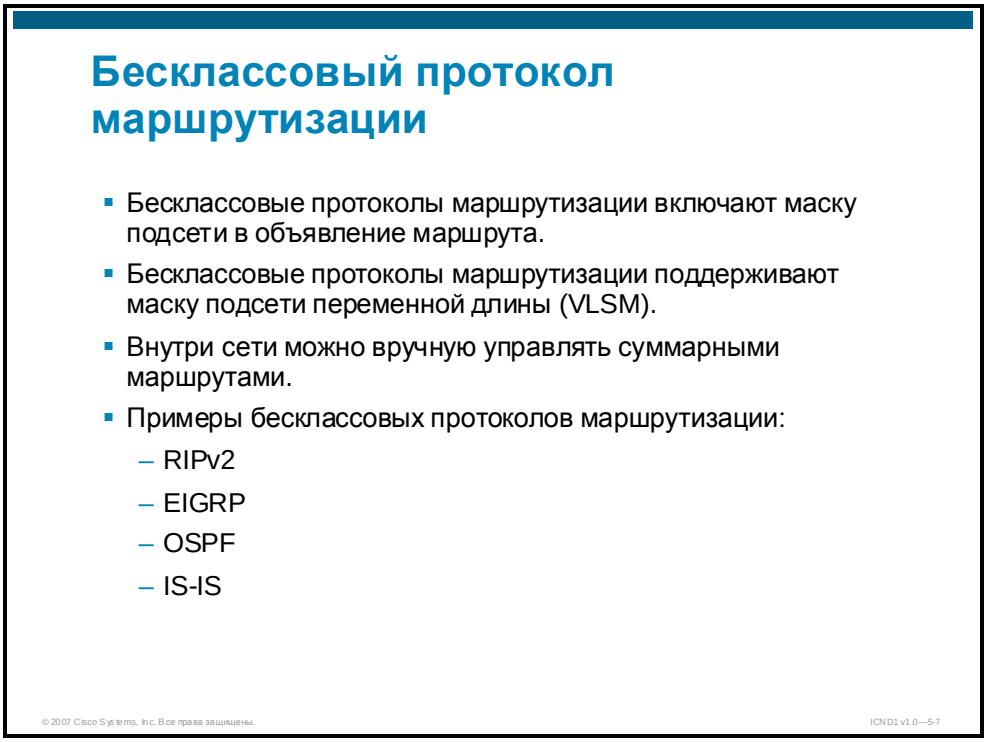


Классовая маршрутизация является следствием того, что в объявлениях маршрутизации, создаваемых большинством дистанциооно-векторных протоколов маршрутизации, *не* указывается маска подсети.

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

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

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



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

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

В бесклассовой среде процесс суммирования контролируются вручную и как правило может выполняться для любого бита в адресе. Поскольку маршруты подсети распространяются по всему домену маршрутизации, для сохранения приемлемого размера таблиц маршрутизации может потребоваться суммирование вручную. Примерами бесклассовых протоколов маршрутизации являются RIPv2, EIGRP, OSPF и IS-IS.

Выбор маршрута дистанционно-векторного протокола

В этом разделе рассматривается процесс выбора маршрутов дистанционно-векторного протокола.

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

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

Пример: дистанционно-векторные протоколы маршрутизации

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

Традиционно дистанционно-векторные протоколы являлись также классовыми протоколами. Протоколы RIPv2 и EIGRP – примеры более совершенных дистанционно-векторных протоколов, работающих в бесклассовом режиме. EIGRP также имеет ряд характеристик протоколов, использующих алгоритм состояния канала.

На рисунке интерфейсы к сетям с прямым подключением изображены с расстоянием 0.

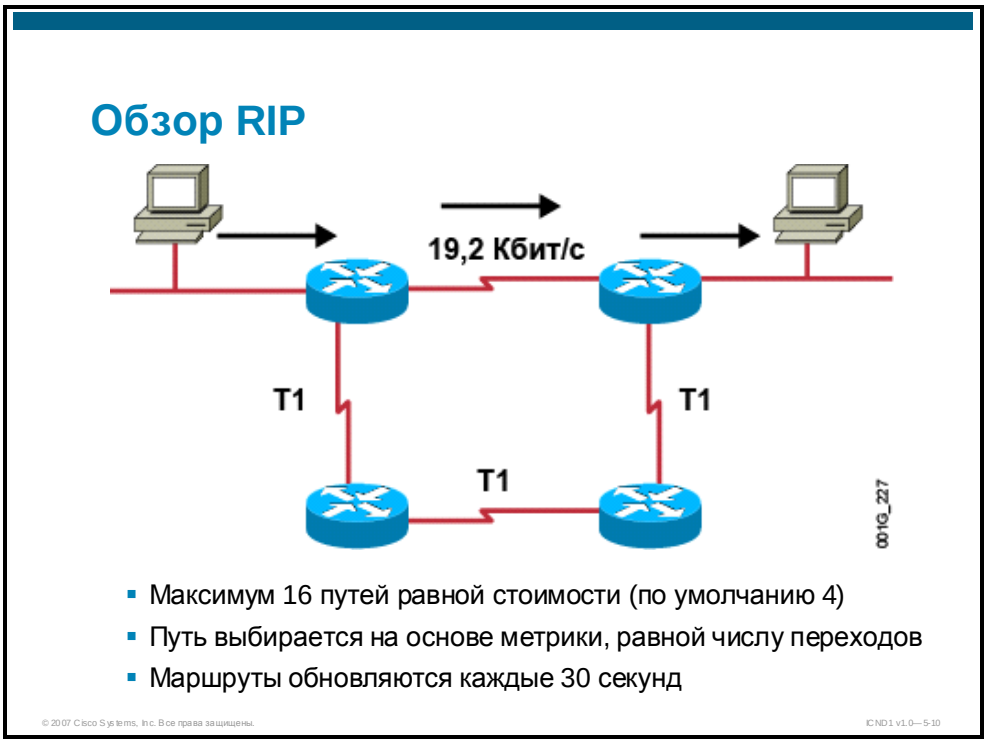
На последующих этапах процесса обнаружения сети по дистанционно-векторному алгоритму, маршрутизаторы обнаруживают сети назначения, не имеющие прямого подключения к ним, с помощью накопленных метрик, полученных от каждого соседнего узла. Соседние маршрутизаторы предоставляют сведения о маршрутах, не имеющих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

Пример: источники информации и обнаружение маршрутов

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

Функции протокола RIP

В этом разделе описываются функции протокола RIP.



Протокол RIP имеет следующие ключевые характеристики:

- RIP – это дистанционно-векторный протокол маршрутизации.
- В качестве метрики для выбора маршрута служит число переходов.
- Максимально допустимое число переходов составляет 15.
- Широковещательная рассылка обновлений маршрутизации по умолчанию выполняется каждые 30 секунд.
- Протокол RIP обеспечивает балансировку нагрузки по шестнадцати маршрутам с равной стоимостью. (По умолчанию используется четыре маршрута.)

Сравнение протоколов RIPv1 и RIPv2

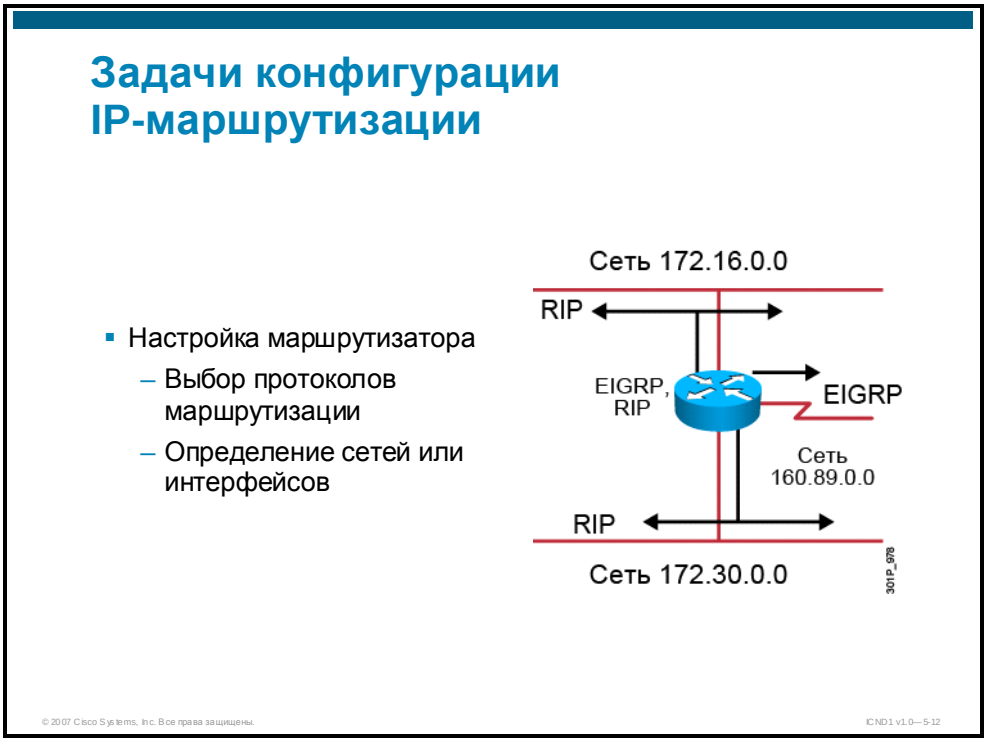
В этом разделе рассматриваются различия между RIPv1 и RIPv2.

Определение максимального количества параллельных путей, разрешенных в таблице маршрутизации, обеспечивает балансировку нагрузки протоколом RIP. При использовании RIP пути должны иметь равную стоимость. Если максимальное количество путей равно единице, балансировка нагрузки отключена.

Примечание	Маршрутизаторы Cisco поддерживают протоколы RIPv1 и RIPv2. В этом курсе рассматривается только настройка протокола RIPv2.

Задачи конфигурации динамической маршрутизации

В этом разделе описываются задачи, необходимые для активации протокола динамической маршрутизации на маршрутизаторе Cisco.



Чтобы включить протокол динамической маршрутизации, необходимо выполнить следующие действия:

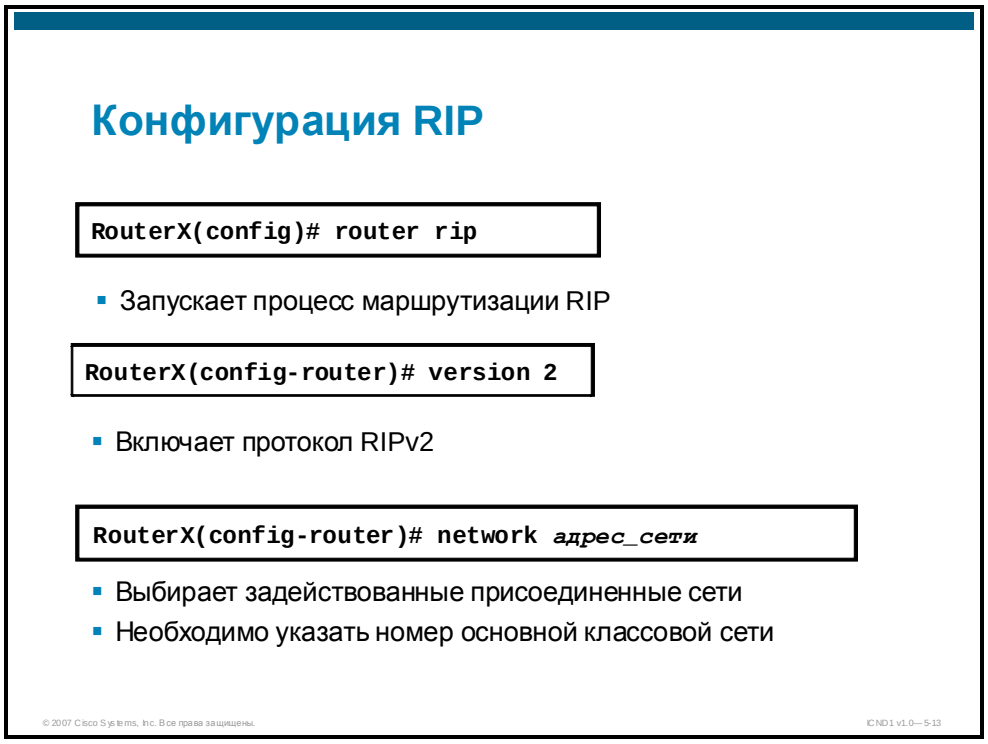
Шаг 1 Выберите протокол маршрутизации: RIP, EIGRP или OSPF.

Шаг 2 Определите адреса IP-сетей без указания значений подсетей (кроме OSPF).

Примечание	Необходимо также назначить интерфейсам адреса сети или подсети и соответствующую маску подсети.

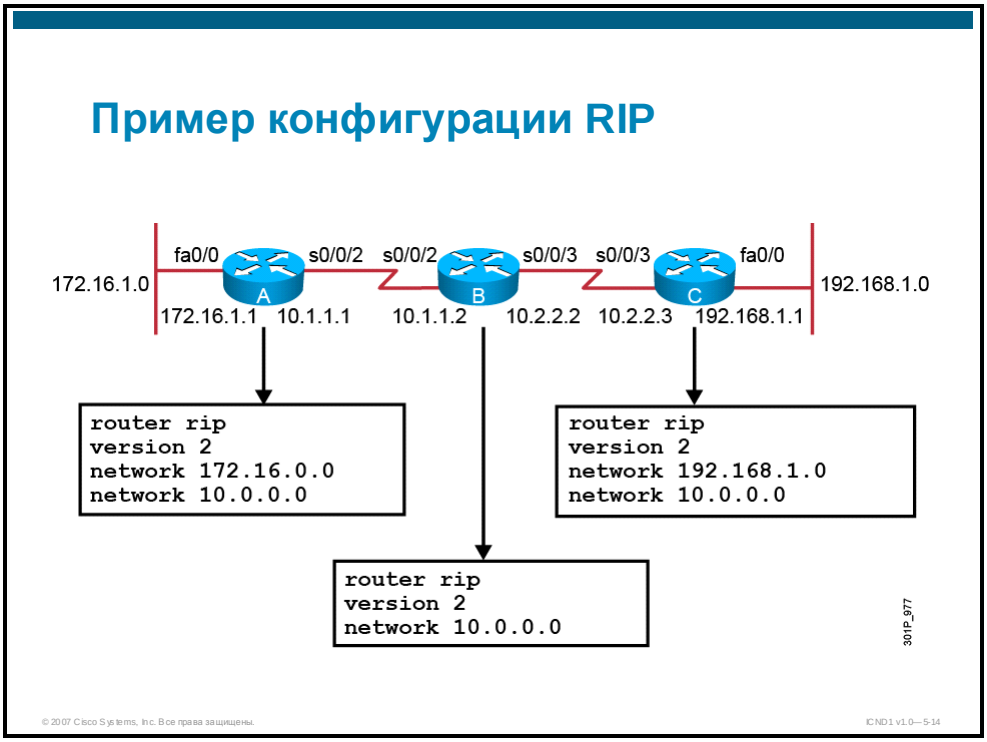
Конфигурация RIP

В этом разделе описывается настройка базовой маршрутизации RIP.



Команда **router rip** выбирает RIP в качестве протокола маршрутизации.

Команда **network** служит для назначения адреса основной сети, к которой маршрутизатор подключен напрямую. Процесс маршрутизации RIP связывает адреса интерфейсов с объявленным адресом сети и начинает обработку пакетов RIP на указанных интерфейсах.



Пример: конфигурация RIP

В данном примере маршрутизатор A имеет следующую конфигурацию.

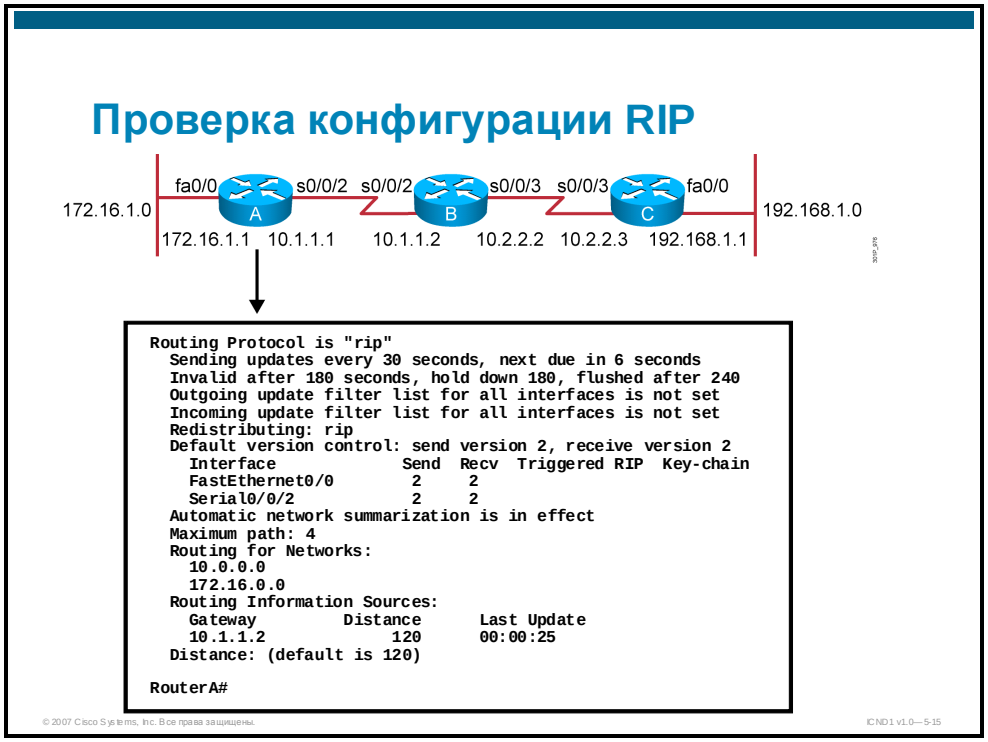
- **Router rip:** Выбирает протокол RIP в качестве протокола маршрутизации.
- **Version 2:** Включает протокол RIPv2.
- **Network 172.16.0.0:** Определяет сеть с прямым подключением.
- **Network 10.0.0.0:** Определяет сеть с прямым подключением.

Интерфейсы маршрутизатора A, подключенного к сетям 172.16.0.0 и 10.0.0.0 или их подсетям, будут отправлять и получать обновления RIP. Эти обновления маршрутизации позволяют маршрутизаторам получать данные о топологии сети.

Маршрутизаторы B и C имеют аналогичные конфигурации RIP, но с другим адресами сетей.

Проверка конфигурации RIP

В этом разделе описывается использование команд **show** для проверки конфигурации RIP.



Команда **show ip protocols** отображает параметры протоколов маршрутизации и данные таймеров протокола маршрутизации, связанного с маршрутизатором.

В таблице описаны важные поля вывода команды.

Поле	Описание
Routing Protocol is «rip»	Указывает используемый протокол маршрутизации.
Sending updates every 30 seconds	Указывает время между отправкой обновлений.
next due in 6 seconds	Определяет время отправки следующего обновления.
Invalid after 180 seconds	Определяет значение таймера «invalid».
hold down 180	Определяет текущее значение таймера удержания.
flushed after 240	Определяет время (в секундах) после которого отдельная запись маршрутизации будет удалена (сброшена).
Outgoing update	Указывает, настроен ли исходящий список фильтрации.
Incoming update	Указывает, настроен ли входящий список фильтрации.
Redistributing	Указывает перераспределяемый протокол.
Default version control	Указывает версию отправляемых и получаемых пакетов RIP.
Routing	Указывает сети, в которые процесс маршрутизации вводит маршруты в данный момент.
Routing Information Sources	Выводит все источники маршрутизации, используемые программным обеспечением Cisco IOS для построения таблицы маршрутизации. Для каждого источника отображается следующая информация: ■ IP-адрес; ■ административное расстояние; ■ время получения последнего обновления от этого источника.

Пример: проверка конфигурации RIP

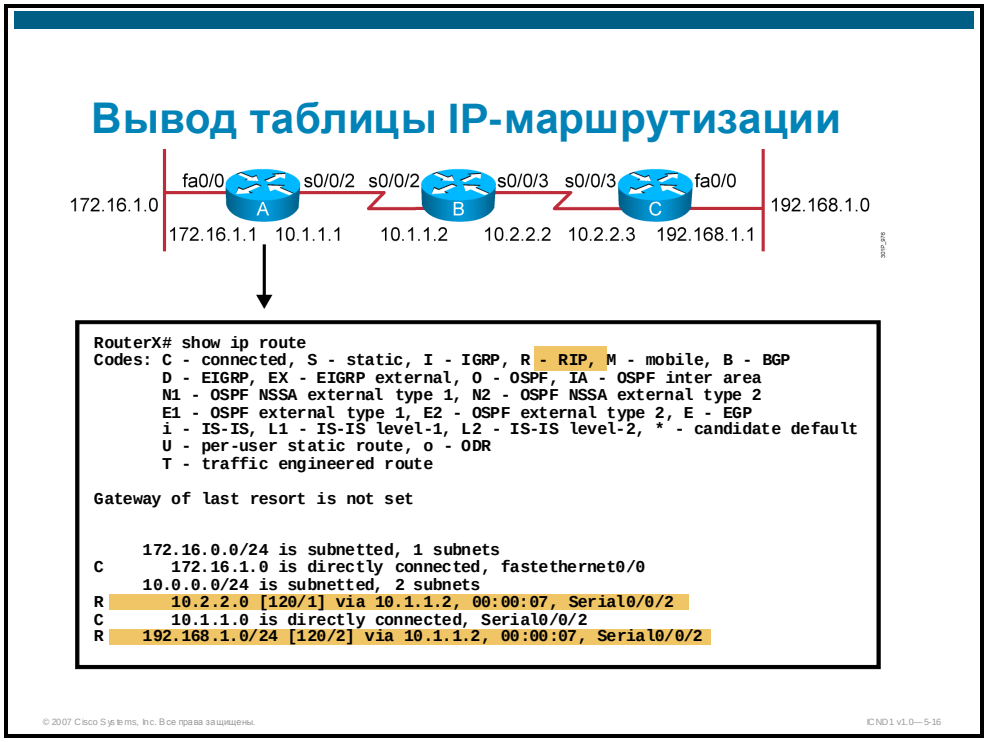
В этом примере на маршрутизаторе A настроен протокол RIP, и маршрутизатор отправляет обновленные данные таблицы маршрутизации каждые 30 секунд. (Этот интервал можно изменить.) Если маршрутизатор с протоколом RIP не получает обновления от другого маршрутизатора в течение 180 секунд или более, он помечает обслуживаемые им маршруты как недействительные. На рисунке таймер удержания установлен на 180 секунд. В результате отключенный, а затем восстановленный, маршрут будет оставаться на удержании (состоянии «possibly down») до истечения интервала 180 секунд.

Если обновление не поступает спустя 240 секунд (таймер сброса), маршрутизатор удаляет записи из таблицы маршрутизации. На рисунке прошло 24 секунды после получения маршрутизатором A обновления от маршрутизатора B.

Маршрутизатор вводит маршруты для сетей, перечисленных в строке «Routing for Networks». Маршрутизатор получает маршруты от соседних маршрутизаторов RIP, перечисленных в строке «Routing Information Sources».

Расстояние по умолчанию, равное 120, относится к административному расстоянию для маршрута RIP.

Кроме того, можно использовать команду **show ip interface brief** для получения сводной информации по IP-адресам и состоянию всех интерфейсов.



Команда **show ip route** отображает содержимое таблицы IP-маршрутизации.

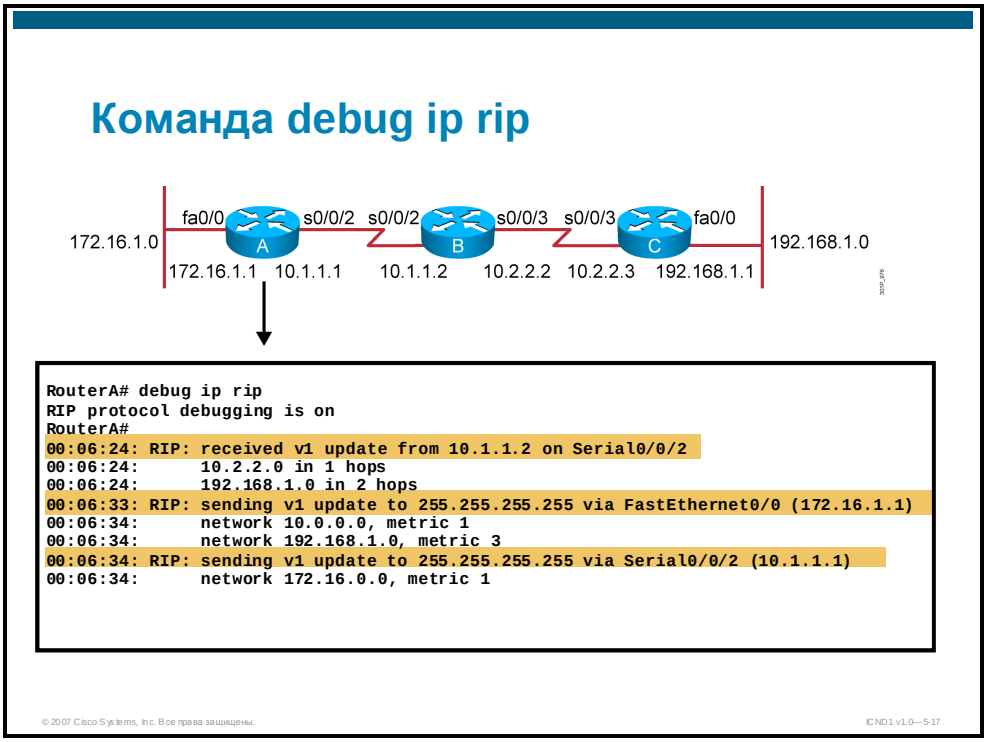
В таблице маршрутизации представлены записи обо всех известных сетях и подсетях, а также код, указывающий на способ получения этой информации. В таблице приводится вывод и функции основных полей команды **show ip route**.

Вывод	Описание
R or C	Указывает источник маршрута. Например, «C» означает, что маршрут получен от прямого подключения к интерфейсу маршрутизатора. «R» означает, что маршрут определен протоколом RIP.
192.168.1.0 10.2.2.0	Указывает адрес удаленной сети.
120/1	Первый номер в скобках соответствует административному расстоянию источника данных, второе число – метрику маршрута (здесь 1 переход).
via 10.1.1.2	Указывает адрес маршрутизатора следующего перехода к удаленной сети.
00:00:07	Указывает время, прошедшее с момента последнего обновления (в данном случае 7 секунд).
Serial0/0/2	Определяет интерфейс, через который можно получить доступ к указанной сети.

Если данные маршрутизации не обновляются (то есть вывод команды **show ip route** не содержит записей, полученных от протокола маршрутизации), воспользуйтесь командами **show running-config** или **show ip protocols** в привилегированном режиме EXEC, чтобы определить возможные ошибки в конфигурации протокола маршрутизации.

Поиск и устранение неполадок конфигурации RIP

В этом разделе описывается использование команды **debug ip rip**.



Команда **debug ip rip** отображает обновления маршрутизации RIP в порядке их отправки или получения. Команда **no debug all** отключает отладку.

В следующем выводе показан адрес источника, с которого были получены обновления:

```
RIP: received v1 update from 10.1.1.2 on Serial0/0/2
```

В следующем выводе показан адрес назначения по которому были отправлены обновления:

```
RIP: sending v1 update to 255.255.255.255 via FastEthernet0/0
(172.16.1.1)
RIP: sending v1 update to 255.255.255.255 via Serial0/0/2
(10.1.1.1)
```

Пример: команда debug ip rip

В данном примере показано, что маршрутизатор, на котором осуществляется отладка, получил обновления от одного маршрутизатора с адресом источника 10.1.1.2. Этот маршрутизатор отправил данные о двух местах назначения в обновлении таблицы маршрутизации. Маршрутизатор, на котором осуществляется отладка, в обоих случаях отправляет обновления по широковещательному адресу назначения 255.255.255.255. Адрес в скобках – это адрес источника, инкапсулированный в заголовок протокола IP.

Кроме того, вывод команды **debug ip rip** может содержать следующие записи:

```
RIP: broadcasting general request on FastEthernet0/0
RIP: broadcasting general request on FastEthernet1/0
```

Такие записи могут появляться при запуске или во время таких событий, как перемещение интерфейса или очистка пользователем таблицы маршрутизации вручную. Следующая запись, скорее всего, вызвана получением поврежденного пакета с передающего устройства:

```
RIP: bad version 128 from 160.89.80.43
```


Резюме

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

Резюме

- Маршрутизация является процессом доставки информации от одного объекта к другому.
- Протоколы динамической маршрутизации определяют способ передачи обновлений, передаваемую информацию и способ определения получателей обновлений.
- Протокол маршрутизации с меньшим административным расстоянием считается более надежным, чем протокол с более высоким расстоянием.
- Существует три класса протоколов маршрутизации: дистанционно-векторные, состояния канала и сбалансированные гибридные.
- Команда **ip classless** позволяет предотвратить отбрасывание на маршрутизаторе пакета, адресованного к неизвестной сети, если настроен маршрут по умолчанию.

Резюме (прод.)

- RIP – это дистанционно-векторный протокол, который использует число переходов в качестве метрики для выбора маршрута и выполняет широковещательную рассылку обновлений каждые 30 секунд.
- Протокол RIPv1 использует классовый алгоритм маршрутизации; RIPv2 – бесклассовый алгоритм. RIPv2 поддерживает VLSM (маски подсети переменной длины), суммирование маршрутов вручную и аутентификацию. В протоколе RIPv1 эти функции не поддерживаются.
- Для включения протокола динамической маршрутизации сначала выбирается протокол маршрутизации, а затем назначаются адреса IP-сетей без задания параметров (кроме OSPF).
- Команда **router** запускает процесс маршрутизации. Команда **network** позволяет процессу маршрутизации определить интерфейсы, участвующие в отправке и получении обновлений маршрутизации.

Резюме (прод.)

- Команда **router RIP** указывает RIP в качестве протокола маршрутизации. Команда **network** выбирает задействованные присоединенные сети.
- Команда **show ip** выводит информацию о протоколах маршрутизации и таблице маршрутизации.
- Команда **debug ip rip** выводит информацию о транзакциях маршрутизации RIP.

Резюме модуля

В этом разделе приводится резюме вопросов, рассмотренных в модуле.

Резюме модуля

- Распределенная сеть позволяет передавать данные на большие расстояния. В работе распределенных сетей используется несколько технологий, включая устройства, такие как маршрутизаторы, коммуникационные серверы и модемы, а также программные функции.
- Распространенный тип подключения к РВС – соединение «точка-точка», которое также называется последовательным соединением или соединением по арендованной линии, так как такие линии арендуются у поставщика (обычно у телефонной компании) и выделяются арендующей компании.
- Коммутация каналов позволяет нескольким площадкам подключаться к коммутируемой сети поставщика и связываться друг с другом. Эта технология предоставляет более экономичный вариант подключения к РВС и включает собственный набор технологий, таких как ТфОП.

Резюме модуля (прод.)

- Данные маршрутизации обрабатываются в виде записей в таблице маршрутизации, при этом каждая запись соответствует идентифицированному маршруту. Таблица маршрутизации может обновляться вручную или автоматически для учета изменений сети.
- Дистанционно-векторные алгоритмы маршрутизации позволяют каждому маршрутизатору полностью или частично отправлять свою таблицу маршрутизации соседним узлам.
- Протоколы маршрутизации на основе состояния канала ведут сложную базу данных топологии, которая обеспечивает их полную осведомленность об удаленных маршрутизаторах.

Резюме модуля (прод.)

- Алгоритмы сбалансированной гибридной маршрутизации сочетают характеристики маршрутизации на основе векторов расстояния и состояния канала.
- RIP используется в небольших однородных сетях.
- NAT и PAT преобразуют IP-адреса частных внутренних сетей в зарегистрированные IP-адреса для транспортировки по общедоступным внешним сетям, таким как Интернет, без необходимости в зарегистрированном адресе для подсети.
- Маршрутизатор может получить адрес интерфейса от DHCP-сервера.

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 точно описывают распределенные сети? (Выберите три варианта.) (Источник: общие сведения о технологиях распределенных сетей)

А) Компании, в которых внедрены распределенные сети, обычно ими владеют.
Б) Распределенные сети связывают устройства, разделенные обширными географическими областями.
В) В распределенных сетях используются услуги таких операторов, как телефонные компании, компании, предоставляющие услуги кабельной связи, спутниковые системы и поставщики сетевых услуг.
Г) По распределенным сетям обычно передается ограниченное число типов данных с высокими скоростями.
Д) В распределенных сетях последовательные соединения различных типов используются для предоставления доступа к полосе пропускания.
Е) Распределенные сети связывают устройства, расположенные в небольших географических областях.

В2) Какие три потребности в связи удовлетворяет PBC? (Выберите три варианта.) (Источник: общие сведения о технологиях распределенных сетей)

А) Работникам малых предприятий нужна возможность связи и обмена данными друг с другом.
Б) Административному персоналу школы нужна возможность совместного использования информации о расписании с учителями.
В) Организациям нередко требуется совместно использовать информацию с другими организациями, которые удалены на большие расстояния.
Г) Отделам необходимо быстро предоставлять большие файлы для совместного использования.
Д) Студентам для выполнения учебных заданий необходим доступ к библиотечным каталогам и публикациям, расположенным в других частях страны или мира.
Е) Сотрудникам филиала крупной копании нужна возможность совместного использования проектных данных.

В3) Какие два утверждения точно описывают различие между локальными и распределенными сетями? (Выберите два варианта.) (Источник: общие сведения о технологиях распределенных сетей)

А) По распределенным сетям данные передаются быстрее, чем по локальным.
Б) По локальным сетям данные передаются быстрее, чем по распределенным.
В) Локальная сеть связывает компьютеры, периферийные и другие устройства в одном здании или небольшой географической области, по распределенной сети данные передаются на большие расстояния.
Г) Компании или организации обычно владеют аппаратным или программным обеспечением, необходимым для поддержки распределенных сетей.
Д) Локальные сети могут охватывать крупные географические сети, если администратор правильно настроит их.

В4) На каком уровне OSI протоколы распределенных сетей описывают создание электрических, механических, оперативных и эксплуатационных подключений к услугам оператора связи? (Источник: общие сведения о технологиях распределенных сетей)

А) Уровень 1
Б) Уровень 2
В) Уровень 3
Г) Уровень 4

В5) На каком уровне OSI протоколы распределенных сетей определяют инкапсуляцию данных для передачи на удаленную площадку и механизмы передачи кадров, полученных при инкапсуляции? (Источник: общие сведения о технологиях распределенных сетей)

А) Уровень 1
Б) Уровень 2
В) Уровень 3
Г) Уровень 4

В6) Сопоставьте каждый тип устройств распределенной сети с его функцией. (Источник: общие сведения о технологиях распределенных сетей)

_____ 1. Они преобразуют цифровой сигнал отправляющего устройства в аналоговый формат для передачи по аналоговым линиям, а затем преобразуют сигнал обратно в цифровую форму, чтобы принимающее устройство могло получить и обработать его.

_____ 2. Они объединяют входящие и исходящие коммутируемые сеансы пользователей.

_____ 3. Они обеспечивают соединение сетей и предоставляют интерфейсные порты для доступа к распределенным сетям.

_____ 4. В распределенных сетях они используются для предоставления доступа.

А) маршрутизаторы
Б) коммуникационные серверы
В) модемы (DSU/CSU)
Г) другие сетевые устройства

B7) Сопоставьте каждый тип подключения на маршрутизаторе с соответствующей функцией. (Источник: общие сведения о технологиях распределенных сетей)

_____ 1. Позволяет маршрутизатору подключаться к локальным сетям с через Ethernet и некоторые другие технологии ЛВС, такие как Token Ring и ATM.

_____ 2. Создаются через интерфейс распределенной сети на маршрутизаторе для подключения к поставщику услуг, удаленной площадке или Интернету.

_____ 3. предоставляют текстовое подключение для настройки маршрутизатора и устранения неполадок

А) порты управления
Б) интерфейсы ЛВС
В) интерфейсы ГВС

B8) Какие два утверждения точно описывают протоколы канального уровня в распределенных сетях? (Выберите два варианта.) (Источник: общие сведения о технологиях распределенных сетей)

А) Во многих протоколах канального уровня используется механизм формирования кадров, подобный HDLC.
Б) Протоколы канального уровня определяют тип кабелей, используемых в распределенной сети.
В) ICMP – пример протокола канального уровня.
Г) Протоколы канального уровня определяют способ инкапсуляции данных для передачи на удаленные площадки, а также механизмы для передачи результирующих кадров, чтобы создать подключение по линии связи между отправляющим и принимающим устройствами.
Д) RIP – пример протокола канального уровня.

B9) Сопоставьте каждый тип мультиплексирования с его функцией. (Источник: общие сведения о технологиях распределенной сетей)

_____ 1. временное мультиплексирование

_____ 2. частотное мультиплексирование

_____ 3. статистическое мультиплексирование

А) Оно создает и объединяет несколько каналов в одной линии. Полоса пропускания выделяется для каждого канала передачи данных на основе частоты сигнала трафика.
Б) Полоса пропускания выделяется для каждого канала передачи данных на основе коротких предварительно заданных таймслотов, независимо от наличия передаваемых данных.
В) Полосы пропускания динамически назначается каналам передачи данных, по которым передается информация.

В10) Сопоставьте каждый тип канала связи с его функцией в распределенной сети. (Источник: общие сведения о технологиях распределенных сетей)

_____ 1. выделенные каналы связи

_____ 2. коммутируемые каналы связи

_____ 3. каналы связи с коммутацией пакетов

А) передача данных в помеченных ячейках, кадрах или пакетах
Б) предоставление установленного абонентского канала PBC через сеть поставщика услуг к удаленному месту назначения
В) динамическое создание выделенного виртуального соединения для передачи голоса или данных между отправителем и получателем

В11) Какие три утверждения точно описывают функции канала PBC с коммутацией пакетов? (Выберите три варианта.) (Источник: подключение к сети Интернет)

А) Коммутация пакетов – это метод связи, в котором пользователи получают выделенный канал между источником и местом назначения.
Б) Маршрут, по которому пакеты достигают места назначения, меняется.
В) В сетях с коммутацией пакетов пакеты данных пересылаются по различным маршрутам общедоступной сети, принадлежащей оператору связи, чтобы достичь одной и той же точки назначения.
Г) В сети с коммутацией пакетов каждый клиент использует всю полосу пропускания своего виртуального канала.
Д) В ТфОП используется коммутация пакетов.
Е) Для клиента стоимость сети с коммутацией пакетов обычно ниже стоимости арендуемых линий «точка-точка».

В12) Какие три утверждения точно описывают DSL? (Выберите три варианта.) (Источник: подключение к сети Интернет)

А) Для подключения корпоративных пользователей через DSL не требуется поставщик услуг Интернета.
Б) В современных технологиях DSL используются сложные способы кодирования и модуляции, чтобы достичь скоростей передачи данных вплоть до 10 Мбит/с.
В) Абонент может напрямую подключаться к корпоративной DSL-сети.
Г) Технология DSL – это технология соединений с коммутацией каналов, в которой существующие телефонные линии на основе витой пары используются для высокоскоростной передачи данных, таких как мультимедиа и видео, абонентам.
Д) Технология DSL позволяет использовать местные линии связи для обычного голосового телефонного соединения и постоянного подключения к сети.
Е) Технологии DSL обеспечивают передачу данных (в обоих направлениях) на частотах над окном 4 кГц, что позволяет одновременно передавать голос и данные при использовании услуг цифровой абонентской линии.

В13) Какие два ответа соответствуют типам DSL? (Выберите два варианта.) (Источник: подключение к сети Интернет)

А) ADSL
Б) IDSL
В) LDSL
Г) D-lite
Д) GDSL

В14) Какие три утверждения относятся к DSL? (Выберите три варианта.) (Источник: подключение к сети Интернет)

А) DSL не обладает обратной совместимостью с аналоговыми голосовыми соединениями.
Б) Услуга DSL может быть постепенно внедрена в любой области.
В) Для использования большинства современных услуг DSL клиент должен находиться в пределах 3000 м от центрального офиса поставщика услуг.
Г) У DSL есть ограничения по расстоянию.
Д) Скорость передачи в прямом направлении обычно выше скорости передачи в обратном направлении.
Е) Технология DSL доступна не во всех регионах.

В15) Какие три утверждения точно описывают кабельные соединения PBC? (Выберите три варианта.) (Источник: подключение к сети Интернет)

А) Изначально кабель был однонаправленным носителем, предназначенным для предоставления цифровых видеоканалов вещания клиентам (или абонентам).
Б) Некоторые поставщики услуги кабельного подключения обещают скорости передачи данных в 20 превышающие скорости передачи по арендованным линиям T1.
В) Первоначальной целью ассоциации Multimedia Cable Network System Partners Ltd. было определение стандарта продуктов и систем, поддерживающего передачу данных и предоставление перспективных услуг через станции кабельного телевидения.
Г) Кабельные модемы поддерживают двухстороннюю высокоскоростную передачу данных по коаксиальным линиям, которые используются для передачи сигналов кабельного телевидения.
Д) Кабельный доступ обеспечивает более высокие скорости, чем арендованные линии, при меньших затратах и более простой установке.
Е) Кабельные модемы используют инфраструктуру телефонных систем, поэтому взимается плата за местные линии связи.

В16) Какие три утверждения точно описывают историю Интернета? (Выберите три варианта.) (Источник: подключение к сети Интернет)

А) Выход в 1993 году удобного графического обозревателя под названием Navigator популяризировал Интернет.
Б) Исследователи Министерства обороны изобрели способ разбивать сообщения на части, отправляя каждую часть к месту назначения по отдельности. Достигнув места назначения сообщение должно собираться в исходную форму. Сегодня этот метод передачи данных известен как пакетная система.
В) В университете Южной Калифорнии был установлен первый компьютер с пакетной системой, разработанной министерством обороны.
Г) Предтеча Интернета началась с потребности Министерства обороны в сети управления запасами, которая бы связывала несколько вычислительных центров по стране.
Д) В 1972 году разработчики ARPANET создали первое программное обеспечение для обмена электронными сообщениями, чтобы упростить связь и координацию проектов.
Е) В 1984 году была введена система DNS, которая дала миру суффиксы доменов (такие как .edu, .com, .gov и .org) и серию кодов стран.

В17) Сопоставьте термины NAT с их определениями. (Источник: подключение к сети Интернет)

_____ 1. статическое NAT

_____ 2. динамическое NAT

_____ 3. внутренняя сеть

_____ 4. внешний глобальный IP-адрес

А) набор сетей для преобразования NAT
Б) IP-адрес внутреннего хоста, которые доступен во внешней сети (преобразованный IP-адрес)
В) форма NAT, в которой незарегистрированные IP-адреса преобразуются зарегистрированные IP-адреса по принципу «один к одному»
Г) форма NAT, в которой незарегистрированный IP-адрес преобразуется в зарегистрированный IP-адрес из группы зарегистрированных IP-адресов

В18) При настройке NAT какой параметр определяет число одновременных активных преобразований NAT? (Источник: подключение к сети Интернет)

А) размер очереди памяти NAT
Б) число адресов в пуле NAT
В) число неиспользуемых номеров TCP-портов
Г) отношение числа UDP- и TCP-сеансов

В19) При настройке NAT какому из приведенных ниже терминов соответствует интерфейс Интернета? (Источник: подключение к сети Интернет)

А) локальный интерфейс NAT
Б) внутренний интерфейс NAT
В) глобальный интерфейс NAT
Г) внешний интерфейс NAT

В20) Какая команда удаляет указанную запись динамического преобразования из таблицы преобразований NAT? (Источник: подключение к сети Интернет)

А) **clear ip nat translation ***
Б) **clear ip nat translation inside**
В) **clear ip nat translation outside**
Г) **clear ip nat translation protocol inside**

В21) Вывод какой команды отобразит активные преобразования таблицы преобразования NAT? (Источник: подключение к сети Интернет)

А) **show ip nat statistics**
Б) **show ip nat translations**
В) **clear ip nat translation ***
Г) **clear ip nat translation outside**

B22) Вы выполняете поиск и устранение проблемы подключения NAT на маршрутизаторе Cisco. Вы обнаруживаете, что соответствующая запись не установлена в таблицу преобразования. Какие три действия следует выполнить в такой ситуации? (Выберите три варианта.) (Источник: подключение к сети Интернет)

А) Определить, достаточно ли адресов в пуле NAT.
Б) Выполнить команду **debug ip nat detailed**, чтобы определить источник проблемы.
В) Убедиться, что выбранный маршрут существует, с помощью команды **show ip route**.
Г) Убедиться, что внутренние и внешние интерфейсы NAT на маршрутизаторе заданы корректно.
Д) Убедиться, что список контроля доступа, на который ссылается команда NAT, разрешает все необходимые локальные IP-адреса.

B23) Какое утверждение наилучшим образом описывает статические и динамические маршруты? (Источник: обеспечение статической маршрутизации)

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

B24) Что задает команда **ip route 186.157.5.0 255.255.255.0 10.1.1.3**? (Источник: обеспечение статической маршрутизации)

А) Для 186.157.5.0 и 10.1.1.3 используется маска 255.255.255.0.
Б) Маршрутизатор должен использовать сеть 186.157.5.0, чтобы получить доступ к 10.1.1.3.
В) Маршрутизатор должен трассировать маршрут к сети 186.157.5.0 через 10.1.1.3.
Г) Маршрутизатор должен использовать 10.1.1.3, чтобы получить доступ к сети 186.157.5.0.

B25) Какая команда отображает информацию о конфигурации статических маршрутов на маршрутизаторе Cisco? (Источник: обеспечение статической маршрутизации)

А) **show route ip**
Б) **show ip route**
В) **show ip route static**
Г) **show route ip static**

В26) Какой из следующих протоколов может служить примером протокола внешнего шлюза? (Источник: обеспечение статической маршрутизации)

А) RIP
Б) BGP
В) IGRP
Г) EIGRP

В27) В каких ситуациях используется административное расстояние? (Источник: обеспечение статической маршрутизации)

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

В28) Маршрутизатор получает пакет с адресом назначения, соответствующим неизвестной подсети, принадлежащей сети с прямым подключением. Какова стандартная реакция на это событие, если команда **ip classless** не включена? (Источник: обеспечение статической маршрутизации)

А) отбросить пакет
Б) переслать пакет маршрутизатору по умолчанию
В) переслать пакет по следующему переходу сети с прямым подключением
Г) выполнить широковещательную рассылка пакета через все интерфейсы, кроме интерфейса, через который этот пакет был получен

В29) Какие три утверждения точно описывают характеристики и функции сетей с коммутацией каналов? (Выберите три варианта.) (Источник: настройка последовательной инкапсуляции)

А) При использовании коммутации каналов для каждого сеанса связи создается, поддерживается и разрывается выделенный физический канал в сети оператора.
Б) Коммутация каналов позволяет нескольким площадкам подключаться к коммутируемой сети поставщика и связываться друг с другом.
В) При использовании коммутации каналов каждое соединение может поддерживать только две площадки.
Г) ATM – пример технологии коммутации каналов.
Д) ICMP – пример сети с коммутацией каналов.
Е) Frame Relay – пример технологии коммутации каналов.

В30) Какие три утверждения описывают характеристики ТфОП как канала связи? (Выберите три варианта.) (Источник: настройка последовательной инкапсуляции)

А) Не требует дополнительного оборудования, кроме модема.
Б) Высокая скорость передачи больших файлов данных.
В) Затраты на внедрение канала ТфОП для ГВС относительно низки.
Г) Высокое качество обслуживания телефонной сети общего пользования с небольшим числом случаев недоступности линий.
Д) Для подключения через глобальную сеть требуется немного времени.
Е) Нет ограничений на скорость передачи сигнала по соединению ТфОП.

В31) Какие три утверждения точно описывают канал «точка-точка»? (Выберите три варианта.) (Источник: настройка последовательной инкапсуляции)

А) Канал связи «точка-точка» (последовательный канал) обеспечивает отдельный постоянный коммуникационный путь PBC от абонента к удаленной сети через сеть оператора, например телефонной компании.
Б) Операторы связи обычно сдают линии «точка-точка» в аренду, поэтому они часто называют арендованными линями.
В) Канал «точка-точка» или последовательный канал, как правило, соединяет две относительно близких площадки.
Г) Для канала «точка-точка» оператор выделяет фиксированную полосу пропускания и вспомогательное оборудование для арендуемой линии.
Д) Назначение устройств DSU/CSU в канале «точка-точка» – обеспечение надежной доставки пакетов данных по установленному соединению.
Е) Технологии мультиплексирования не используются в каналах «точка-точка».

В32) Какие три утверждения точно описывают полосу пропускания соединений PBC? (Выберите три варианта.) (Источник: настройка последовательной инкапсуляции)

А) В Северной Америке полоса пропускания обычно выражается номером DS (DS0, DS1 и т. д.), который с технической точки зрения отражает скорость передачи и формат сигнала.
Б) Для создания линии DS1 (также называемой линией T1) можно объединить 12 линий DS0, что обеспечивает суммарную скорость 1 544 Мбит/с.
В) Полосы пропускания последовательного соединения могут постепенно увеличиваться в соответствии с потребностью в более быстрой передачи данных.
Г) Скорость базового канала составляет 1 544 Мбит/с (DS1), что соответствует полосе пропускания, необходимой для несжатого оцифрованного телефонного вызова.
Д) В оптических сетях используется иерархия полос пропускания, которая отличается в Северной Америке и Европе. В Европе варианты полосы пропускания определяет стандарт OC, а в Северной Америке они определяются SDH.
Е) Полоса пропускания обозначает скорость передачи данных по каналу связи.

В33) Какие три утверждения точно описывают функции протокола HDLC? (Выберите три варианта.) (Источник: настройка последовательной инкапсуляции)

А) HDLC поддерживает конфигурации «точка-точка» и многоточечные конфигурации.
Б) Протокол HDLC включает метод аутентификации.
В) Протоколы HDLC, используемые в устройствах различных производителей, совместимы.
Г) Протокол HDLC определяет метод инкапсуляции данных в каналах синхронной последовательной передачи данных с использованием кадра и контрольной суммы.
Д) Протокол HDLC поддерживает только многоточечные конфигурации.
Е) Реализация протокола HDLC от Cisco включает механизм размера окна и управление потоками.

В34) Какие три утверждения описывают функцию протокола PPP? (Выберите три варианта.) (Источник: настройка последовательной инкапсуляции)

А) Этап аутентификации сеанса PPP является обязательным.
Б) Протокол PPP обеспечивает соединения «маршрутизатор-маршрутизатор» и «хост-сеть» в асинхронных каналах.
В) PPP был создан как протокол инкапсуляции, используемый для передачи IP-трафика через каналы «точка-точка».
Г) Протокол PPP установил стандарт для управления TCP-сеансами.
Д) Протокол PPP обеспечивает соединения «маршрутизатор-маршрутизатор» и «хост-сеть» в синхронных и асинхронных каналах.
Е) Протокол LCP используется в PPP для установления, настройки и тестирования канала передачи данных.

В35) Какие три утверждения описывают характеристики каналов «точка-точка»? (Выберите три варианта.) (Источник: настройка последовательной инкапсуляции)

А) Установка и обслуживание каналов «точка-точка» требует минимального опыта.
Б) Каналы «точка-точка» обычно предоставляют высокое качество обслуживания.
В) Каналы «точка-точка» предоставляют постоянную выделенную линию связи, которая всегда доступна.
Г) Для арендованных линий полоса пропускания линии соответствует требованиям к связи.
Д) Каналы «точка-точка» предоставляются на условиях совместного доступа.
Е) В каналах «точка-точка» конечные точки совместно используют интерфейсы маршрутизатора, что снижает затраты на оборудование.

В36) Какие команды включают протокол HDLC? (Источник: настройка последовательной инкапсуляции)

А) Router (config)**# hdlc encapsulation**
Б) Router (config)**# encapsulation hdlc**
В) Router (config-if)**# hdlc encapsulation**
Г) Router (config-if)**# encapsulation hdlc**

В37) Как проприетарный протокол HDLC компании позволяет нескольким протоколам сетевого уровня совместно использовать один последовательный канал? (Источник: настройка последовательной инкапсуляции)

А) Добавляет новое поле типа.
Б) Разбивает контрольное поле на несколько частей.
В) Добавляет дополнительные значения в поле FCS.
Г) Включает данные о протоколе в поле данных.

В38) В каком режиме командной строки Cisco вводится команда для задания аутентификации PPP? (Источник: настройка последовательной инкапсуляции)

А) пользовательский режим
Б) режим монитора ROM
В) режим глобальной конфигурации
Г) режим конфигурации интерфейса

В39) Что настраивает команда **ppp authentication chap pap**? (Источник: настройка последовательной инкапсуляции)

А) Будет всегда использоваться аутентификация CHAP.
Б) Будет использоваться метод CHAP или PAP, выбор между ним будет случайным по соображениям безопасности.
В) Будет использоваться аутентификации CHAP, только если удаленный маршрутизатор не запросит PAP.
Г) Если не удается использовать аутентификацию CHAP, предпринимается попытка использования PAP.

В40) В каком поле вывода команды **show interface** указывается, что протокол PPP настроен правильно? (Источник: настройка последовательной инкапсуляции)

А) Encaps = PPP
Б) PPP encapsulation
В) Encapsulation PPP
Г) Encapsulation HDLC using PPP

В41) Какие три утверждения правильно описывают Frame Relay? (Выберите три варианта.) (Источник: настройка последовательной инкапсуляции)

А) Frame Relay действует на прикладном уровне.
Б) Для подключения к границе сети часто используется выделенная линия, однако некоторые поставщики услуг предоставляют коммутируемые подключения с использованием каналов ISDN или xDSL.
В) В протоколе Frame Relay отсутствует исправление ошибок и управление потоком.
Г) Доступные скорости передачи данных для Frame Relay обычно не превышают 10 Мбит/с.
Д) Большинство соединений Frame Relay составляют каналы SVC, а не PVC.
Е) Frame Relay предоставляет услуги PVC и SVC с помощью подключений с общей полосой пропускания, по которым передается голосовой трафик и трафик данных.

В42) Какие три утверждения точно описывают ATM? (Выберите три варианта.) (Источник: настройка последовательной инкапсуляции)

А) ATM основывается на виртуальных каналах.
Б) Сеть ATM включает маршрутизаторы ATM, которые отвечают за пересылку ячеек и пакетов.
В) Виртуальные каналы обеспечивают двунаправленный путь связи от одного конечного устройства ATM к другому.
Г) Виртуальный канал ATM является физическим соединением, созданным между двумя конечными устройствами ATM в сети ATM.
Д) ATM может работать только по коаксиальному кабелю с помощью DS3.
Е) ATM представляет собой технологию соединения на основе коммутации ячеек, способную обеспечить передачу голосовых и видеосигналов и данных через частные и общедоступные сети.

В43) Как маршрутизатор, работающий по дистанционно-векторному алгоритму, получает сведения о сетях без прямого подключения к нему. (Источник: активация протокола RIP)

А) от исходного маршрутизатора
Б) от соседних маршрутизаторов
В) от маршрутизатора назначения
Г) узнает только о сетях с прямым подключением

В44) Что маршрутизатор, работающий по дистанционно-векторному алгоритму, посылает соседним маршрутизаторам в периодических обновлениях таблицы маршрутизации? (Источник: активация протокола RIP)

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

В45) Каково максимально допустимое число переходов для протокола RIP? (Источник: активация протокола RIP)

А) 6
Б) 15
В) 30
Г) 60

В46) При использовании протокола RIP балансировка нагрузки осуществляется по нескольким маршрутам. Чем они характеризуются? (Источник: активация протокола RIP)

А) равная стоимость
Б) равный вес
В) равное расстояние
Г) равная полоса пропускания

В47) Какая команда правильно задает RIP в качестве протокола маршрутизации? (Источник: активация протокола RIP)

А) Router(config)#**rip**
Б) Router(config)#**router rip**
В) Router(config-router)#**rip {AS no.}**
Г) Router(config-router)#**router rip {AS no.}**

В48) Каково значение по умолчанию таймера удержания RIP? (Источник: активация протокола RIP)

А) 30 секунд
Б) 60 секунд
В) 90 секунд
Г) 180 секунд

Ответы на вопросы для самопроверки по модулю

В1) Б, В, Д

В2) В, Г, Д

В3) Б, В

В4) А

В5) Б

В6) 1 = В, 2 = Б, 3 = А, 4 = Г

В7) 1 = Б, 2 = В, 3 = А

В8) А, Г

В9) 1 = Б, 2 = А, 3 = В

В10) 1 = Б, 2 = В, 3 = А

В11) Б, В, Е

В12) Г, Д, Е

В13) А, Б

В14) Б, Г, Е

В15) В, Г, Д

В16) Б, Д, Е

В17) 1 = В, 2 = Г, 3 = А, 4 = Б

В18) Б

В19) 1 = А, 2 = Б, 3 = Д, 4 = Г, 5 = В

В20) Г

В21) Б

В22) А, Г, Д

В23) Б

В24) Г

В25) Б

В26) Б

В27) В

В28) А

В29) А, Б, Д

В30) А, В, Г

В31) А, Б, Г

В32) А, В, Е

В33) А, Б, Г

В34) В, Д, Е

В35) А, Б, В

В36) Г

В37) А

В38) Г

В39) Г

В40) В

В41) Б, В, Е

В42) А, В, Е

В43) Б

В44) А

В45) Б

В46) А

В47) Б

В48) Г

Модуль 6

Управление сетевой средой

Обзор

Сетевые администраторы обязаны обеспечить, чтобы базовая коммуникационная инфраструктура поддерживала задачи бизнеса и связанные с ними приложения. Кроме того, сетевые администраторы ответственны за управление всеми устройствами в сети в соответствии с передовым опытом, а также за сокращение времени простоя устройств. В этом модуле описываются команды и процессы, используемые для определения рабочего состояния сети, сбора информации об удаленных устройствах и управления образами Cisco IOS, файлами конфигурации и сетевыми устройствами.

Задачи модуля

По окончании этого модуля вы сможете управлять сетевыми устройствами. Это значит, что вы сможете выполнять следующие задачи:

- использовать интерфейс командной строки для обнаружения соседних узлов в сети;
- управлять запуском и конфигурацией маршрутизатора;
- управлять образами Cisco IOS, файлами конфигурации и сетевыми устройствами.

Занятие 1

Обнаружение соседних устройств в сети

Обзор

Большинство сетевых устройств по определению не работает изолированно. С устройством Cisco в сети часто соседствуют другие устройства Cisco, и возможность получения информации о таких устройствах очень полезна при принятии решений о структуре сети, устранении неполадок и внесении изменений в оборудование. На этом занятии описывается сбор информации об устройствах Cisco в сети и использование этой информации для создания карты сетевой среды.

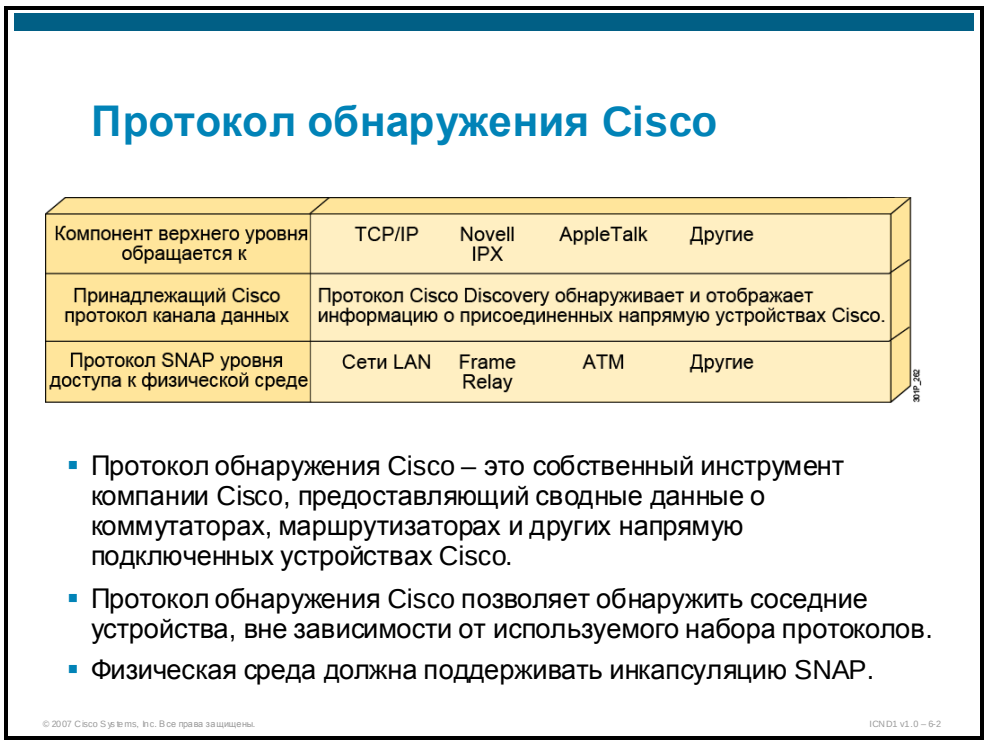
Задачи

По окончании этого занятия вы сможете использовать интерфейс командной строки для обнаружения соседних устройств в сети и определения их рабочего состояния. Это значит, что вы сможете выполнять следующие задачи:

- описывать цель и функцию протокола обнаружения Cisco (CDP);
- описывать данные, предоставляемые протоколом обнаружения Cisco (CDP);
- включать и отключать протокол обнаружения Cisco (CDP);
- определять имена хостов и адреса соседних устройств Cisco с помощью протокола обнаружения Cisco (CDP);
- отслеживать и поддерживать в актуальном состоянии сведения о соседних устройствах Cisco с помощью протокола обнаружения Cisco (CDP);
- использовать информацию, собранную с помощью протокола обнаружения Cisco (CDP), для создания карты сетевой среды.

Протокол обнаружения Cisco (CDP)

Протокол обнаружения Cisco – это средство сбора информации, используемое сетевыми администраторами для получения сведений о напрямую подключенных устройствах Cisco. В этом разделе описывается назначение и функции протокола обнаружения Cisco.



Протокол обнаружения Cisco – это собственный инструмент компании Cisco, позволяющий получить сводные данные о протоколах и адресах, используемых другими, напрямую подключенными к устройству, на котором выполняются команды протокола обнаружения, устройствами Cisco.

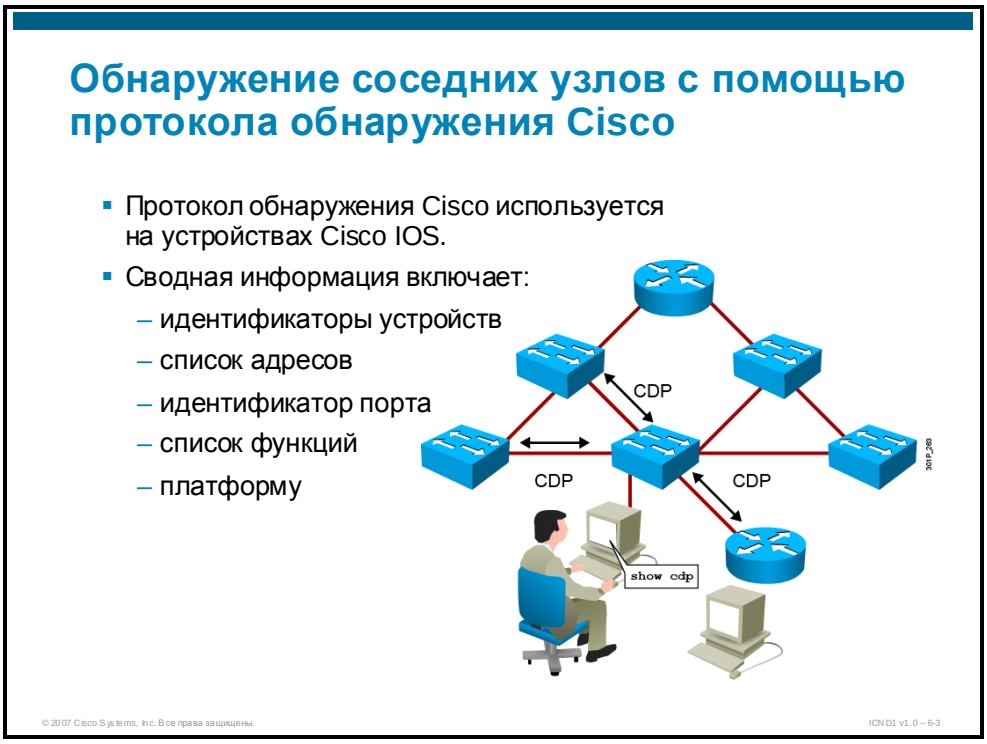
Протокол обнаружения Cisco функционирует на канальном уровне, связывая физическую среду с протоколами верхнего уровня (ULP). Так как протокол обнаружения Cisco действует на канальном уровне, два или более сетевых устройства Cisco, таких как маршрутизаторы, поддерживающие различные протоколы сетевого уровня (например, IP и Novell IPX) могут получить данные друг о друге.

Физическая среда, соединяющая устройства, на которых выполняется протокол обнаружения Cisco, должна поддерживать инкапсуляцию SNAP (Subnetwork Access Protocol). К таким средам относятся все ЛВС, Frame Relay, а также другие РВС и сети ATM.

При запуске устройства Cisco протокол обнаружения по умолчанию инициируется и автоматически обнаруживает соседние устройства Cisco с поддержкой данного протокола, вне зависимости от используемого набора протоколов сетевого уровня.

Информация, получаемая с помощью протокола обнаружения Cisco

Протокол обнаружения Cisco обеспечивает обмен информацией об аппаратном и программном обеспечении с соседними устройствами, подключенными напрямую. В этом разделе описываются сведения, предоставляемые протоколом обнаружения Cisco.



На этом рисунке представлен пример использования протокола обнаружения Cisco для обмена информацией с соседними, напрямую подключенными, устройствами. Результат такого обмена информацией можно вывести на консоль, подключенную к сетевому устройству, на интерфейсах которого настроена поддержка протокола обнаружения Cisco.

Протокол обнаружения Cisco предоставляет следующую информацию о соседних устройствах.

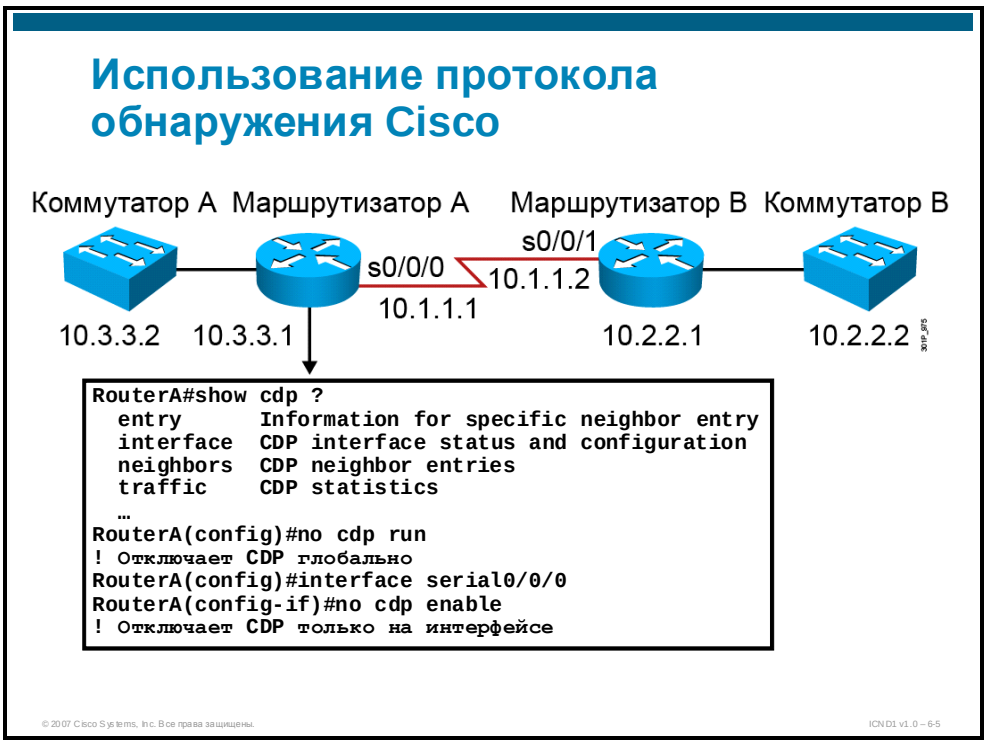
- **Идентификаторы устройств:** например, имя хоста коммутатора.
- **Список адресов:** до одного адреса сетевого уровня для каждого поддерживаемого протокола.
- **Идентификатор порта:** имена локального и удаленного портов – в виде строки символов ASCII, например ethernet0.
- **Список функций:** поддерживаемые функции, например, устройство, действующее как мост с маршрутизацией от источника и как маршрутизатор.
- **Платформа:** аппаратная платформа устройства, например, маршрутизатор серии Cisco 7200.

Обратите внимание, что на рисунке верхний маршрутизатор не подключен напрямую к консоли администратора. Чтобы получить данные протокола обнаружения Cisco о верхнем маршрутизаторе на консоли администратора, сетевой администратор должен воспользоваться протоколом Telnet, чтобы подключиться к коммутатору, имеющему прямое подключение к данному устройству.

Протокол обнаружения Cisco версии 2 является последей редакцией данного протокола. Он предоставляет более интеллектуальные возможности отслеживания устройств. Эти функции включают в себя механизм создания отчетов, который позволяет ускорить отслеживание ошибок, тем самым снижая дорогостоящее время простоя. Созданное сообщение об ошибке может быть отправлено на консоль или серверу журналирования (logging server).

Внедрение протокола обнаружения Cisco

Протокол обнаружения Cisco на маршрутизаторе можно отключить или включить в целом (глобально) или для каждого порта в отдельности (по интерфейсам). В этом разделе описывается включение и отключение протокола обнаружения Cisco, а также вывод данных этого протокола.

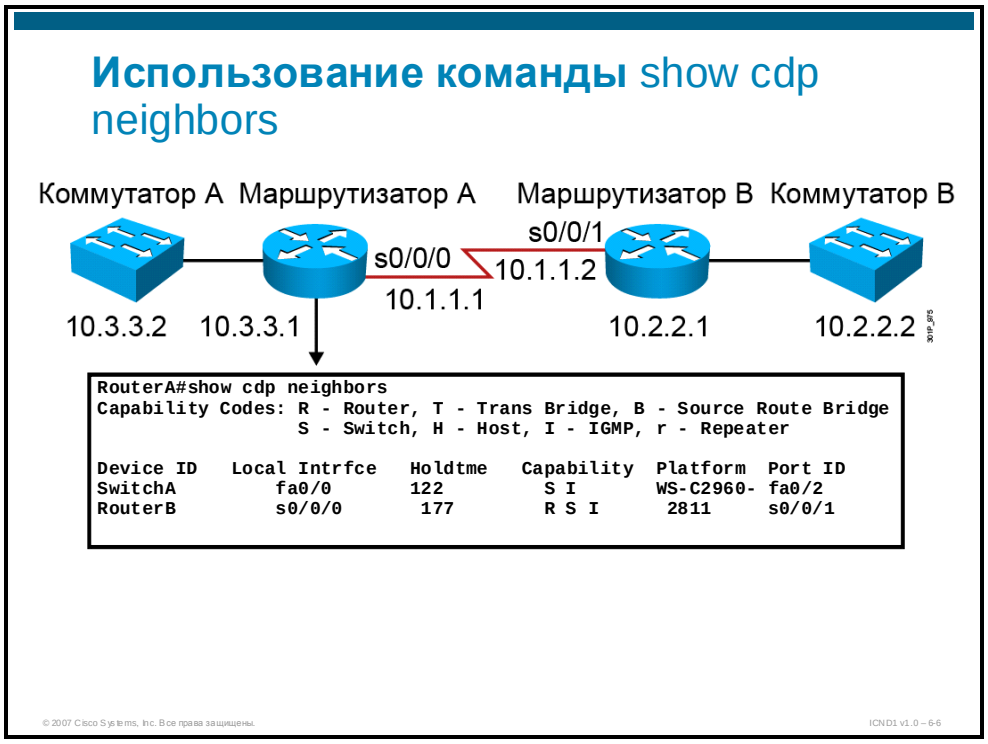


Данные протокола обнаружения Cisco можно вывести с помощью команды **show cdp**. Данной команде определено несколько ключевых слов, позволяющих получить доступ к различным типам сведений с разным уровнем детализации. CDP разработан и реализован как очень простой и удобный протокол. Пакеты протокола обнаружения Cisco имеют небольшой размер (от 80 байтов) и в основном состоят из ASCII-строк с данными, пример которых приводится рисунке.

Поддержка протокола обнаружения Cisco по умолчанию включена на всех интерфейсах (кроме многоточечных подинтерфейсов Frame Relay), но может быть отключена на уровне устройства. Некоторые интерфейсы, например, интерфейсы ATM, не поддерживают протокол обнаружения Cisco. Чтобы помешать другим устройствам с поддержкой протокола обнаружения Cisco получить доступ к информации о конкретном устройстве, используется команда глобальной конфигурации **no cdp run** Чтобы отключить протокол обнаружения Cisco только на интерфейсе, используется команда **no cdp enable**. Чтобы включить протокол обнаружения Cisco на интерфейсе, используется команда конфигурации интерфейса **no cdp enable**.

Использование команды show cdp neighbors

Команда **show cdp neighbors** используется для отображения информации о соседних устройствах, поддерживающих протокол обнаружения Cisco. В этом разделе описываются сведения, предоставляемые командой **show cdp neighbors**.



На рисунке показан вывод команды **show cdp neighbors** для маршрутизатора A. Для каждого соседнего устройства с поддержкой протокола обнаружения Cisco отображается следующая информация:

- идентификатор устройства;
- локальный интерфейс;
- время удержания в секундах;
- коды функциональности устройства;
- аппаратная платформа;
- идентификатор удаленного порта.

Время удержания указывает, как долго принимающее устройство сохраняет пакет протокола обнаружения Cisco, прежде чем его отбросить.

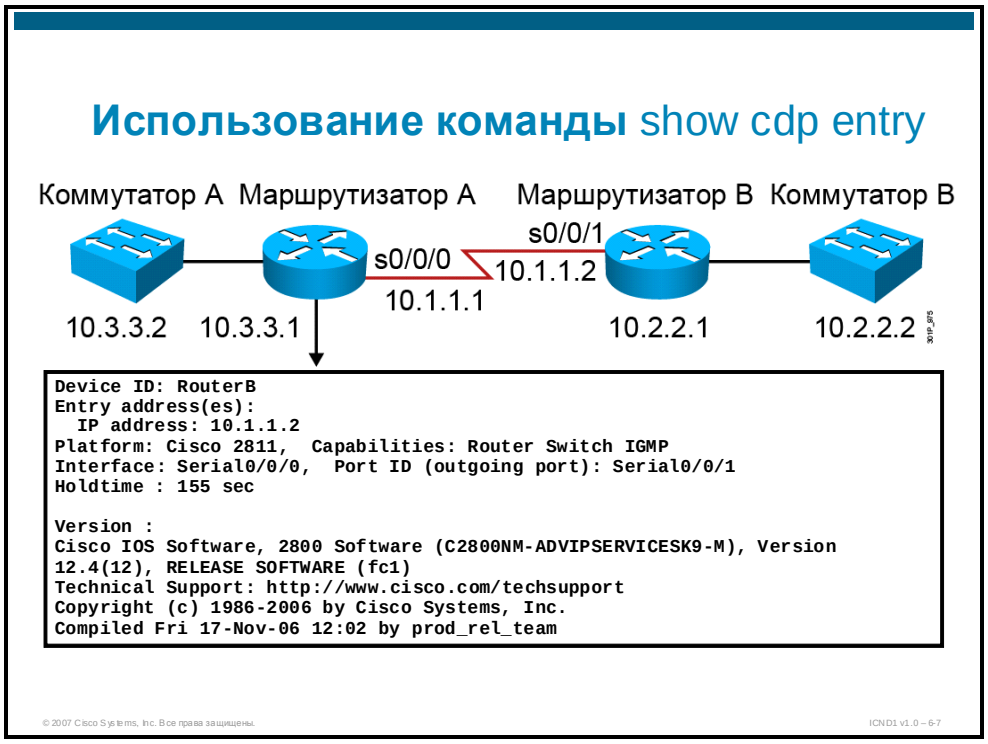
Формат вывода команды **show cdp neighbors** зависит от типа устройства, но информация об устройствах обычно совпадает.

Команду **show cdp neighbors** можно использовать на коммутаторе Cisco Catalyst для просмотра обновлений протокола обнаружения Cisco, полученных на локальных интерфейсах. Обратите внимание, что локальные интерфейсы коммутатора называются локальными портами.

Если к команде **show cdp neighbors** добавить аргумент *detail*, вывод будет содержать дополнительную информацию, такую как адреса сетевого уровня соседних устройств. Вывод команды **show cdp neighbors detail** идентичен выводу командой **show cdp entry ***.

Отслеживание и поддержка протокола обнаружения Cisco

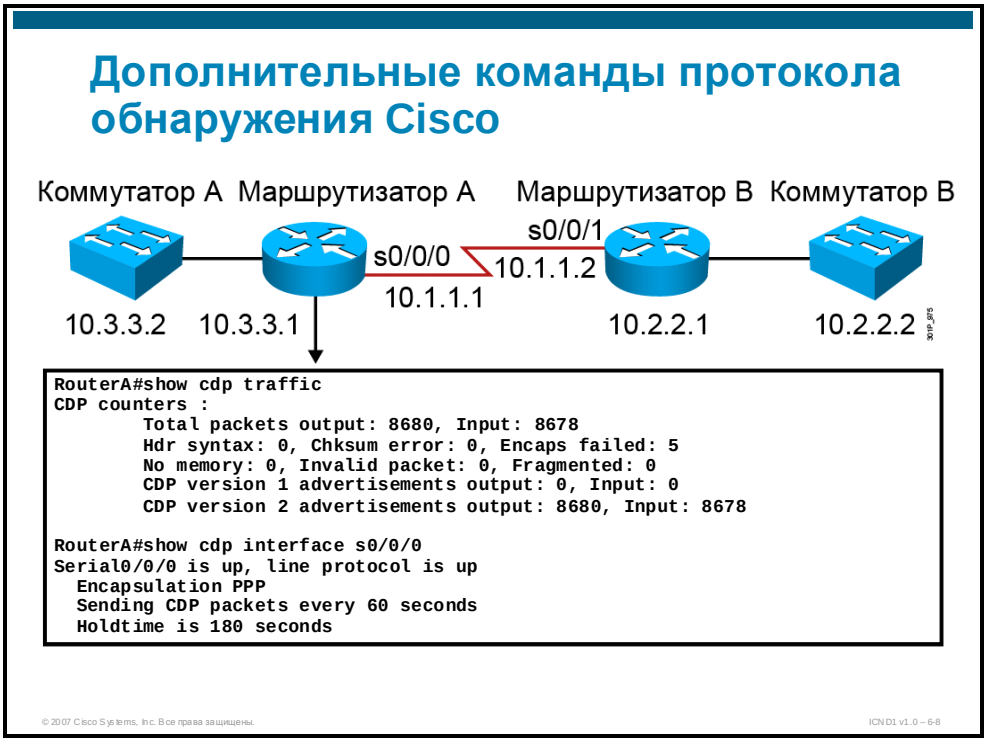
Команды **show cdp entry**, **show cdp traffic** и **show cdp interface** выдают подробные сведения, предоставляемые протоколом обнаружения Cisco. В этом разделе описывается вывод этих трех **show** команд.



Команда **show cdp entry** используется для вывода подробной информации о соседних устройствах. Для вывода сведений о конкретном соседнем устройстве, такая команда должна содержать IP-адрес или идентификатор соседнего устройства. Знак звездочки (*****) используется для отображения информации обо всех соседних устройствах. Вывод команды **show cdp entry** содержит следующее:

- идентификатор соседнего устройства;
- информация протокола 3-го уровня (например, IP-адреса);
- платформа устройства;
- функции устройства;
- тип локального интерфейса и идентификатор удаленного порта;
- время удержания, в секундах;
- тип и версию программного обеспечения Cisco IOS.

Вывод этой команды содержит все адреса 3-го уровня интерфейсов соседних устройств (до одного адреса 3-го уровня на протокол).



Команда **show cdp traffic** используется для вывода информации о трафике протокола CDP, проходящем через интерфейс. Отображается число отправленных и полученных пакетов. Также отображаются счетчики ошибок следующих типов:

- синтаксическая ошибка;
- ошибка контрольной суммы;
- неудачные инкапсуляции;
- недостаточно памяти;
- неверные пакеты;
- фрагментированные пакеты;
- число отправленных пакетов протокола обнаружения Cisco версии 1;
- число отправленных пакетов протокола обнаружения Cisco версии 2.

Примечание Команда **show cdp traffic** недоступна на коммутаторах Catalyst 1900.

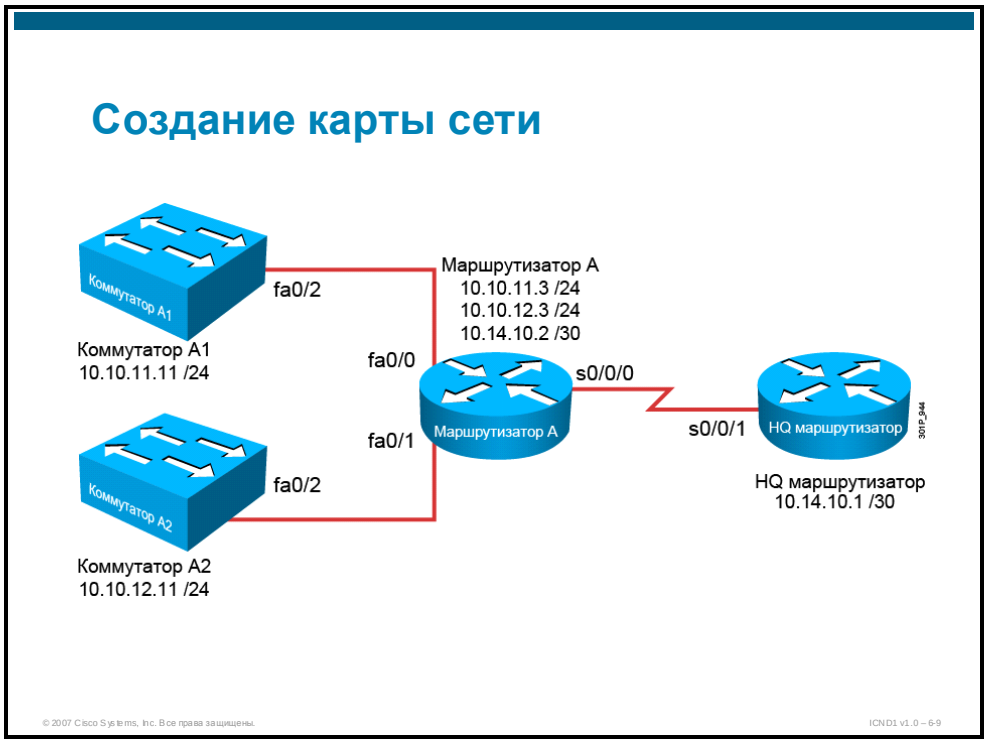
Команда **show cdp interface** используется для отображения следующей информации о состоянии интерфейса и конфигурации локального устройства:

- состояние линии или канала передачи данных интерфейса;
- тип инкапсуляции на интерфейсе;
- частота отправки пакетов протокола обнаружения Cisco (по умолчанию 60 секунд);
- время удержания, в секундах (по умолчанию 180 секунд).

Протокол обнаружения Cisco ограничивается сбором информации о соседних, напрямую подключенных, устройствах Cisco. Для сбора информации об удаленных устройствах, которые не подключены напрямую, используются другие средства, такие как Telnet.

Создание карты сетевой среды

После обнаружения всех устройств интерсети важно задокументировать сеть, чтобы обеспечить ее оперативную поддержку. В этом разделе описывается создание карты сетевой среды.



Документация по топологии используется для проверки соответствия проектным рекомендациям, а также для проектирования, изменения и устранения неполадок в будущем. Документация по топологии должна включать как логическую, так и физическую документацию по следующим компонентам:

- подключения;
- адресация;
- типы сред;
- устройства;
- расположение стоек;
- назначение плат;
- кабельная разводка;
- идентификация кабелей;
- конечные устройства;
- сведения об электропитании;
- идентификационные данные каналов.

Ведение точной документации по топологии сети является ключом к успешному управлению конфигурацией. Для создания среды с поддержкой ведения документации по топологии, необходимо обеспечить обновление соответствующей информации. Компания Cisco настоятельно рекомендует обновлять документацию по топологии при любом ее изменении.

Резюме

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

Резюме

- Протокол CDP – это средство сбора информации для сетевых администраторов, которое позволяет получать сведения об устройствах.
- Протокол CDP обеспечивает обмен данными об аппаратном и программном обеспечении с соседними , напрямую подключенными, устройствами с поддержкой протокола CDP.
- Протокол CDP на маршрутизаторе можно отключить или включить глобально или для каждого порта в отдельности.
- Команда **show cdp neighbors** используется для вывода данных о соседних устройствах, поддерживающих протокол CDP.
- Команды **show cdp entry**, **show cdp traffic** и **show cdp interface** выдают подробные сведения об устройстве Cisco, предоставляемые протоколом CDP.
- На основе вывода команды **show cdp** можно создать карту топологии сети, которая может помочь при устранении неполадок.

Занятие 2

Управление запуском и конфигурацией маршрутизатора Cisco

Обзор

Во время загрузки маршрутизатор Cisco выполняет определенную последовательность действий. Несколько раз в течение этого процесса маршрутизатор принимает решение о следующем действии. Знание последовательности загрузки может быть очень полезно при решении проблем с маршрутизатором Cisco, а также при изменении его конфигурации. На этом занятии описываются все этапы загрузки маршрутизатора.

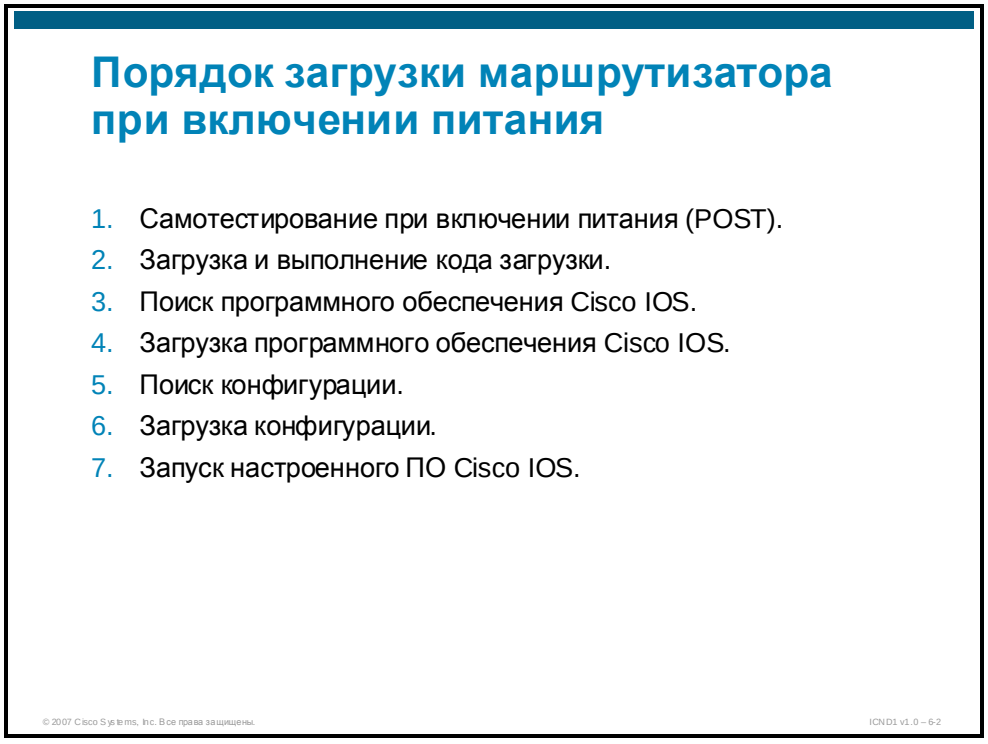
Задачи

По окончании этого занятия вы сможете описывать настройку маршрутизатора Cisco и управление им. Это значит, что вы сможете выполнять следующие задачи:

- описывать последовательность загрузки маршрутизатора и проверку правильности его загрузки;
- определять внутренние компоненты маршрутизаторов Cisco;
- описывать процесс обнаружения образа Cisco IOS;
- проверять и изменять настройки загрузки в конфигурационном регистре.

Порядок загрузки маршрутизатора при включении питания

Во время загрузки маршрутизатор выполняет последовательность процедур: выполняет тесты, находит и загружает программное обеспечение Cisco IOS, находит и загружает конфигурации и, наконец, запускает программное обеспечение Cisco IOS. В этом разделе описывается последовательность событий, имеющих место во время загрузки маршрутизатора.



Последовательность событий, происходящих при включении питания (загрузке) маршрутизатора, очень важна. Знание этой последовательности помогает при выполнении задач эксплуатации и устранении неполадок, связанных с маршрутизатором.

Порядок событий, происходящих при включении питания маршрутизатора, представлен в следующей таблице.

№	Событие	Описание
1.	Самотестирование при включении питания (POST).	Это серия аппаратных тестов, в ходе которых проверяется работоспособность всех компонентов маршрутизатора Cisco. Кроме того, во время этой проверки маршрутизатор определяет текущий состав оборудования. Процедура POST выполняется на основе микрокода из системного ПЗУ.
2.	Загрузка и выполнение кода загрузки.	Код загрузки используется для последовательности действий, таких как обнаружение программного обеспечения Cisco IOS, его загрузка и исполнение. После загрузки и запуска программного обеспечения Cisco IOS код загрузки не используется до следующей перезагрузки или выключения и включения питания.
3.	Поиск программного обеспечения Cisco IOS	Код начальной загрузки определяет местонахождение запускаемого программного обеспечения Cisco IOS. Обычно образ программного обеспечения Cisco IOS находится во флэш-памяти. Конфигурационный регистр и файл конфигурации определяют, где находятся образы программного обеспечения Cisco IOS и какой файл образа использовать.
4.	Загрузка программного обеспечения Cisco IOS	После обнаружения требуемого образа код начальной загрузки распаковывает его в ОЗУ и запускает программное обеспечение Cisco IOS. На некоторых маршрутизаторах образ ПО Cisco IOS не загружается в ОЗУ, а выполняется прямо из флэш-памяти.
5.	Поиск конфигурации.	По умолчанию сохраненный файл конфигурации, startup-config, ищется в энергонезависимой памяти.
6.	Загрузка конфигурации.	Нужная конфигурация маршрутизатора загружается и выполняется. Если конфигурации нет, маршрутизатор запускает программа начальной настройки или AutoInstall, чтобы найти файл конфигурации на TFTP-сервере.
7.	Запуск настроенного ПО Cisco IOS	Маршрутизатор Cisco запускает настроенное программное обеспечение Cisco IOS.

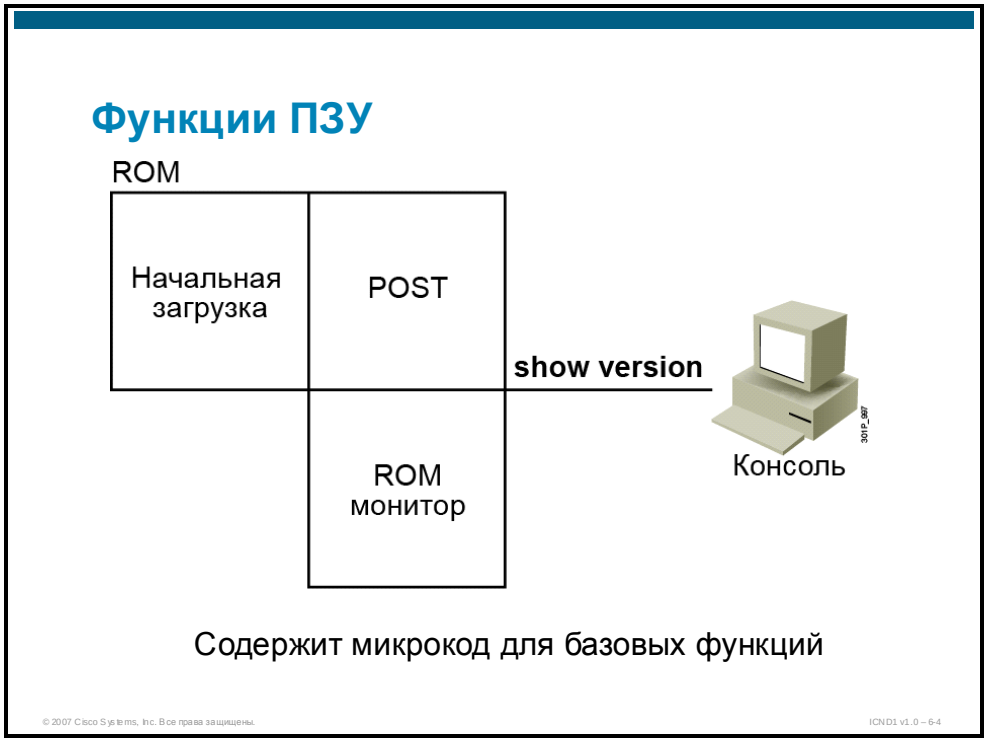
Внутренние компоненты маршрутизатора

Основные внутренние компоненты маршрутизатора Cisco – это интерфейсы, ОЗУ, ПЗУ, флэш-память, энергонезависимая память (NVRAM) и конфигурационный регистр. В этом разделе описываются эти основные внутренние компоненты.

Основные компоненты маршрутизатора представлены на рисунке. Большинство из них представляют собой аппаратные компоненты.

- **ОЗУ (RAM):** В этой памяти с поддержкой записи и чтения содержится программное обеспечение и структуры данных, обеспечивающие работу маршрутизатора. Основное программное обеспечение в ОЗУ – образ программного обеспечения Cisco IOS и текущая конфигурация. В ОЗУ также содержатся таблицы маршрутизации и буферы пакетов. ОЗУ – это энергозависимая память, содержимое которой теряется после отключения питания.
- **ПЗУ (ROM):** В памяти этого типа содержится микрокод основных функций для запуска и обслуживания маршрутизатора, включая код загрузки и процедуры POST. В ПЗУ содержится монитор ROM (ROMMON), обеспечивающий функции аварийного восстановления маршрутизатора, такие как восстановление пароля. В ПЗУ также содержится часть Cisco IOS, которая используется для восстановления файла образа Cisco IOS, например, при удалении файла образа Cisco IOS из флэш-памяти. ПЗУ – это энергонезависимая память, содержимое которой сохраняется и после отключения питания.
- **Флэш-память:** Флэш-память с поддержкой чтения и записи в основном используется для хранения образа программного обеспечения Cisco IOS. На некоторых маршрутизаторах образ программного обеспечения Cisco IOS запускается прямо из флэш-памяти и не требует помещения в ОЗУ. На некоторых часть программного обеспечения Cisco IOS содержится во флэш-памяти, а не в ПЗУ. Флэш-память является энергонезависимой, ее содержимое сохраняется и после отключения питания.

- **Энергонезависимая память (NVRAM):** Эта память с поддержкой чтения и записи в основном используется для хранения файла конфигурации, который называется startup-config. В энергонезависимой памяти используется встроенный аккумулятор для сохранения данных после отключения питания маршрутизатора.
- **Конфигурационный регистр:** Конфигурационный регистр используется для управления загрузкой маршрутизатора. Конфигурационный регистр является частью NVRAM.
- **Интерфейсы:** Интерфейсы – это физические подключения к внешним объектам, некоторые типы интерфейсов перечислены ниже:
  - Ethernet, Fast Ethernet и Gigabit Ethernet;
  - асинхронные и синхронные последовательные подключения;
  - Token Ring
  - распределенный интерфейс передачи данных по волоконно-оптическим каналам (FDDI);
  - ATM;
  - консольные и вспомогательные порты.



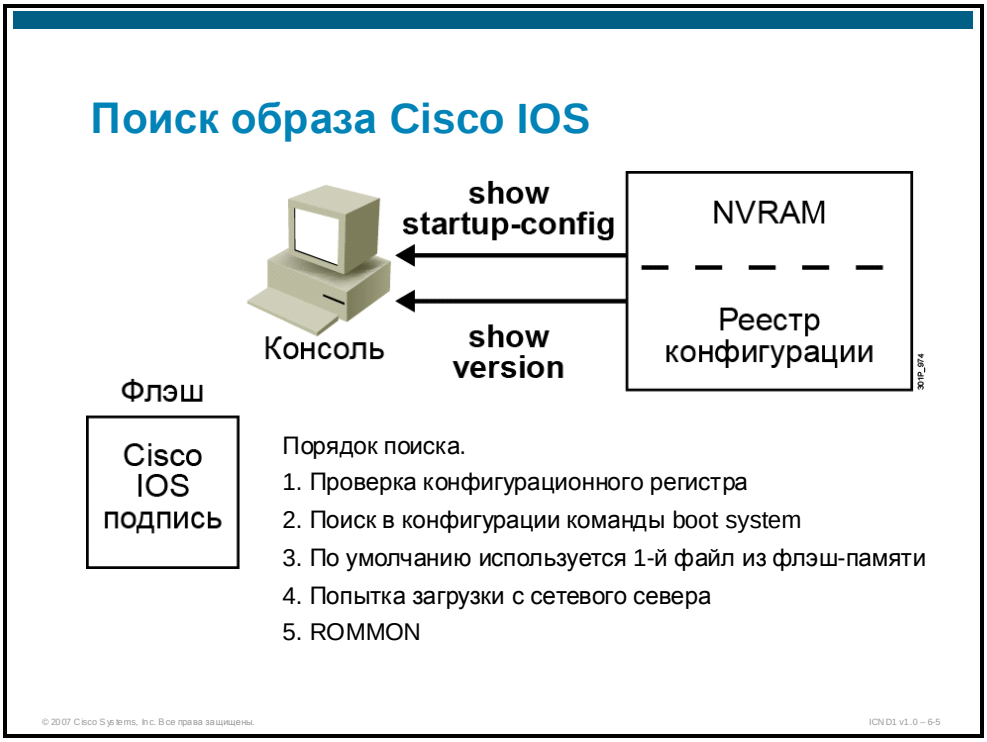
Ниже описываются три основные области микрокода, которые обычно содержатся в ПЗУ.

- **Код загрузки:** Код загрузки используется для активации маршрутизатора во время инициализации. Он считывает значение конфигурационного регистра, чтобы определить способ загрузки, а затем, если есть соответствующие инструкции, загружает программное обеспечение Cisco IOS.
- **POST:** Процедура POST – это микрокод, используемый для тестирования основных функциональных возможностей оборудования маршрутизатора и определения доступных компонентов.
- **ROMMON:** Это низкоуровневая операционная система, обычно используемая для производственного тестирования, устранения неполадок и восстановления пароля. В режиме ROMMON маршрутизатор не поддерживает маршрутизацию и протокол IP.

Примечание	В зависимости от конкретной платформы маршрутизатора Cisco перечисленные компоненты могут храниться во флэш-памяти или в загрузочной памяти, чтобы обеспечить обновление до более поздних версий..

Как устройство обнаруживает и загружает образ Cisco IOS и файлы конфигурации

Во время загрузки маршрутизатор Cisco выполняет поиск образа Cisco IOS в определенном порядке: местоположение, указанное в конфигурационном регистре, флэш-память, TFTP-сервер и ПЗУ. В этом разделе описывается процесс обнаружения образа Cisco IOS.



За обнаружение программного обеспечения Cisco IOS отвечает код загрузки. Он выполняет поиск образа в следующей последовательности.

1. Код загрузки проверяет поле загрузки в конфигурационном регистре. Поле загрузки – это младшие 4 бита конфигурационного регистра, которые используются для указания способа загрузки маршрутизатора. Эти биты могут указывать на флэш-память с образом Cisco IOS, файл загрузочной конфигурации (если есть) с командами, определяющими начальную загрузку маршрутизатора, или удаленный TFTP-сервер. Кроме того, эти биты могут указывать на то, что образа Cisco IOS для загрузки нет и требуется просто загрузить мини-образ Cisco IOS из ПЗУ. Биты конфигурационного регистра также выполняют другие функции, такие как указание скорости обмена данными с консолью в бодах и указание, использовать ли файла конфигурации (startup-config), сохраненный в NVRAM.

   Например, если в конфигурационном регистре содержится значение 0x2102 («0x» указывает на то, что последующие цифры соответствуют шестнадцатеричному представлению), то значение поля загрузки – 0x2 (правая цифра значения регистра – 2, представляющая нижние 4 бита регистра).

2. Если поле загрузки конфигурационного регистра содержит значения в пределах от 0x2 до 0xF, код загрузки анализирует файл загрузочной конфигурации в энергонезависимой памяти, чтобы найти команды **boot system**, в которых указывается имя и расположение загружаемого образа программного обеспечения Cisco IOS. Может быть введена последовательность из нескольких команд **boot system** для создания плана отказоустойчивой загрузки.

   Команда **boot system** – это команда глобальной конфигурации, которая позволяет указывать источник загружаемого образа программного обеспечения Cisco IOS. Доступно несколько вариантов синтаксиса, в том числе:

   — **boot system flash** [*имя_файла*]

   — **boot system tftp** [*имя_файла*][*адрес-сервера*]

   — **boot system rom**

3. Если в конфигурации нет команд **boot system**, маршрутизатор по умолчанию загружает первый допустимый образ Cisco IOS из флэш-памяти и запускает его.

4. Если допустимый образ Cisco IOS не находится в флэш-памяти, маршрутизатор пытается выполнить загрузку с сетевого TFTP-сервера, используя значение поля загрузки как часть имени файла образа Cisco IOS.

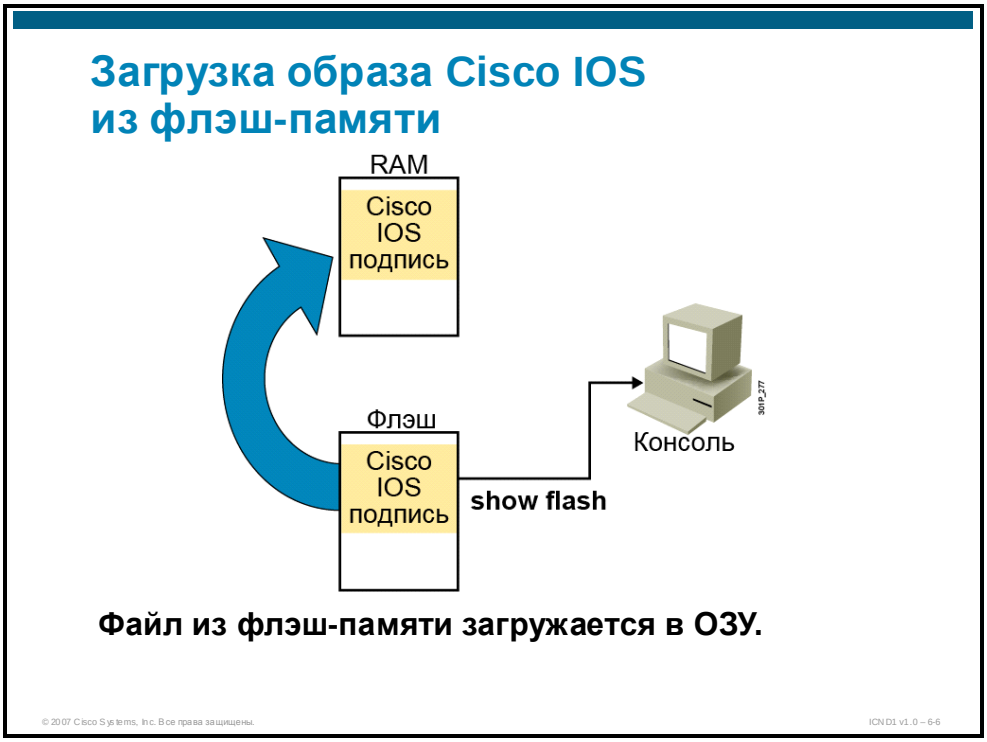
Примечание Загрузка образа программного обеспечения Cisco IOS с сетевого TFTP-сервера используется редко.

Примечание Не на каждом маршрутизаторе есть вспомогательный образ загрузки, поэтому шаги 5 и 6 выполняются не всегда.

---

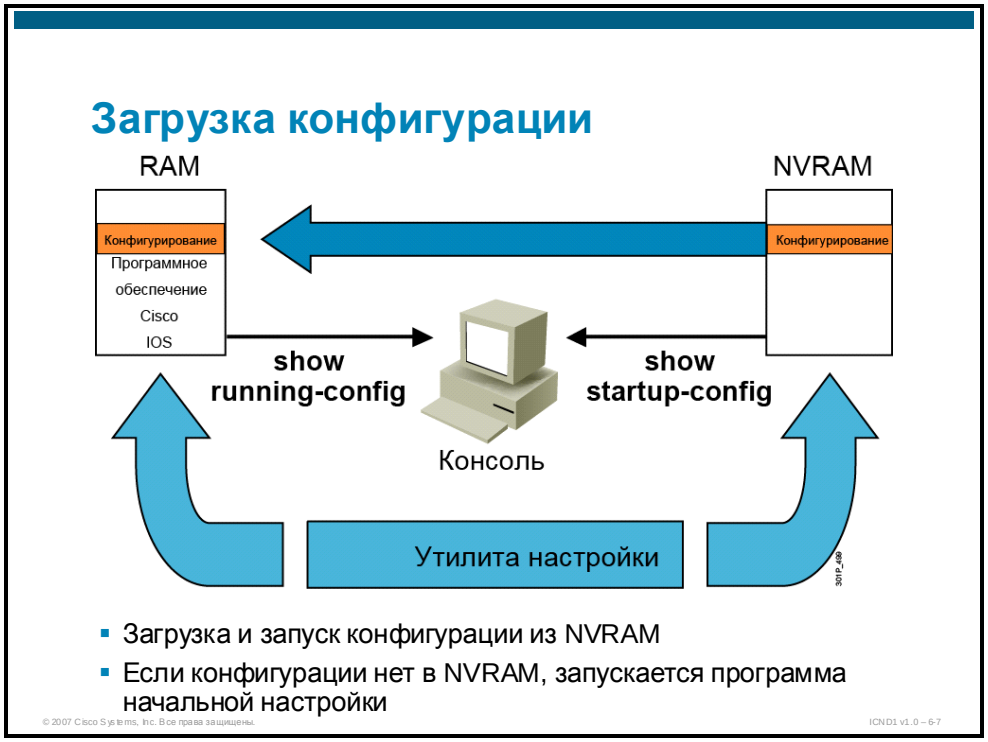
5. По умолчанию после пяти неудачных попыток загрузки с сетевого TFTP-севера маршрутизатор загружает из ПЗУ вспомогательный образ загрузки (мини-образ Cisco IOS). Пользователь также может задать значение 0 для 13-го бита конфигурационного регистра, чтобы маршрутизатор непрерывно пытался загрузиться с TFTP-сервера без загрузки из ПЗУ мини-образ Cisco IOS после пяти неудачных попыток.

6. Если вспомогательного образа загрузки нет или он поврежден, маршрутизатор попытается загрузить ROMMON из ПЗУ.



Когда маршрутизатор находит допустимый файл образа Cisco IOS во флэш-памяти, этот образ загружается в ОЗУ для выполнения. На некоторых маршрутизаторах, включая маршрутизаторы серии Cisco 2500, недостаточно ОЗУ для хранения образа Cisco IOS, поэтому образ Cisco IOS выполняется напрямую из флэш-памяти.

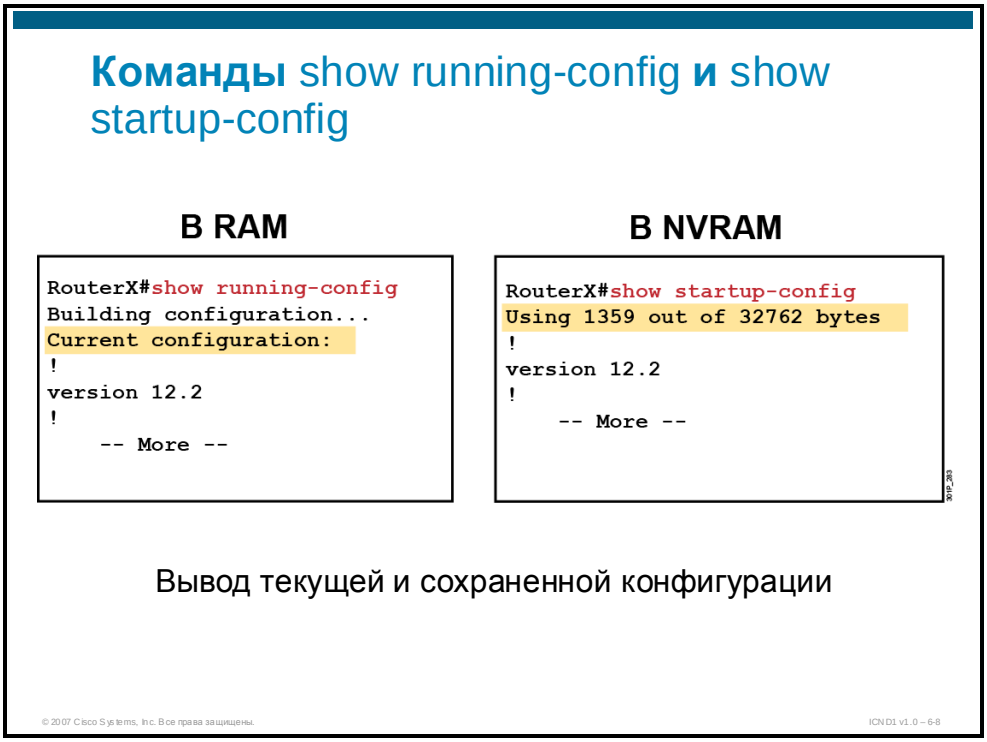
Перед загрузкой образа из флэш-памяти в ОЗУ его необходимо распаковать. После распаковки файла в ОЗУ он запускается. Образы Cisco IOS, выполняющиеся из флэш-памяти, не сжаты.



После загрузки и запуска образа программного обеспечения Cisco IOS маршрутизатор необходимо настроить. Если в NVRAM сохранен файл конфигурации (startup-config), он выполняется. Если файл конфигурации не сохранен, маршрутизатор запускает AutoInstall или программа начальной настройки.

AutoInstall пытается загрузить конфигурацию с TFTP-сервера. Для использования AutoInstall требуется подключение к сети и предварительно настроенный TFTP-сервер для ответа на запрос загрузки.

Программа начальной настройки запрашивает ввод данных конфигурации с консоли, чтобы создать базовую начальную конфигурацию для маршрутизатора.



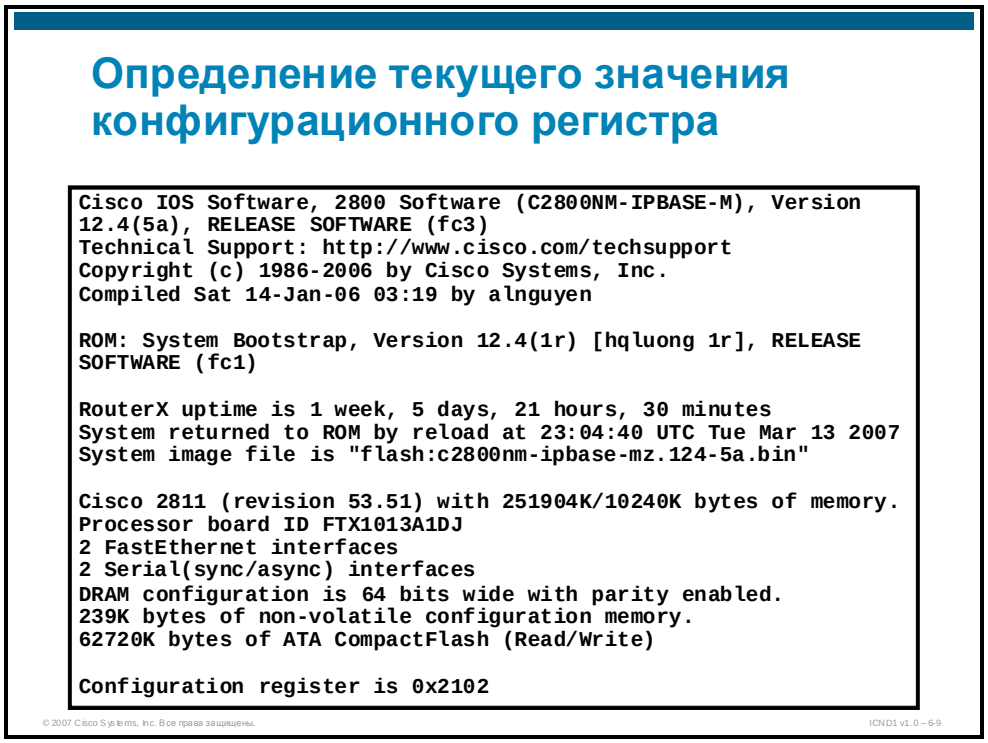
Команды **show running-config** и **show startup-config** входят в число наиболее часто используемых команд программного обеспечения Cisco IOS, так как они позволяют выводить текущую конфигурацию маршрутизатора из ОЗУ и загрузочную конфигурацию из файла в NVRAM, который маршрутизатор будет использовать при следующем перезапуске.

Если отображаются слова «Current configuration» (текущая конфигурация), то на экране представлена активная конфигурации из ОЗУ.

Если в верхней части экрана выведено сообщение об объеме используемой энергонезависимой памяти, то отображается файла конфигурации загрузки из NVRAM.

Конфигурационный регистр

Конфигурационный регистр указывает местонахождение образа программного обеспечения Cisco IOS. Содержимое данного регистра можно вывести с помощью команды **show version**, а для изменения значения регистра используется команда глобальной конфигурации **config-register**. В этом разделе описывается вывод и изменение информации о загрузке в конфигурационном регистре.

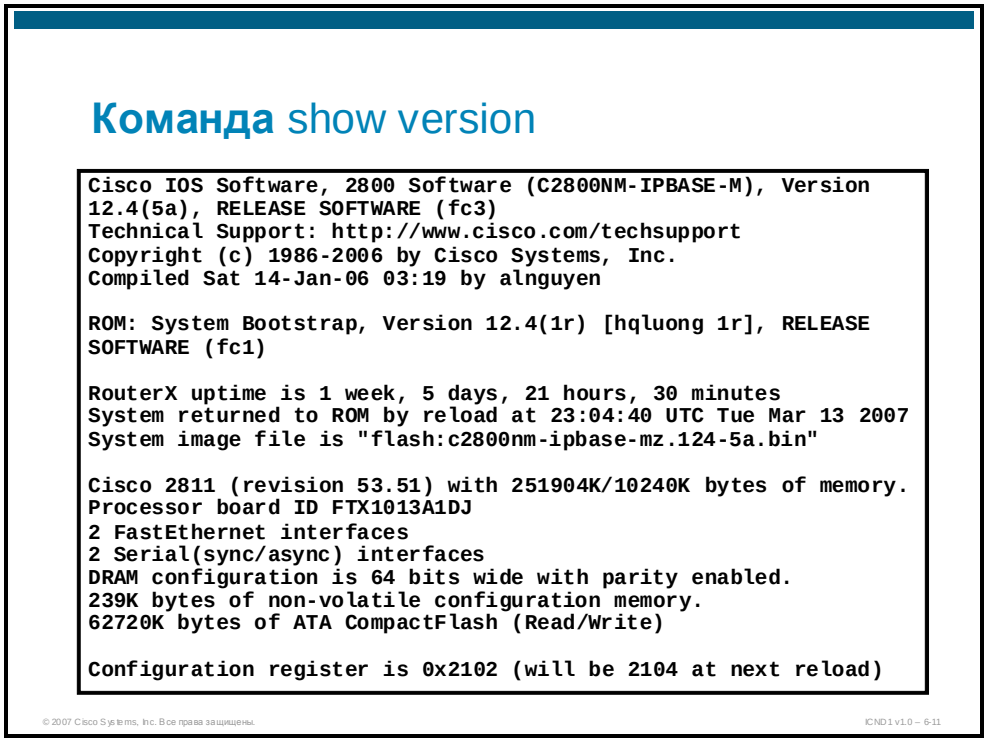


Перед изменением конфигурационного регистра следует определить, как маршрутизатор загружает образ программного обеспечения в данный момент. Команда **show version** отображает текущее значение конфигурационного регистра. Значение конфигурационного регистра содержится в последней строке на экране.

Значение конфигурационного регистра по умолчанию можно изменить с помощью команды глобальной конфигурации **config-register**. Конфигурационный регистр – это 16-разрядный регистр. 4 младших бита конфигурационного регистра (биты 3, 2, 1 и 0) образуют поле загрузки. При задании значения конфигурационного регистра в качестве параметра указывается шестнадцатеричное число. Значение конфигурационного регистра по умолчанию – 0x2102.

Ниже приводятся рекомендации по изменению поля загрузки.

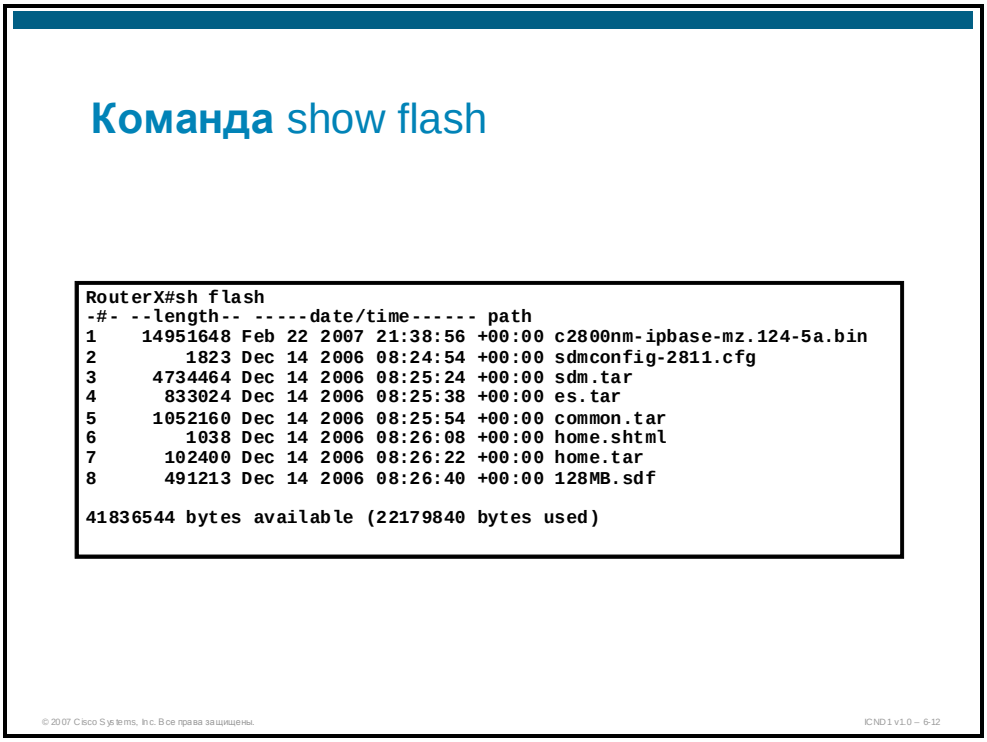
- Полю загрузки назначается значение 0 для автоматического перехода в режим ROMMON. Это значение устанавливает биты поля загрузки в состояние 0000. В режиме ROMMON маршрутизатор отображает строку приглашения «>» или «rommon>» в зависимости от типа маршрутизатора. В режиме ROMMON можно использовать команду **boot** для загрузки маршрутизатора вручную.
- Полю загрузки назначается значение 1, чтобы настроить систему на автоматическую загрузку мини-образа Cisco IOS из ПЗУ. Биты поля загрузки устанавливаются в состояние 0001. В этом режиме маршрутизатор отображает строку приглашения «Router(boot)>».
- Полю загрузки назначается любое значение от 0x2 до 0xF, чтобы настроить систему на использование команд **boot system** из файла загрузочной конфигурации из NVRAM. Значение по умолчанию – 0x2. Эти значения устанавливают биты поля загрузки в состояние 1111.



Команда **show version** используется для проверки изменений значения конфигурационного регистра. Новое значение конфигурационного регистра вступает в силу при перезагрузке маршрутизатора.

В рассмотренном примере вывод команды **show version** указывает, что при следующей перезагрузке маршрутизатора будет использоваться значение конфигурационного регистра – 0x2104.

Примечание	При использовании команды **config-register** задаются все 16 бит конфигурационного регистра. Следует соблюдать осторожность и изменять только те биты, которые требуется изменить, например, поле загрузки, а остальные биты оставлять без изменения. Следует помнить, что другие биты конфигурационного регистра выполняют функции, такие как выбор скорости обмена данными с консолью в бодах и пропуск файла конфигурации, сохраненного в NVRAM.



Команда **show flash** выводит на экран содержимое флэш-памяти, включая имена и размеры файлов образов.

В рассматриваемом примере в нижней строке указывается объем доступной флэш-памяти. Некоторая ее часть может быть занята.

Резюме

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

Резюме

- Во время загрузки маршрутизатор выполняет тесты, находит и загружает ПО и конфигурацию, а также запускает это ПО.
- Основные внутренние компоненты маршрутизатора - это ОЗУ, ПЗУ, флэш-память, энергонезависимая память и конфигурационный регистр.
- Во время загрузки маршрутизатор ищет образ Cisco IOS в определенном порядке: местоположение, указанное в конфигурационном регистре, флэш-память, TFTP-сервер и ПЗУ.
- Конфигурационный регистр указывает местоположение образа программного обеспечения Cisco IOS. Значение регистра можно вывести с помощью команды **show version** и изменить с помощью команды глобальной конфигурации **config-register**.

Занятие 3

Управление устройствами Cisco

Обзор

Качественное управление образами Cisco IOS и файлами конфигурации снижает время простоя устройств и соответствует передовой практике. Файлы образов Cisco IOS содержат программное обеспечение Cisco IOS, необходимое для работы устройства Cisco, а в файлах конфигурации содержатся заданные пользователем команды конфигурации для функционирования устройства Cisco. На этом занятии описываются процедуры и команды, необходимые для управления образами Cisco IOS, файлами конфигурации и сетевыми устройствами.

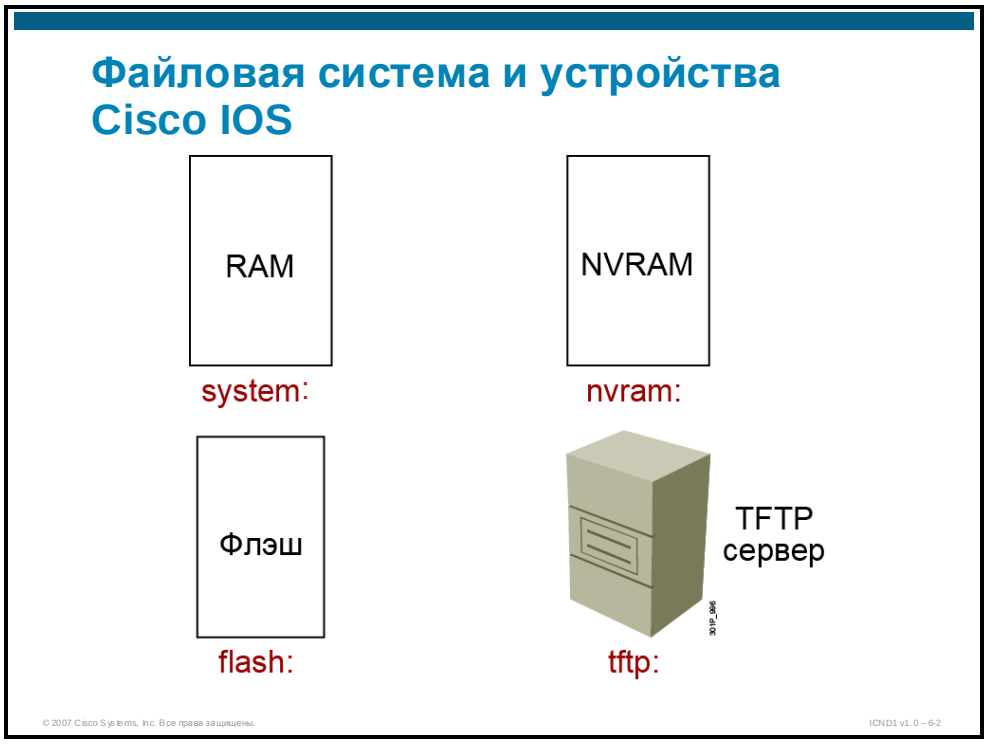
Задачи

По окончании этого занятия вы сможете управлять образами Cisco IOS, файлами конфигурации и сетевыми устройствами. Это значит, что вы сможете выполнять следующие задачи:

- описывать файловые системы, используемые маршрутизаторами Cisco;
- управлять файлами образов Cisco IOS для поддержки доступности этих образов;
- управлять файлами конфигурации устройств для сокращения времени простоя;
- использовать команду **copy** для перемещения конфигураций;
- использовать команды и процедуры для устранения неполадок, для минимизации любого потенциального негативного воздействия на устройства Cisco.

Файловая система и устройства Cisco IOS

Файловая система Cisco IOS (Cisco IFS) предоставляет единый интерфейс доступа ко всем файловым системам, используемых маршрутизатором. В этом разделе описываются файловые системы, используемые маршрутизаторами Cisco.



Файловая система Cisco IFS предоставляет единый интерфейс ко всем файловым системам, используемым маршрутизатором, включая следующие.

- Файловые системы флэш-памяти.
- Сетевые файловые системы: TFTP, Remote Copy Protocol (RCP) и FTP. (В этом занятии обсуждаются только команды, используемые для обмена образами Cisco IOS и файлами конфигурации с TFTP-сервером.)
- Любые другие конечные точки для чтения или записи данных (такие как энергонезависимая память, рабочая конфигурация в ОЗУ и т. д.)

Одна из ключевых возможностей Cisco IFS – использование стандарта URL для указания файлов на сетевых устройствах и других ресурсах сети.

В следующей таблице приводятся некоторые широко используемые URL-префиксы для сетевых устройств Cisco.

Префикс	Описание
bootflash:	Загрузочная флэш-память.
flash:	Флэш-память. Этот префикс доступен на всех платформах. На платформах, на которых нет устройства с именем flash, для префикса flash: используется псевдоним slot0. Поэтому префикс flash: можно использовать для ссылки на основную область хранения во флэш-памяти на всех платформах.
flh:	Вспомогательные файлы журналов загрузки из флэш-памяти.

Префикс	Описание
ftp:	Сетевой FTP-сервер.
nvram:	NVRAM.
rcp:	Сетевой RCP-сервер.
slot0:	Первая карта флэш-памяти PCMCIA.
slot1:	Вторая карта флэш-памяти PCMCIA.
system:	Указывает на системную память с текущей рабочей конфигурацию.
tftp:	Сетевой TFTP-сервер.

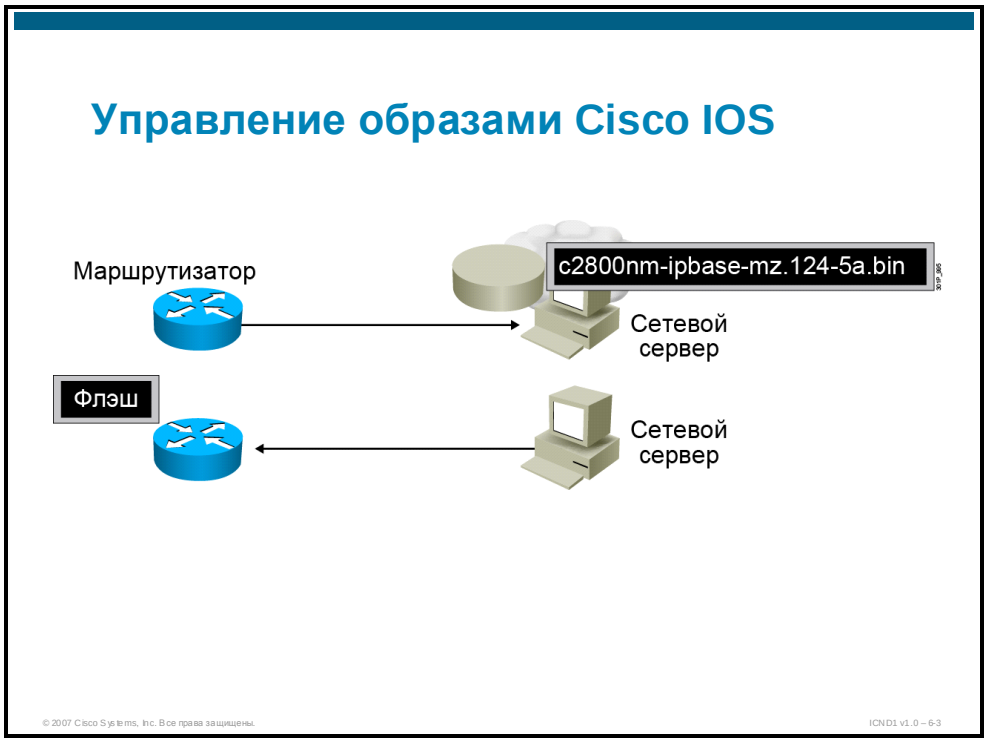
В Cisco IOS Release 12.0 команды, используемые для копирования и передачи файлов конфигурации или системных файлов, изменены, в соответствии с новой спецификацией Cisco IFS.

В таблице ниже представлены команды версий Cisco IOS, предшествующих Release 12.0 и Cisco IOS Release 12.0 и выше, используемые для перемещения и управления файлами конфигурации. Обратите внимание, что в командах Cisco IOS Release 12.0 и выше путь к файлам конфигурации указывается после двоеточия в следующем формате: [[[//местоположение]/каталог]/имя_файла].

Команды Cisco IOS до Release 12.0	Команды Cisco IOS Release 12.0 или выше
configure network (до Cisco IOS Release 10.3) **copy rcp running-config** **copy tftp running-config**	**copy ftp: system:running-config** **copy rcp: system:running-config** **copy tftp: system:running-config**
configure overwrite-network (до Cisco IOS Release 10.3) **copy rcp startup-config** **copy tftp startup-config**	**copy ftp: nvram:startup-config** **copy rcp: nvram:startup-config** **copy tftp: nvram:startup-config**
show configuration (до Cisco IOS Release 10.3) **show startup-config**	**more nvram:startup-config**
write erase (до Cisco IOS Release 10.3) **erase startup-config**	**erase nvram:**
write memory (до Cisco IOS Release 10.3) **copy running-config startup-config**	**copy system:running-config nvram:startup-config**
write network (до Cisco IOS Release 10.3) **copy running-config rcp** **copy running-config tftp**	**copy system:running-config ftp:** **copy system:running-config rcp:** **copy system:running-config tftp:**
write terminal (до Cisco IOS Release 10.3) **show running-config**	**more system:running-config**

Управление образами Cisco IOS

В условиях роста сети хранение образов программного обеспечения Cisco IOS и файлов конфигурации на центральном TFTP-сервере позволяет управлять числом и версиями образов Cisco IOS и файлами конфигурации, которые необходимо поддерживать. В этом разделе описывается создание и загрузка резервной копии образа Cisco IOS с TFTP-сервера в случае потери образа Cisco IOS на маршрутизаторе.



Производственные интерсети обычно занимают обширные области и содержат несколько маршрутизаторов. В любой сети всегда разумно хранить резервную копию образа программного обеспечения Cisco IOS на случай повреждения или случайного удаления системного образа на маршрутизаторе.

Маршрутизаторам, находящимся на большом расстоянии друг от друга, необходим источник или место для хранения резервных образов программного обеспечения Cisco IOS. Использование сетевого TFTP-сервера позволяет загружать файлы образов и конфигураций по сети. Такой TFTP-сервер может быть маршрутизатором, рабочей станцией или хостом.

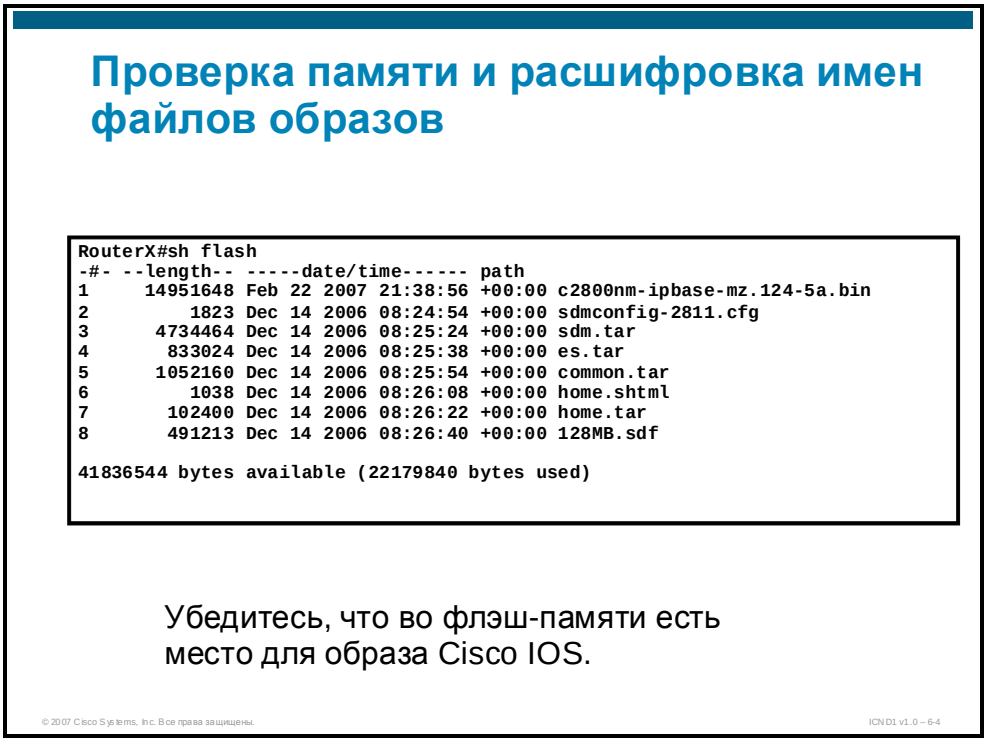
Перед копированием образов программного обеспечения Cisco IOS из флэш-памяти маршрутизатора на сетевой TFTP-сервер следует выполнить следующие действия.

Действие 1 Убедитесь в доступности TFTP-сервера. Для проверки связи с TFTP-сервером можно использовать ping.

Действие 2 Убедитесь, что на диске TFTP-сервера достаточно места для размещения образа программного обеспечения Cisco IOS. Для определения размера файла образа Cisco IOS можно воспользоваться командой **show flash:** на маршрутизаторе.

Действие 3 Проверьте требования к именам файлов на TFTP-сервере. Они могут отличаться в зависимости от того, какая ОС используется на сервере – Microsoft Windows, UNIX или другая.

Действие 4 При необходимости создайте файл назначения, в который будет загружен файл. Это действие зависит от операционной системы сетевого сервера.



Команда **show flash** является важным средством сбора информации о флэш-памяти маршрутизатора и файле образа. Команда **show flash** позволяет получать следующие данные:

- общий объем флэш-памяти на маршрутизаторе;
- объем доступной флэш-памяти;
- имена всех файлов, хранящихся во флэш-памяти.

Имя файла образа Cisco IOS состоит из нескольких частей, каждая из которых имеет определенное значение. Например, в имени на рисунке «c2800nm-ipbase-mz.124-5a.bin» содержится следующая информация.

- Первая часть имени образа идентифицирует платформу, на которой выполняется образ. В данном примере это платформа c2800.
- Вторая часть имени указывает место запуска образа и сжатие файла. В данном примере «mz» означает, что файл сжат и запускается из ОЗУ.
- В третьей части имени указывается номер версии. В данном примере номер версии 124-5a.
- Последняя часть имени – расширение файла. Расширение .bin означает, что это двоичный исполняемый файл.

Стандарты именования ПО Cisco IOS, значения полей, содержимое образов, и другие сведения могут меняться. За обновлениями можно обратиться к торговым представителям или дистрибьюторам Cisco. Кроме того, можно посетить веб-сайт Cisco.com.

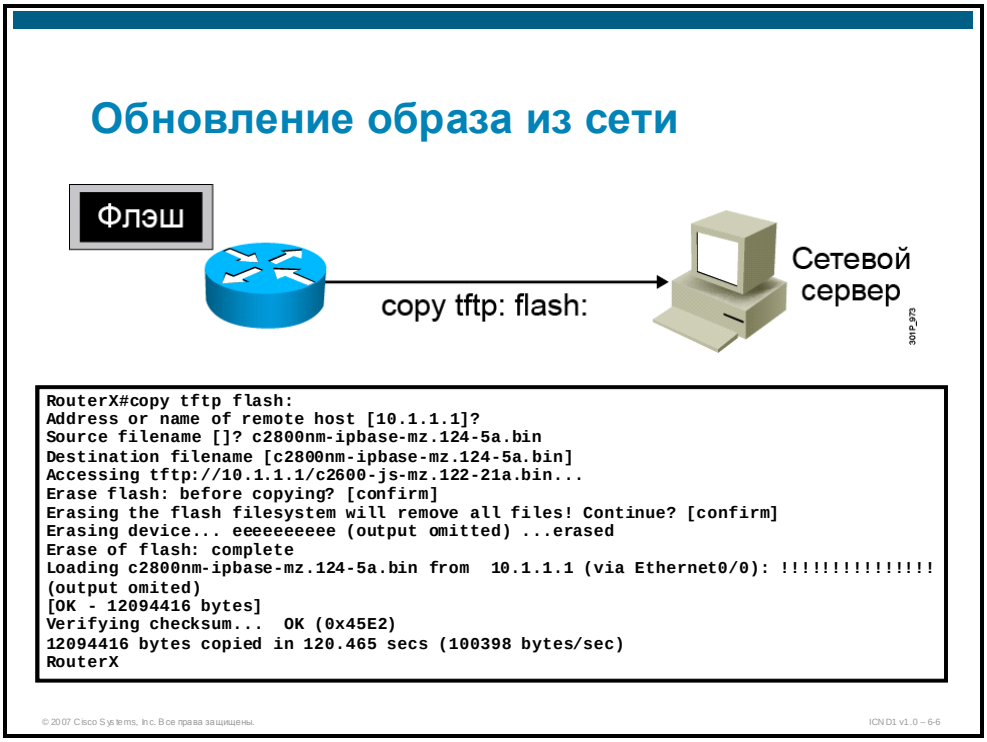
Резервная копия файла образа программного обеспечения создается путем копирования файла образа с маршрутизатора на сетевой TFTP-сервер. Чтобы скопировать текущий системный файл образа с маршрутизатора на сетевой TFTP-сервер, используйте следующую команду в привилегированном режиме EXEC:

```
Router#copy flash: tftp:
```

В команде **copy flash: tftp:** необходимо указать IP-адрес удаленного хоста, а также имена исходного и конечного системных файлов образов.

Восклицательные знаки (!!!…) указывают на процесс копирования из флэш-памяти маршрутизатора на TFTP-сервер. Каждый восклицательный знак (!) означает успешную передачу одного UDP-сегмента.

Перед размещением во флэш-памяти нового образа Cisco IOS текущий образ Cisco IOS следует скопировать на TFTP-сервер. Резервное копирование обеспечивает резерв на случай, когда во флэш-памяти достаточно места только для одного образа.



При обновлении системы на новую версией программного обеспечения на маршрутизатор необходимо загрузить другой системный файл образа. Для загрузки нового образа с сетевого TFTP-сервера используйте следующую команду:

```
Router#copy tftp: flash:
```

При выполнении этой команды запрашивается IP-адрес удаленного хоста, а также имена исходного и конечного системных файлов образов. Введите имя файла образа обновления так, как оно отображается на сервере.

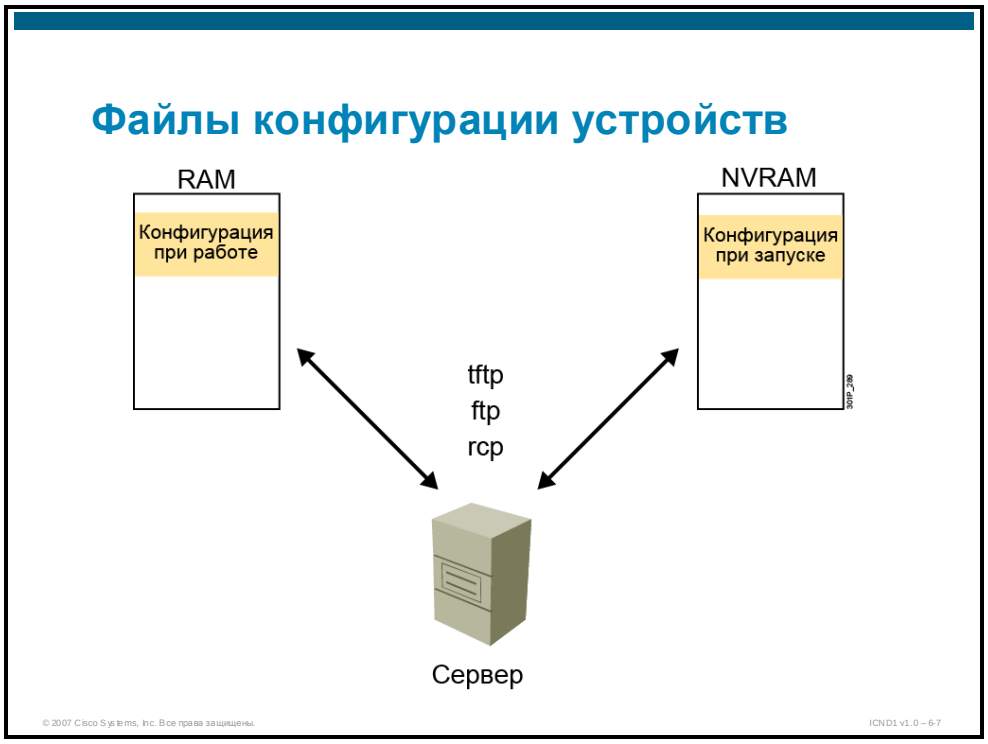
После подтверждения ввода данных запрашивается подтверждение очистки флэш-памяти. При очистке флэш-памяти освобождается место для нового образа. Очищайте флэш-память, если ее объема недостаточно для нескольких образов Cisco IOS. Если доступной свободной флэш-памяти нет, то перед копированием новых файлов необходимо выполнить процедуру очистки. Система информирует пользователя об этих условиях и запрашивает ответ.

Каждый восклицательный знак (!) означает успешную передачу одного UDP-сегмента.

Примечание	Обязательно загружайте образ Cisco IOS, соответствующий платформе маршрутизатора. Если загружен неверный образ Cisco IOS, маршрутизатор может перестать загружаться, требуя вмешательства через ROM-монитор (ROMMON).

Управление файлами конфигурации устройств

В файлах конфигурации устройства содержатся заданные пользователем команды конфигурации функций устройства Cisco. В этом разделе описываются файлы конфигурации и их расположение.



В файлах конфигурации содержатся команды ПО Cisco IOS, используемые для настройки функций маршрутизирующего устройства Cisco, например маршрутизатора, сервера доступа, коммутатора и т. д. При загрузке системы из файла загрузочной конфигурации или при вводе команд в режиме конфигурации интерфейса командной строки выполняется синтаксический разбор команд, т. е., они преобразуются и выполняются программным обеспечением Cisco IOS.

Файлы конфигурации хранятся в следующих местах:

- Текущая конфигурация хранится в ОЗУ.
- Загрузочная конфигурация хранится в NVRAM.

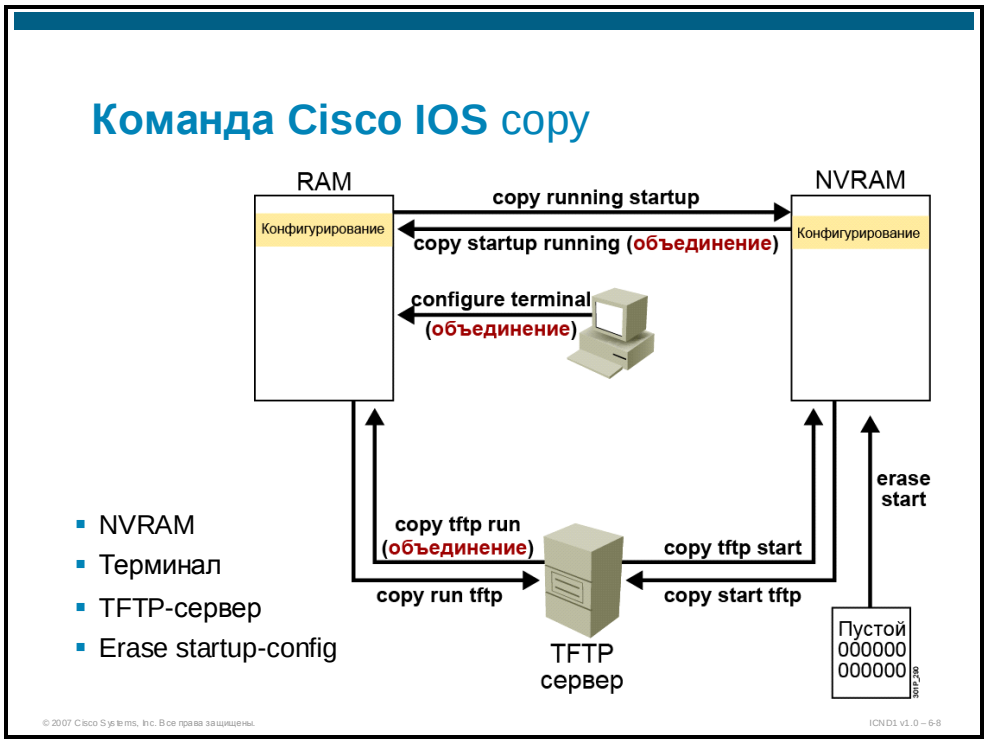
Файлы конфигурации можно скопировать с маршрутизатора на файловый сервер с помощью протоколов FTP, RCP или TFTP. Например, перед изменением содержимого текущего файла конфигурации его можно скопировать на сервер, что позволит восстановить исходный файл конфигурации с сервера. Тип используемого протокола зависит от типа используемого сервера.

Файлы конфигурации можно скопировать с TFTP-, RCP- или FTP-сервера в ОЗУ в текущую конфигурацию или в файл загрузочной конфигурации в NVRAM маршрутизатора в следующих целях:

- Чтобы восстановить резервную копию файла конфигурации.
- Чтобы использовать этот файл конфигурации на другом маршрутизаторе. Например, при добавлении к сети нового маршрутизатора может потребоваться, чтобы его конфигурация совпадала с конфигурацией исходного маршрутизатора. Копирование файла конфигурации с сетевого сервера и внесение изменений, отражающих требования к настройке нового маршрутизатора, позволяет сэкономить время, избежав создания полного файла.
- Чтобы загрузить один набор команд конфигурации на все маршрутизаторы сети для обеспечения единообразия их конфигураций.

Команда copy ПО Cisco IOS

Команда **copy** программного обеспечения Cisco IOS используется для перемещения конфигураций между компонентами или устройствами, такими как ОЗУ, энергонезависимая память и TFTP-сервер. В этом разделе описывается использование команд **copy**.



Кроме AutoInstall, программы установки и интерфейса командной строки для загрузки и создания конфигурации можно использовать несколько других источников.

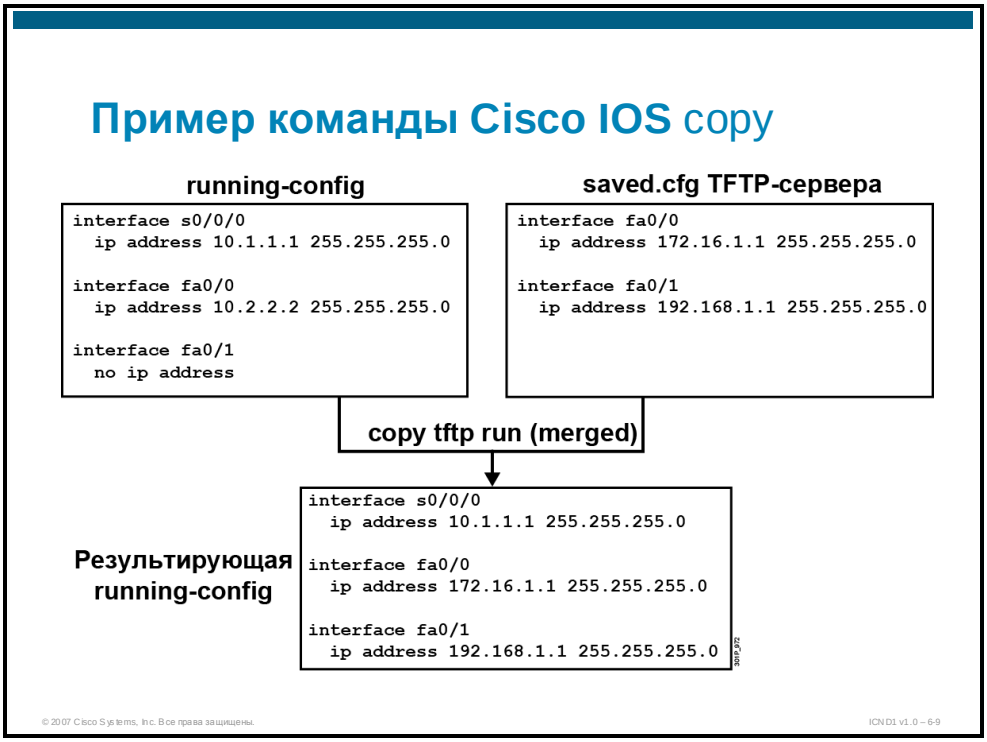
Команду **copy** ПО Cisco IOS можно использовать для перемещения конфигураций с одного компонента или устройства в другое. Согласно синтаксису команды **copy** в качестве первого аргумента необходимо указать источник (откуда конфигурация копируется), а за ним – назначение (куда конфигурация копируется). Например, при выполнении команды **copy running-config: tftp:** текущая конфигурация копируется из ОЗУ на TFTP-сервер.

Команда **copy running-config: startup-config:** используется после изменения конфигурации в ОЗУ, чтобы сохранить изменения в файле загрузочной конфигурации в NVRAM. Аналогично файл загрузочной конфигурации из NVRAM копируется обратно в ОЗУ с помощью команды **copy startup running:**. Обратите внимание, что команды можно сокращать.

Существуют аналогичные команды для копирования между TFTP-сервером и NVRAM или ОЗУ.

Команда **configure terminal:** используется для интерактивного создания конфигурации в ОЗУ с консоли или удаленного терминала.

Команда **erase startup-config:** используется для удаления файла загрузочной конфигурации из NVRAM.



На рисунке показан пример использования команды **copy tftp run** для объединения текущей конфигурации в ОЗУ с файлом конфигурации, сохраненным TFTP-сервере.

Примечание	При копировании конфигурации в ОЗУ из любого источника она объединяется с существующей в ОЗУ конфигурацией или накладывается на нее (без перезаписи). Новые параметры конфигурации добавляются, а изменения существующих параметров перезаписываются вместо старых значений. Команды конфигурации в ОЗУ, для которых нет соответствующих команд в NVRAM, остаются без изменений. При копировании конфигурации из ОЗУ в NVRAM файл загрузочной конфигурации перезаписывается.

Команды copy run tftp и copy tftp run

```
RouterX#copy running-config tftp:
Address or name of remote host []? 10.1.1.1
Destination filename [running-config]? wgroa.cfg
.!!
1684 bytes copied in 13.300 secs (129 bytes/sec)

RouterX#copy tftp: running-config
Address or name of remote host []? 10.1.1.1
Source filename []? wgroa.cfg
Destination filename [running-config]?
Accessing tftp://10.1.1.1/wgroa.cfg...
Loading wgroa.cfg from 10.1.1.1 (via Ethernet0): !
[OK - 1684/3072 bytes]

1684 bytes copied in 17.692 secs (99 bytes/sec)
```

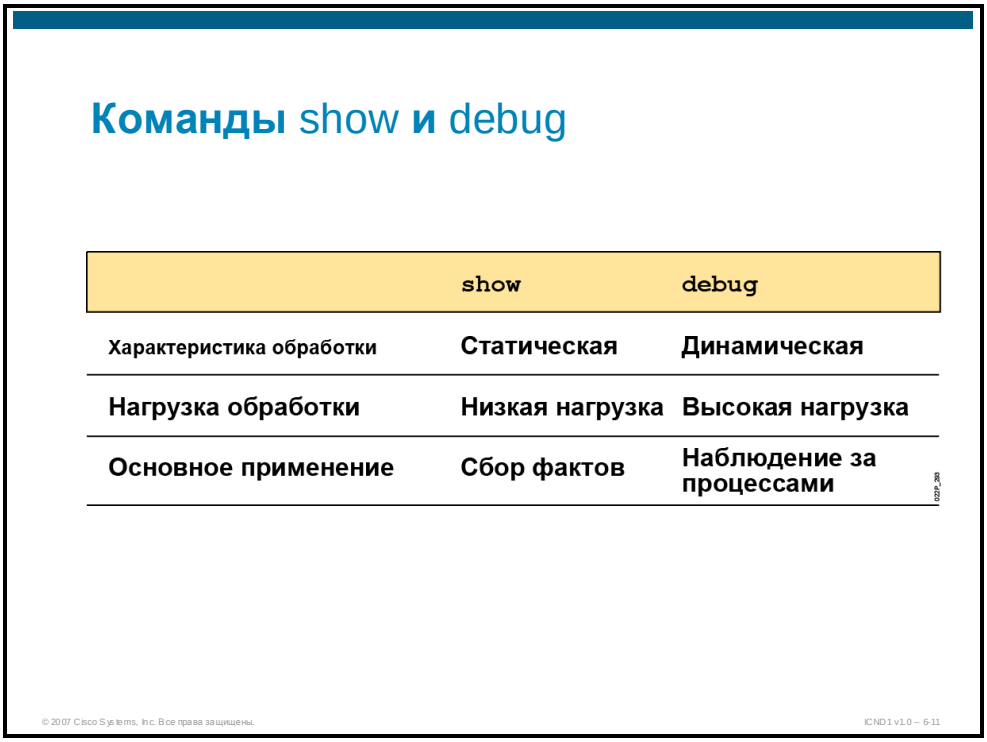

TFTP-серверы можно использовать для хранения конфигураций на центральном узле для централизованного управления и обновления. Независимо от размера сети следует хранить резервную копию текущей конфигурации.

Команда **copy running-config tftp:** позволяет сохранить текущую конфигурацию на TFTP-сервере. В данном случае необходимо указать IP-адрес или имя TFTP-сервера и имя файла назначения. На экране процесс загрузки отображается серией восклицательных знаков.

Команда **copy tftp: running-config** используется для загрузки файла конфигурации с TFTP-сервера в ОЗУ в качестве текущей конфигурации. В данном случае также необходимо указать IP-адрес или имя TFTP-сервера и имена исходного и конечного файлов. Так как файл копируется в текущую конфигурацию, имя файла назначения должно быть running-config. Это процесс слияния, а не перезаписи.

Использование команд show и debug на устройствах Cisco

Команды **show** и **debug** – встроенные средства устранения неполадок. Команда **show** используется для вывода статической информации, а команда **debug** – для отображения динамических данных и событий. В этом разделе сравниваются команды **show** и **debug** и предоставляются рекомендации по использованию команд **debug**.

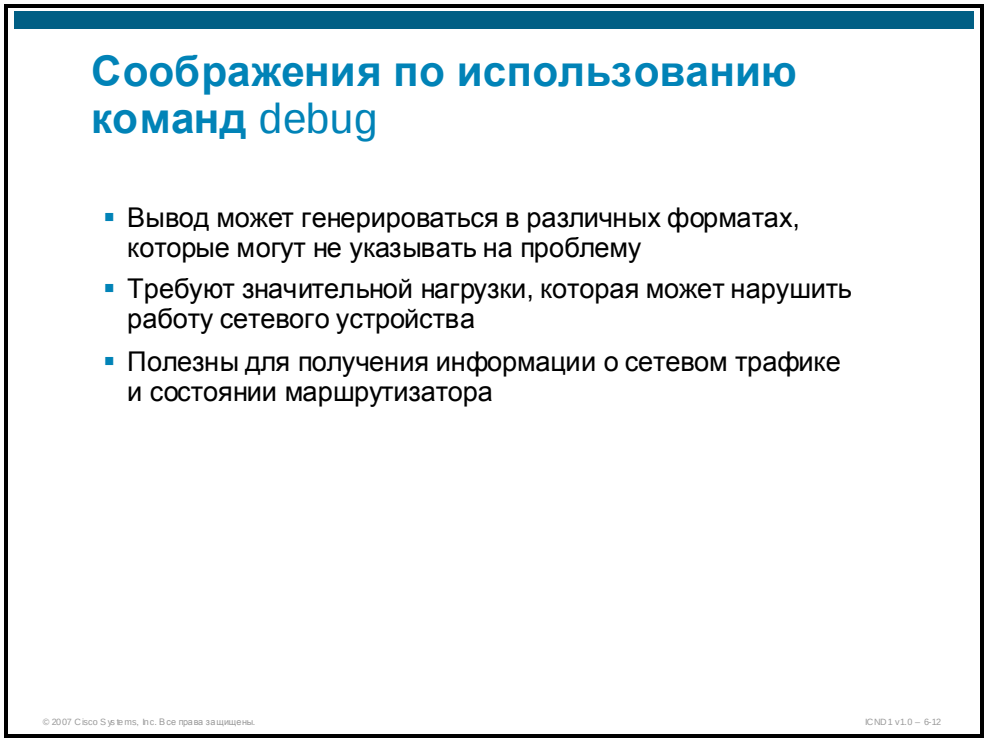


Команды **show** и **debug** выполняют следующие функции:

- **show:** предоставляет данные о текущих проблемах с интерфейсами, средой или производительностью сети.
- **debug:** используется для поиска в потоке трафика протоколов неполадок, ошибок протоколов или ошибок в конфигурации.

В следующей таблице описываются основные различия между командами **show** и **debug**.

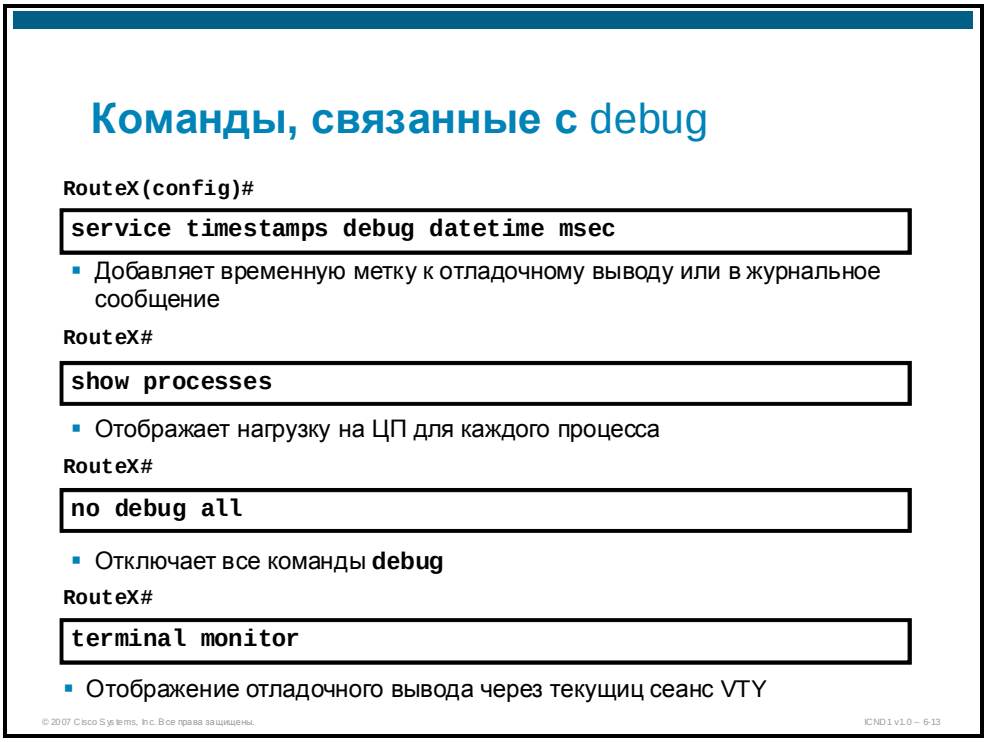
Команда	Описание
show	Предоставляет статический набор данных о состоянии сетевого устройства, соседних устройств и производительности сети. Команды **show** используются для сбора сведений для изоляции неполадок в системе локальных сетей, включая неполадки с интерфейсами, узлами, средой, серверами, клиентами или приложениями.
debug	Выдает поток информации о трафике, проходящем через интерфейсы, сообщениях об ошибках, создаваемых сетевыми узлами, диагностических пакетах конкретных протоколов и другие данные, полезные при устранении неполадок. Команды **debug** используются для просмотра операций на маршрутизаторе или в сети и проверки потока событий или пакетов.



Команды **debug** используются для изоляции неполадок, а не для мониторинга нормальной работы сети. Так как применение команд **debug** вызывает значительную нагрузку, которая может нарушить работу маршрутизатора, команды **debug** следует использовать только для поиска специальных типов трафика или проблем, которые разделены на группы наиболее вероятных причин.

Ниже обсуждаются некоторые аспекты использования команд **debug**:

- Следует помнить о том, что команды **debug** могут создавать большое количество данных, малополезных для решения конкретной проблемы. Обычно для правильной интерпретации выходных отладочных данных необходимо знать, отладка каких протоколов выполняется.
- Так как применение команд **debug** вызывает значительную нагрузку на ЦП, которая может нарушить работу сетевого устройства, команды **debug** следует использовать только для поиска специальных типов трафика или проблем, которые разделены на группы наиболее вероятных причин.
- При использовании команд **debug** следует помнить о том, что форматы вывода зависят от протокола. Для каждого пакета может создаваться одна строка вывода или несколько строк.
- Некоторые команды **debug** создают большой объем вывода, при выполнении других команд вывод может генерироваться только в отдельных случаях. Некоторые команды создают строки текста, другие – информацию в виде полей.
- Команды **debug** рекомендуется использовать для получения информации о сетевом трафике и состоянии маршрутизатора. Такие команды следует применять с большой осторожностью.
- Если у вас есть сомнения в последствиях использования команд **debug**, на веб-сайте http://www.cisco.com можно получить более подробные сведения или проконсультироваться у представителей службы технической поддержки.



В следующей таблице перечисляются команды, которые можно использовать вместе с командами **debug**.

Команда	Описание
service timestamps	Эта команда используется для добавления временной метки в сообщение команды **debug** или в журнальное сообщение. Это позволяет получить ценную информацию о времени выполнения элементов отладки и интервале между событиями.
show processes	Отображает нагрузку на ЦП для каждого процесса. Такие данные учитываются при принятии решений об использовании команд **debug**, так как производственная система может быть слишком загруженной для использования команды **debug**.
no debug all	Отключение всех команд **debug**. Эта команда позволяет освободить системные ресурсы после завершения отладки.
terminal monitor	Отображение выходных данных команды **debug** и сообщений о системных ошибках для текущего терминала и сеанса.

Так как неполадки возникают достаточно редко, можно пойти на временный компромисс, снижая эффективность ради быстрой диагностики и устранения неполадки. Для эффективного использования средств отладки необходимо проанализировать следующее:

- влияние, которое средство поиска и устранения неполадок оказывает на производительность маршрутизатора;
- наиболее выборочное и направленное использование данного средства диагностики;
- способы минимизации влияния процесса поиска и устранения неполадок на другие процессы, конкурирующие за ресурсы сетевого устройства;
- способы остановки средства поиска и устранения неполадок после завершения диагностики, чтобы маршрутизатор мог вернуться к наиболее эффективному режиму работы.

Рекомендуется потренироваться в использовании команд **debug** для поиска и устранения неполадок в лабораторной сети без трафика приложений конечных пользователей. Затем можно переходить к применению команд **debug** в производственной сети, которая используется пользователями для передачи данных. Без надлежащих мер предосторожности применение команд **debug**, влияющих на большое количество узлов, может ухудшить ситуацию.

При правильном, избирательном и временном использовании команд **debug** можно легко получить потенциально полезную информацию без анализатора протоколов или других инструментов, сторонних производителей.

Другие соображения по использованию команд **debug**.

- В идеале команды **debug** лучше всего использовать в периоды с минимальным трафиком и числом пользователей. Отладка в такие периоды приводит к снижению влияния на других пользователей.
- После анализа необходимой информации, полученной с помощью команды **debug**, и завершения отладки (любых других операций, связанных с настройкой параметров конфигурации), маршрутизатор может вернуться к режиму работы с максимальной производительностью. Можно вернуться к устранению неполадок, усовершенствовать план действий и устранить сетевую проблему.

Все команды **debug** вводятся в привилегированном режиме EXEC, и у большинства команд **debug** нет аргументов.

Примечание Не используйте команду **debug all**, так как она может привести к нарушению работоспособности системы.

Чтобы вывести список команд отладки и краткое описание их параметров, введите команду **debug ?** в привилегированном режиме EXEC.

По умолчанию сетевой сервер отправляет вывод команд **debug** и сообщения о системных ошибках на консоль. При использовании этого режима по умолчанию отладочный вывод следует отслеживать с помощью виртуального терминального подключения, а не через порт консоли. Для перенаправления отладочного вывода следует использовать параметры команды **logging** в режиме конфигурации. К возможным местам назначения относятся консоль, vty, внутренний буфер и хосты UNIX с сервером syslog. Формат syslog совместим с 4.3 Berkeley Software Distribution (4.3 BSD) UNIX и его производными.

Примечание Важно отключить отладку после завершения поиска и устранения неполадок.

Резюме

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

Резюме

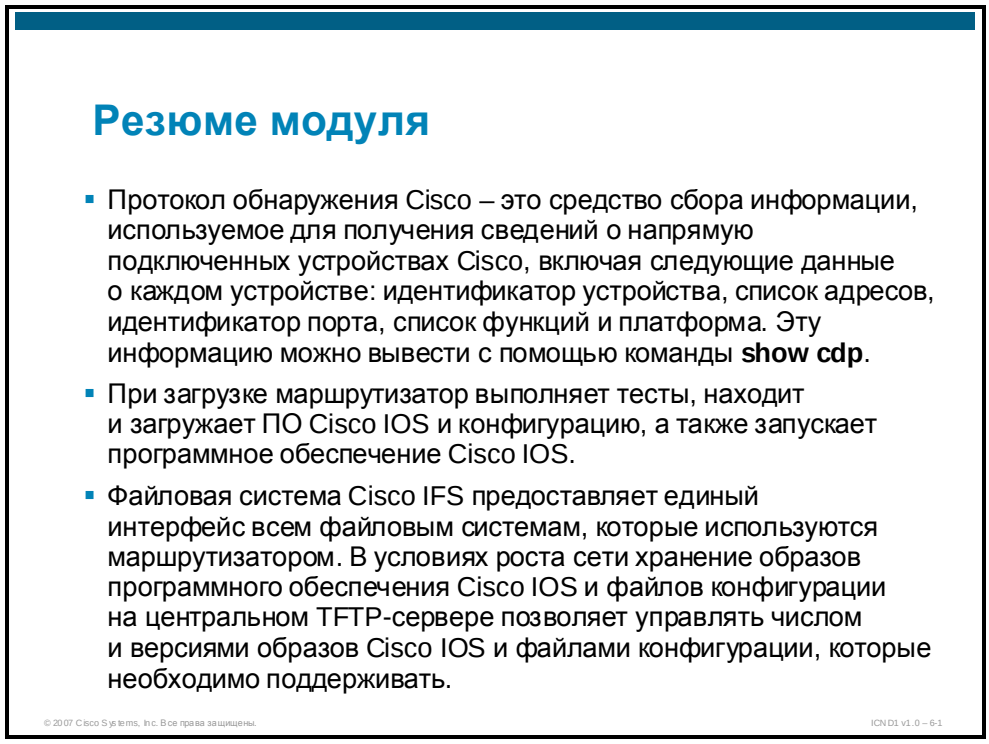
- Файловая система Cisco IFS предоставляет единый интерфейс всем файловым системам (NVRAM, ОЗУ, TFTP, флэш-память), которые используются маршрутизатором.
- В условиях роста сети хранение образов программного обеспечения Cisco IOS и файлов конфигурации на центральном TFTP-сервере позволяет управлять числом и версиями образов Cisco IOS и файлами конфигурации, которые необходимо поддерживать.
- Хранение резервной копии текущей конфигурации устройства на TFTP-сервере может помочь сократить время простоя устройства.

Резюме (прод.)

- Команда ПО Cisco IOS **copy** может использоваться для перемещения конфигураций между компонентами или устройствами, такими как ОЗУ, NVRAM и файловым сервер.
- Команды **show** и **debug** – встроенные средства устранения неполадок. Команда **show** используется для отображения статических данных, а команда **debug** – для отображения динамических данных.

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) Какие два утверждения о протоколе обнаружения Cisco верны? (Выберите два варианта.) (Источник: обнаружение соседних узлов в сети)

А) это проприетарный протокол
Б) это открытый протокол
В) собирает сведения о напрямую подключенных устройствах Cisco
Г) получает сведения обо всех устройствах в сети
Д) действует на сетевом уровне.

В2) Можно ли с помощью протокола обнаружения Cisco получить информацию об удаленном устройстве, которое не подключено напрямую? (Источник: обнаружение соседних узлов в сети)

А) С помощью команды **show cdp neighbors** *адрес*.
Б) С помощью команды **show cdp neighbors** *имя хоста*.
В) С помощью SSH или Telnet для доступа к устройству Cisco, напрямую подключенному к целевому устройству.
Г) С помощью протокола обнаружения Cisco невозможно получить информацию об удаленном устройстве.

В3) Какие два элемента данных включены в пакет обновления протокола обнаружения Cisco? (Выберите два варианта.) (Источник: обнаружение соседних узлов в сети)

А) платформа
Б) обновления маршрутов
В) идентификаторы устройств
Г) список MAC-адресов
Д) скорость канала

В4) Какая команда отключает протокол обнаружения Cisco для всех интерфейсов устройства? (Источник: обнаружение соседних узлов в сети)

А) **no run cdp**
Б) **no cdp run**
В) **no cdp enable**
Г) **no cdp execute**

В5) Что делает команда **cdp enable**? (Источник: обнаружение соседних узлов в сети)

А) отключает протокол обнаружения Cisco на конкретном интерфейсе
Б) включает протокол обнаружения Cisco для всех интерфейсов устройства
В) включает поддержку протокола обнаружения Cisco на отдельном интерфейсе
Г) включает протокол обнаружения Cisco на конкретном типе интерфейсов

В6) Какая команда Cisco IOS выдает тот же результат, что команда **show cdp neighbors detail**? (Источник: обнаружение соседних узлов в сети)

А) **show cdp traffic**
Б) **show cdp entry ***
В) **show cdp neighbors**
Г) **show cdp interface all**

В7) Какие ключевые слова добавляются к команде **show cdp neighbors** для включения в вывод дополнительной информации? (Источник: обнаружение соседних узлов в сети)

А) **full**
Б) **detail**
В) **verbose**
Г) **complete**

В8) Какая команда Cisco IOS отображает частоту отправки пакетов? (Источник: обнаружение соседних узлов в сети)

А) **show cdp entry**
Б) **show cdp traffic**
В) **show cdp interface**
Г) **show cdp neighbors**

В9) Какая информация содержится в выводе команды **show cdp interface**? (Источник: обнаружение соседних узлов в сети)

А) идентификатор удаленного порта
Б) идентификатор удаленного устройства
В) тип инкапсуляции
Г) число отправленных пакетов протокола обнаружения Cisco

В10) Какая команда выводит данные о платформе напрямую подключенного устройства? (Источник: обнаружение соседних узлов в сети)

А) **show cdp entry**
Б) **show cdp traffic**
В) **show cdp interface**
Г) **show cdp platform**

В11) Какая команда отображает ошибки контрольной суммы пакетов протокола обнаружения Cisco? (Источник: обнаружение соседних узлов в сети)

А) **show cdp entry**
Б) **show cdp traffic**
В) **show cdp interface**
Г) **show cdp neighbors**

В12) Какие три утверждения определяют основные предназначения карты сети? (Выберите три варианта.) (Источник: обнаружение соседних узлов в сети)

А) отслеживание изменений архитектуры сети
Б) инвентаризация программного обеспечения
В) отслеживание изменений топологии
Г) устранение неполадок сети
Д) отслеживание изменений конфигурации протоколов
Е) внедрение новых конфигураций

В13) Какой этап является последним этапом загрузки маршрутизатора Cisco? (Источник: управление запуском и конфигурацией маршрутизатора)

А) POST
Б) поиск и загрузка программного обеспечения Cisco IOS
В) поиск и загрузка кода загрузки
Г) поиск и загрузка конфигурации

В14) На каком этапе загрузки маршрутизатора Cisco проверяется работоспособность всех компонентов маршрутизатора? (Источник: управление запуском и конфигурацией маршрутизатора)

А) POST
Б) поиск программного обеспечения Cisco IOS
В) поиск кода загрузки
Г) поиск конфигурации

В15) Какой компонент маршрутизатора Cisco в основном используется для хранения файла загрузочной конфигурации? (Источник: управление запуском и конфигурацией маршрутизатора)

А) ОЗУ
Б) ПЗУ
В) NVRAM
Г) флэш-память
Д) конфигурационный регистр

В16) Какая из указанных ниже низкоуровневых операционных систем обычно используется для производственного тестирования и устранения неполадок. (Источник: управление запуском и конфигурацией маршрутизатора)

А) POST
Б) программа загрузки
В) мини Cisco IOS
Г) ROMMON

В17) Что маршрутизатор Cisco делает во время загрузки, если значение поля загрузки равно 0x2? (Источник: управление запуском и конфигурацией маршрутизатора)

А) запускает управляющую монитор ROM
Б) загружает образ Cisco IOS из флэш-памяти
В) загружает образ части Cisco IOS из ПЗУ
Г) ищет в файле загрузочной конфигурации команды **boot system**

В18) Что происходит, если во время загрузки маршрутизатор не может найти допустимый файл загрузочной конфигурации в NVRAM? (Источник: управление запуском и конфигурацией маршрутизатора)

А) Маршрутизатор переходит в режим установки.
Б) Маршрутизатор пытается перезапуститься.
В) Маршрутизатор запускает ROM-монитор.
Г) Маршрутизатор завершает работу.

В19) На большинстве маршрутизаторов программное обеспечение Cisco IOS загружается в _____ для выполнения, но на некоторых маршрутизаторах, оно выполняется прямо из _____. (Источник: управление запуском и конфигурацией маршрутизатора)

А) ОЗУ, NVRAM
Б) ОЗУ, флэш-память
В) флэш-память, ОЗУ
Г) NVRAM, флэш-память

В20) Из какого источника команда **show startup-config** отображает конфигурацию? (Источник: управление запуском и конфигурацией маршрутизатора)

А) ПЗУ
Б) ОЗУ
В) NVRAM
Г) флэш-память

В21) Какие биты конфигурационного регистра составляют поле загрузки? (Источник: управление запуском и конфигурацией маршрутизатора)

А) младший октет
Б) старший октет
В) 4 младших бита
Г) 4 старших бита

В22) Какая команда Cisco IOS используется для загрузки копии файла образа Cisco IOS с TFTP-сервера? (Источник: управление устройствами Cisco)

А) **copy IOS tftp**
Б) **copy tftp flash**
В) **copy flash tftp**
Г) **backup flash tftp**

В23) Какая часть имени системного файла образа c2600-js-mz.122-21a.bin указывает платформу? (Источник: управление устройствами Cisco)

А) mz
Б) js
В) 122-21a
Г) c2600

В24) Какие команды Cisco IOS отображают доступный объем памяти, в которой маршрутизатор хранит образ Cisco IOS? (Источник: управление устройствами Cisco)

А) **show flash**
Б) **show nvram**
В) **show memory**
Г) **show running-config**

В25) Где на маршрутизаторе обычно хранится текущая конфигурация? (Источник: управление устройствами Cisco)

А) BIOS
Б) ОЗУ
В) NVRAM
Г) загрузочная флэш-память

В26) Какая команда Cisco IOS объединят файл конфигурации из NVRAM с конфигурацией в ОЗУ? (Источник: управление устройствами Cisco)

А) **copy startup running**
Б) **copy running-config tftp**
В) **copy startup-config RAM**
Г) **copy NVRAM running-config**

В27) Что делает команда **copy tftp startup**? (Источник: управление устройствами Cisco)

А) копирует конфигурацию из NVRAM на TFTP-сервер
Б) загружает файл конфигурации с TFTP-сервера в ОЗУ
В) загружает файл конфигурации с TFTP-сервера в NVRAM
Г) объединяет конфигурацию в ОЗУ с файлом конфигурации на TFTP-сервере

В28) Что происходит с предыдущей конфигурацией при копировании конфигурации в ОЗУ из другого источника? (Источник: управление устройствами Cisco)

А) Она перезаписывается.
Б) Она сохраняется в текущем состоянии.
В) Она объединяется с новой конфигурацией, приоритет получают существующие значения конфигурации.
Г) Она объединяется с новой конфигурацией, приоритет получают новые значения конфигурации.

В29) Команды **debug** следует использовать для _____ неполадок, а не для мониторинга нормальной работы сети. (Источник: управление устройствами Cisco)

А) тестирования
Б) устранения
В) изоляции
Г) дублирования

В30) Почему необходимо соблюдать осторожность при использовании команд **debug**? (Источник: управление устройствами Cisco)

А) Они оказывают разрушительное действие.
Б) Они открывают бреши в системе безопасности.
В) Они препятствуют нормальной обработке трафика.
Г) Они могут оказывать негативное влияние на производительность.

В31) Какая команда добавляет временную метку к сообщению команды debug или в журнальное сообщение. (Источник: управление устройствами Cisco)

А) **timestamps debug**
Б) **debug timestamps**
В) **service timestamps**
Г) **service debug timestamps**

В32) Какое действие может привести к нарушению работоспособности программного обеспечения на устройстве Cisco? (Источник: управление устройствами Cisco)

А) отключение привилегированной команды EXEC **debug** на интенсивно используемом производственном маршрутизаторе
Б) включение привилегированной команды EXEC **debug** на интенсивно используемом производственном маршрутизаторе
В) включение привилегированной команды EXEC **debug** на не интенсивно используемом производственном маршрутизаторе
Г) отключение привилегированной команды EXEC **debug** на не интенсивно используемом производственном маршрутизаторе

В33) Какая команда Cisco IOS позволяет получать консольные сообщения в сеансе Telnet? (Источник: управление устройствами Cisco)

А) **terminal monitor**
Б) **terminal debug monitor**
В) **terminal debug messages**
Г) **terminal console messages**

В34) В идеале команды **debug** лучше всего использовать в периоды с _____ трафиком и _____ числом пользователей. (Источник: управление устройствами Cisco)

А) меньшим, большим
Б) меньшим, небольшим
В) большим, большим
Г) большим, небольшим

В35) Включение команды **debug** привелигированного режима EXEC на интенсивно используемом производственном маршрутизаторе может быть _____. (Источник: управление устройствами Cisco)

А) удобным
Б) полезным
В) вредным
Г) трудным

Ответы на вопросы для самопроверки по модулю

В1) А, В

В2) Г

В3) А, В

В4) Б

В5) В

В6) Б

В7) Б

В8) В

В9) В

В10) А

В11) Б

В12) А, В, Г

В13) Г

В14) А

В15) В

В16) Г

В17) Г

В18) А

В19) Б

В20) В

В21) В

В22) Б

В23) Г

В24) А

В25) Б

В26) А

В27) В

В28) Г

В29) В

В30) Г

В31) В

В32) Б

В33) А

В34) Б

В35) В

