ICND2

Interconnecting Cisco Networking Devices Part 2

Том 2

Версия 1.0

Руководство для студента

Номер текста по каталогу: 97-2510-01

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

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

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

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

Содержание

Том 2

Модуль 5

Внедрение EIGRP

Обзор

В этом модуле описываются функции EIGRP, протокола маршрутизации компании Cisco, разработанного для снятия ограничений как протоколов на основе вектора расстояния, так и протоколов состояния канала. В модуле подробно рассматриваются базовые технологии EIGRP, включая процесс выбора пути.

Задачи модуля

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

- описывать принцип работы и настройку EIGRP, включая выравнивание нагрузки и аутентификацию;
- определять методы выявления распространенных проблем EIGRP и предлагать решения этих проблем.

Занятие 1

Внедрение EIGRP

Обзор

EIGRP – это усовершенствованный протокол вектора расстояния, разработанный корпорацией Cisco. Протокол EIGRP подходит для многих топологий и сред. В качественно спроектированной сети протокол EIGRP хорошо масштабируется и обеспечивает высокую скорость конвергенции при минимальных издержках. Протокол EIGRP часто выбирают в качестве протокола маршрутизации на устройствах Cisco. В этом занятии описывается настройка и мониторинг протокола EIGRP.

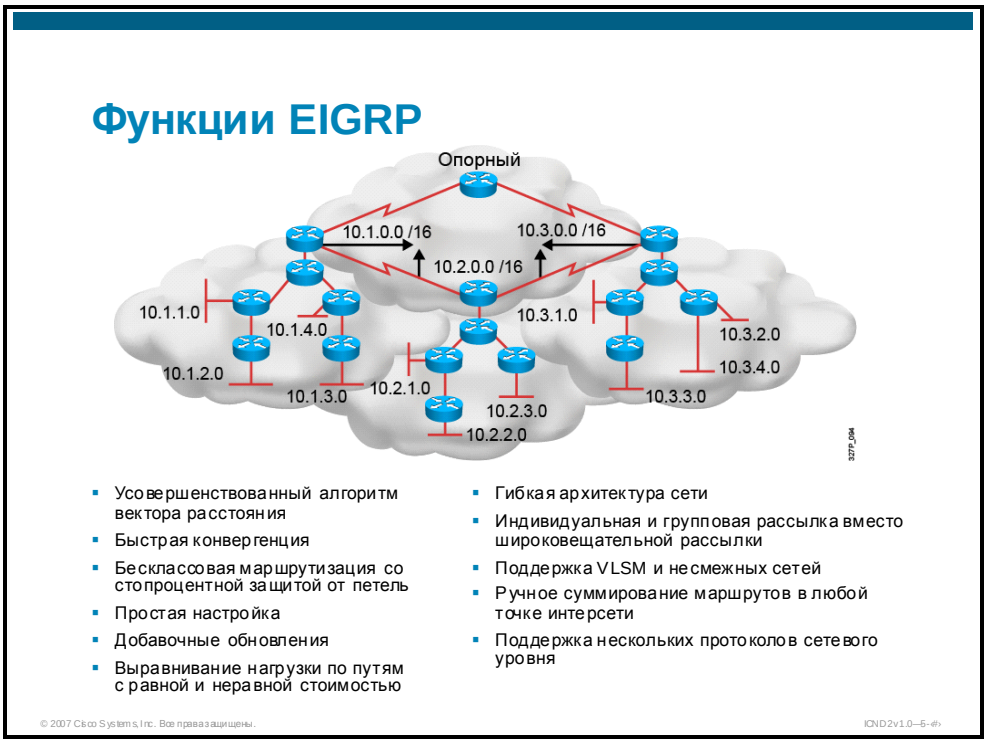
Задачи

По окончании этого занятия вы сможете описывать принцип работы и настройку протокола EIGRP, включая выравнивание нагрузки и аутентификацию. Это значит, что вы сможете выполнить следующие задачи:

- описывать функции EIGRP;
- настраивать и проверять EIGRP;
- настраивать выравнивание нагрузки с использованием EIGRP;
- настраивать аутентификацию MD5 для EIGRP.

Общие сведения о EIGRP

В этом разделе описываются функции протокола EIGRP.



EIGRP – это проприетарный протокол маршрутизации Cisco, объединяющий преимущества протоколов маршрутизации на основе состояния канала и на основе вектора расстояния. EIGRP представляет собой усовершенствованный протокол вектора расстояния или гибридный протокол маршрутизации и предлагает следующие функции.

- **Быстрая конвергенция.** EIGRP использует алгоритм DUAL для ускорения конвергенции. Маршрутизатор под управлением EIGRP сохраняет все доступные резервные маршруты к местам назначения и может быстро адаптироваться к альтернативным маршрутам. Если в таблице маршрутизации нет подходящих маршрутов или резервных маршрутов, EIGRP запрашивает соседние узлы, чтобы обнаружить альтернативный маршрут.
- **Сниженное потребление полосы пропускания.** Протокол EIGRP не рассылает периодические обновления. Вместо этого он отправляет частичные обновления при изменении пути или метрики маршрута. При изменении данных о пути DUAL посылает обновление только для этого пути, а не полную таблицу.
- **Поддержка нескольких протоколов сетевого уровня.** EIGRP поддерживает протоколы AppleTalk, IPv4, IPv6 и Novell IPX, использующие модули PDM. PDM удовлетворяют требования протоколов, относящиеся к сетевому уровню.
- **Бесклассовая маршрутизация.** Поскольку EIGRP является бесклассовым протоколом маршрутизации, он объявляет маску маршрутизации для каждой сети назначения. Маска маршрутизации позволяет EIGRP работать с несмежными подсетями и масками подсети переменной длины (VLSM).

- **Рассылка меньшего объема служебных данных.** EIGRP использует многоадресную и одноадресную, а не широковещательную рассылку. В результате обновления маршрутизации и запросы данных топологии не затрагивают конечные станции.
- **Выравнивание нагрузки.** EIGRP поддерживает выравнивание нагрузки по маршрутам с неравными метриками, что позволяет администраторам более эффективно распределять потоки трафика в сети.
- **Простое суммирование.** EIGRP позволяет администраторам создавать суммарные маршруты в любой точке сети, не ограничиваясь традиционным классовым суммированием протоколов вектора расстояния, которое можно использовать только на границах основной сети.

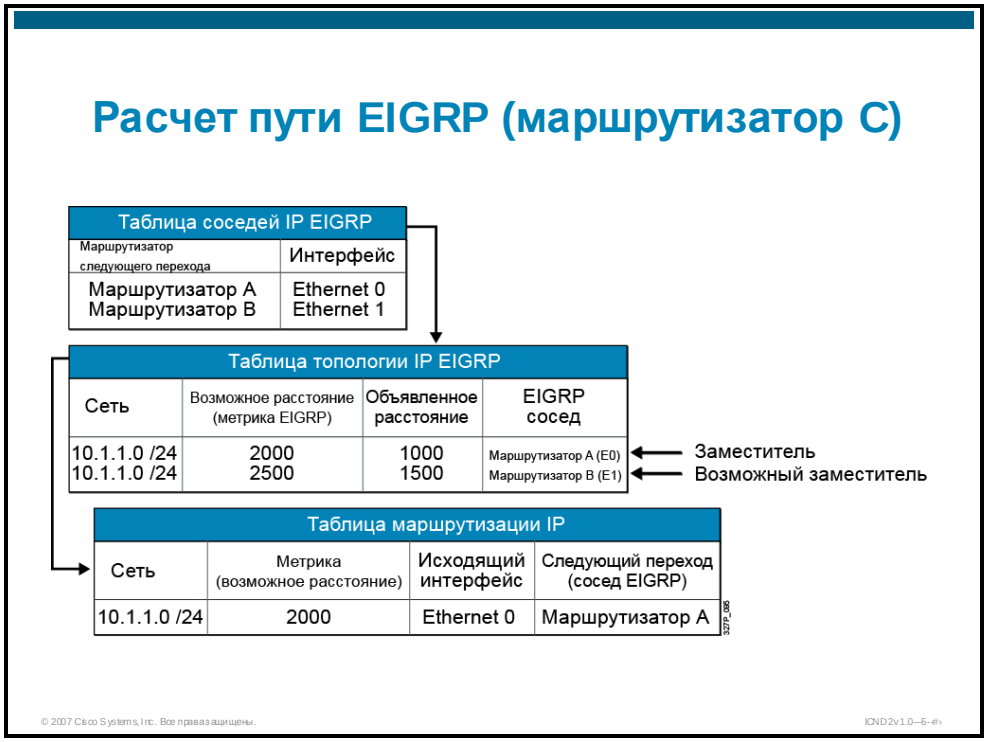
Каждый маршрутизатор EIGRP ведет таблицу соседних узлов. Эта таблица включает список подключенных напрямую маршрутизаторов EIGRP, сформировавших отношения смежности с данным маршрутизатором.

Каждый маршрутизатор EIGRP ведет таблицу топологии для каждой конфигурации протокола. Таблица топологии включает записи маршрутов для каждого места назначения, известного маршрутизатору. EIGRP выбирает наилучшие маршруты из таблицы топологии и помещает их в таблицу маршрутизации.

Чтобы определить лучший маршрут и резервный (альтернативный) маршрут к месту назначения, EIGRP использует два параметра.

- **Объявленное расстояние.** Метрика EIGRP, которая определяет способность соседнего узла EIGRP достичь той или иной сети.
- **Расстояние лучшего маршрута.** Объявленное расстояние для определенной сети, полученное от соседнего узла EIGRP + метрика EIGRP, определяющая стоимость доступа к этому соседнему узлу.

Маршрутизатор сравнивает все доступные расстояния к определенной сети, а затем выбирает самое низкое расстояние и помещает его в таблицу маршрутизации. Расстояние выбранного лучшего маршрута становится метрикой EIGRP, определяющей стоимость доступа к этой сети, в таблице маршрутизации.



Пример: Расчет пути EIGRP (маршрутизатор C)

База данные топологии EIGRP содержит все маршруты, известные всем соседним узлам EIGRP. Как показано в примере, маршрутизаторы A и B отправляют свои таблицы маршрутизации маршрутизатору C (его таблица маршрутизации показана на рисунке). Маршрутизаторы A и B имеют пути к сети 10.1.1.0/24 и другим сетям, не показанным на рисунке.

В таблице топологии маршрутизатора C доступно две записи с путями к 10.1.1.0/24. Метрика EIGRP для маршрутизатора C, определяющая стоимость доступа к маршрутизаторам A и B, равняется 1000. Добавьте эту стоимость (1000) к соответствующему объявленному расстоянию для каждого маршрутизатора и вы получите расстояния лучших маршрутов от маршрутизатора C до сети 10.1.1.0/24.

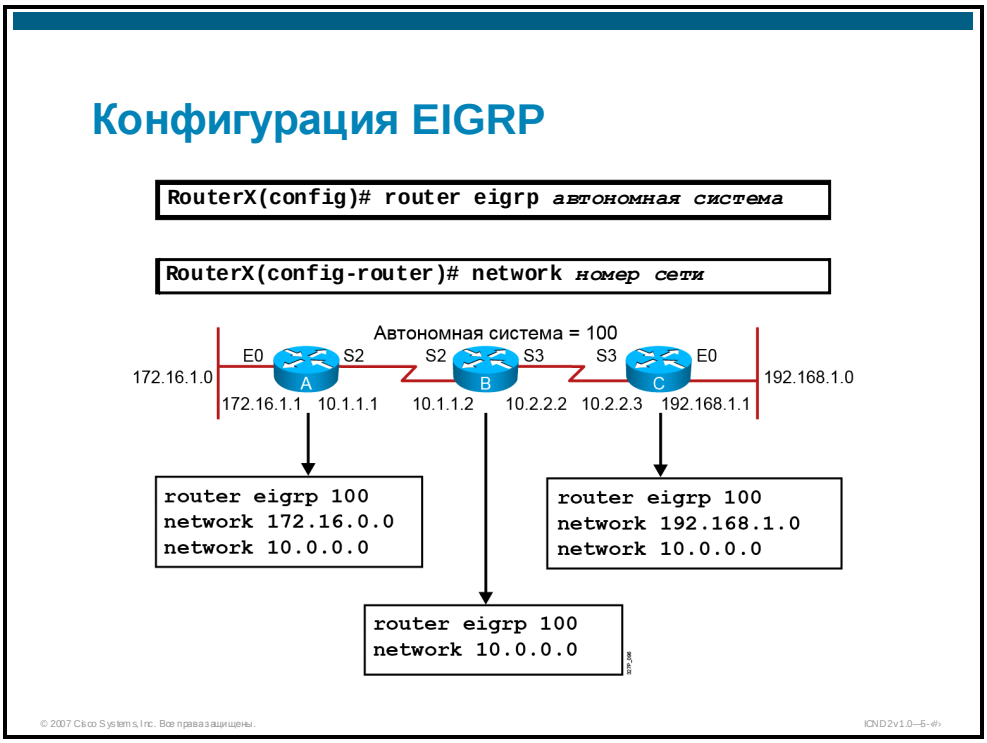
Маршрутизатор C выбирает расстояние лучшего маршрута с минимальной стоимостью (2000) и устанавливает его в таблицу маршрутизации IP в качестве лучшего маршрута к сети 10.1.1.0/24. Маршрут с наименьшим расстоянием, который устанавливается в таблицу маршрутизации, называется лучшим маршрутом.

Затем маршрутизатор C выбирает резервный маршрут, который называется альтернативным маршрутом (если такой маршрут доступен). Чтобы маршрут стал альтернативным маршрутом, маршрутизатор на следующем переходе должен иметь объявленное расстояние меньше, чем расстояние текущего лучшего маршрута.

Если лучший маршрут перестает действовать, из-за изменения топологии или метрики на соседнем узле, алгоритм DUAL проверяет наличие альтернативных маршрутов к месту назначения. Если альтернативный маршрут найден, алгоритм DUAL использует его, что позволяет избежать повторного вычисления маршрута. Если альтернативные маршруты отсутствуют, для определения нового лучшего маршрута выполняется повторное вычисление.

Настройка и проверка EIGRP

В этом занятии описывается настройка и проверка протокола EIGRP.



Используйте команды **router eigrp** и **network** для создания процесса маршрутизации EIGRP. Обратите внимание, что протокол EIGRP требует номера автономной системы (AS). Номер AS не обязательно должен быть зарегистрирован. Однако все маршрутизаторы автономной системы должны использовать одинаковые номера AS для обмена информацией.

Команда **network** задает номер основной сети, к которой подключен маршрутизатор. Процесс маршрутизации EIGRP находит интерфейсы с IP-адресами, которые принадлежат сетям, заданным с помощью команды **network** и запускает процесс маршрутизации EIGRP на этих интерфейсах.

Пример: Конфигурация EIGRP

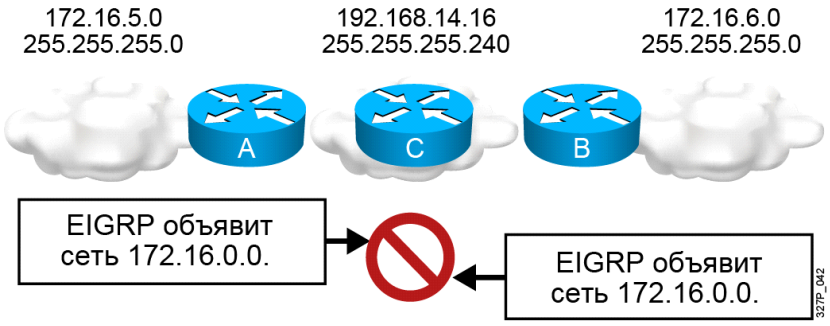
Таблица ниже относится к конфигурациям EIGRP на маршрутизаторе A в примере конфигурации EIGRP.

Примеры команд EIGRP

Команда	Описание
router eigrp 100	Включает процесс маршрутизации EIGRP для AS 100
network 172.16.0.0	Связывает сеть 172.16.0.0 с процессом маршрутизации EIGRP
network 10.0.0.0	Связывает сеть 10.0.0.0 с процессом маршрутизации EIGRP

Примечание EIGRP рассылает обновления из интерфейсов в сетях 10.0.0.0 и 172.16.0.0. Обновления включают сведения о сетях 10.0.0.0, 172.16.0.0 и любых других сетях, известных EIGRP.

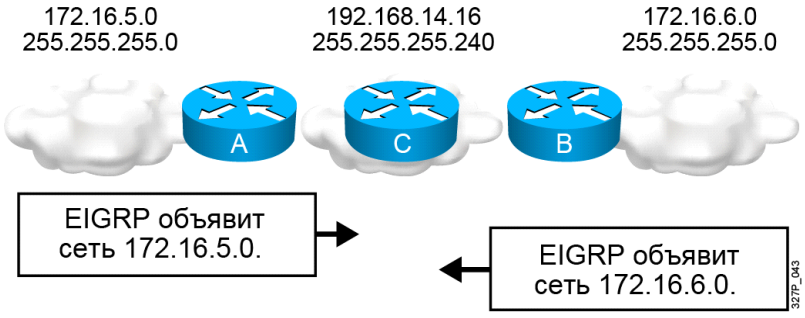
EIGRP и несмежные сети
Конфигурация по умолчанию



По умолчанию протокол EIGRP не объявляет подсети и, следовательно, не поддерживает несмежные подсети.

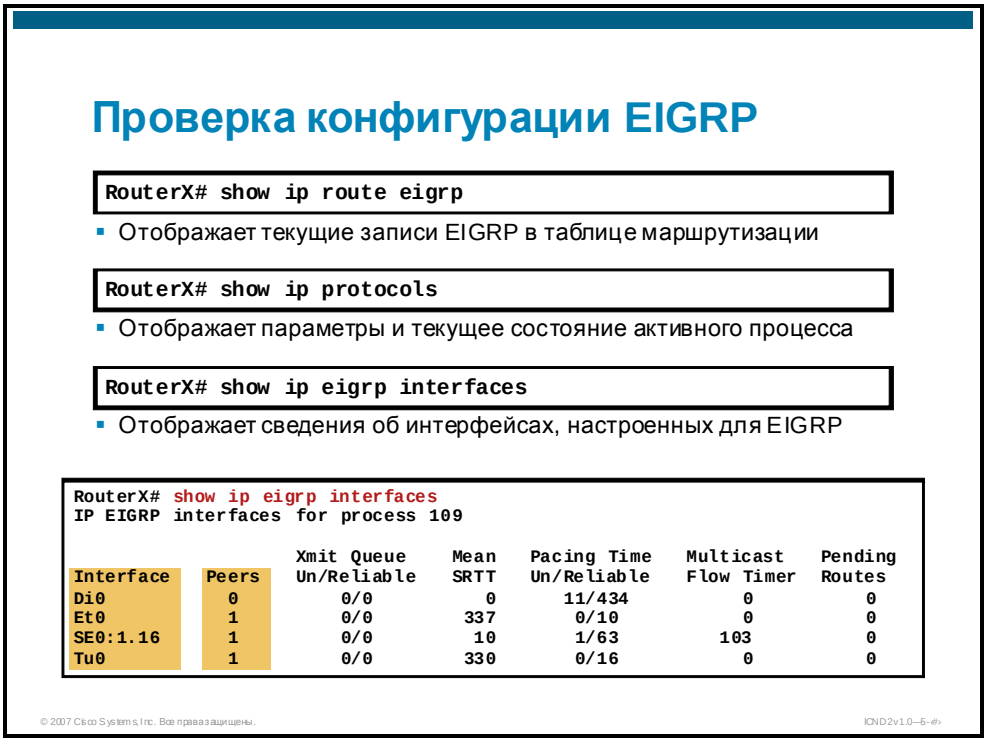
EIGRP автоматически суммирует маршруты на классовой границе. В некоторых случаях автоматическое суммирование может быть нежелательно. Например, если в среде присутствуют несмежные сети, автоматическое суммирование следует отключить, чтобы свести к минимуму дезорганизацию маршрутизаторов.

EIGRP и несмежные сети при использовании параметра auto-summary



Протокол EIGRP с параметром **no auto-summary** может объявлять подсети и, следовательно, поддерживает несмежные подсети.

Чтобы отключить автоматическое суммирование, используйте команду **no auto-summary** в режиме конфигурации маршрутизатора EIGRP.



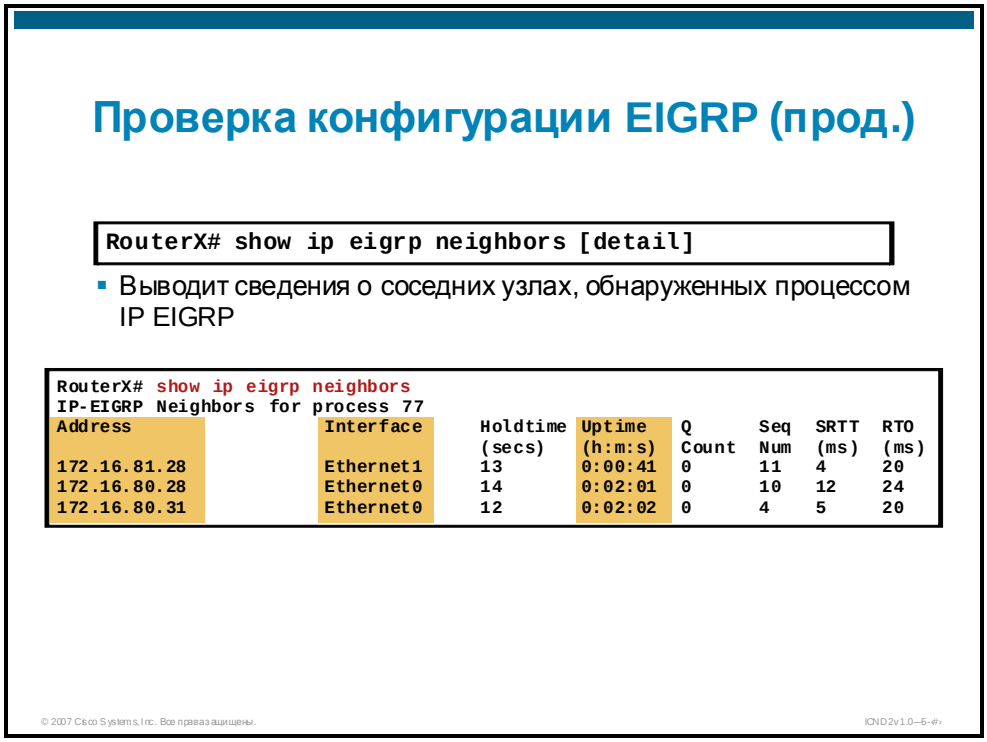
Команда **show ip route eigrp** отображает текущие записи EIGRP в таблице маршрутизации.

Команда **show ip protocols** отображает параметры и текущее состояние активного процессора маршрутизации. Эта команда выводит номер автономной системы EIGRP. Кроме того, выводятся номера фильтрации и перераспределения, а также сведения о соседстве и расстоянии.

Используйте команду **show ip eigrp interfaces** [*type number*] [*as-number*], чтобы определить, какие интерфейсы EIGRP активны и вывести данные о том, как протокол EIGRP связан с этими интерфейсами. Если вы укажете интерфейс в параметре *type number*, будет отображаться информация только для этого интерфейса. В противном случае будут выведены сведения обо всех маршрутизаторах, на которых работает протокол EIGRP. Если вы укажете автономную систему в параметре *as-number*, будет отображаться только процесс маршрутизации для указанной автономной системы. В противном случае будут отображаться все процессы EIGRP.

Вывод команды show ip eigrp interfaces

Поле	Описание
Interface	Интерфейс, на котором настроен протокол EIGRP
Peers	Количество соседних узлов EIGRP с прямым подключением к интерфейсу
Xmit Queue Un/Reliable	Количество пакетов в надежной и ненадежной очередях
Mean SRTT	Средний интервал SRTT (в миллисекундах) для всех соседних узлов интерфейса
Pacing Time Un/Reliable	Время в миллисекундах, которое должно пройти после отправки надежных и ненадежных пакетов
Multicast Flow Timer	Время ожидания подтверждения многоадресного пакета от всех соседних узлов (в миллисекундах). По истечение этого периода отправляется следующий многоадресный пакет
Pending Routes	Количество маршрутов в пакетах, которые находятся в очереди на передачу



Используйте команду **show ip eigrp neighbors**, чтобы вывести сведения о соседних узлах, обнаруженных протоколом EIGRP, и определить, когда соседние узлы стали активными или неактивными. Кроме того, эта команда может быть полезна при поиске и устранении некоторых проблем транспорта.

В таблице ниже описываются значимые поля вывода команды **show ip eigrp neighbors**.

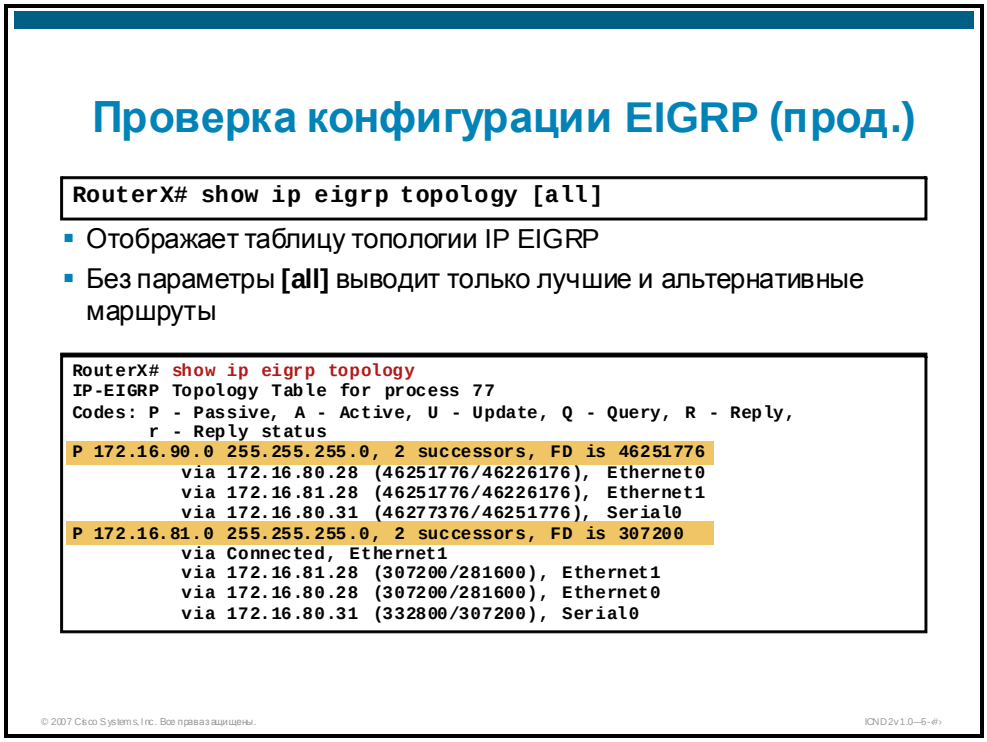
Вывод команды show ip eigrp neighbors

Поле	Описание
process 77	Номер автономной системы, заданный с помощью команды **router**.
Address	IP-адрес узла EIGRP.
Interface	Интерфейс, на котором маршрутизатор получает пакеты приветствия от соседнего узла.
Holdtime	Время ожидания ответа от узла (в секундах), по истечении которого ПО Cisco IOS объявляет узел недоступным. Если узел использует параметр Holdtime по умолчанию, это число будет меньше 15. Если узел использует нестандартный параметр Holdtime, будет отображаться его значение.
Uptime	Время (часы:минуты:секунды), прошедшее с момента, когда локальный маршрутизатор получил первые данные от соседнего узла.
Q Count	Количество пакетов EIGRP (обновления, запроса и ответа), ожидающих отправки программным обеспечением.
Seq Num	Последовательный номер последнего пакета обновления, запроса или ответа, полученного от соседнего узла.
SRTT	Время в миллисекундах, которое необходимо для отправки пакета EIGRP в соседний узел и получения подтверждения доставки пакета на локальном маршрутизаторе.
RTO	Время ожидания повторной передачи (в миллисекундах). Это период времени, по истечении которого ПО повторно отправляет пакет из очереди повторной передачи в соседний узел.

В таблице описываются значимые поля вывода команды **show ip eigrp neighbors detail**.

Вывод команды show ip eigrp neighbors detail

Поле	Описание
process 77	Номер автономной системы, заданный с помощью команды конфигурации маршрутизатора.
H	В этом столбце приводится порядок, в котором был установлен одноранговый сеанс с указанным соседним узлом. Порядок указывается с использованием последовательной нумерации начиная с 0.
Address	IP-адрес узла EIGRP.
Interface	Интерфейс, на котором маршрутизатор получает пакеты приветствия от соседнего узла.
Holdtime	Время ожидания ответа от узла (в секундах), по истечении которого ПО Cisco IOS объявляет узел недоступным. Если узел использует параметр Holdtime по умолчанию, это число будет меньше 15. Если узел использует нестандартный параметр Holdtime, будет отображаться его значение.
Uptime	Время (часы:минуты:секунды), прошедшее с момента, когда локальный маршрутизатор получил первые данные от соседнего узла.
Q Count	Количество пакетов EIGRP (обновления, запроса и ответа), ожидающих отправки программным обеспечением.
Seq Num	Последовательный номер последнего пакета обновления, запроса или ответа, полученного от соседнего узла.
SRTT	Время в миллисекундах, которое необходимо для отправки пакета EIGRP в соседний узел и получения подтверждения доставки пакета на локальном маршрутизаторе.
RTO	Период времени (в миллисекундах), по истечении которого ПО повторно отправляет пакет из очереди повторной передачи в соседний узел.
Version	Версия ПО, работающая на указанном узле.
Retrans	Количество операций повторной передачи пакета.
Retries	Количество попыток повторной передачи пакета.
Restart time	Время (часы:минуы:секунды), прошедшее с момент перезапуска указанного соседнего узла.



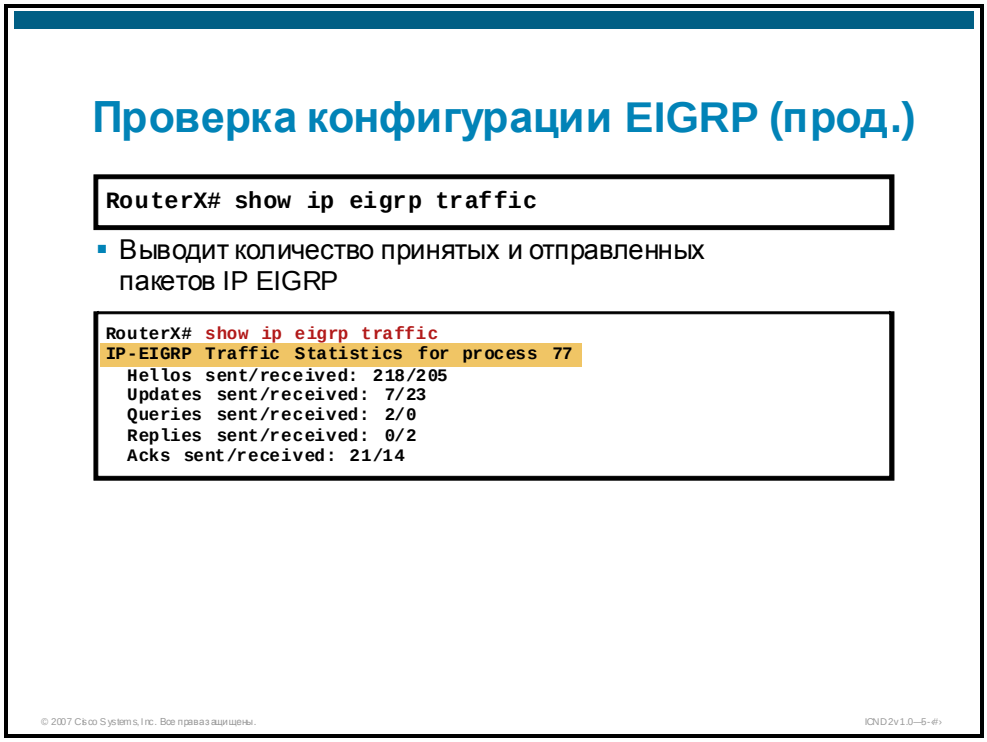
Команда **show ip eigrp topology** выводит таблицу топологии EIGRP, сведения об активном и пассивном состоянии маршрутов, количество лучших маршрутов и расстояние лучшего маршрута к месту назначения.

В таблице ниже описываются значимые поля вывода команды **show ip eigrp topology**.

Вывод команды show ip eigrp topology

Поле	Описание
Codes	Состояние записи таблицы топологии. Значения Passive и Active обозначают состояния EIGRP с точки зрения места назначения. Значения Update, Query и Reply обозначают тип отправляемого пакета.
P - Passive	Указывает, что вычисления EIGRP для этого места назначения не выполняются.
A - Active	Указывает, что для этого места назначения выполняются вычисления EIGRP.
U - Update	Указывает, что в место назначения был отправлен пакет обновления.
Q - Query	Указывает, что в место назначения был отправлен пакет запроса.
R - Reply	Указывает, что в место назначения был отправлен пакет ответа.
r - Reply status	Флаг, который устанавливается после того, как ПО отправляет запрос и начинает ждать ответа.
172.16.90.0	Номер IP-сети места назначения.
255.255.255.0	Маска подсети места назначения.
successors	Количество лучших маршрутов. Это число соответствует числу следующих переходов в таблице маршрутизации IP. Если слово «successors» написано в верхнем регистре, значит маршрут или следующий маршрутизатор находятся в переходном состоянии.

Поле	Описание
FD	Расстояние лучшего маршрута – это лучшая метрика доступа к месту назначения или лучшая метрика, которая была известна, когда маршрутизатор перешел в активное состояние. Это значение используется при проверке условия альтернативности. Если заявленное расстояние маршрутизатора (метрика после косой черты) меньше расстояния лучшего маршрута, условие альтернативности выполняется и путь становится альтернативным маршрутом. После того, как программное обеспечение определит альтернативный путь, ему больше не понадобится отправлять запрос в место назначения.
replies	Количество необработанных (не полученных) ответов с точки зрения адресата. Эти сведения отображаются только если адресат находится в состоянии Active.
state	Точное состояние EIGRP, в котором находится адресат. Может принимать значения 0, 1, 2 или 3. Эти сведения отображаются только если адресат находится в состоянии Active.
via	IP-адрес соседнего узла, который сообщил программному обеспечению об адресате. Первые *n* записей, где *n* – число лучших маршрутов, соответствуют текущим лучшим маршрутам. Остальные записи соответствуют альтернативным маршрутам.
(46251776/46226176)	Первое число – метрика EIGRP, которая отражает стоимость доступа к адресату. Второе число – метрика EIGRP, объявленная соседним узлом.
Ethernet0	Интерфейс, от которого была получена информация.
Serial0	Интерфейс, от которого была получена информация.



Команда **show ip eigrp traffic** отображает количество полученных и отправленных пакетов.

В таблице описываются поля, которые могут быть включены в вывод.

Вывод команды show ip eigrp traffic

Поле	Описание
process 77	Номер автономной системы, заданный с помощью команды **router**
Hellos sent/received	Количество принятых и отправленных пакетов приветствия
Updates sent/received	Количество принятых и отправленных пакетов обновления
Queries sent/received	Количество принятых и отправленных пакетов запроса
Replies sent/received	Количество принятых и отправленных пакетов ответа
Acks sent/received	Количество принятых и отправленных пакетов подтверждения

Команда debug ip eigrp

```
RouterX# debug ip eigrp
IP-EIGRP: Processing incoming UPDATE packet
IP-EIGRP: Ext 192.168.3.0 255.255.255.0 M 386560 - 256000 130560 SM 360960 –
256000 104960
IP-EIGRP: Ext 192.168.0.0 255.255.255.0 M 386560 - 256000 130560 SM 360960 –
256000 104960
IP-EIGRP: Ext 192.168.3.0 255.255.255.0 M 386560 - 256000 130560 SM 360960 –
256000 104960
IP-EIGRP: 172.69.43.0 255.255.255.0, - do advertise out Ethernet0/1
IP-EIGRP: Ext 172.69.43.0 255.255.255.0 metric 371200 - 256000 115200
IP-EIGRP: 192.135.246.0 255.255.255.0, - do advertise out Ethernet0/1
IP-EIGRP: Ext 192.135.246.0 255.255.255.0 metric 46310656 - 45714176 596480
IP-EIGRP: 172.69.40.0 255.255.255.0, - do advertise out Ethernet0/1
IP-EIGRP: Ext 172.69.40.0 255.255.255.0 metric 2272256 - 1657856 614400
IP-EIGRP: 192.135.245.0 255.255.255.0, - do advertise out Ethernet0/1
IP-EIGRP: Ext 192.135.245.0 255.255.255.0 metric 40622080 - 40000000 622080
IP-EIGRP: 192.135.244.0 255.255.255.0, - do advertise out Ethernet0/1
```

Примечание. Обмен маршрутами EIGRP выполняется только при изменении топологии.

Команда **debug ip eigrp** привилегированного режима EXEC помогает анализировать пакеты EIGRP, получаемые и отправляемые интерфейсом. Поскольку команда **debug ip eigrp** выводит значительный объем данных, используйте ее только когда через сеть проходят малые объемы трафика.

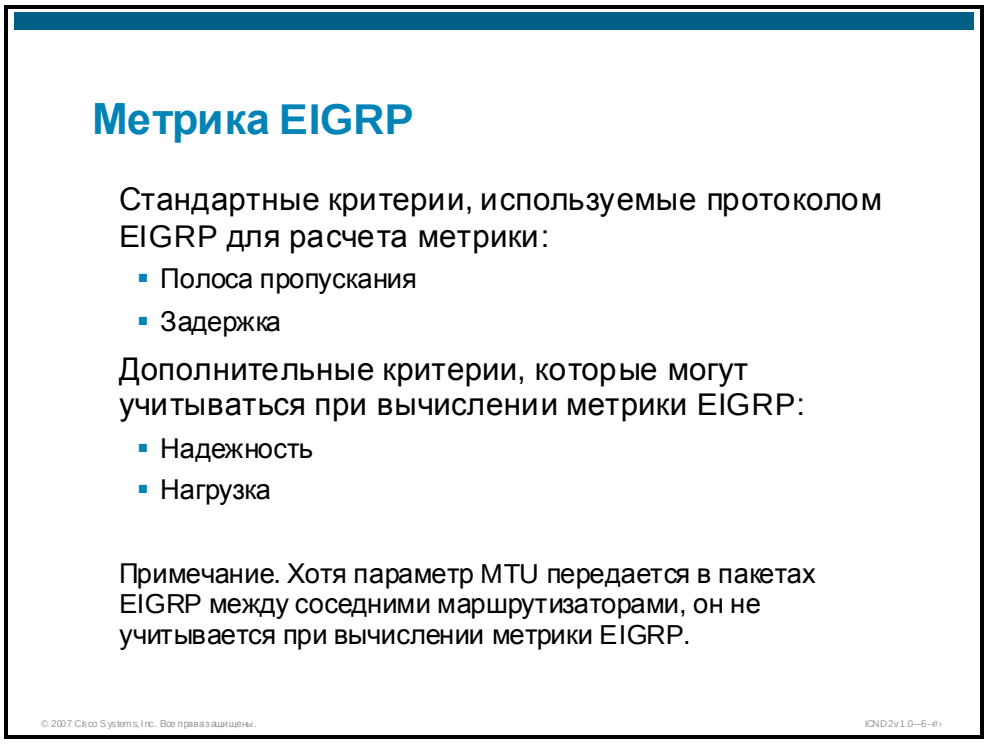
В таблице описываются поля примера вывода команды **debug ip eigrp**.

Вывод команды debug ip eigrp

Поле	Описание
IP-EIGRP	Сообщает, что пакет является пакетом IP EIGRP.
Ext	Указывает, что следующий адрес является внешним, а не внутренним (обозначается кодом «Int»)
do not advertise out	Указывает интерфейсы, из которых EIGRP не будет объявлять данный маршрут. Эта конфигурация предотвращает образование петель маршрутизации (метод Split horizon).
M	Выводит вычисленную метрику, которая включает отправленную метрику (SM) и стоимость соединения данного маршрутизатора и соседнего маршрутизатора. Первое число – составная метрика. Следующие два числа – инвертированная полоса пропускания и задержка соответственно.
SM	Отображает метрику, заявленную соседним узлом.

Выравнивание нагрузки с помощью EIGRP

В этом разделе описывается настройка выравнивания нагрузки с помощью EIGRP.



Метрика EIGRP

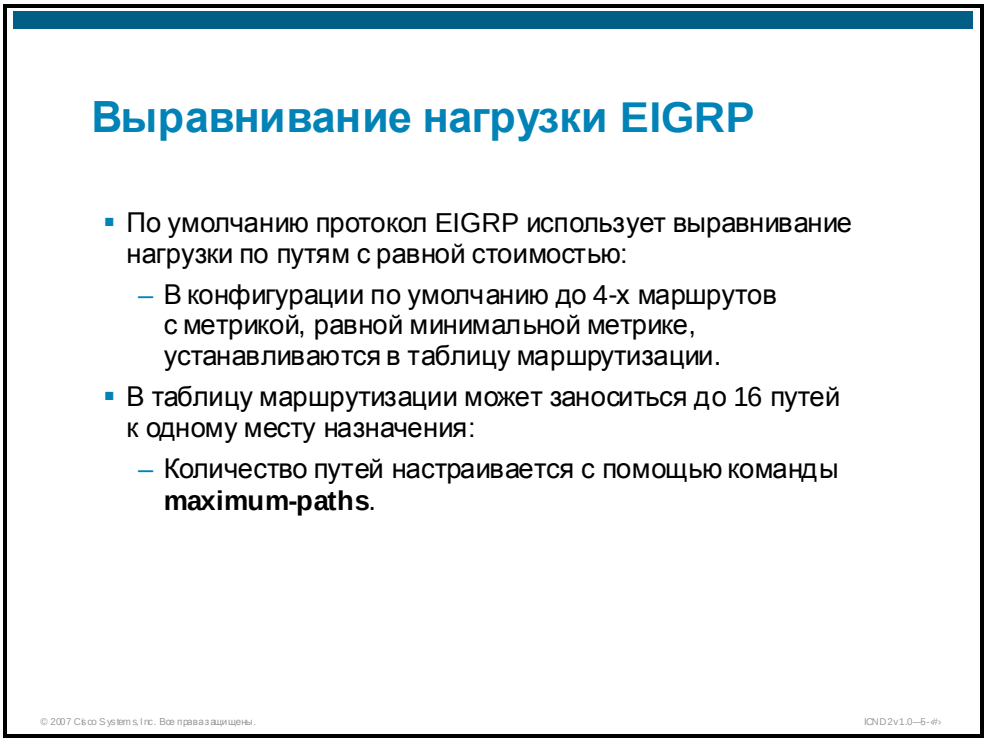
Метрика EIGRP может основываться на нескольких критериях, но по умолчанию EIGRP использует только два из них.

- **Полоса пропускания.** Минимальная полоса пропускания между источником и местом назначения.
- **Задержка.** Совокупная задержка интерфейсов, которые находятся на пути.

Также можно использовать следующие критерии, однако это не рекомендуется, так как они приводят к частому перерасчету таблицы маршрутизации.

- **Надежность.** Это значение представляет худшую надежность между источником и местом назначение и основывается на параметрах Keepalive.
- **Нагрузка.** Это значение представляет худшую нагрузку в канале между источником и местом назначения, которая рассчитывается на основе скорости передачи и пакетов и заданной полосы пропускания интерфейса.

Примечание	Хотя параметр MTU передается в пакетах EIGRP между соседними маршрутизаторами, он не учитывается при вычислении метрики EIGRP.

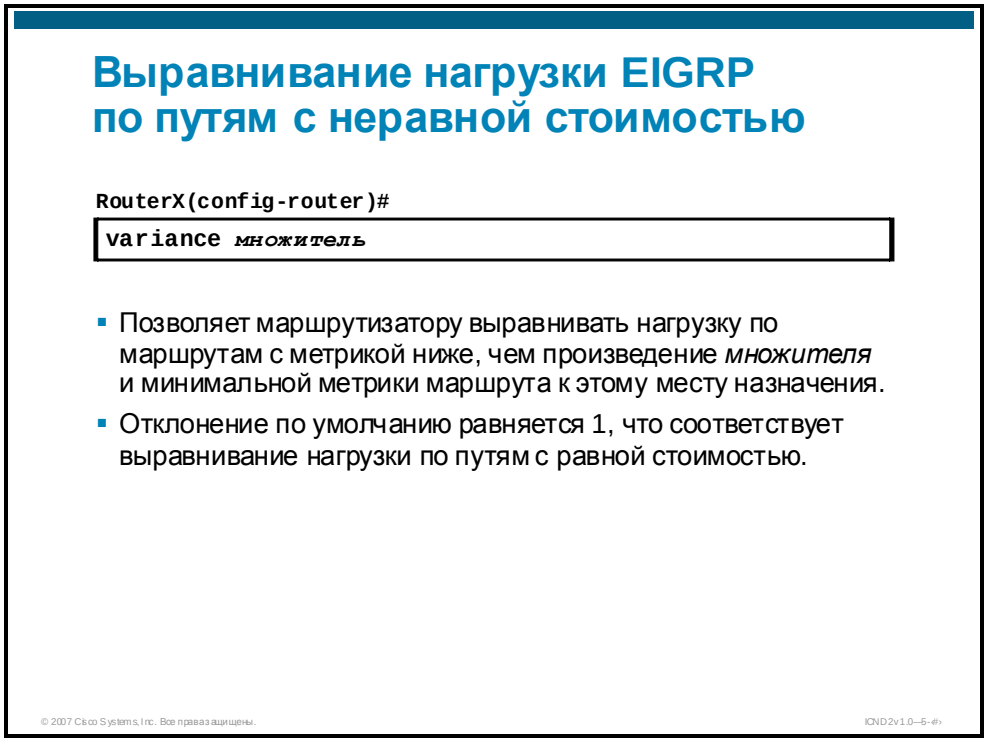


Выравнивание нагрузки по путям с равной стоимостью

Выравнивание нагрузки по путям с одинаковой стоимостью – это способность маршрутизатора распределять трафик по сетевым портам, обеспечивающим пути с одинаковой стоимостью к адресу назначения. Выравнивание нагрузки повышает коэффициент использования сетевых сегментов и эффективную полосу пропускания сети.

Для протокола IP ПО Cisco IOS реализует выравнивание нагрузки по четырем путям (по умолчанию). С помощью команды конфигурации интерфейса **maximum-paths** *максимальное число путей* можно увеличить максимальное число путей с равной стоимостью до 16. Чтобы отключить выравнивание нагрузки, установите значение 1 для параметра *максимальное число путей*. При использовании процесса коммутации пакетов, выравнивание нагрузки по путям с одинаковой стоимостью выполняется для отдельных пакетов. При использовании быстрой коммутации, выравнивание нагрузки по путям с одинаковой стоимостью выполняется для мест назначения.

Примечание	При тестировании выравнивания нагрузки не отправляйте эхо-запросы с маршрутизаторов с интерфейсов быстрой коммутации или на них. Пакеты, генерируемые такими маршрутизаторами, используют коммутацию процессов, а не быструю коммутацию. Эхо-запрос может вернуть противоречивые результаты.



Настройка выравнивания нагрузки по путям с неравной стоимостью

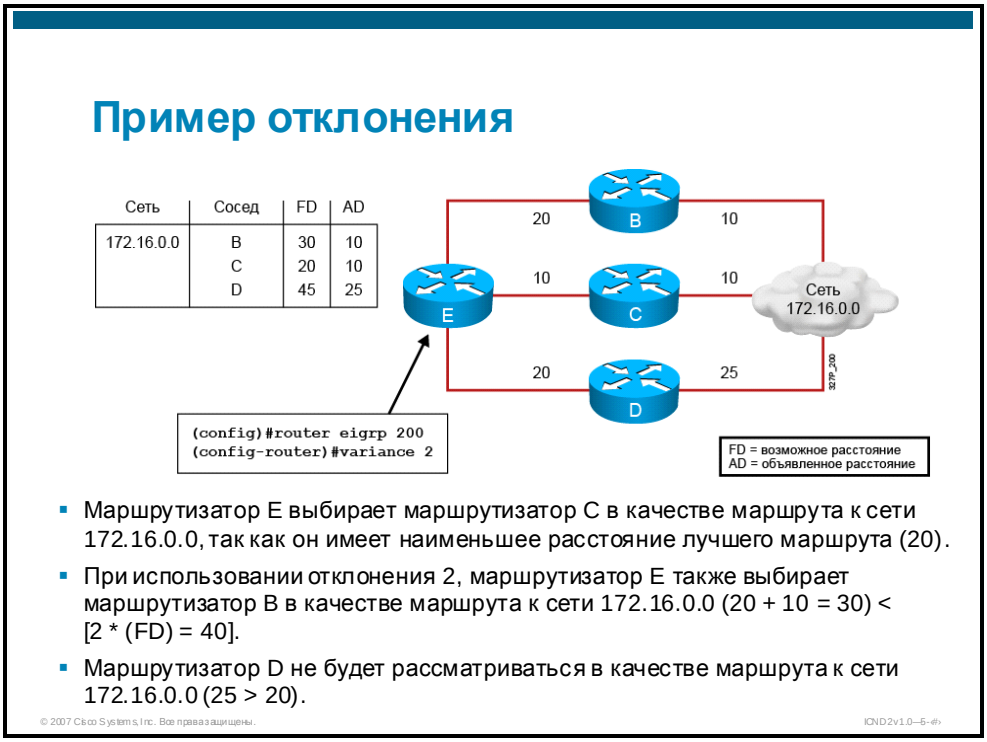
EIGRP также может распределять трафик по нескольким маршрутам с разными метриками. Эта функция называется выравнивание нагрузки по путям с неравной стоимостью. Уровень выравнивания нагрузки EIGRP управляется командой **variance**, как показано на рисунке.

В таблице ниже описывается параметр команды **variance**.

Параметр команды variance

Команда	Описание
множитель	Значение от 1 до 128, используется для выравнивания нагрузки. Значение по умолчанию 1 соответствует выравнивание нагрузки по путям с равной стоимостью. Множитель задает диапазон значений метрики, использование которых допускается при выравнивании нагрузки процессом EIGRP.

Примечание По умолчанию трафик распределяется по каналам с неравной стоимостью пропорционально их метрике.



Пример: Отклонения

На рисунке задано отклонение (variance) 2 и диапазон значений метрики, который представляет расстояния лучших маршрутов маршрутизатора E к сети 172.16.0.0, составляет 20 – 45. Этот диапазон значений определяет пригодность пути для использования в качестве альтернативного маршрута.

Маршрут считается пригодным, если следующий маршрутизатор на пути находится ближе к месту назначения, чем текущий маршрутизатор, и метрика альтернативного маршрута находится в пределах отклонения. Для выравнивания маршрута могут использоваться только альтернативные пути, и только альтернативные пути добавляются в таблицу маршрутизации. Условия альтернативности маршрута выглядят следующим образом.

- Локальная лучшая метрика, которая является текущим расстоянием лучшего маршрута, должна быть выше, чем лучшая метрика (объявленное расстояние), полученное от следующего маршрутизатора. Другими словами, следующий маршрутизатор на пути должен быть ближе к месту назначения, чем текущий маршрутизатор. Это позволяет предотвратить образование петель маршрутизации.
- Метрика альтернативного пути должна быть ниже, чем отклонение, умноженное на локальную лучшую метрику (текущее расстояние лучшего маршрута).

Если маршрут соответствует обоим условиям, он определяется как альтернативный и может быть добавлен в таблицу маршрутизации.

На рисунке к сети 172.16.0.0 доступно три пути со следующими метриками:

- **Путь 1:** 30 (через маршрутизатор B)
- **Путь 2:** 20 (через маршрутизатор C)
- **Путь 3:** 45 (через маршрутизатор D)

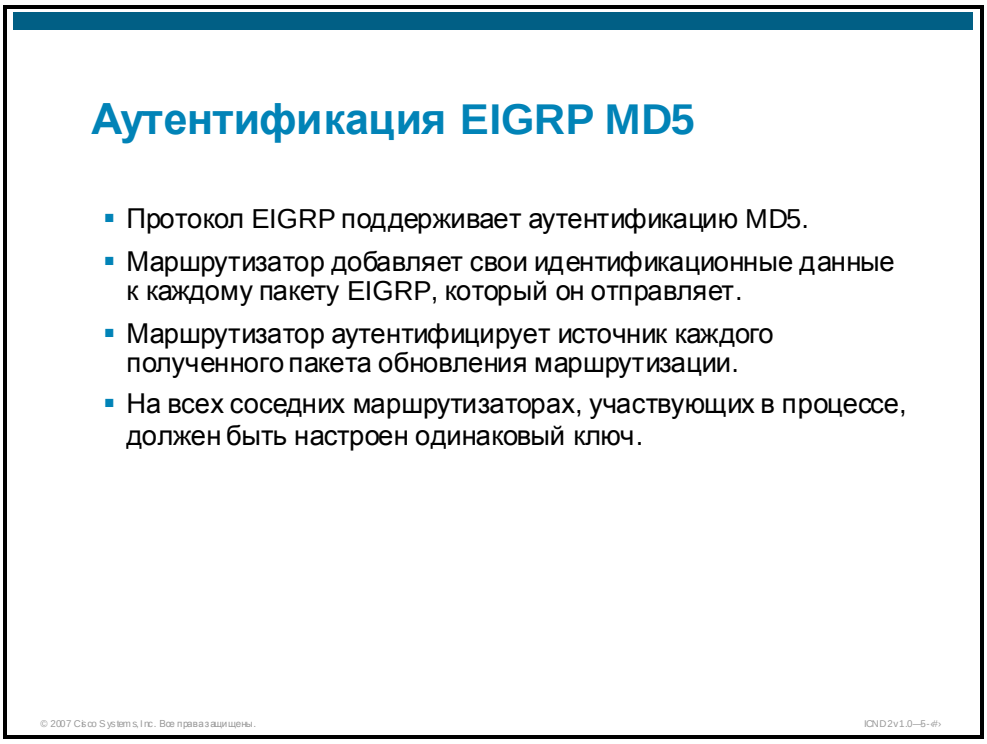
По умолчанию маршрутизатор помещает в таблицу маршрутизации только путь 2 (через маршрутизатор C), поскольку он имеет наименьшую стоимость. Для выравнивания нагрузки по путям 1 и 2, используйте отклонение 2, так как значение 20 * 2 = 40 больше, чем метрика пути 1.

В этом примере маршрутизатор E использует маршрутизатор C в качестве лучшего маршрута, так как он имеет наименьшее расстояние лучшего маршрута (20). После выполнения команды **variance 2** на маршрутизаторе E, путь через маршрутизатор B будет удовлетворять критериям выравнивания нагрузки. В этом случае расстояние пути через маршрутизатор B будет ниже, чем удвоенное расстояние лучшего маршрута (маршрутизатор C).

Маршрутизатор D не рассматривается для выравнивания нагрузки при использовании этого отклонения, так как расстояние пути через маршрутизатор D превышает удвоенное расстояние лучшего маршрута (маршрутизатор C). Однако в этом примере маршрутизатор D не станет альтернативным маршрутом, какое бы отклонение вы не задали. Это решение основывается на том, что объявленное расстояние маршрутизатора D равняется 25, а это выше, чем расстояние лучшего маршрута для маршрутизатора E (20), поэтому, чтобы избежать образования петли маршрутизации, маршрутизатор D не рассматривается в качестве альтернативного маршрута.

Аутентификация EIGRP

В этом разделе описывается настройка аутентификации для EIGRP.



Аутентификация соседних узлов EIGRP (также известная как аутентификация соседних маршрутов или аутентификация маршрутов) позволяет маршрутизаторам принимать участие в процессе маршрутизации только при наличии пароля. По умолчанию аутентификация для пакетов EIGRP не используется. Для протокола EIGRP можно настроить аутентификацию Message Digest 5 (MD5).

Маршрутизатор, на котором настроена аутентификация соседних узлов, аутентифицирует источник каждого полученного пакета обновления маршрутизации. Для аутентификации EIGRP MD5 необходимо настроить ключ аутентификации и идентификатор ключа на маршрутизаторе-получателе и маршрутизаторе-отправителе. Иногда этот ключ называют паролем.

Этапы конфигурации EIGRP MD5

1. Создание цепочки ключей, группы доступных ключей (паролей).
2. Назначение идентификатора каждому ключу.
3. Идентификация ключей.
4. (Необязательно) Задание срока действия ключа.
5. Включение аутентификации MD5 на интерфейсе.
6. Задание цепочки ключей для интерфейса.

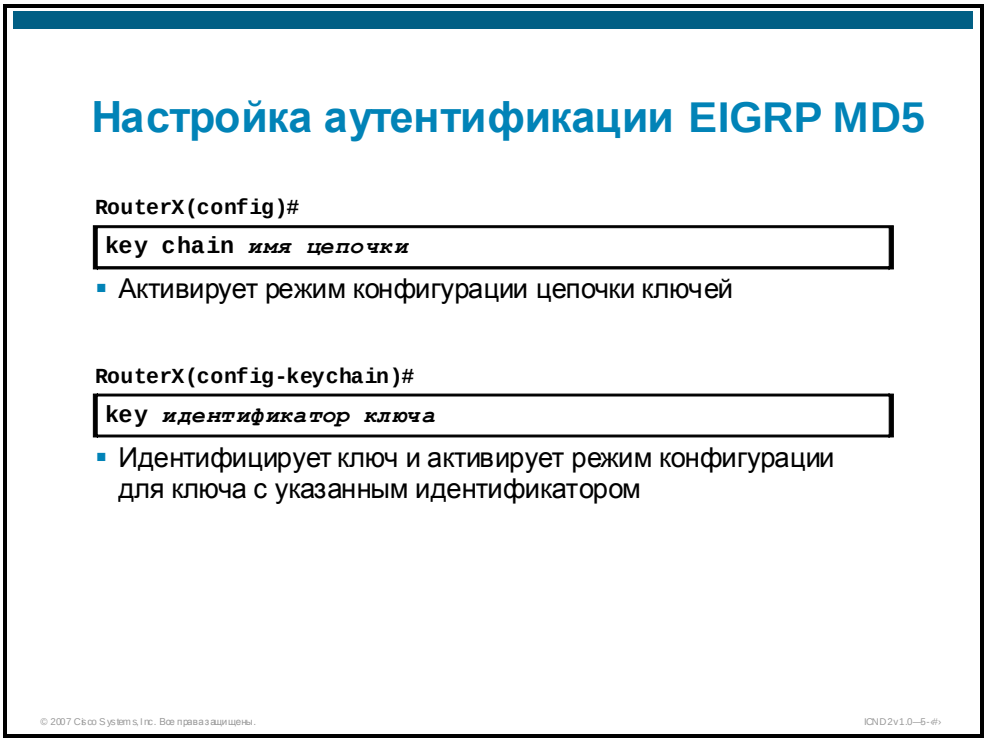
Добавление дайджеста MD5 с ключом в каждый пакет EIGRP предотвращает распространение неавторизованных или поддельных обновлений маршрутизации от неодобренных источников.

Каждому ключу присваивается идентификатор, который маршрутизатор хранит локально. Сочетание идентификатора ключа и интерфейса, связанного с сообщением, позволяет уникально идентифицировать алгоритм аутентификации и используемый ключ MD5.

EIGRP позволяет управлять ключами с помощью цепочек ключей. Определение каждого ключа в цепочке ключей может содержать период времени, на который активирован ключ (время жизни ключа). В течение времени жизни ключа пакеты обновления маршрутизации отправляются с этим активированным ключом. Отправляется только один пакет аутентификации, независимо от числа действительных ключей. Программное обеспечение проверяет номера ключей снизу вверх и использует первый действительный ключ.

Ключи нельзя использовать в периоды времени, когда они не активированы. Поэтому в цепочке ключей рекомендуется настраивать перекрывающиеся периоды, чтобы хотя бы один из ключей был активен в любой момент времени. Если в течение определенного интервала активные ключи отсутствуют, аутентификация выполняться не будет и обновление маршрутизации будет невозможно.

Примечание Важно, чтобы маршрутизаторы знали точное время для обеспечения синхронного перехода между ключами на маршрутизаторах, участвующих в процессе. Это позволит гарантировать, что маршрутизаторы используют одинаковые ключи в заданный момент времени.



Для создания цепочки ключей выполните следующие действия:

Действие 1 Введите команду **key chain**, чтобы перейти в режим конфигурации цепочки ключей (см. рисунок). В таблице описывается параметр этой команды.

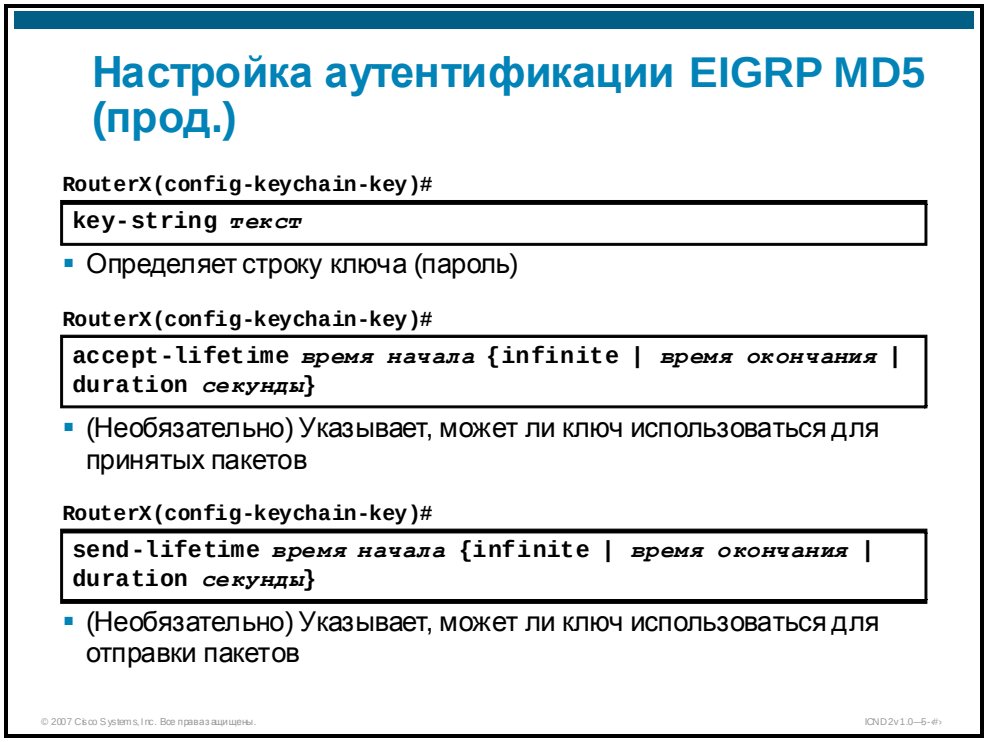
Параметр команды key chain

Параметр	Описание
имя цепочки	Имя цепочки ключей аутентификации, из которой необходимо извлечь ключ.

Действие 2 С помощью команды **key** задайте идентификатор ключа и перейдите в режим конфигурации для этого ключа (см. рисунок). В таблице описывается параметр этой команды.

Параметр команды key

Параметр	Описание
идентификатор ключа	Идентификационный номер ключа аутентификации в цепочке ключей. Диапазон номеров ключей: 0 – 2147483647. Идентификационные номера не обязательно должны быть последовательными.



Действие 3 С помощью команды **key-string** задайте строку ключа (пароль) (см рисунок). В таблице описывается параметр этой команды.

Параметр команды key-string

Параметр	Описание
текст	Строка, используемая для аутентификации принимаемых и отправляемых пакетов EIGRP. Строка может содержать от 1 до 80 буквенно-цифровых символов в верхнем или нижнем регистре. Первый символ не может быть цифрой, строка вводится с учетом регистра.

Действие 4 (Необязательно) Кроме того, можно использовать команду **accept-lifetime**, чтобы задать время, в течение которого допускается использование ключа для принимаемых пакетов (см. рисунок). Если вы не введете команду **accept-lifetime**, будет использоваться бесконечный период. В таблице описываются параметры этой команды.

Параметры команды accept-lifetime

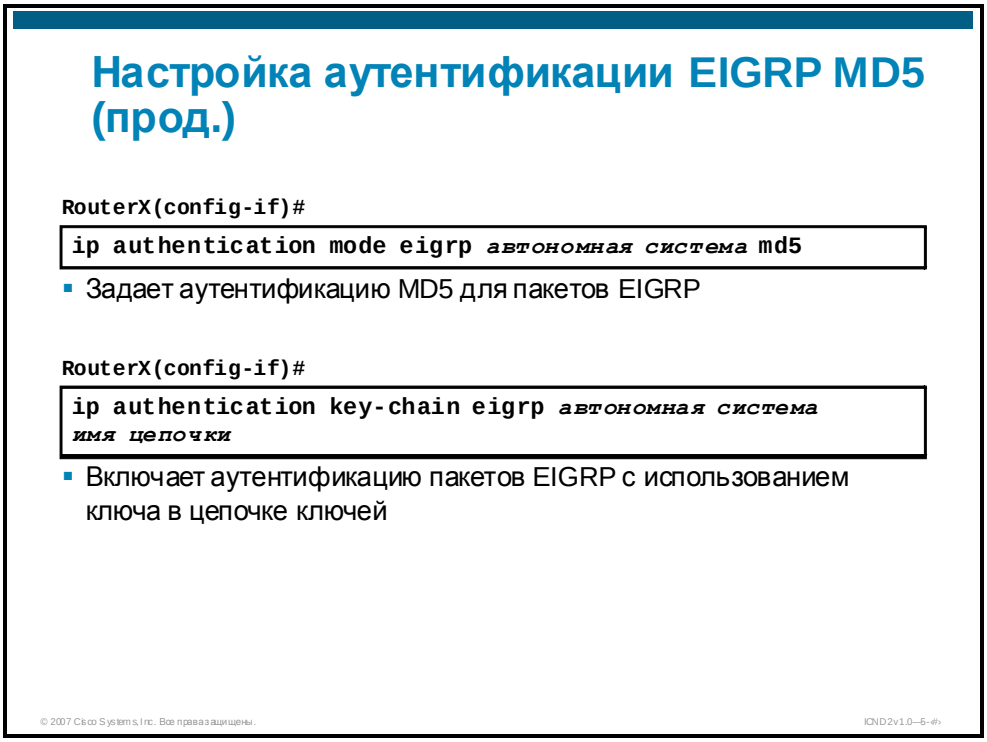
Параметр	Описание
время начала	Начало периода, в течение которого ключ, указанный с помощью команды **key**, можно использовать для принимаемых пакетов. Синтаксис может иметь следующий вид. ■ чч:мм:сс месяц дата год ■ чч:мм:сс дата месяц год — ***чч*:** часы — ***мм*:** минуты — ***сс*:** секунды — ***месяц*:** первые три буквы названия месяца — ***дата*:** дата (1 – 31) — ***год*:** год (4 цифры) Время начала по умолчанию. Самая ранняя допустимая дата: 1 января, 1993 г.
infinite	Ключ можно использовать для принимаемых пакетов начиная с *времени начала* без ограничений по времени окончания.
время окончания	Ключ можно использовать для принимаемых пакетов с *времени начала* до *времени окончания*. Синтаксис аналогичен параметру *время начала*. *Время окончания* должно быть позже *времени начала*. Значение по умолчанию – infinite.
секунды	Период времени (в секундах) в течение которого ключ можно использовать для принимаемых пакетов. Диапазон значений: 1 – 2147483646.

Действие 5 (Необязательно) Введите команду **send-lifetime**, чтобы задать время, в течение которого допускается использование ключа для отправляемых пакетов (см. рисунок). Если вы не введете команду **send-lifetime**, будет использоваться бесконечный период. В таблице описываются параметры этой команды.

Параметры команды send-lifetime

Параметр	Описание
время начала	Начало периода, в течение которого ключ, указанный с помощью команды **key**, можно использовать для отправляемых пакетов. Синтаксис может иметь следующий вид. ■ чч:мм:сс месяц дата год ■ чч:мм:сс дата месяц год — ***чч*:** часы — ***мм*:** минуты — ***сс:*** секунды — ***месяц:*** первые три буквы названия месяца — ***дата:*** дата (1 – 31) — ***год:*** год (4 цифры) Время начала по умолчанию и самая ранняя допустимая дата: 1 января, 1993 г.
infinite	Ключ можно использовать для отправляемых пакетов начиная с *времени начала* без ограничений по времени окончания.
время окончания	Ключ можно использовать для отправляемых пакетов с *времени начала* до *времени окончания*. Синтаксис аналогичен параметру *время начала*. *Время окончания* должно быть позже *времени начала*. Значение по умолчанию – infinite.
секунды	Период времени (в секундах) в течение которого ключ можно использовать для отправляемых пакетов. Диапазон значений: 1 – 2147483646.

Примечание Если при настройке аутентификации EIGRP не была использована команда **service password-encryption**, ключ будет сохранен в конфигурации маршрутизатора в виде нешифрованного текста. Если команда **service password-encryption** была введена, ключ сохраняется и отображается в зашифрованном виде. Когда пароль выводится, перед ним отображается тип шифрования 7.



Чтобы настроить аутентификацию MD5 для EIGRP, выполните следующие действия:

Действие 1 Перейдите в режим конфигурации для интерфейса, на котором необходимо включить аутентификацию.

Действие 2 С помощью команды **ip authentication mode eigrp md5** включите аутентификацию MD5 для пакетов EIGRP (см. рисунок). В таблице описывается параметр этой команды.

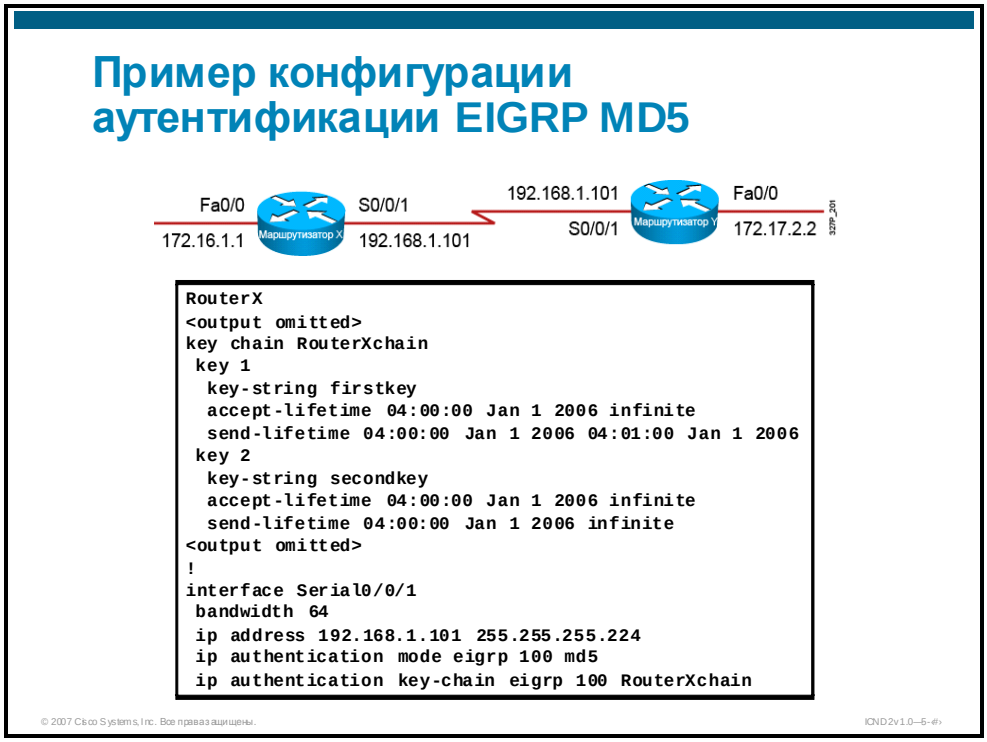
Параметр команды ip authentication mode eigrp md5

Параметр	Описание
автономная система	Номер автономной системы EIGRP, для которой будет использоваться аутентификация

Действие 3 Укажите цепочку ключей, которая будет использоваться для аутентификации пакетов EIGRP с помощью команды **ip authentication key-chain eigrp**. Параметры это команды описываются в таблице.

Параметры команды ip authentication key-chain eigrp

Параметр	Описание
автономная система	Номер автономной системы EIGRP, для которой будет использоваться аутентификация
имя цепочки	Имя цепочки ключей аутентификации, из которой необходимо извлечь ключ



Пример: Конфигурация аутентификации MD5

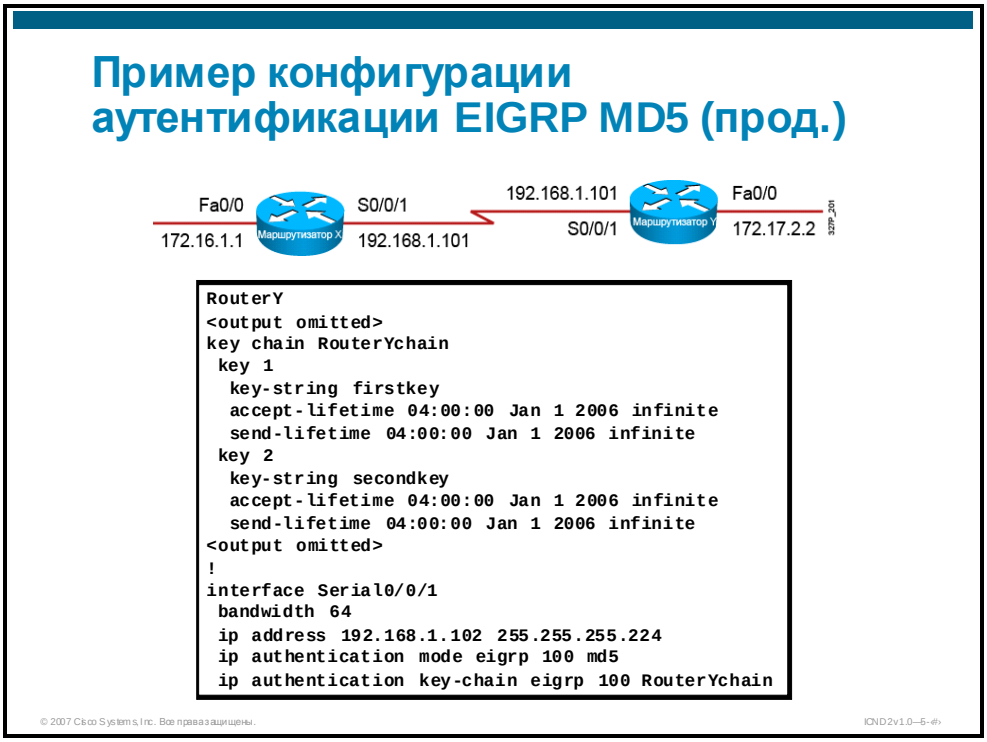
На рисунке приводится конфигурация аутентификации EIGRP MD5 для маршрутизатора X.

Аутентификация MD5 настраивается на последовательном интерфейсе 0/0/1 с помощью команды **ip authentication mode eigrp 100 md5**. Команда **ip authentication key-chain eigrp 100 RouterXchain** активирует использование цепочки ключей RouterXchain для автономной системы EIGRP AS 100.

Команда **key chain RouterXchain** активирует режим конфигурации для цепочки ключей RouterXchain. Задаются два ключа. Ключ 1 задается в качестве «первого ключа» с помощью команды **key-string firstkey**. Этот ключ будет использоваться для пакетов, принятых маршрутизатором X, начиная с 4:00 (0400) 1-го января 2006 г. (команда **accept-lifetime 04:00:00 Jan 1 2006 infinite**). Команда **send-lifetime 04:00:00 Jan 1 2006 04:01:00 Jan 1 2006** указывает, что этот ключ можно использовать для отправляемых пакетов только в течение одной минуты 1-го января 2006 г. После этого ключ станет недействительным аутентификации отправляемых пакетов.

Ключ 2 задается в качестве «второго ключа» с помощью команды **key-string secondkey**. Этот ключ будет использоваться для пакетов, принятых маршрутизатором X, начиная с 4:00 (0400) 1-го января 2006 г. (команда **accept-lifetime 04:00:00 Jan 1 2006 infinite**). Кроме того, это ключ можно использовать для пакетов, отправленных с 4:00 (0400) 1-го января 2006 г. (команда **send-lifetime 04:00:00 Jan 1 2006 infinite**).

Таким образом маршрутизатор X принимает и пытается проверить дайджест MD5 всех пакетов EIGRP с идентификатором ключа 1. Кроме того, маршрутизатор X примет пакет с идентификатором ключа 2. Все остальные пакеты MD5 будут отброшены. Маршрутизатор X отправляет все пакеты EIGRP с ключом 2, поскольку ключ 1 больше не действителен для отправки пакетов.



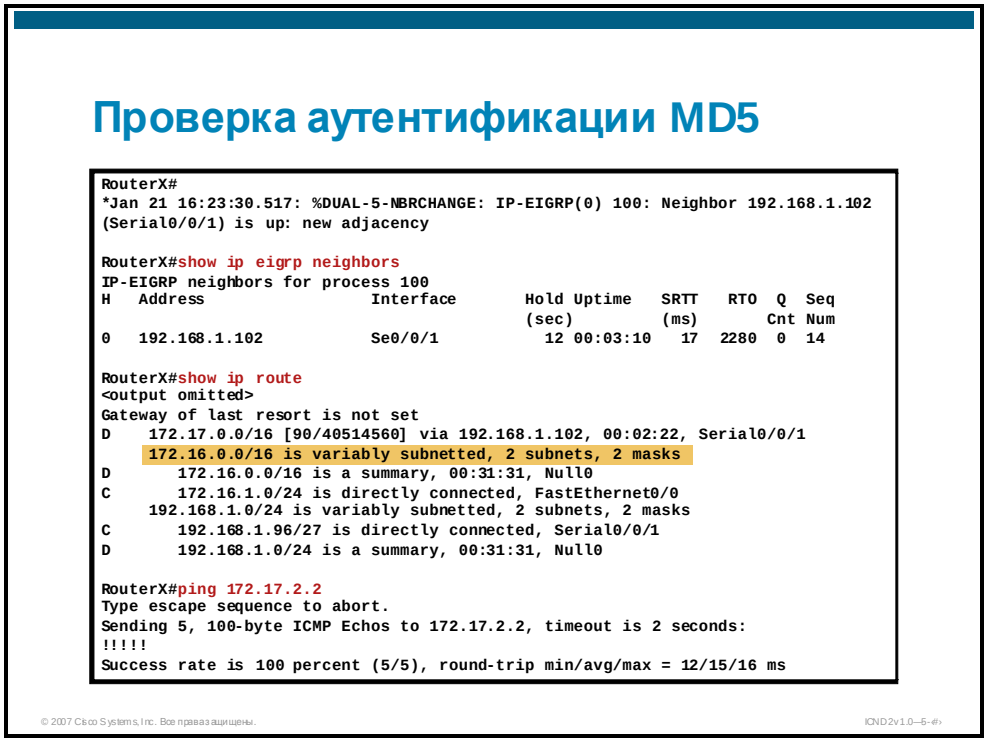
На рисунке приводится конфигурация аутентификации EIGRP MD5 для маршрутизатора Y.

Аутентификация MD5 настраивается на последовательном интерфейсе 0/0/1 с помощью команды **ip authentication mode eigrp 100 md5**. Команда **ip authentication key-chain eigrp 100 RouterYchain** активирует использование цепочки ключей RouterXchain для автономной системы EIGRP AS 100.

Команда **key chain RouterYchain** активирует режим конфигурации для цепочки ключей RouterXchain. Задаются два ключа. Ключ 1 задается в качестве «первого ключа» с помощью команды **key-string firstkey**. Этот ключ будет использоваться для пакетов, принятых маршрутизатором Y, начиная с 4:00 (0400) 1-го января 2006 г. (команда **accept-lifetime 04:00:00 Jan 1 2006 infinite**). Кроме того, это ключ можно использовать для пакетов, отправленных с 4:00 (0400) 1-го января 2006 г. (команда **send-lifetime 04:00:00 Jan 1 2006 infinite**).

Ключ 2 задается в качестве «второго ключа» с помощью команды **key-string secondkey**. Этот ключ будет использоваться для пакетов, принятых маршрутизатором Y, начиная с 4:00 (0400) 1-го января 2006 г. (команда **accept-lifetime 04:00:00 Jan 1 2006 infinite**). Кроме того, это ключ можно использовать для пакетов, отправленных с 4:00 (0400) 1-го января 2006 г. (команда **send-lifetime 04:00:00 Jan 1 2006 infinite**).

Таким образом маршрутизатор X принимает и пытается проверить дайджест MD5 всех пакетов EIGRP с идентификатором ключа 1 или 2. Кроме того, маршрутизатор Y будет использовать ключ 1 для отправки всех пакетов EIGRP, так как это первый действующий ключ в цепочке ключей.



Проверка аутентификации MD5

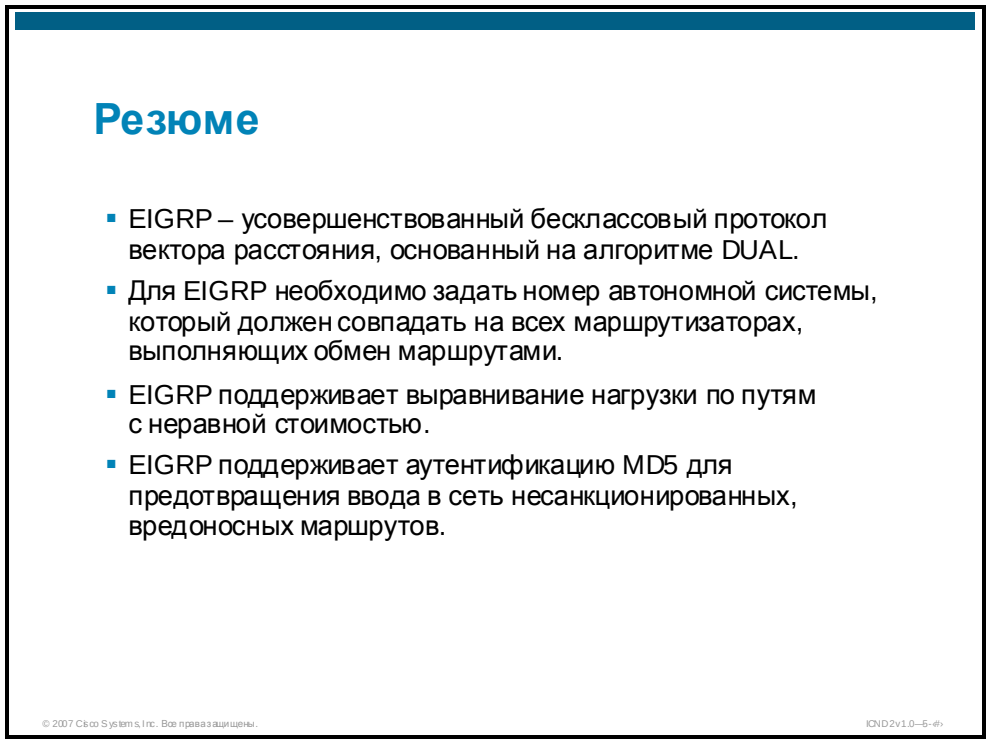
На рисунке приводится вывод команд **show ip eigrp neighbors** и **show ip route**.

Тот факт, что в таблице соседних узлов отображается IP-адрес маршрутизатора Y указывает на то, что два маршрутизатора успешно сформировали смежность EIGRP. Таблица маршрутизации подтверждает, что адрес 172.17.0.0 был получен через протокол EIGRP от последовательного интерфейса. Таким образом аутентификация MD5 для EIGRP между маршрутизаторам X и Y выполнена успешно.

Также приводятся результаты отправки эхо-запроса в интерфейс Fast Ethernet маршрутизатора Y, чтобы доказать работоспособность канала.

Резюме

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



Занятие 2

Устранение неполадок EIGRP

Обзор

Будучи усовершенствованным протоколом маршрутизации на основе вектора расстояния, EIGRP хорошо масштабируется с ростом сети. Но эта масштабируемость усложняет проектирование, настройку и обслуживание сети. В этом занятии описывается несколько общих проблем, возникающих в сети EIGRP, а также метод поиска и устранения этих проблем на основе рабочей диаграммы.

Задачи

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

- описывать основные составляющие процедуры поиска и устранения неполадок сети под управлением EIGRP;
- выявлять и устранять проблемы отношений соседства EIGRP;
- выявлять и устранять проблемы таблицы маршрутизации EIGRP;
- выявлять и устранять проблемы аутентификации EIGRP.

Составляющие процедуры поиска и устранения неполадок EIGRP

В этом разделе описываются основные составляющие процедуры поиска и устранения неполадок сети под управлением EIGRP.

Основные составляющие процедуры поиска и устранения неполадок EIGRP:

- отношения соседства EIGRP;
- маршруты EIGRP в таблице маршрутизации;
- аутентификация EIGRP.

Поиск и устранение неполадок соседства EIGRP

В этом разделе описывается выявление и устранение ошибок, связанных с состоянием соседства EIGRP.

Пример вывода команды **show ip eigrp neighbors** показывает, что отношения соседства между двумя маршрутизаторами установлены успешно.

```
RouterX# show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address         Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                    (sec)         (ms)       Cnt Num
1   10.23.23.2      Se0/0/1          13 00:02:26   29   2280  0  15
0   10.140.1.1      Se0/0/0          10 00:28:26   24   2280  0  25
```

Чтобы маршрутизаторы EIGRP могли сформировать отношения соседства, два маршрутизатора должны быть подключены к общей IP-подсети. Сообщение журнала о том, что соседние узлы EIGRP не находятся в общей сети, означает, что на одном из двух соседних интерфейсов EIGRP настроен неверный IP-адрес. Используйте команду **show interface** *интерфейс* для проверки IP-адреса.

В выводе ниже отображается адрес 10.2.2.3/24.

```
RouterX# sh ip int fa0/0
FastEthernet0/0 is up, line protocol is up
  Internet address is 10.2.2.3/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
```

```
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
```

Команда **network**, выполненная для процесса маршрутизации EIGRP, позволяет определить, какие интерфейсы маршрутизатора будут участвовать в процессе EIGRP. В разделе «Routing for Networks» вывода команды **show ip protocols** перечисляются настроенные сети и интерфейсы в этих сетях, участвующие в процессе EIGRP. Вывод ниже показывает, что процесс EIGRP работает на всех интерфейсах с IP-адресом в сетях 10.0.0.0 и 192.168.1.0.

```
RouterX# sh ip protocols
Routing Protocol is «eigrp 100»
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 100
--output omitted --
  Maximum path: 4
  Routing for Networks:
    10.0.0.0
    192.168.1.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    (this router)         90      00:01:08
    10.140.1.1            90      00:01:08
  Distance: internal 90 external 170
```

Команда **sh ip eigrp interfaces** позволяет быстро определить, какие интерфейсы EIGRP включены и сколько соседних узлов задано для каждого из интерфейсов. В выводе ниже для интерфейса Fast Ethernet 0/0 не заданы соседние узлы, и для последовательного интерфейса 0/0/0 задан один соседний узел.

```
RouterX# sh ip eigrp interfaces
IP-EIGRP interfaces for process 100

              Xmit Queue   Mean   Pacing Time   Multicast    Pending
Int    Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Fa0/0    0        0/0         0       0/1            0           0
Se0/0/0  1        0/0        38      10/380        552           0
```


Маршрутизаторы EIGRP создают отношения соседства за счет обмена пакетами приветствия. Для формирования отношений соседства EIGRP поля пакета приветствия должны совпадать.

- номер автономной системы (AS) EIGRP;
- значения EIGRP K.

Примечание Значения EIGRP K используются в процессе выбора лучшего пути EIGRP и рассматриваются в курсе Cisco CCNP®.

Для поиска и устранения неполадок при несовпадении данных в пакетах можно использовать команду **debug eigrp packets**. В примере ниже не совпадают значения K.

```
RouterX# debug eigrp packets

Mismatched adjacency values
01:39:13: EIGRP: Received HELLO on Serial0/0 nbr 10.1.2.2
01:39:13:AS 100, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0 peerQ
un/rely 0/0
01:39:13:        K-value mismatch
```

Поиск и устранение неполадок таблиц маршрутизации EIGRP

В этом разделе описывается выявление и устранение проблем маршрутов EIGRP в таблице маршрутизации.

Код «D» в записи EIGRP таблицы маршрутизации обозначает маршруты внутри автономной системы, код «D EX» обозначает внешние маршруты. Маршруты EIGRP в таблице маршрутизации не позволяют выявить проблемы уровней 2 и 3, а также проблемы соседства EIGRP.

В примере вывода сеть 172.16.31.0/24 является маршрутом внутри автономной системы, а сеть 10.3.3.0/24 – маршрутом, перераспределенным в EIGRP.

```
RouterX# sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
D       172.16.31.0/24 [90/40640000] via 10.140.1.1, 00:01:09,
Serial0/0/0
O       172.16.31.100/32 [110/1563] via 10.140.1.1, 00:26:55,
Serial0/0/0
```



```
     10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
C       10.23.23.0/24 is directly connected, Serial0/0/1
D EX      10.3.3.0/24 [170/40514560] via 10.23.23.2, 00:01:09,
Serial0/0/1
C       10.2.2.0/24 is directly connected, FastEthernet0/0
```

Команда **show ip eigrp topology** отображает идентификатор маршрутизатора EIGRP. В качестве идентификатора маршрутизатора EIGRP используется самый высокий IP-адрес интерфейса возвратной петли. Если интерфейсы возвратной петли не заданы, в качестве идентификатора маршрутизатора используется IP-адрес, назначенный любому из активных интерфейсов. Два маршрутизатора EIGRP не могут иметь одинаковый идентификатор маршрутизатора EIGRP. В этом случае при обмене данными между этими маршрутизаторами могут возникнуть проблемы.

В примере вывода идентификатор маршрутизатора – 192.168.1.65.

```
RouterX# show ip eigrp topology
IP-EIGRP Topology Table for AS(100)/ID(192.168.1.65)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 10.1.1.0/24, 1 successors, FD is 40514560
        via 10.140.1.1 (40514560/28160), Serial0/0/0
P 10.2.2.0/24, 1 successors, FD is 28160
        via Connected, FastEthernet0/0
P 10.3.3.0/24, 1 successors, FD is 40514560
        via 10.23.23.2 (40514560/28160), Serial0/0/1
P 10.23.23.0/24, 1 successors, FD is 40512000
        via Connected, Serial0/0/1
P 192.168.1.64/28, 1 successors, FD is 128256
        via Connected, Loopback0
P 192.168.1.0/24, 1 successors, FD is 40640000
        via 10.23.23.2 (40640000/128256), Serial0/0/1
P 10.140.2.0/24, 2 successors, FD is 41024000
        via 10.23.23.2 (41024000/40512000), Serial0/0/1
        via 10.140.1.1 (41024000/40512000), Serial0/0/0
P 10.140.1.0/24, 1 successors, FD is 40512000
        via Connected, Serial0/0/0
P 172.16.31.0/24, 1 successors, FD is 40640000
```

Наличие в таблице топологии маршрутов EIGRP, которые отсутствуют в таблице маршрутизации может указывать на проблему, для решения которой может потребоваться помощь Cisco Technical Assistance Center (TAC).

Фильтрация маршрутов позволяет исключить маршруты из объявлений маршрутизации EIGRP при поступлении объявления от соседнего узла или при передаче объявления в соседний узел. Эти фильтры могут стать причиной отсутствия маршрутов в таблице маршрутизации. Команда **show ip protocols** позволяет определить, используются ли фильтры в процессе EIGRP.

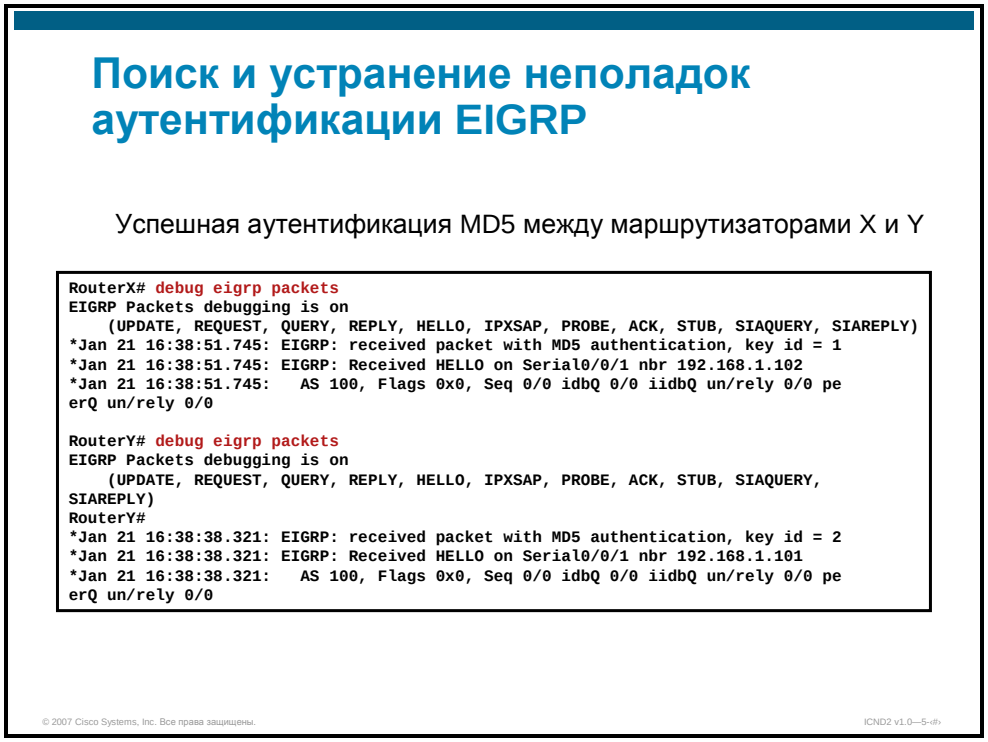
По умолчанию протокол EIGRP работает в классовом режиме и выполняет автоматическое суммирование маршрутов. Автоматическое суммирование маршрутов может привести к возникновению проблем в несмежных сетях. Команда **show ip protocols** позволяет проверить, включено ли автоматическое суммирование маршрутов.

В примере вывода фильтры для процесса EIGRP AS 100 не заданы, и автоматическое суммирование сетей включено.

```
RouterX# sh ip protocols
Routing Protocol is «eigrp 100»
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 100
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is in effect
  Automatic address summarization:
    192.168.1.0/24 for FastEthernet0/0, Serial0/0/0, Serial0/0/1
      Summarizing with metric 128256
    10.0.0.0/8 for Loopback0
      Summarizing with metric 28160
  Maximum path: 4
```


Поиск и устранение неполадок аутентификации EIGRP

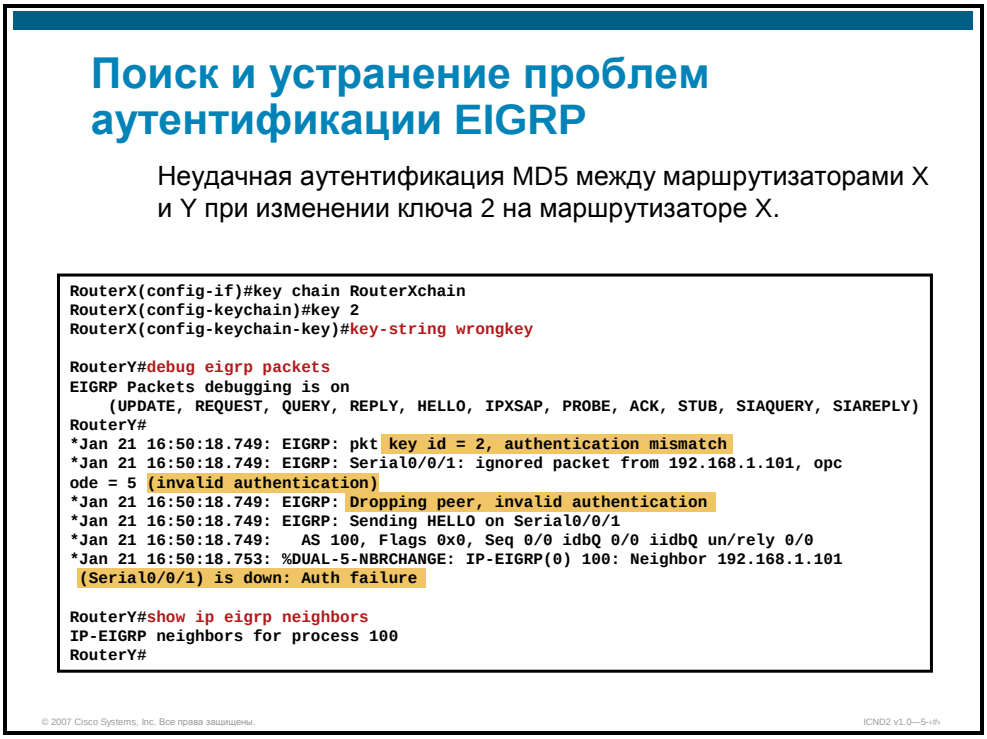
В этом разделе описывается поиск и устранение неполадок аутентификации Message Digest 5 (MD5) для протокола EIGRP.



Пример: Успешная аутентификация MD5

Вывод команды **debug eigrp packets**, выполненной на маршрутизаторе X, на рисунке показывает, что маршрутизатор X принимает пакеты EIGRP с аутентификацией MD5 и идентификатором ключа 1 от маршрутизатора Y.

Вывод команды **debug eigrp packets**, выполненной на маршрутизаторе Y, на рисунке показывает, что маршрутизатор Y принимает пакеты EIGRP с аутентификацией MD5 и идентификаторам ключа 2 от маршрутизатора X.



Пример: устранение неполадок аутентификации MD5

В этом примере строка ключа 2 маршрутизатора X, которая используется при отправке пакета EIGRP, изменена, чтобы отличаться от строки, которой ожидает маршрутизатор Y.

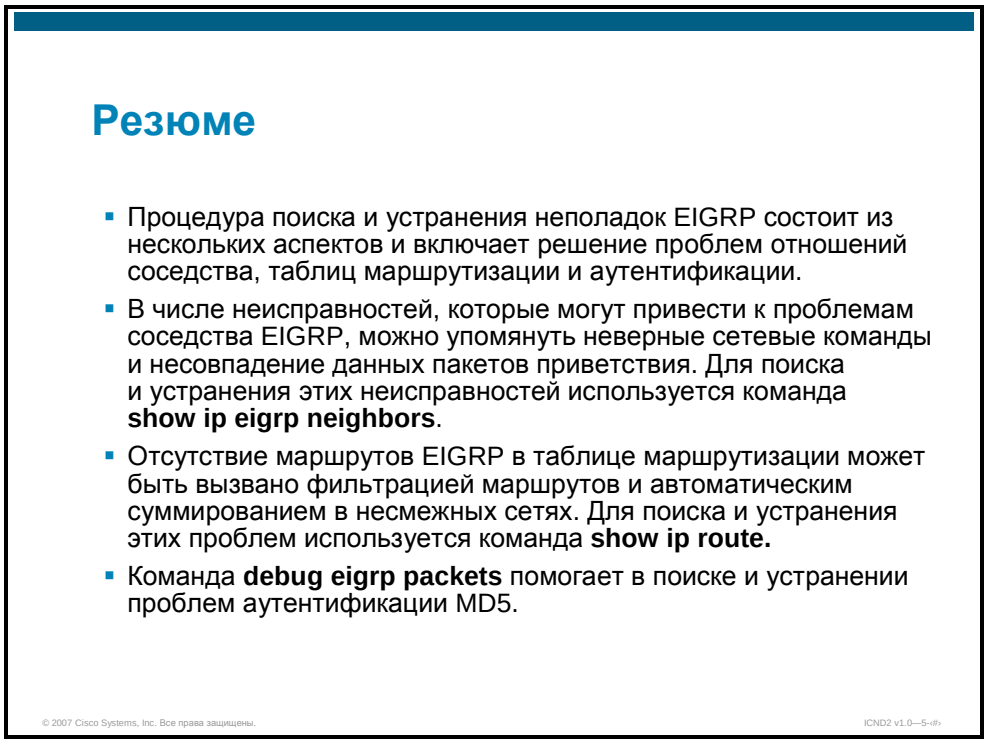
Вывод команды **debug eigrp packets**, выполненной на маршрутизаторе Y, на рисунке показывает, что маршрутизатор Y принимает пакеты EIGRP с аутентификацией MD5 и идентификатором ключа 2 от маршрутизатора X, но строки аутентификации не совпадают. Пакеты EIGRP от маршрутизатора X игнорируются, и отношения соседства объявляются неисправными. Вывод команды **show ip eigrp neighbors** подтверждает, что у маршрутизатора Y нет соседних узлов EIGRP.

Два маршрутизатора продолжат попытки восстановить отношения соседства. Поскольку в этом сценарии для маршрутизаторов используются разные ключи, маршрутизатор X аутентифицирует сообщения приветствия, отправленные маршрутизатором Y, используя ключ 1. Однако, когда маршрутизатор X отправляет сообщение приветствия маршрутизатору Y, используя ключ 2, происходит несовпадение ключей аутентификации. С точки зрения маршрутизатора X отношения соседства будут активны в течение определенного периода времени, но затем время ожидания истечет. Эта ситуация иллюстрируется сообщениями, полученными маршрутизатором X, в следующем примере. Вывод команды **show ip eigrp neighbors** на маршрутизаторе X также показывает, что маршрутизатор Y присутствует в таблице соседних узлов маршрутизатора X в течение короткого периода времени.

```
RouterX#
*Jan 21 16:54:09.821: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor
192.168.1.102 (Serial0/0/1) is down: retry limit exceeded
*Jan 21 16:54:11.745: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor
192.168.1.102 (Serial0/0/1) is up: new adjacency
RouterX# show ip eigrp neighbors
H   Address         Interface   Hold Uptime   SRTT   RTO  Q  Seq
                                (sec)          (ms)       Cnt Num
0   192.168.1.102   Se0/0/1       13 00:00:38    1   5000  1  0
```

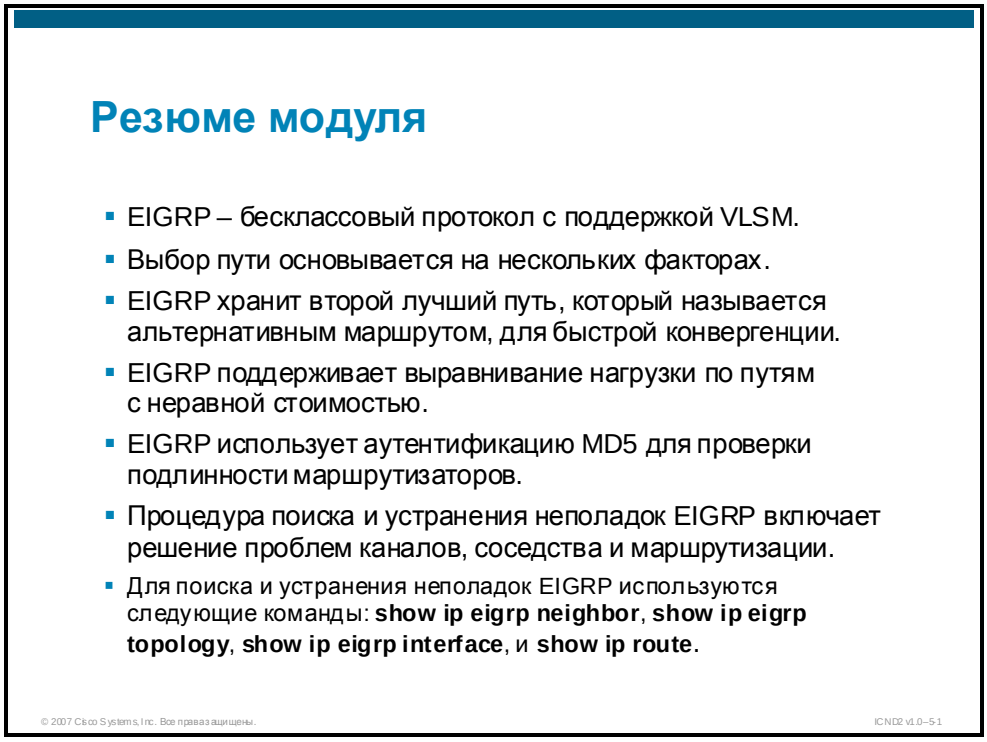

Резюме

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



Резюме модуля

В этом разделе приводится резюме вопросов, рассмотренных в модуле.



EIGRP – протокол маршрутизации Cisco, разработанный для снятия ограничений как протоколов на основе вектора расстояния, так и протоколов состояния канала. Кроме того, в модуле описываются базовые технологии EIGRP, включая процесс выбора пути, изменения в топологии, выравнивание нагрузки, аутентификацию, а также поиск и устранение общих проблем.

Вопросы для самопроверки по модулю

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

В1) Как снизить потребность пакетов EIGRP в полосе пропускания? (Источник: внедрение EIGRP)

А) необходимо распространять только пакеты данных
Б) необходимо распространять только пакеты приветствия
В) необходимо распространять только изменения таблицы маршрутизации и пакеты приветствия
Г) необходимо распространять полную таблицу маршрутизации только среди маршрутизаторов, затронутых изменением

В2) Какая команда указывает, что сеть 10.0.0.0 напрямую подключена к маршрутизатору под управлением EIGRP? (Источник: внедрение EIGRP)

А) Router(config)#**network** 10.0.0.0
Б) Router(config)#**router eigrp** 10.0.0.0
В) Router(config-router)#**network** 10.0.0.0
Г) Router(config-router)#**router eigrp** 10.0.0.0

В3) Какая команда отображает период времени, прошедший с момента последнего получения данных от соседнего узла EIGRP? (Источник: внедрение EIGRP)

А) **show ip eigrp traffic**
Б) **show ip eigrp topology**
В) **show ip eigrp interfaces**
Г) **show ip eigrp neighbors**

В4) Какую команду необходимо выполнить для процесса EIGRP, чтобы маска подсети передавалась вместе с маршрутом? (Источник: устранение неполадок EIGRP)

А) **ip classless**
Б) **no auto-summary**
В) **no summary**
Г) **ip subnet vlsm**

В5) Какая команда позволяет узнать, внедрена ли фильтрация маршрутов? (Источник: устранение неполадок EIGRP)

А) show interface
Б) **show access-list**
В) **show ip protocols**
Г) **show route-filter**

В6) Какой тип аутентификации поддерживает EIGRP? (Источник: внедрение EIGRP)

А) нешифрованный текст
Б) 3DES
В) MD5
Г) A и C

В7) Что значит сообщение EIGRP «neighbor not on common subnet»?
(Источник: устранение неполадок EIGRP)

А) Маршрутизаторы EIGRP имеют одинаковые идентификаторы.
Б) Два смежных соседних интерфейса имеют адреса в разных IP-сетях.
В) На двух соседних смежных маршрутизаторах заданы разные размеры MTU.
Г) Команда EIGRP **network** не была введена в бесклассовом формате.

Ответы на вопросы для самопроверки по модулю

В1) В

В2) В

В3) Г

В4) Б

В5) В

В6) В

В7) Б

Модуль 6

Списки контроля доступа

Обзор

Стандартные и расширенные списки контроля доступа (ACL) ПО Cisco IOS используются для классификации IP-пакетов. Списки контроля доступа позволяют применять ряд функций, таких как шифрование, маршрутизация на основе политик, качество обслуживания (QoS), преобразование сетевых адресов (NAT) и преобразование адресов портов (PAT) к классифицированным пакетам.

Кроме того, стандартные и расширенные списки контроля доступа Cisco IOS можно задать на интерфейсах маршрутизаторов для контроля доступа (безопасности). Функции Cisco IOS могут использоваться на интерфейсах в заданном направлении (для входящего и исходящего трафика). В этом модуле описывается принцип работы списков контроля доступа различных типов, а также настройка списков контроля доступа для IPv4.

Задачи модуля

По окончании этого модуля вы сможете определять способ применения списка контроля доступа в зависимости от требований сети, а также настраивать, проверять и устранять неполадки списков контроля доступа в сети среднего размера. Это значит, что вы сможете выполнять следующие задачи:

- описывать различные типы списков контроля доступа для IPv4;
- выполнять настройку и устранение неполадок стандартных и расширенных, именованных и нумерованных списков контроля доступа для IPv4.

Занятие 1

Введение в списки контроля доступа

Обзор

Чтобы определить наилучший сценарий внедрения списков контроля доступа для сети Cisco, вы должны понимать способы применения списков контроля доступа. Списки контроля доступа предлагают важные функции безопасности и позволяют фильтровать пакеты на входящих и исходящих интерфейсах маршрутизатора.

В этом занятии описываются некоторые из способов применения списков контроля доступа в сетях Cisco, приводятся определения различных типов списков контроля доступа, а также сведения о том, как ПО Cisco IOS обрабатывает списки контроля доступа.

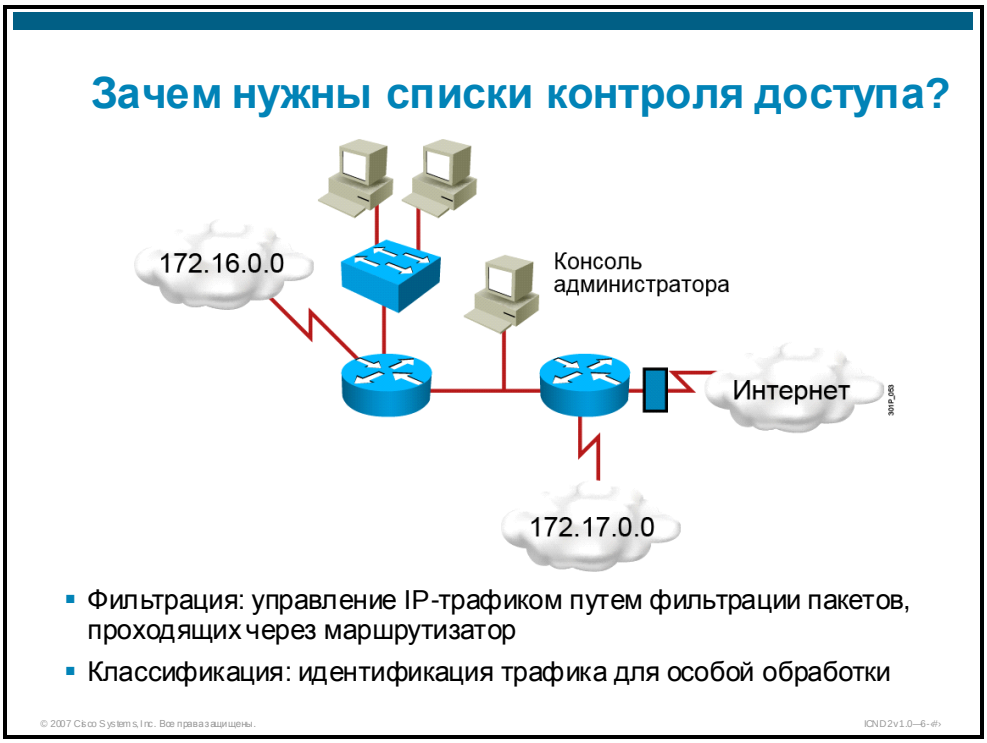
Задачи

По окончании этого занятия вы сможете описывать различные типы списков контроля доступа для IPv4. Это значит, что вы сможете выполнять следующие задачи:

- объяснять назначение списков контроля доступа и приводить примеры ситуаций, в которых их следует использовать;
- объяснять принцип работы входящих и исходящих списков контроля доступа;
- описывать нумерованные и именованные, стандартные и расширенные списки контроля доступа для IPv4;
- описывать временные, рефлексивные и динамические списки контроля доступа;
- использовать шаблонные маски для создания списков контроля доступа для IPv4.

Общие сведения о списках контроля доступа

В этом разделе описывается назначение списков контроля доступа.



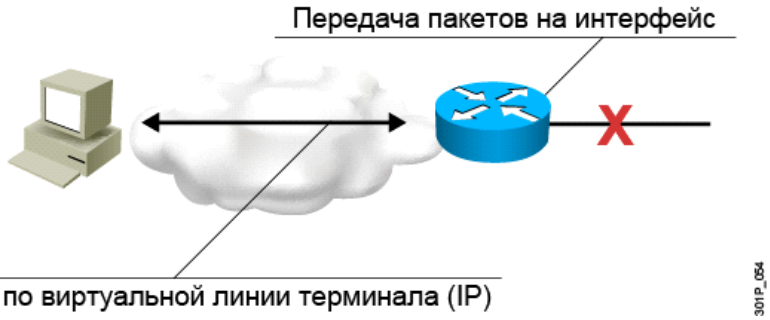
Фильтрация

С увеличением числа подключений маршрутизатора к внешним сетям и расширением использования Интернета, в процедурах контроля доступа возникают новые проблемы. Администраторы сети сталкиваются со сложной дилеммой: как запретить нежелательный трафик, но при этом обеспечить необходимый уровень доступа. Например, список контроля доступа можно использовать для предотвращения доступа к секретным данным подсети финансового отдела из других частей сети.

Классификация

Маршрутизаторы также используют списки контроля доступа для идентификации трафика. Как только список контроля доступа идентифицирует и классифицирует трафик, вы можете настроить инструкции по обработке этого трафика на маршрутизаторе. Например, можно использовать список контроля доступа для идентификации подсети руководства и присвоения этому трафику приоритета над другими типами трафика в перегруженном канале WAN.

Способы применения списков контроля доступа: фильтрация



- Принятие и отклонение пакетов, проходящих через маршрутизатор.
- Разрешение или запрет доступа к маршрутизатору или с маршрутизатора через линии VTY.
- Без списков контроля доступа все пакеты могли бы передаваться во все части сети.

Списки контроля доступа предлагают важный инструмент для контроля трафика в сети. Фильтрация пакетов помогает контролировать перемещение пакетов по сети.

В системах Cisco списки контроля доступа могут запрещать и разрешать следующее:

- прохождение входящих и исходящих пакетов через указанные интерфейсы маршрутизатора и транзитные потоки трафика через маршрутизатор;
- входящий или исходящий трафик Telnet на портах VTY для администрирования маршрутизатора.

По умолчанию весь входящий и исходящий IP-трафик разрешен на всех интерфейсах маршрутизатора.

Когда маршрутизатор отбрасывает пакет, некоторые протоколы возвращают особый пакет, сообщающий отправителю, о том, что место назначения недоступно. Для протокола IP при отклонении пакета списком контроля доступа в ответ на эхо-запрос возвращается сообщение «Destination unreachable (U.U.U.)». В ответ на запрос Traceroute возвращается сообщение «Administratively prohibited (!A * !A)».

Списки контроля доступа могут классифицировать и разделять трафик. Классификация позволяет применять особую обработку к трафику, заданному в списке контроля доступа, в частности:

- определять тип трафика для шифрования через VPN-подключение;
- определять маршруты, которые должны быть перераспределены из одного протокола маршрутизации в другой;
- использовать фильтрацию для определения маршрутов, которые должны быть включены в обновления маршрутизации, рассылаемые между маршрутизаторами;
- использовать маршрутизацию на основе политик для определения типа трафика, который следует направить через выделенный канал;
- использовать совместно с преобразованием сетевых адресов (NAT) для определения адресов, которые необходимо преобразовать.

Принцип работы списков контроля доступа

В этом разделе описывается принцип работы списков контроля доступа.

Списки контроля доступа представляют набор правил, которые обеспечивают дополнительный контроль над пакетами, которые принимаются интерфейсами, транзитными пакетами, которые передаются через маршрутизатор, а также пакетами, которые отправляются из интерфейсов маршрутизатора. Списки контроля доступа не применяются к пакетам, созданным маршрутизатором. Списки представляют собой инструкции, определяющие обработку потоков трафика через указанные интерфейсы маршрутизатора.

Списки контроля доступа работают в двух режимах.

- **Входящие списки контроля доступа.** Входящие пакеты обрабатываются перед перенаправлением на исходящий интерфейс. Входящий список контроля доступа эффективен, так как уменьшает объем служебной информации, связанной с поиском данных маршрутизации, который выполняется, если пакет отклонен в результате фильтрации. Если пакет успешно проходит проверки, он передается на обработку для маршрутизации.
- **Исходящие списки контроля доступа.** Исходящие пакеты направляются в исходящий интерфейс, а затем обрабатываются исходящим списком контроля доступа.

Пример: Исходящий список контроля доступа

На рисунке приводится пример исходящего списка контроля доступа. Когда пакет прибывает на интерфейс, маршрутизатор проверяет таблицу маршрутизации, чтобы определить, подлежит ли пакет маршрутизации. Если пакет не подлежит маршрутизации, он отбрасывается.

Затем маршрутизатор проверяет, задан ли интерфейс назначения в списке контроля доступа. Если интерфейс не задан, пакет отправляется в выходной буфер. Примеры работы исходящего списка контроля доступа:

- Если используется исходящий интерфейс S0, который не задан в исходящем списке контроле доступа, пакет отправляется в интерфейс S0 напрямую.
- Если используется исходящий интерфейс S1, который задан в списке контроля доступа, пакет отправляется в интерес S1 только после проверки на соответствие инструкциям списка контроля доступа. В зависимости от результата проверки пакет принимается или отклоняется.

Для исходящих списков контроля доступа принятие означает отправку пакета в выходной буфер, а отклонение – отбрасывание пакета.

Пример: Исходящий список контроля доступа

При использовании входящего списка контроля доступа, когда пакет прибывает на интерфейс, маршрутизатор проверяет, задан ли интерфейс-источник в списке контроля доступа. Если интерфейс-источник не задан, маршрутизатор проверяет таблицу маршрутизации, чтобы определить, подлежит ли пакет маршрутизации. Если пакет не подлежит маршрутизации, он отбрасывается.

Примеры работы входящего списка контроля доступа:

- Если используется входящий интерфейс E0, который не задан во входящем списке доступа, пакет обрабатывается как обычно. Маршрутизатор проверяет, подлежит ли пакет маршрутизации.
- Если используется исходящий интерфейс E1, который задан во входящем списке контроля доступа, пакет отправляется в интерфейс E1 только после проверки на соответствие инструкциям списка контроля доступа. В зависимости от результата проверки пакет принимается или отклоняется.

Для исходящих списков контроля доступа принятие означает продолжение обработки пакета после его получения на входящем интерфейсе, а отклонение – отбрасывание пакета.

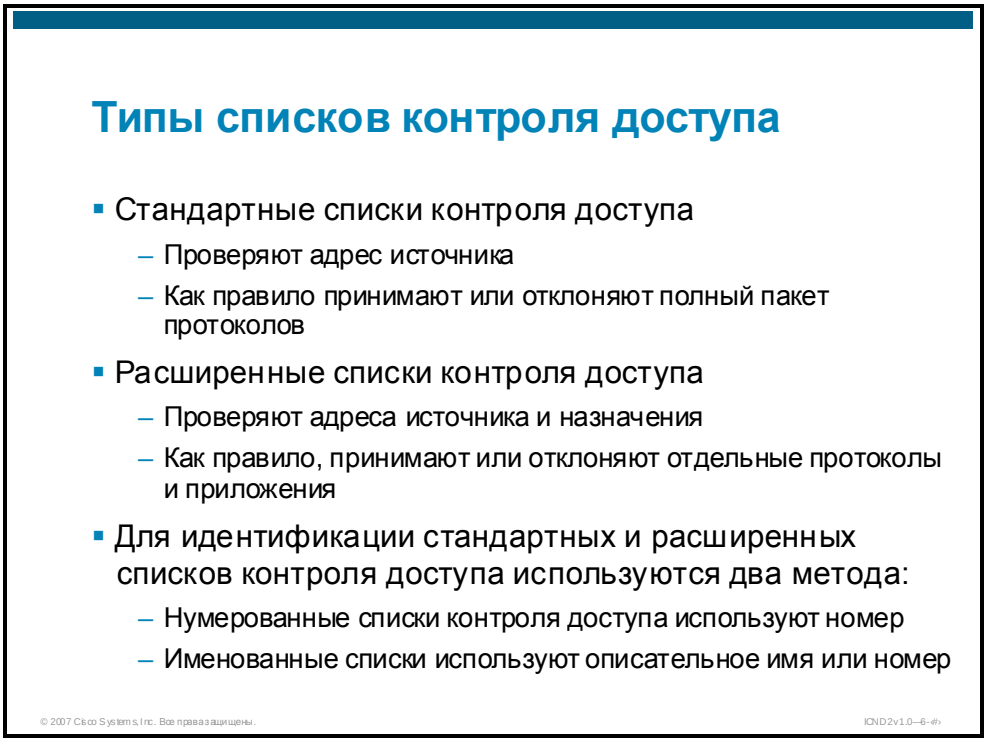
Инструкции списков контроля доступа выполняются в логической последовательности. Они оценивают пакеты сверху вниз по одной инструкции за раз. Если заголовок пакета соответствует инструкции списка контроля доступа, остальные инструкции пропускается, и пакет принимается или отклоняется, в зависимости от инструкции. Если заголовок пакета не соответствует инструкции списка контроля доступа, пакет проверяется на соответствие следующей инструкции в списке. Этот процесс повторяется, пока не доходит до конца списка инструкций.

Последняя инструкция охватывает все пакеты, не удовлетворяющие условиям проверки. Это условие проверки соответствует всем оставшимся пакетам и инициирует инструкцию «отклонить». Маршрутизатор отбрасывает все оставшиеся пакеты, не передавая их в интерфейс или из интерфейса. Эта последняя инструкция часто называется инструкцией «отклонить все». Из-за этой инструкции список контроля доступа должен иметь хотя бы одну разрешающую инструкцию, в противном случае он будет отклонять весь трафик.

Список контроля доступа можно применить к нескольким интерфейсам. Однако для каждого протокола, направления и интерфейса можно задать только один список контроля доступа.

Типы списков контроля доступа

В этом разделе описываются различные типы списков контроля доступа для IPv4 и методы их идентификации.

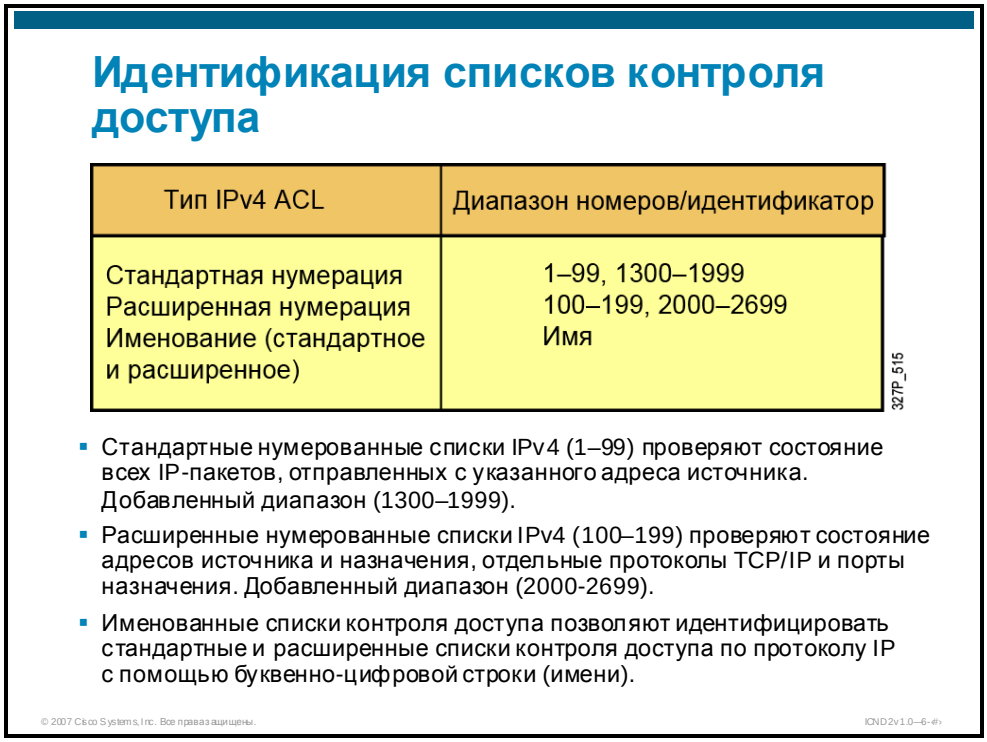


Списки контроля доступа можно разделить на следующие типы.

- **Стандартные списки контроля доступа.** Стандартные списки контроля доступа по протоколу IP проверяют адреса источников маршрутизируемых пакетов. В результате данные полного пакета протоколов принимаются или отклоняются в зависимости от IP-адреса сети-источника, подсети или хоста.
- **Расширенные списки контроля доступа.** Расширенные списки контроля доступа проверяют адреса источника и назначения, протоколы, номера портов и другие параметры, что обеспечивает администраторам дополнительную гибкость и контроль.

Существует два типа идентификации стандартных и расширенных списков контроля доступа:

- нумерованные списки контроля доступа используют номер;
- именованные списки используют описательное имя или номер.



Идентификация списков контроля доступа

При создании нумерованного списка контроля доступа в качестве первого аргумента глобальной инструкции списка контроля доступа вводится номер. Условия проверки зависят от того, на какой тип списка контроля доступа указывает номер – стандартный или расширенный.

Для каждого протокола можно создать несколько списков контроля доступа. Номера списков контроля доступа для данного протокола должны быть разными. Однако для каждого протокола, направления и интерфейса можно задать только один список контроля доступа.

Номера списков от 1 до 99 и от 1 300 до 1 999 настраивают маршрутизатор на принятие инструкций стандартного нумерованного списка контроля доступа для IPv4. Номера списков от 100 до 199 и от 2 000 до 2 699 настраивают маршрутизатор на принятие инструкций расширенного нумерованного списка контроля доступа для IPv4.

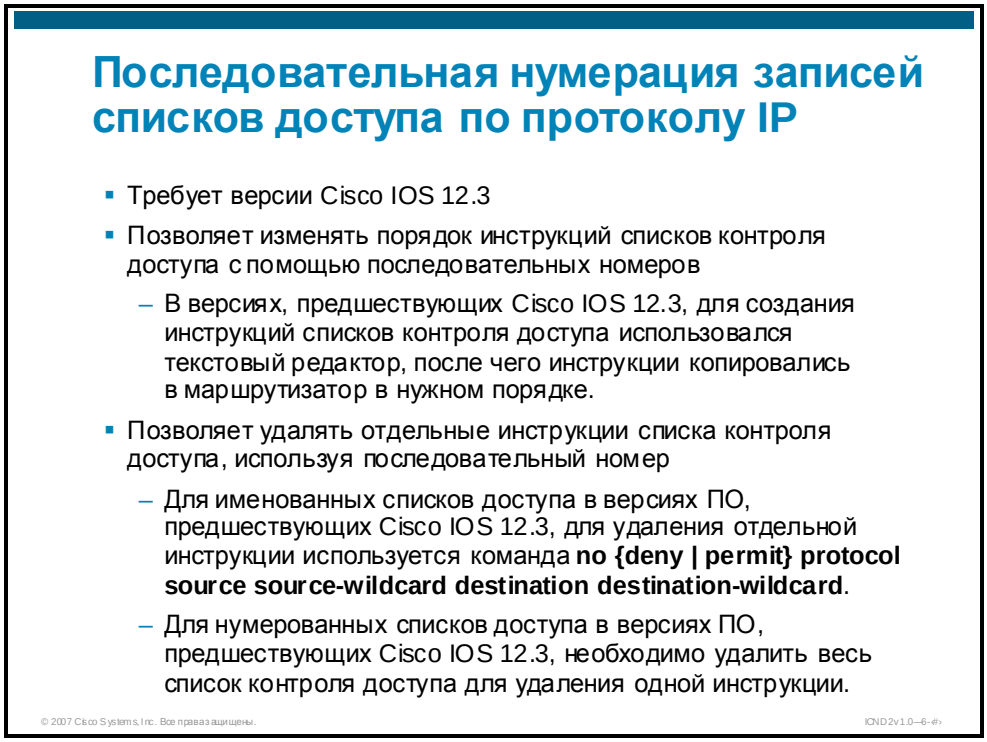
В таблице ниже представлены различные диапазоны номеров списков контроля доступа для каждого протокола.

Номера списков контроля доступа по протоколам

Протокол	Диапазон
IP	1 – 99
Расширенный IP	100 – 199
Код типа Ethernet	200 – 299
Ethernet-адрес	700 – 799
Transparent bridging (тип протокола)	200 – 299
Transparent bridging (код производителя)	700 – 799
Extended transparent bridging	1 100 – 1 199
DECnet и Extended DECnet	300 – 399
Xerox Network Services (XNS)	400 – 499
Extended XNS	500 – 599
AppleTalk	600 – 699
Source-route bridging (тип протокола)	200 – 299
Source-route bridging (код производителя)	700 – 799
Internetwork packet exchange (IPX)	800 – 899
Extended IPX	900 – 999
IPX Service Advertisement Protocol (SAP)	1 000 – 1 099
Standard Banyan Virtual Integrated Network Service (VINES)	1 – 100
Extended Banyan VINES	101 – 200
Simple Banyan VINES	201 – 300
Стандартный IP (увеличенный диапазон)	1 300 – 1 999
Расширенный IP (увеличенный диапазон)	2 000 – 2 099

Примечание Начиная с версии Cisco IOS 12.0, диапазоны номеров списков контроля доступа для IPv4 были расширены. Как показано в таблице, к диапазону номеров стандартных списков для IPv4 добавлены номера от 1 300 до 1 999 и к диапазону расширенных списков для IPv4 добавлены номера от 2 000 до 2 099.

Именованные списки контроля доступа позволяют идентифицировать стандартные и расширенные списки контроля доступа по протоколу IP с помощью буквенно-цифровой строки (имени) вместо номера. Именованные списки контроля доступа по протоколу IP предлагают дополнительную гибкость при работе с записями.



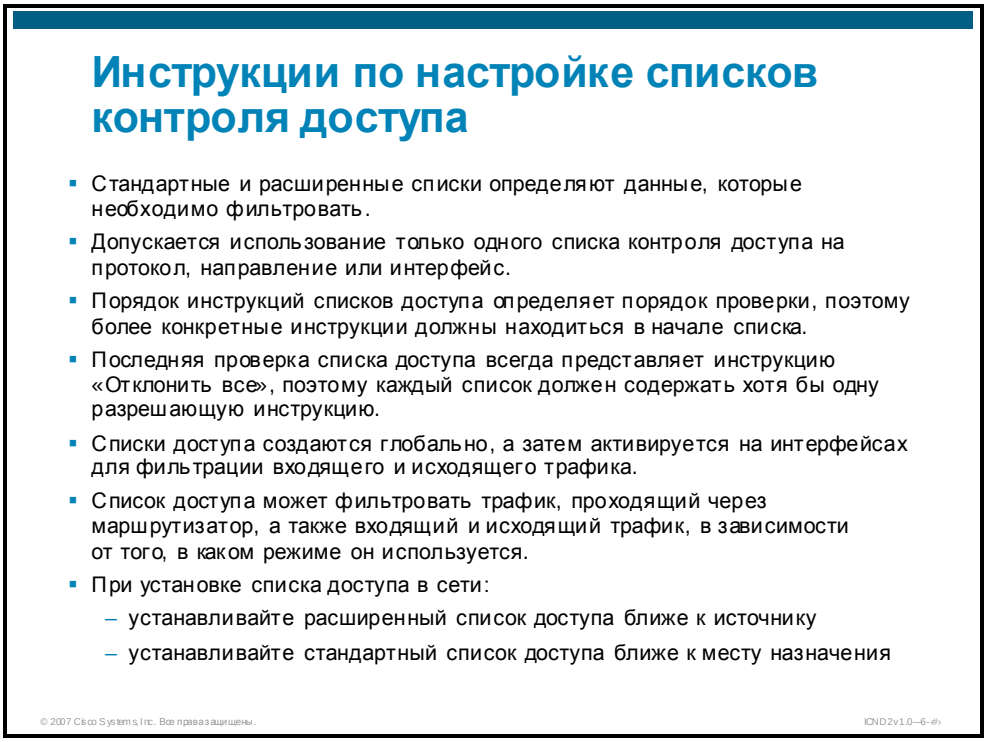
Последовательная нумерация записей списков доступа по протоколу IP предлагает несколько преимуществ:

- вы можете изменять порядок инструкций списков контроля доступа;
- вы можете удалять отдельные инструкции из списка контроля доступа.

Место установки дополнений в списки контроля доступа зависит от того, используете ли вы последовательную нумерацию. Последовательная нумерация не поддерживается в версиях ПО, предшествующих Cisco IOS 12.3. Поэтому все дополнения из ранних версий ПО помещаются в конец списка контроля доступа.

Последовательная нумерация записей списка контроля доступа по протоколу IP – новая функция ПО Cisco IOS, которая позволяет добавлять, удалять и изменять порядок инструкций в списке IP ACL. Начиная с версии Cisco IOS 12.3 дополнения можно устанавливать в любое место списка контроля доступа, используя последовательный номер.

В версиях, предшествующих Cisco IOS 12.3, только именованные списки контроля доступа допускали удаление отдельных инструкций с помощью команды **{deny | permit}** *protocol source source-wildcard destination destination-wildcard*, параметры *protocol source source-wildcard destination destination-wildcard* соответствуют удаляемой строке. Для нумерованных списков потребовалось бы удаление и повторное создание списка с нужными инструкциями. Начиная с версии Cisco IOS 12.3 можно использовать команду **no** *последовательный номер* для удаления указанной записи списка доступа.



Качественно спроектированный и внедренный список контроля доступа – важный компонент безопасности сети. Чтобы добиться требуемых результатов при создании списков, следуйте следующим инструкциям:

- в соответствии с условиями проверки выберите стандартный или расширенный, именованный или нумерованный список контроля доступа;
- допускается использование только одного списка контроля доступа на протокол, направление или интерфейс, использование нескольких списков контроля доступа на интерфейс разрешается, но они должны быть заданы для разных протоколов или направлений;
- список контроля доступа должен быть организован для обработки сверху вниз; создавайте список так, чтобы более конкретные ссылки на сети или подсети находились до более общих ссылок, поместите условия, которые встречаются чаще перед более редкими условиями;
- в конце списка контроля доступа должна присутствовать инструкция «отклонить все»;
  - если в конце списка контроля доступа не задана инструкция «разрешить все», по умолчанию список контроля доступа будет отклонять весь трафик, не соответствующий хотя бы одной из его инструкций;
  - любой список контроля доступа должен содержать хотя бы одну разрешающую инструкцию, в противном случае будет отклоняться весь трафик.
- список контроля доступа необходимо создать, перед активацией на интерфейсе; в большинстве версий ПО Cisco IOS интерфейс с пустым списком контроля доступа принимает весь трафик;

- в зависимости от способа активации списка контроля доступа, он фильтрует трафик, который проходит через маршрутизатор, трафик который принимается маршрутизатором или трафик, который отправляется маршрутизатором (например, входящий и исходящий трафик линии VTY);
- как правило, расширенные списки контроля доступа следует устанавливать как можно ближе к источнику трафика, который необходимо отклонить; поскольку стандартные списки контроля доступа не включают адреса назначения, их следует устанавливать как можно к месту назначения трафика, который необходимо отклонить, чтобы источник мог обращаться к промежуточным сетям.

Дополнительные типы списков контроля доступа

В этом разделе описываются дополнительные типы списков контроля доступа (динамические, рефлексивные и временные).

Стандартные и расширенные списки контроля доступа могут стать основой для дополнительных типов, обеспечивающих дополнительные функциональные возможности. Дополнительные списки контроля доступа:

- динамические списки контроля доступа (замок и ключ);
- рефлексивные списки контроля доступа;
- временные списки контроля доступа.

Динамические списки контроля доступа

Динамические списки контроля доступа зависят от возможностей подключения Telnet, аутентификации (локальной или удаленной) и расширенных списков контроля доступа. Настройка «ключа и замка» начинается с внедрения расширенного списка контроля доступа для блокировки трафика, проходящего через маршрутизатор. Пользователи, которые пытаются передать данные через маршрутизатор, блокируются расширенным списком контроля доступа, пока они не подключатся к маршрутизатору через Telnet и не аутентифицируются. Затем Telnet-подключение сбрасывается и к существующему расширенному списку контроля доступа добавляется новый динамический список с одной записью. Он пропускает трафик в течение определенного периода времени, можно задать как период бездействия так и абсолютное значение времени ожидания.

Когда следует использовать динамические списки контроля доступа

Некоторые из причин, по которым следует внедрить динамический список контроля доступа, приводятся ниже.

- Используйте динамический список контроля доступа, если необходимо, чтобы удаленный пользователь или группа пользователей получили доступ к сети с удаленных хостов через Интернет. Динамический список доступа аутентифицирует пользователей и разрешает ограниченный доступ через брандмауэр-маршрутизатор к хосту или подсети в течение конечного периода времени.
- Используйте динамический список контроля доступа, если необходимо, чтобы подмножество хостов локальной сети получило доступ к хосту в удаленной сети, защищенной брандмауэром. Динамический список доступа позволяет разрешить доступ к удаленному хосту только заданному набору локальных хостов. Динамический список доступа требует аутентификации через сервер TACACS+ или другой сервер безопасности для предоставления доступа локальных хостов к удаленным хостам.

Преимущества динамических списков контроля доступа

Динамические списки контроля доступа предлагают следующие преимущества для системы безопасности по сравнению со стандартными и статическими расширенными списками:

- использование механизма вызова для аутентификации отдельных пользователей;
- упрощенное управление в крупных интерсетях;
- во многих случая обеспечивает снижение объема вычислений на маршрутизаторе, в котором нуждаются списки контроля доступа;
- снижение вероятности взлома сети хакерами;
- динамический доступ пользователя через брандмауэр, не подвергающий риску другие ограничения безопасности.

Пример динамического списка контроля доступа

Хотя полная конфигурация динамического списка контроля доступа не рассматривается в этом курсе, в примере ниже описываются основные действия для настройки такого списка контроля доступа.

Следующая конфигурация создает имя пользователя и пароль для аутентификации. Время бездействия установлено на 10 минут.

```
RouterX(config)#username test password 0 test
RouterX(config)#username test autocommand access-enable host
timeout 10
```

Следующая конфигурация позволяет пользователям открыть сеанс Telnet с маршрутизатором для аутентификации и блокирует весь остальной трафик.

```
RouterX(config)#access-list 101 permit tcp any host 10.1.1.1
eq telnet
RouterX(config)#interface Ethernet0/0
RouterX(config-if)#ip address 10.1.1.1 255.255.255.0 ip
access-group 101 in
```

Следующая конфигурация создает динамический список контроля доступа, который будет автоматически применяться к существующему списку access-list 101. Задано абсолютное время ожидания 15 минут.

```
RouterX(config)#access-list 101 dynamic testlist timeout 15
permit ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
```

Следующая конфигурация включает аутентификацию пользователей, пытающихся открыть сеанс Telnet с маршрутизатором.

```
RouterX(config)#line vty 0 4
RouterX(config-line)#login local
```

После создания этих конфигураций, когда пользователь 10.1.1.2 успешно создает сеанс Telnet с интерфейсом 10.1.1.1, применяется динамический список доступа. Затем сеанс сбрасывается и пользователь получает доступ к сети 172.16.1.x.

Рефлексивные списки контроля доступа

Рефлексивные списки контроля доступа обеспечивают фильтрацию IP-пакетов в соответствии с данными сеанса верхнего уровня. Они используются для разрешения исходящего трафика и ограничения входящего трафика в ответ на сеансы, созданные в сетях маршрутизатора. Рефлексивные списки контроля доступа создают только временные записи. Эти записи автоматически генерируются при запуске нового сеанса IP, например исходящим пакетом. Записи автоматически удаляются в конце сеанса. Рефлексивные списки контроля доступа не применяются напрямую к интерфейсу, но вносятся в расширенный именованный список контроля доступа, который активируется на интерфейсе.

Рефлексивные списки контроля доступа предлагают более «истинную» форму фильтрации сеансов, чем расширенный список контроля доступа с параметром **established**. Рефлексивные списки контроля доступа гораздо сложнее обмануть, так как перед принятием пакета необходимо обеспечить соответствия большему числу критериев. Проверяются не только биты подтверждения (ACK) и сброса (RST), но и адреса источника и назначения, а также номера портов.

Преимущества рефлексивных списков контроля доступа

Рефлексивные списки контроля доступа являются важным элементом защиты сети от хакеров и могут быть добавлены в брандмауэры. Рефлексивные списки контроля доступа добавляют уровень защиты от подделки пакетов и DoS-атак. Они просты в использование и предлагают больше гибкости и контроля над пакетами, по сравнению с обычными списками контроля доступа.

Пример рефлексивного списка контроля доступа

Хотя полная конфигурация рефлексивного списка контроля доступа не рассматривается в этом курсе, в примере ниже описываются основные действия для настройки такого списка контроля доступа. Пример рефлексивного списка контроля доступа разрешает входящий и исходящий трафик ICMP и пропускает только трафик TCP, отправленный изнутри. Весь остальной трафик отклоняется.

Следующая конфигурация заставляет маршрутизатор отслеживать трафик, инициированный изнутри.

```
RouterX(config)#ip access-list extended outboundfilters permit
icmp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 permit tcp
10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 reflect tcptraffic
```

Следующая конфигурация создает политику, которая требует, чтобы маршрутизатор проверял весь входящий трафик, чтобы определить, был ли он инициирован изнутри и привязывает рефлексивную часть списка контроля доступа outboundfilters (которая называется tcptraffic) к списку контроля доступа inboundfilters.

```
RouterX(config)#ip access-list extended inboundfilters permit
icmp 172.16.1.0 0.0.0.255 10.1.1.0 0.0.0.255 evaluate
tcptraffic
```

Следующая конфигурация применяет входящий и исходящий список контроля доступа к интерфейсу.

```
RouterX(config)#interface Ethernet0/1
RouterX(config-if)#ip address 172.16.1.2 255.255.255.0
RouterX(config-if)#ip access-group inboundfilters in
RouterX(config-if)#ip access-group outboundfilters out
```

Рефлексивные списки контроля доступа могут быть заданы только как расширенные именованные списки контроля доступа по протоколу IP. Их нельзя задать как нумерованные или стандартные списки доступа по протоколу IP или как списки доступа по другому протоколу. Рефлексивные списки контроля доступа можно использовать с другими стандартными и статическими расширенными списками контроля доступа.

Временные списки контроля доступа

Временные списки контроля доступа аналогичны расширенным спискам, но они поддерживают контроль доступа в зависимости от времени. Чтобы внедрить временные списки контроля доступа, необходимо задать временной диапазон для каждого дня и недели. Временной диапазон идентифицируется именем, на которое ссылается функция. Поэтому временные ограничения применяются к самой функции.

Преимущества временных списков контроля доступа

Временные списки контроля доступа предлагают много преимуществ.

- Администратор сети имеет больше контроля над разрешением и запрещением доступа пользователей к ресурсам. В числе таких ресурсов могут быть: приложение, идентифицируемое IP-адресом, парой масок и номером порта, маршрутизация на основе политик или канал по требованию, идентифицируемый значимым трафиком, направленным к абоненту.
- Администраторы сети могут задать политики безопасности в зависимости от времени:
  - безопасность на основе периметра с использованием набора функций Cisco IOS Firewall или списков контроля доступа;
  - конфиденциальность на основе Cisco Encryption Technology или IP Security (IPsec).
- Функция маршрутизации на основе политик и очередей усовершенствованы.
- Если частота обращения к ресурсам провайдера меняется в зависимости от времени суток, администраторы могут обеспечить экономичную автоматическую маршрутизацию трафика.

- Поставщики услуг могут динамически изменять выделенную частоту обращения (CAR) для поддержки соглашений об уровне обслуживания QoS, которые пересматриваются в определенное время суток.
- Администраторы сети могут контролировать сообщения журналов. Записи списков контроля доступа могут вести журнал трафика в определенное время суток, но не круглосуточно. Поэтому администраторы могут просто запретить доступ, не анализируя журналы, созданные в пиковые часы.

Пример временного списка контроля доступа

Хотя полная конфигурация временного списка контроля доступа не рассматривается в этом курсе, в примере ниже описываются основные действия для настройки такого списка контроля доступа. В этом примере запуск сеансов Telnet разрешен из внутренней сети во внешнюю сети по понедельникам, средам и пятницам.

Конфигурация ниже определяет временной диапазон списка контроля доступа и назначает ему имя.

```
RouterX(config)#time-range EVERYOTHERDAY
RouterX(config-time-range)#periodic Monday Wednesday Friday
8:00 to 17:00
```

Следующая конфигурация применяет временной диапазон к списку контроля доступа.

```
RouterX(config)#access-list 101 permit tcp 10.1.1.0 0.0.0.255
172.16.1.0 0.0.0.255 eq telnet time-range EVERYOTHERDAY
```

Следующая конфигурация применяет список контроля доступа к интерфейсу.

```
RouterX(config)#interface Ethernet0/0
RouterX(config-if)#ip address 10.1.1.1 255.255.255.0
RouterX(config-if)#ip access-group 101 in
```

Временной диапазон зависит от системных часов маршрутизатора. Можно использовать часы маршрутизатора, однако эта функция лучше всего работает с синхронизацией NTP.

Шаблонные маски списков контроля доступа

В этом разделе описывается использование шаблонных масок с списками контроля доступа.

Фильтрация адресов выполняется при использовании шаблонных масок адресов для списков контроля доступа, которые проверяют или игнорируют соответствующие биты IP-адреса. Шаблонные маски для битов IP-адреса используют числа 1 и 0, чтобы определить, как обрабатывать соответствующие биты.

- **Бит 0 шаблонной маски:** значение соответствующего бита адреса должно совпадать.
- **Бит 1 шаблонной маски:** значение соответствующего бита адреса не проверяется (игнорируется).

Примечание Иногда шаблонную маску называют обратной маской.

Точная настройка шаблонных масок позволит разрешить или отклонить проверку с помощью одной инструкции списка контроля доступа. Вы можете выбрать любой идентификатор или IP-адрес.

На рисунке показано, как задать соответствующие биты адреса.

Примечание Шаблонные маски для списков контроля доступа работают не так, как маски IP-подсетей. Нулевой бит в маске списка контроля доступа указывает, что соответствующие биты адресов должны совпадать. Бит «1» в маске списка контроля доступа указывает, что соответствующие биты адресов могут быть проигнорированы.

Пример: процесс создания шаблонной маски для IP-подсетей

В примере на рисунке администратор хочет протестировать диапазон IP-подсетей, которые должны быть приняты или отклонены. Предположим, что в качестве IP-адреса используется адрес класса B (первые два октета выделены под номер сети), для подсетей используется 8 бит (третий октет). Администратор хочет использовать биты шаблонной маски IP для сопоставления подсетей 172.30.16.0/24 подсетям 172.30.31.0/24.

Чтобы сопоставить диапазон подсетей с помощью одной инструкции списка контроля, введите IP-адрес 172.30.16.0 (первая подсеть), а затем нужную маску подсети.

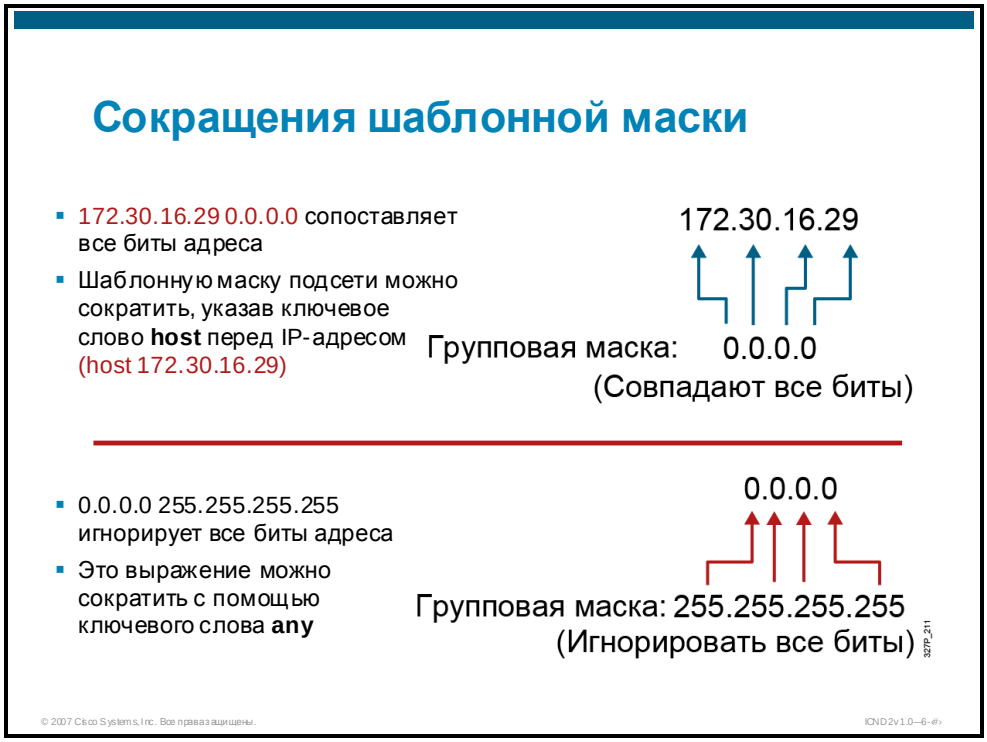
Сначала маска подсети сопоставит первые два октета (172.30) IP-адреса с помощью соответствующих нулевых битов в первых двух октетах маски.

Поскольку номер хоста неважен, шаблонная маска игнорирует последний октет (бит «1» в маске подсети). Последний октет шаблонной маски в десятичном выражении будет 255.

В третьем октете с адресом подсети десятичное выражение маски составит 15 (двоичное – 00001111). Маска сопоставляет 4 старших бита IP-адреса. В нашем случае шаблонная маска будет соответствовать подсетям, начиная с 172.30.16.0/24. Последние (младшие) 4 бита в октете игнорируются маской подсети. Значение в этих битах может быть двоичным числом 0 или 1. Поэтому шаблонная маска соответствует подсетям 16, 17, 18 и так далее до подсети 31. Шаблонная маска не соответствует другим подсетям.

В этом примере адрес 172.30.16.0 с маской подсети 0.0.15.255 соответствует подсетям от 172.30.16.0/24 до 172.30.31.0/24.

В некоторых случая для обеспечения соответствия диапазона подсетей может потребоваться несколько инструкций списка контроля доступа, например для диапазона 10.1.4.0/24 – 10.1.8.0/24 следует использовать инструкции 10.1.4.0 0.0.3.255 и 10.1.8.0 0.0.0.255.



Биты 0 и 1 в шаблонной маске списка контроля доступа заставляют список контроля доступа проверять или игнорировать соответствующий бит в IP-адресе. Работа с десятичными представлениями двоичной шаблонной маски может быть трудоемкой. В распространенных сценариях вместо шаблонных масок можно использовать сокращения. Сокращения позволяют уменьшить количество чисел, которое необходимо ввести при настройке условий проверки адреса.

Пример: Шаблонные маски для одного IP-адреса

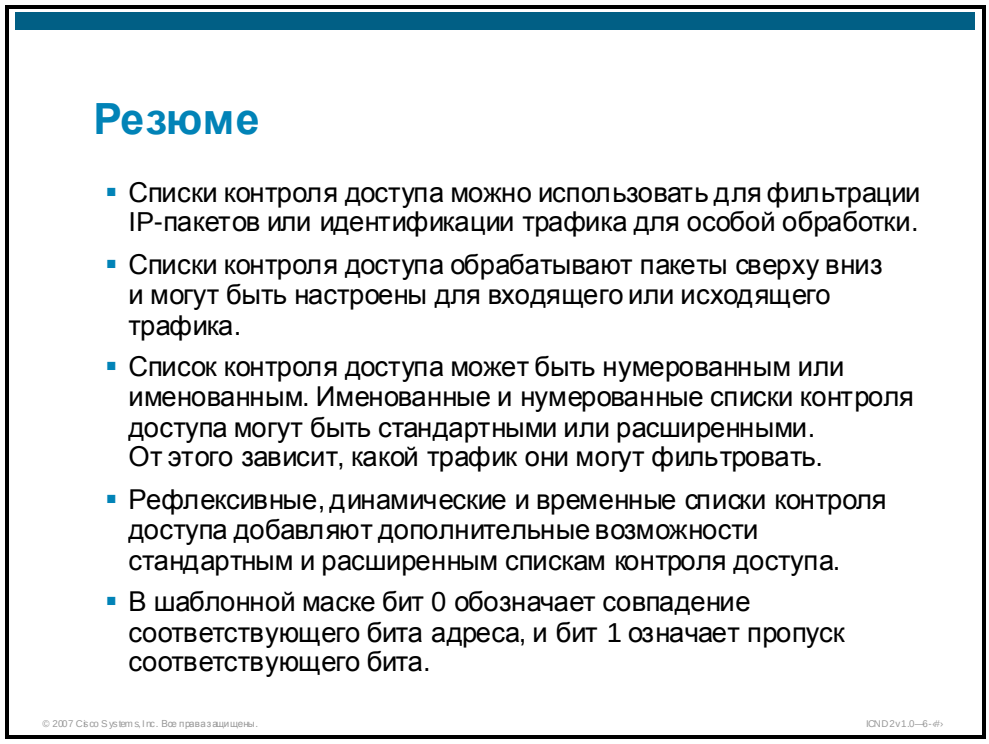
В этом примере вместо инструкции 172.30.16.29 0.0.0.0 можно ввести строку **host 172.30.16.29**. Сокращение **host** передает аналогичное условие проверки в список контроля доступа ПО Cisco IOS.

Пример: Шаблонные маски для всех IP-адресов

В этом примере вместо инструкции 0.0.0.0 255.255.255.255 можно указать ключевое слово **any**. Сокращение **any** передает аналогичное условие проверки в список контроля доступа ПО Cisco IOS.

Резюме

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



Занятие 2

Настройка и устранение неполадок списков контроля доступа (ACL)

Обзор

В этом занятии описываются действия по поиску и устранению неполадок в нумерованных и именованных, стандартных и расширенных списках контроля доступа (ACL). Кроме того, в занятии рассматривается проверка правильности работы списков ACL и некоторые распространенные ошибки конфигурации, которых следует избегать.

Задачи

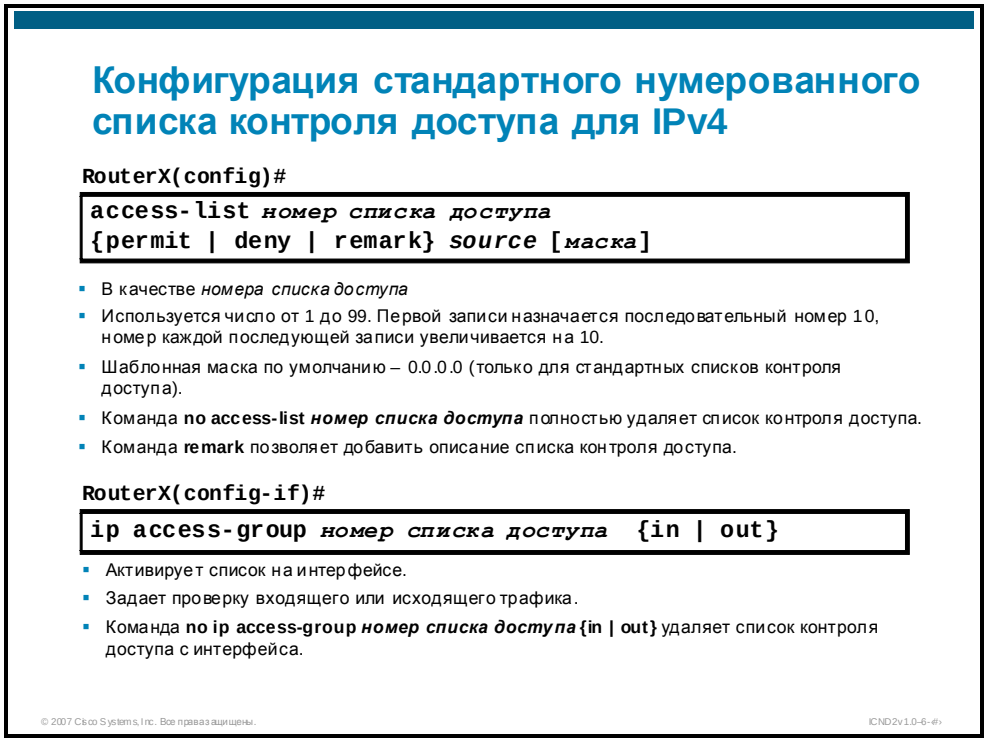
По окончании этого занятия вы сможете выполнять настройку, поиск и устранение неполадок стандартных и расширенных, нумерованных и именованных списков контроля доступа для IPv4. Это значит, что вы сможете выполнять следующие задачи:

- настраивать и проверять стандартные нумерованные списки контроля доступа для IPv4;
- настраивать и проверять расширенные нумерованные списки контроля доступа для IPv4;
- настраивать и проверять расширенные и стандартные именованные списки контроля доступа для IPv4;
- выявлять и устранять распространенные ошибки конфигурации списков контроля доступа.

Настройка стандартных нумерованных списков контроля доступа для IPv4

В этом разделе описывается настройка стандартных нумерованных списков контроля доступа для IPv4.

Стандартным спискам контроля доступа для IPv4 назначаются номера из диапазонов 1 – 99 и 1 300 – 1 999. Они фильтруют пакеты в зависимости от адреса источники и маски и запрещают или разрешают полный пакет протоколов TCP/IP. Стандартные списки контроля доступа могут не обеспечивать нужного уровня контроля над фильтрацией. Администратору могут потребоваться более точные методы фильтрации трафика.



Для настройки стандартного списка доступа для IPv4 на маршрутизаторе Cisco необходимо создать стандартный список для IPv4 и активировать его на интерфейсе. Для создания записи в стандартном списке фильтров трафика для IPv4 используется команда **access-list**. На рисунке описывается синтаксис этой команды.

Команда **ip access-group** привязывает существующий список контроля доступа к интерфейсу. Допускается использование только одного списка контроля доступа на протокол, направление или интерфейс. На рисунке описывается синтаксис этой команды.

Примечание Чтобы удалить список ACL для протокола IP с интерфейса сначала введите команду **no ip access-group** на этом интерфейсе, а затем глобальную команду **no access-list**, чтобы полностью удалить список доступа.

В таблице приводится пример действий по настройке и активации нумерованного стандартного списка контроля доступа на маршрутизаторе.

Процедура настройки стандартного нумерованного списка контроля доступа

№	Действие	Примечания
1.	С помощью команды глобальной конфигурации **access-list** создайте запись в стандартном списке контроля доступа для IPv4. `RouterX(config)# access-list 1 permit 172.16.0.0 0.0.255.255`	Введите глобальную команду **no access-list** *номер списка доступа*, чтобы полностью удалить список контроля доступа. Пример инструкции разрешает все адреса, которые начинаются с 172.16.x.x. Используйте параметр **remark**, чтобы добавить описание к списку контроля доступа.

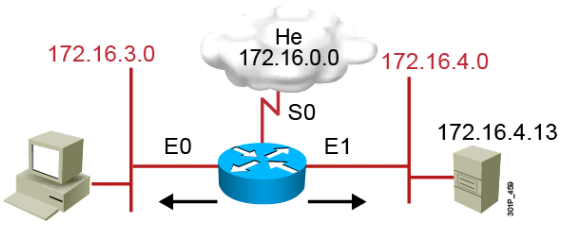
№	Действие	Примечания
2.	Используйте команду конфигурации **interface**, чтобы выбрать интерфейс, к которому следует применить список контроля доступа. `RouterX(config)# **interface ethernet 1**`	После ввода команды **interface** приглашение интерфейса командной строки изменится с (config) # на (config-if) #.
3.	Используйте команду конфигурации интерфейса **ip access-group**, чтобы активировать существующий список контроля доступа на интерфейсе. `RouterX(config-if)# **ip access-group 1 out**`	Чтобы удалить список доступа по протоколу IP с интерфейса, введите команду **no ip access-group** *номер списка доступа* на этом интерфейсе. В этом примере стандартный список IPv4 ACL 1 активируется на интерфейсе в качестве исходящего фильтра.

Пример: Добавление записей с последовательными номерами

В примере ниже в указанный список добавляется новая запись.

```
RouterX# show ip access-list

Standard IP access list 1
2 permit 10.4.4.2, wildcard bits 0.0.255.255
5 permit 10.0.0.44, wildcard bits 0.0.0.255
10 permit 10.0.0.1, wildcard bits 0.0.0.255
20 permit 10.0.0.2, wildcard bits 0.0.0.255

RouterX(config)# ip access-list standard 1

RouterX(config-std-nacl)# 15 permit 10.5.5.5 0.0.0.255

RouterX# show ip access-list

Standard IP access list 1
2 permit 10.4.0.0, wildcard bits 0.0.255.255
5 permit 10.0.0.0, wildcard bits 0.0.0.255
10 permit 10.0.0.0, wildcard bits 0.0.0.255
15 permit 10.5.5.0, wildcard bits 0.0.0.255
20 permit 10.0.0.0, wildcard bits 0.0.0.255
```


Стандартный нумерованный список контроля доступа для IPv4 Пример 1




```
RouterX(config)# access-list 1 permit 172.16.0.0  0.0.255.255
(implicit deny all - not visible in the list)
(access-list 1 deny 0.0.0.0   255.255.255.255)

RouterX(config)# interface ethernet 0
RouterX(config-if)# ip access-group 1 out
RouterX(config)# interface ethernet 1
RouterX(config-if)# ip access-group 1 out
```

Разрешение только внутренней сети

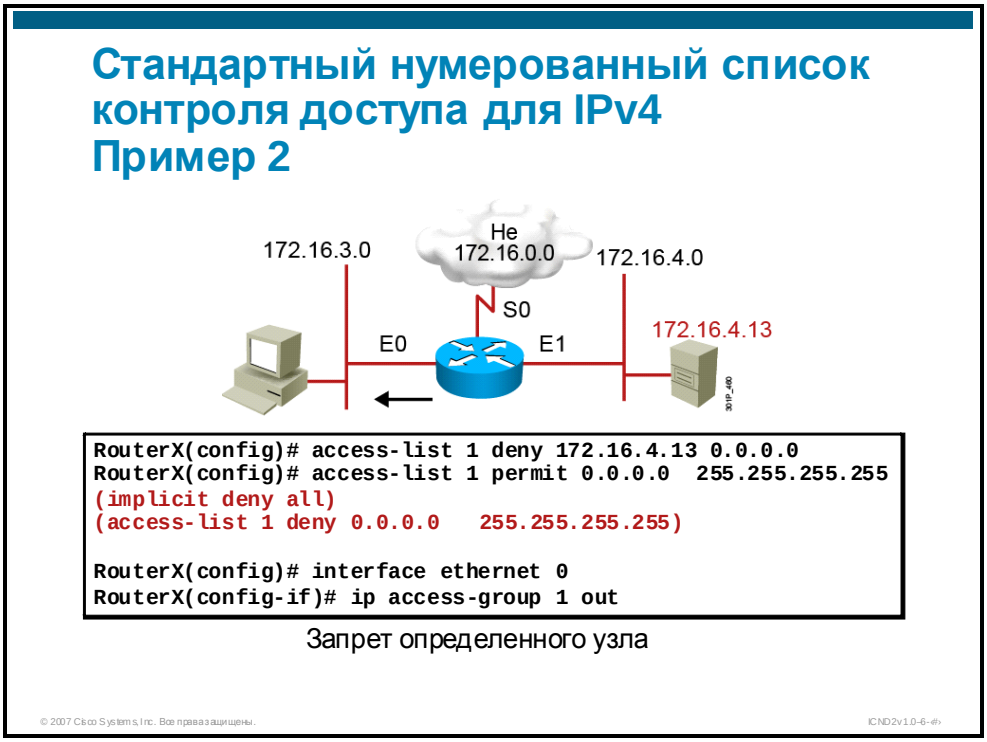
Пример: Нумерованный стандартный список контроля доступа для IPv4, разрешающий только внутреннюю сеть

В таблице описывается синтаксис команды, приведенной на рисунке.

Пример стандартного нумерованного списка контроля доступа для IPv4

Параметры команды access-list	Описание
`1`	Номер списка ACL, который указывает, что список является стандартным.
`permit`	Разрешает пересылку трафика, соответствующего указанным параметрам.
`172.16.0.0`	IP-адрес, который используется вместе с шаблонной маской для идентификации сети-источника.
`0.0.255.255`	Шаблонная маска, нули соответствуют позициям, которые должны совпадать, единицы – игнорируемые позиции.
`ip access-group 1 out`	Привязывает список контроля доступа к интерфейсу в качестве исходящего фильтра.

Этот список контроля доступа разрешает пересылку из интерфейсов E0 и E1 только трафика сети 172.16.0.0. Трафик из всех остальных сетей блокируется.



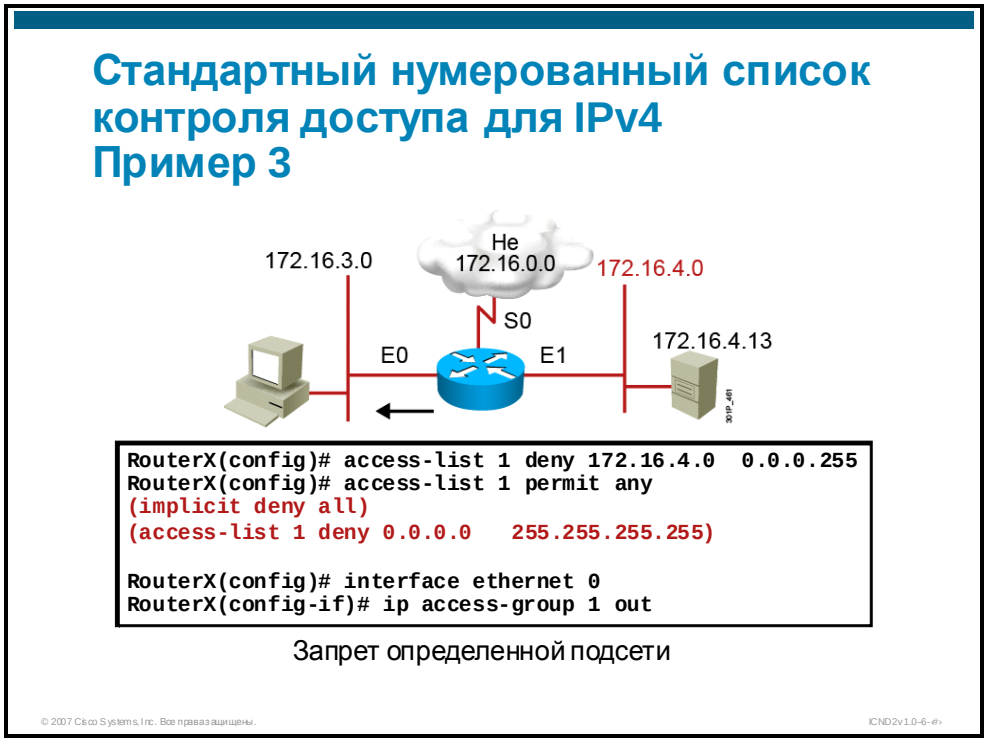
Пример: Нумерованный стандартный список контроля доступа, запрещающий заданный хост

В таблице описывается синтаксис команды, приведенной на рисунке.

Пример стандартного нумерованного списка контроля доступа для IPv4

Параметры команды access-list	Описание
`1`	Номер списка ACL, который указывает, что список является стандартным.
`deny`	Запрещает пересылку трафика, соответствующего указанным параметрам.
`172.16.4.13`	IP-адрес хоста-источника.
`0.0.0.0`	Маска, которая требует совпадения всех битов. (Это маска по умолчанию.)
`permit`	Разрешает пересылку трафика, соответствующего указанным параметрам.
`0.0.0.0`	IP-адрес хоста источника. Все нули указывают на местозаполнитель.
`255.255.255.255`	Шаблонная маска, нули соответствуют позициям, которые должны совпадать, единицы – игнорируемые позиции. Все единицы в маске указывают, что все 32 бита адреса источника *не* проверяются. Другими словами, подойдет любой адрес.

Этот список контроля доступа блокирует трафик с определенного адреса (172.16.4.13) и разрешает пересылку всего остального трафика с интерфейса Ethernet 0. Комбинация IP-адреса и шаблонной маски 0.0.0.0 255.255.255.255 разрешает трафик из любого источника. Эту комбинацию также можно записать с помощью ключевого слова **any**.



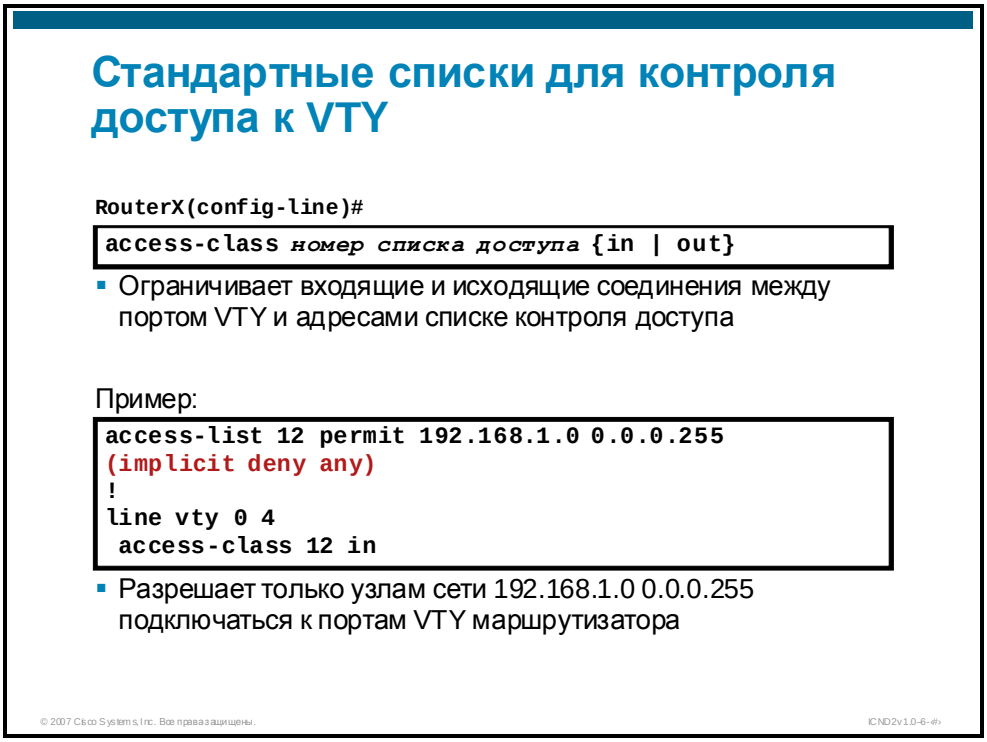
Пример: Нумерованный стандартный список контроля доступа, запрещающий заданную подсеть

В таблице описывается синтаксис команды, приведенной на рисунке.

Пример стандартного нумерованного списка контроля доступа для IPv4

Параметры команды access-list	Описание
`1`	Номер списка ACL, который указывает, что список является стандартным.
`deny`	Запрещает пересылку трафика, соответствующего заданным параметрам.
`172.16.4.0`	IP-адрес подсети источника.
`0.0.0.255`	Шаблонная маска, нули соответствуют позициям, которые должны совпадать, единицы – игнорируемые позиции. Маска с нулями в первых трех октетах указывает, что эти три позиции должны совпадать. 255 в последнем октете означает, что октет не учитывается.
`permit`	Разрешает пересылку трафика, соответствующего указанным параметрам.
`any`	Сокращение IP-адреса источника. Сокращение **any** соответствует адресу 0.0.0.0 и шаблонной маске 255.255.255.255. Все адреса источника удовлетворяют критерию.

Этот список контроля доступа блокирует трафик определенной подсети (172.16.4.0) и разрешает пересылку трафика из интерфейса E0.



Для контроля входящего и исходящего (не транзитного) трафика маршрутизатора необходимо защитить виртуальные порты маршрутизатора. Виртуальный порт также называется линией VTY. По умолчанию доступно пять таких каналов с номерами от VTY 0 до VTY 4. При соответствующей настройке образы ПО Cisco IOS могут поддерживать более пяти портов VTY.

Ограничение доступа к VTY повышает безопасность сети и подразумевает задание адресов, для которых разрешен доступ к процессу EXEC по протоколу Telnet.

Фильтрация трафика Telnet, как правило, рассматривается как функция расширенных списков контроля доступа по протоколу IP, так как подразумевает фильтрацию трафика протокола верхнего уровня. Однако, поскольку команда **access-class** позволяет фильтровать входящие и исходящие сеансы Telnet по адресу источника и применять фильтрацию к линиям VTY, для контроля доступа к VTY можно использовать стандартный список доступа по протоколу IP.

Пример: Доступ к VTY

В этом примере вы разрешаете устройствам в сети 192.168.1.0 0.0.0.255 создавать виртуальный терминальный сеанс связи (Telnet) с маршрутизатором. Безусловно пользователь должен знать пароли для входа пользовательский и привилегированный режим.

Обратите внимания, что для всех линий VTY (от 0 до 4) были заданы одинаковые ограничения, так как администратор не может контролировать, к какой линии VTY подключается пользователь. Инструкция «Отклонить все» все еще применяется в списку контроля доступа, когда он используется как запись класса доступа.

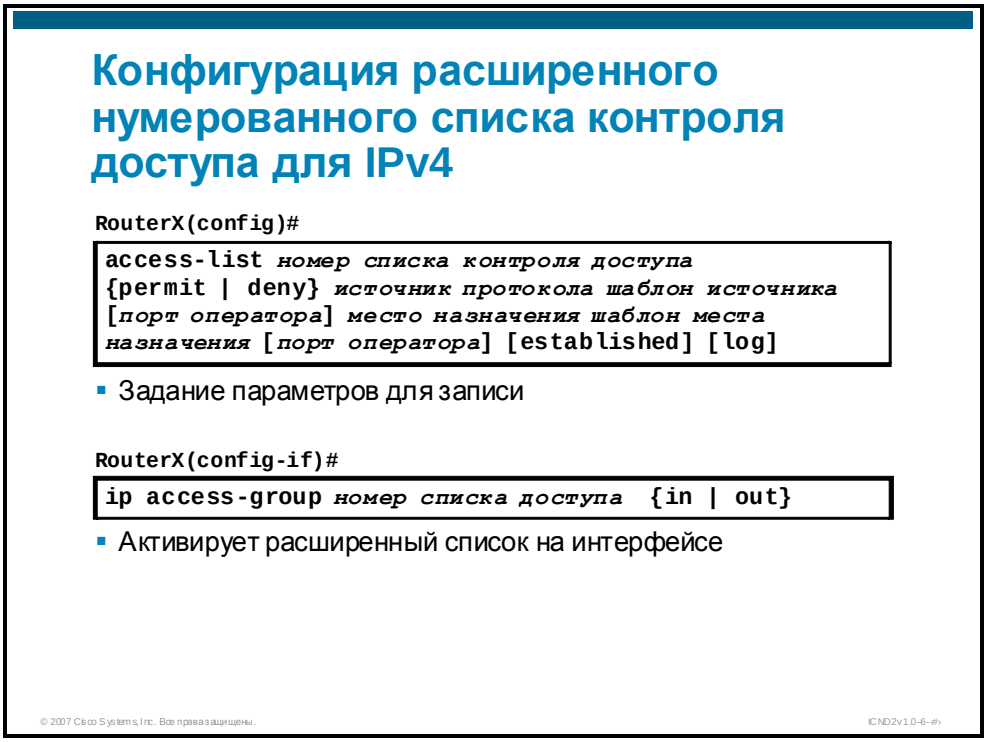
Настройка расширенных нумерованных списков контроля доступа для IPv4

В этом разделе описывается настройка расширенных нумерованных списков контроля доступа для IPv4.

Для более точного контроля над фильтрацией трафика используются расширенные списки доступа для IPv4 с номерами из диапазонов 100 – 199 и 2 000 – 2 699, а также именованные списки, которые проверяют IPv4-адреса источника и назначения. Кроме того, в конце инструкции расширенного списка контроля доступа можно указать протокол и приложение TCP или UDP (необязательно) для более точной фильтрации. Чтобы задать приложение, необходимо указать номер порта или имя широко известного приложения.

Известные номера портов и протоколы IP

Известные номера портов (десятичные)	Протокол IP
20 (TCP)	Данные FTP
21 (TCP)	Управляющие сигналы FTP
23 (TCP)	Telnet
25 (TCP)	Протокол SMTP
53 (TCP/UDP)	DNS
69 (UDP)	TFTP
80 (TCP)	HTTP



Чтобы настроить расширенный нумерованный список контроля доступа для IPv4 на маршрутизаторе Cisco, создайте этот список и активируйте его на интерфейсе. Используйте команду **access-list**, чтобы создать запись с инструкцией в сложном фильтре. В таблице описывается синтаксис команды, которая приводится на рисунке.

Параметры команда для расширенного нумерованного списка контроля доступа

Параметры команды access-list	Описание
номер списка доступа	Назначает списку номер из диапазона 100 – 199 или 2 000 – 2 699.
permit | deny	Разрешает или блокирует указанный адрес.
протокол	IP, TCP, UDP, ICMP, GRE и IGRP.
источник и назначение	Идентифицирует IP-адреса источника и назначения.
шаблон источника и шаблон назначения	Шаблонная маска, нули соответствуют позициям, которые должны совпадать, единицы – игнорируемым позициям.
оператор [*порт*|*имя приложения*]	Доступные операторы **lt** (меньше), **gt** (больше), **eq** (равно), **neq** (не равно). Указанный номер порта может относиться к порту источника или к порту назначения, в зависимости от того, в каком месте списка контроля доступа задается порт. В качестве альтернативы номеру порта можно использовать широко известные имена приложений, такие как Telnet, FTP, SMTP и другие.
established	Только для входящего трафика TCP. Разрешает трафик TCP, если пакет сгенерирован в ответ на сеанс, созданный извне. Для этого типа трафика устанавливаются биты подтверждения (ACK). (См. раздел «Пример расширенного списка контроля доступа с параметром Established».)
log	Отправляет сообщение журнала в консоль.

Примечание Представленный синтаксис команды **access-list** соответствует протоколу TCP. Приведены не все параметры. Полный синтаксис всех форм команды см. в соответствующей документации по программному обеспечению Cisco IOS на портале Cisco.com.

Пример: Расширенный список контроля доступа с параметром Established

В следующем примере параметр **established** расширенного списка контроля доступа разрешает возврат ответа на трафик, созданный почтовым сервером 128.88.1.2, на интерфейс serial 0. Пакет удовлетворяет условиям, если в датаграмме TCP установлены биты ACK и RST, которые указывают, что пакет принадлежит существующему подключению. Без параметра **established** в инструкции списка контроля доступа почтовый сервер сможет принимать SMTP-трафик, но не отправлять его.

```
access-list 102 permit tcp any host 128.88.1.2 established
access-list 102 permit tcp any host 128.88.1.2 eq smtp

interface serial 0
 ip access-group 102 in
```

Команда **ip access-group** привязывает существующий список контроля доступа к интерфейсу. Допускается использование только одного списка контроля доступа на протокол, направление или интерфейс.

В таблице ниже описываются параметры команды **ip access-group**.

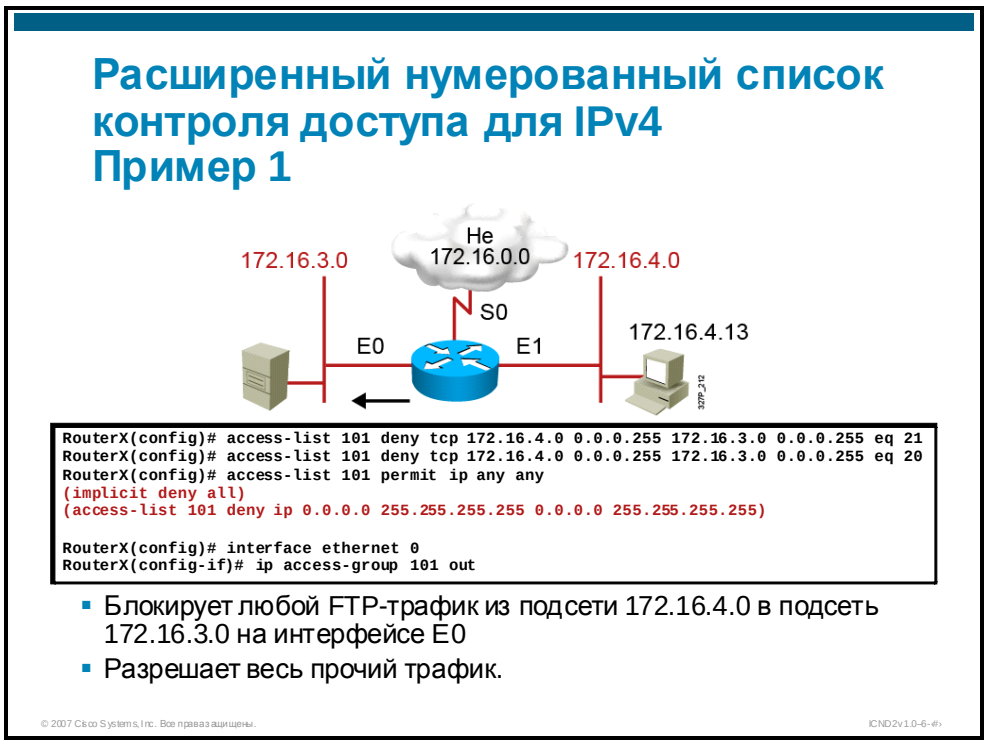
Параметры команды ip access-group

Параметры команды ip access-group	Описание
номер списка доступа	Номер списка контроля доступа, который необходимо привязать к интерфейсу.
in | out	Указывает, в каком режиме будет работать список контроля доступа – входящем или исходящем. Значение по умолчанию – out.

В таблице приводятся пример действий по настройке и активации нумерованного расширенного списка контроля доступа на маршрутизаторе.

Процедура настройки расширенного нумерованного списка контроля доступа

№	Действие	Примечания
1.	Задайте расширенный список доступа для IPv4. Используйте команду глобальной конфигурации **access-list**. `RouterX(config)# access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21`	Команда **show access-lists** отображает содержимое списка контроля доступа. В этом примере список access-list 101 запрещает TCP-трафик из источника 172.16.4.0 с шаблонной маской 0.0.0.255 к месту назначения 172.16.3.0 с шаблонной маской 0.0.0.255 через порт 21 (порт управления FTP).
2.	Выберите интерфейс, который необходимо настроить. Используйте команду глобальной конфигурации **interface.** `RouterX(config)# interface ethernet 0`	После ввода команды **interface** приглашение интерфейса командной строки изменится с (config) # на (config-if) #.
3.	Привяжите расширенный список контроля доступа для IPv4 интерфейсу. Используйте команду конфигурации интерфейса **ip access-group**. `RouterX(config-if)# ip access-group 101 in`	С помощь команды **show ip interfaces** убедитесь, что список контроля доступа по протоколу IP назначен интерфейсу.



Пример: расширенный нумерованный список контроля доступа по протоколу IP, запрещающий FTP-трафик из подсетей

В таблице описывается синтаксис команды, представленной на рисунке.

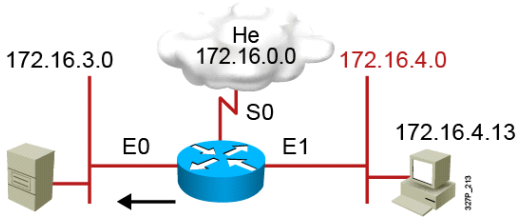
Пример расширенного нумерованного списка контроля доступа для IPv4

Параметры команды access-list	Описание
`101`	Номер списка контроля доступа, указывает на расширенный список контроля доступа для IPv4
`deny`	Запрещает пересылку трафика, соответствующего заданным параметрам
`tcp`	Протокол TCP
`172.16.4.0 0.0.0.255`	IP-адрес источника и маска, первые три октета должны совпадать, последний – нет
`172.16.3.0 0.0.0.255`	IP-адрес назначения и маска, первые три октета должны совпадать, последний – нет
`eq 21`	Порт назначения, в данном примере широко известный порт управления FTP
`eq 20`	Порт назначения, в данном примере широко известный порт передачи данных FTP
`out`	Привязывает список ACL 101 к интерфейсу E0 в качестве исходящего фильтра

Запрещающие инструкции запрещают FTP-трафик из подсети 172.16.4.0 в подсеть 172.16.3.0.

Разрешающая инструкция разрешает отправку всего остального IP-трафика из интерфейса E0.

Расширенный нумерованный список контроля доступа для IPv4 Пример 2




```
RouterX(config)# access-list 101 deny tcp 172.16.4.0  0.0.0.255  any eq 23
RouterX(config)# access-list 101 permit ip any any
(implicit deny all)

RouterX(config)# interface ethernet 0
RouterX(config-if)# ip access-group 101 out
```

- Блокирует только трафик Telnet из подсети 172.16.4.0 на интерфейсе E0.
- Разрешает весь прочий трафик.

Пример: Нумерованный расширенный списки доступа, запрещающий только Telnet-трафик из подсети

В таблице описывается синтаксис команды, представленной на рисунке.

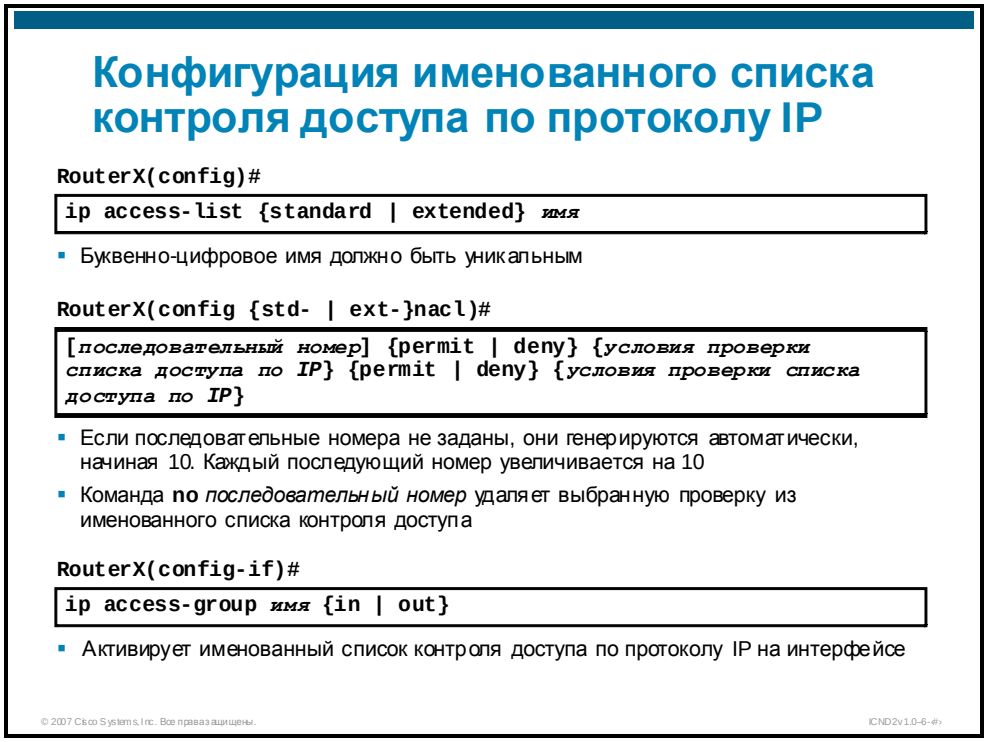
Пример расширенного нумерованного списка контроля доступа для IPv4

Параметры команды access-list	Описание
`101`	Номер списка контроля доступа, указывает на расширенный список контроля доступа для IPv4
`deny`	Запрещает пересылку трафика, соответствующего заданным параметрам
`tcp`	Протокол TCP
`172.16.4.0 0.0.0.255`	IP-адрес и маска источника, первые три октета должны совпадать, последний – нет
`any`	Любой IP-адрес назначения
`eq 23 or eq telnet`	Порт назначения или приложение. В этом примере указывается широко известный порт для Telnet (23)
`permit`	Разрешает пересылку трафика, соответствующего указанным параметрам
`ip`	Любой протокол IP
`any`	Ключевое слово, соответствующее трафику из любого источника
`any`	Ключевое слово, соответствующее трафику к любому месту назначения
`out`	Привязывает список ACL 101 к интерфейсу E0 в качестве исходящего фильтра

В этом примере запрещается Telnet-трафик сети 172.16.4.0, отправленный из интерфейса E0. Весь остальной IP-трафик из любого источника к любому месту назначения разрешается на интерфейсе E0.

Настройка именованных списков контроля доступа

В этом разделе описывается настройка именованных списков контроля доступа.



Именованные списки контроля доступа позволяют идентифицировать стандартные и расширенные списки контроля доступа для протокола IP с помощью буквенно-цифровой строки (имени) вместо номера.

Именованные списки контроля доступа поддерживают удаление отдельных записей. Версия Cisco IOS 12.3 позволяет использовать последовательные номера для вставки инструкций в любое место именованного списка контроля доступа. Версии, предшествующие Cisco IOS 12.3, позволяют добавлять инструкции только в конец именованного списка контроля доступа.

Поскольку именованные списки позволяют удалять отдельные записи, их можно изменять без необходимо в удалении и повторном создании. Используйте именованные списки доступа для протокола IP, если необходима интуитивно-понятная идентификация.

Создание стандартных именованных списков контроля доступа по протоколу IP

Для создания стандартного именованного списка доступа по протоколу IP выполните действия, описанные в таблице. Первое действие следует выполнить в режиме глобальной конфигурации.

Процедура создания стандартных именованных списков доступа по протоколу IP

№	Действие	Примечания
1.	**ip access-list standard** *имя*	Задает стандартный список контроля доступа и присваивает ему имя.
2.	Введите один из следующих параметров: ▪ [*sequence-number*] **deny** {*source* [*source-wildcard*] | **any**} ▪ [*sequence-number*] **permit** {*source* [*source-wildcard*] | **any**}	В режиме конфигурации списка контроля доступа укажите одно или несколько разрешающих или запрещающих условий. Они определяют, будет пакет пропущен или отброшен.
3.	**exit**	Выход из режима конфигурации списка доступа.

Создание расширенных именованных списков контроля доступа по протоколу IP

Для создания расширенного именованного списка доступа по протоколу IP выполните действия, описанные в таблице. Первое действие следует выполнить в режиме глобальной конфигурации.

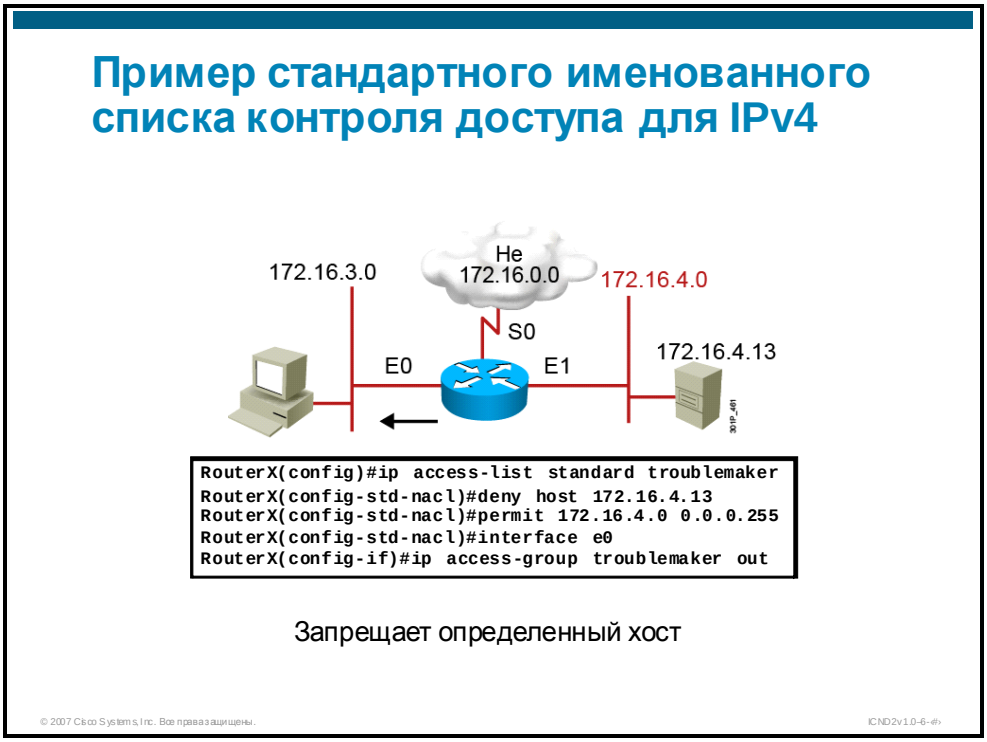
Процедура создания расширенных именованных списков доступа по протоколу IP

№	Действие	Примечания
1.	**ip access-list extended** *имя*	Задает стандартный список контроля доступа и присваивает ему имя.
2.	Введите один из следующих параметров: ▪ *sequence-number*] {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] ▪ sequence-number] {**deny** | **permit**} *protocol* **any any** ▪ sequence-number] {**deny** | **permit**} *protocol* **host** *source* **host** *destination*	В режиме конфигурации списка контроля доступа задайте условия разрешения или запрета. Ключевое слово **any** можно использовать как сокращение инструкции с адресом 0.0.0.0 и шаблонной маской 255.255.255.255 (для адреса источника, адреса назначение или для обоих адресов). Ключевое слово **host** можно использовать как сокращение шаблонной маски 0.0.0.0 для адреса источника или назначения. Ключевое слово **host** необходимо поместить перед адресом.
3.	**exit**	Выход из режима конфигурации списка доступа.

Пример: Добавление записей с последовательными номерами

В примере ниже в указанный список добавляется новая запись.

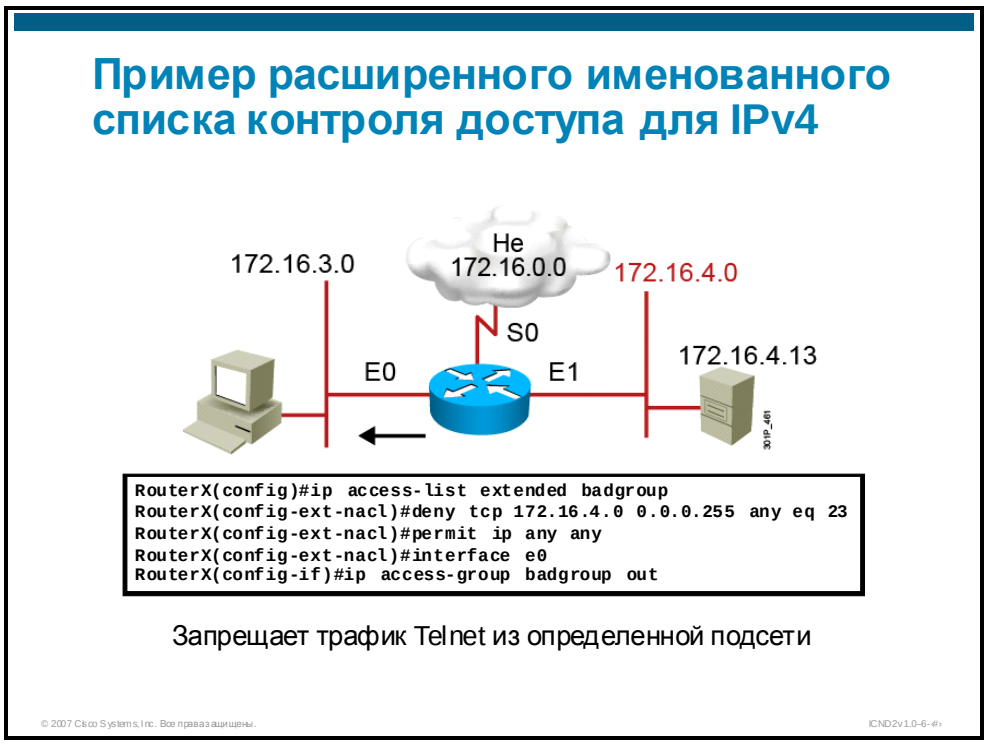
```
RouterX# show ip access-list

Standard IP access list MARKETING
2 permit 10.4.4.2, wildcard bits 0.0.255.255
5 permit 10.0.0.44, wildcard bits 0.0.0.255
10 permit 10.0.0.1, wildcard bits 0.0.0.255
20 permit 10.0.0.2, wildcard bits 0.0.0.255

RouterX(config)# ip access-list standard MARKETING

RouterX(config-std-nacl)# 15 permit 10.5.5.5 0.0.0.255

RouterX# show ip access-list

Standard IP access list MARKETING
2 permit 10.4.0.0, wildcard bits 0.0.255.255
5 permit 10.0.0.0, wildcard bits 0.0.0.255
10 permit 10.0.0.0, wildcard bits 0.0.0.255
15 permit 10.5.5.0, wildcard bits 0.0.0.255
20 permit 10.0.0.0, wildcard bits 0.0.0.255
```



В таблице описывается синтаксис команды, представленной на рисунке.

Пример стандартного именованного списка контроля доступа для IPv4

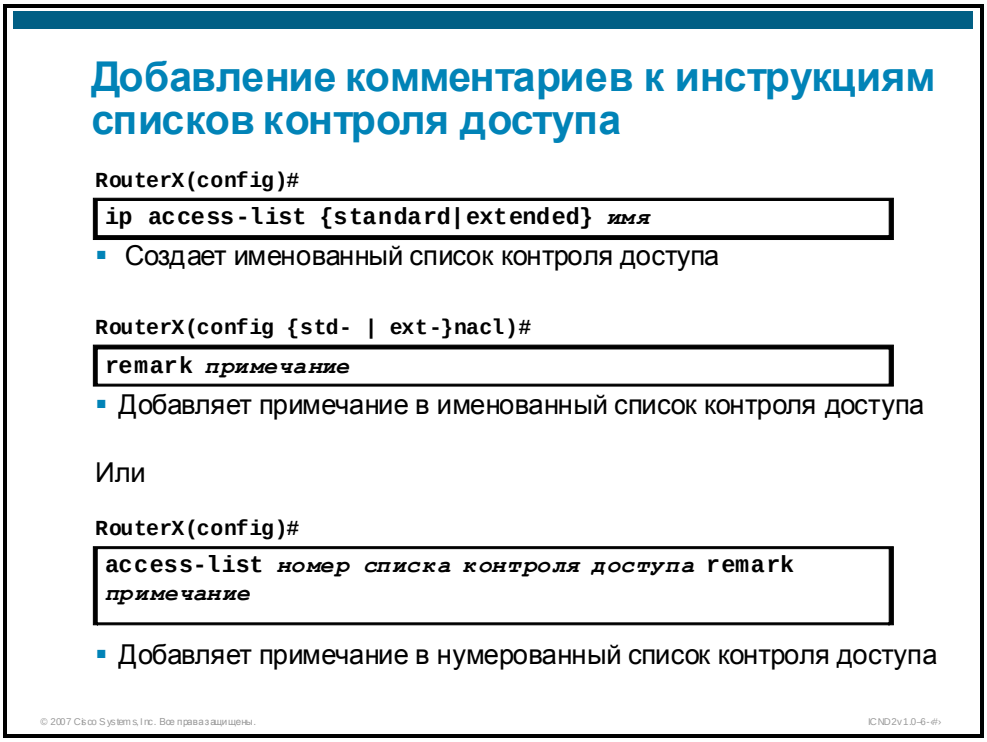
Параметры команды access-list	Описание
`standard`	Определяет именованный список контроля доступа как стандартный
`troublemaker`	Имя списка контроля доступа
`deny`	Запрещает пересылку трафика, соответствующего заданным параметрам
`host 172.16.4.13`	IP-адрес источника, ключевое слов «host» соответствует шаблонной маске 0.0.0.0
`permit`	Разрешает пересылку трафика, соответствующего указанным параметрам
`172.16.4.0 0.0.0.255`	IP-адрес источника и маска, первые три октета должны совпадать, последний – нет
`ip access-group troublemaker out`	Привязывает список «troublemaker» к интерфейсу E0 в качестве исходящего фильтра



В таблице описывается синтаксис команды, представленной на рисунке.

Пример именованного списка контроля доступа по протоколу IP

Параметры команды access-list	Описание
`extended`	Определяет именованный список контроля доступа как расширенный.
`badgroup`	Имя списка контроля доступа.
`deny`	Запрещает пересылку трафика, соответствующего заданным параметрам.
`tcp`	Протокол TCP.
`172.16.4.0 0.0.0.255`	IP-адрес источника и маска, первые три октета должны совпадать, последний – нет.
`any`	Любой IP-адрес назначения.
`eq 23 or eq telnet`	Порт назначения или имя приложения. В этом примере указывается широко известный порт для Telnet (23).
`permit`	Разрешает пересылку трафика, соответствующего указанным параметрам.
`ip`	Протокол сетевого уровня.
`any`	Ключевое слово, соответствующее трафику из любого источника к любому месту назначения.
`ip access-group badgroup out`	Привязывает список «badgroup» к интерфейсу E0 в качестве исходящего фильтра.



Комментариями или примечаниями называются инструкции списков контроля доступа, которые не обрабатываются. Это простые описательные утверждения, которые помогают лучше понять именованные или нумерованные списки контроля доступа, а также устранять неполадки в них.

Длина примечания ограничена 100 символами. Примечание можно добавлять до или после разрешающей или запрещающей инструкции. Однако при добавлении примечаний следует использовать согласованный подход, чтобы пользователя всегда мог понять, к какой запрещающей или разрешающей инструкции относится примечание. Размещение одной части примечаний до инструкций, а другой – после инструкций может привести к путанице.

Для добавления комментария в именованный список контроля доступа по протоколу IP используется команда **remark** *примечание* режима конфигурации списка контроля доступа. Чтобы добавить комментарий в нумерованный список, используйте команду **access-list** *номер списка доступа* **remark** *примечание*.

Пример добавления комментария в нумерованный список контроля доступа:

```
access-list 101 remark Permitting_John to Telnet to Server
access-list 101 permit tcp host 10.1.1.2 host 172.16.1.1 eq
telnet
```

Пример добавления комментария в именованный список контроля доступа:

```
ip access-list standard PREVENTION
remark Do not allow Jones subnet through
deny 171.69.0.0 0.0.255.255
```


Устранение неполадок списков контроля доступа

В этом разделе описывается поиск и устранение распространенных проблем конфигурации списков контроля доступа.

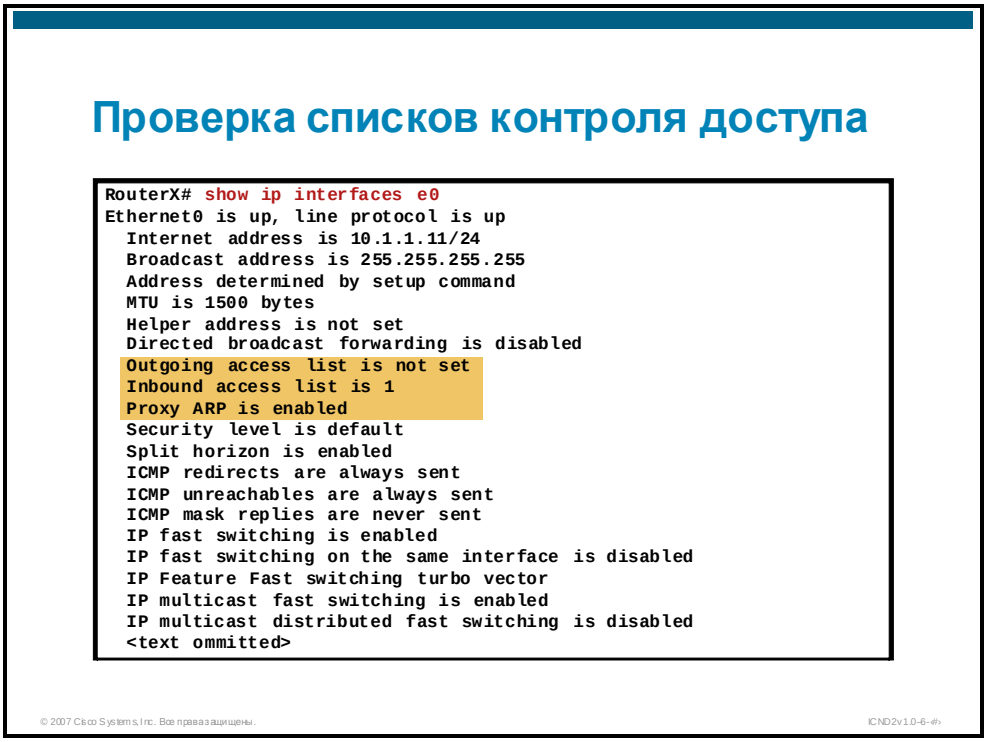
Отслеживание инструкций списка контроля доступа

```
RouterX# show access-lists {номер списка контроля доступа|имя}
```

```
RouterX# show access-lists
Standard IP access list SALES
    10 deny   10.1.1.0, wildcard bits 0.0.0.255
    20 permit 10.3.3.1
    30 permit 10.4.4.1
    40 permit 10.5.5.1
Extended IP access list ENG
    10 permit tcp host 10.22.22.1 any eq telnet (25 matches)
    20 permit tcp host 10.33.33.1 any eq ftp
    30 permit tcp host 10.44.44.1 any eq ftp-data
```

Отображает все списки доступа

Завершив настройку списка контроля доступа, воспользуйтесь командами **show**, чтобы проверить конфигурацию. Команда **show access-lists** отображает содержимое всех списков контроля доступа. Добавив имя или номер списка контроля доступа в качестве параметра этой команды, можно вывести определенный список. Чтобы вывести только содержимое списков доступа по протоколу IP, используйте команду **show ip access-list**.



Команда **show ip interfaces** отображает сведения об интерфейсе IP и о списках контроля доступа, настроенных на этом интерфейсе. В выводе команды **show ip interfaces e0**, представленном на рисунке, отображается исходящий список контроля доступа по протоколу IP, настроенный на интерфейсе E0. Исходящие списки не заданы на интерфейсе E0.

Для поиска и устранения следующей проблемы проанализируйте вывод команды **show access-lists.**

- **Проблема:** У хоста 10.1.1.1 нет подключения к хосту 10.100.100.1.

```
ERROR1# show access-lists 10
Standard IP access list 10
  10 deny  10.1.1.0, wildcard bits 0.0.0.255
  20 permit 10.1.1.1
  30 permit ip any any
```

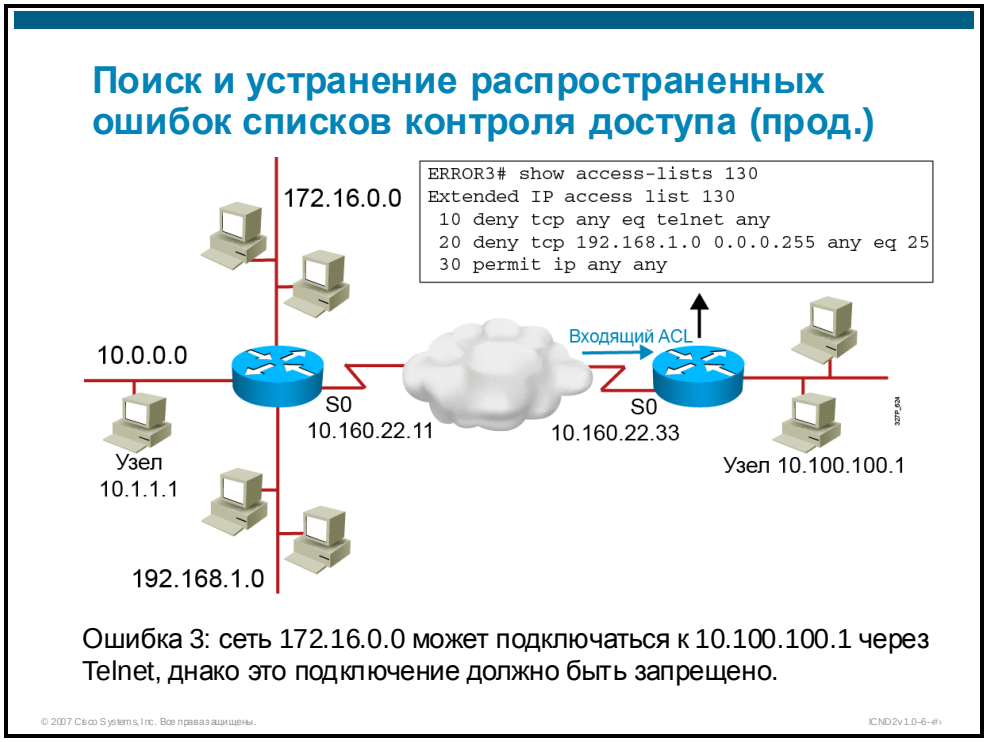
- **Решение:** У хоста 10.1.1.1 нет подключения к 10.100.100.1 из-за порядка правил списка доступа 10. Поскольку маршрутизатор обрабатывает списки контроля доступа сверху вниз, инструкция 10 запретит трафик хоста 10.1.1.1, а инструкция 20 не будет обработана. Инструкции 10 и 20 следует поменять местами.

Для поиска и устранения следующей проблемы проанализируйте вывод команды **show access-lists.**

- **Проблема:** Сеть 192.168.1.0 не может использовать протокол TFTP для подключения к 10.100.100.1.

```
ERROR2# show access-lists 120
Extended IP access list 120
  10 deny tcp 172.16.0.0 0.0.255.255 any eq telnet
  20 deny tcp 192.168.1.0 0.0.0.255 host 10.100.100.1 eq smtp
  30 permit tcp any any
```

- **Решение:** Сеть 192.168.1.0 не может использовать TFTP для подключения к 10.100.100.1, так как протокол TFTP использует транспортный протокол UDP. Инструкция 30 в списке доступа 120 разрешает весь TCP-трафик, а протокол TFTP запрещается, так как использует протокол UDP. Строку 30 следует заменить на **ip any any**.



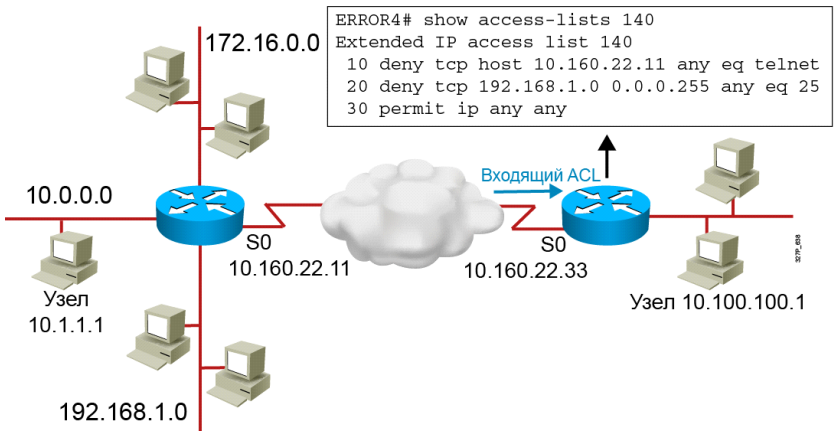
Для поиска и устранения следующей проблемы проанализируйте вывод команды **show access-lists.**

- **Проблема:** Сеть 172.16.0.0 может подключаться к 10.100.100.1 через Telnet, однако это подключение должно быть запрещено.

```
ERROR3# show access-lists 130
Extended IP access list 130
  10 deny tcp any eq telnet any
  20 deny tcp 192.168.1.0 0.0.0.255 host 10.100.100.1 eq smtp
  30 permit ip any any
```

- **Решение:** Сеть 172.16.0.0 может подключаться к 10.100.100.1 через Telnet, так как номер порта Telnet в инструкции 10 списка доступа 130 находится в неверном положении. В данный момент инструкция 10 запрещает все источники с номером порта, равным номеру порта Telnet, которые пытаются подключиться к любому IP-адресу. Чтобы запретить входящий Telnet-трафик на интерфейсе S0, необходимо запретить номер порта назначения, равным номеру порта Telnet, например с помощью инструкции **deny tcp any any eq telnet**.

Поиск и устранение распространенных ошибок списков контроля доступа (прод.)



Ошибка 4: хост 10.1.1.1 может подключаться к 10.100.100.1 через Telnet, однако это подключение должно быть запрещено.

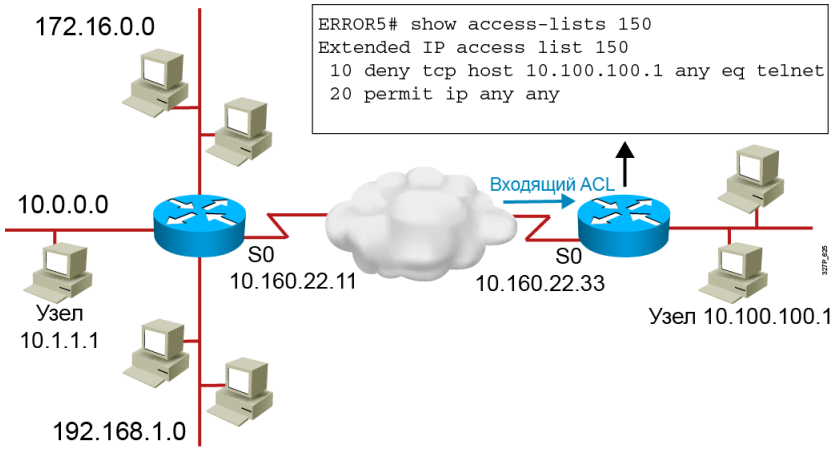
Для поиска и устранения следующей проблемы проанализируйте вывод команды **show access-lists.**

- **Проблема:** Хост 10.1.1.1 может подключаться к 10.100.100.1 через Telnet, однако это подключение должно быть запрещено.

```
ERROR4# show access-lists 140
Extended IP access list 140
  10 deny tcp host 10.160.22.11 10.100.100.0 0.0.0.255 eq telnet
  20 deny tcp 192.168.1.0 0.0.0.255 host 10.100.100.1 eq smtp
  30 permit ip any any
```

- **Решение:** Хост 10.1.1.1 может подключаться к 10.100.100.1 через Telnet, так как не задано никаких правил, запрещающих хост 10.1.1.1 или его сеть как источник трафика. Инструкция 10 списка контроля доступа 140 запрещает интерфейс маршрутизатора, из которого может отправляться трафик. Но когда эти пакеты покидают маршрутизатор, они имеют адрес 10.1.1.1, а не адрес интерфейса маршрутизатора.

Поиск и устранение распространенных ошибок списков контроля доступа (прод.)



Ошибка 5: хост 10.100.100.1 может подключаться к 10.1.1.1 через Telnet, однако это подключение должно быть запрещено.

ICND2v1.0-6-ru

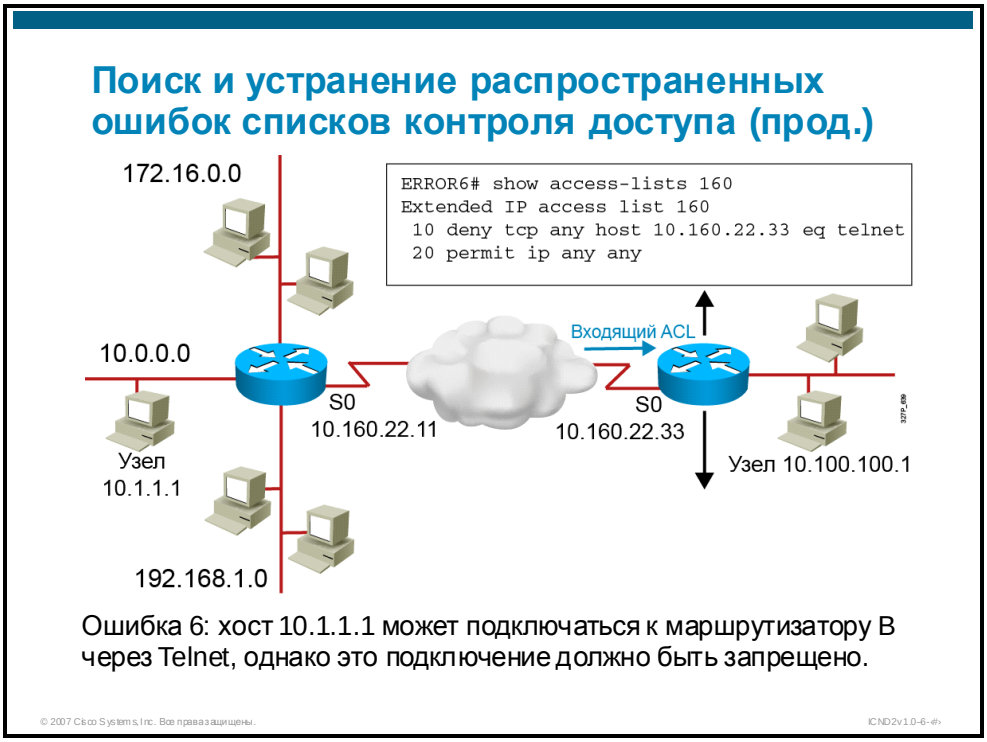
Для поиска и устранения следующей проблемы проанализируйте вывод команды **show access-lists.**

- **Проблема:** Хост 10.100.100.1 может подключаться к 10.1.1.1 через Telnet, однако это подключение должно быть запрещено.

```
ERROR5# show access-lists 150
Extended IP access list 150
  10 deny tcp host 10.100.100.1 any eq telnet
  20 permit ip any any
```

  Список доступа 150 применяется к интерфейсу S0 как входящий.

- **Решение:** Хост 10.100.100.1 может подключаться к 10.1.1.1 через Telnet из-за направления, в котором список доступа 150 активирован на интерфейсе S0. Инструкция 10 запрещает адрес источника 10.100.100.1, но этот адрес может быть источником только для исходящего трафика S0, но не для входящего.



Для поиска и устранения следующей проблемы проанализируйте вывод команды **show access-lists.**

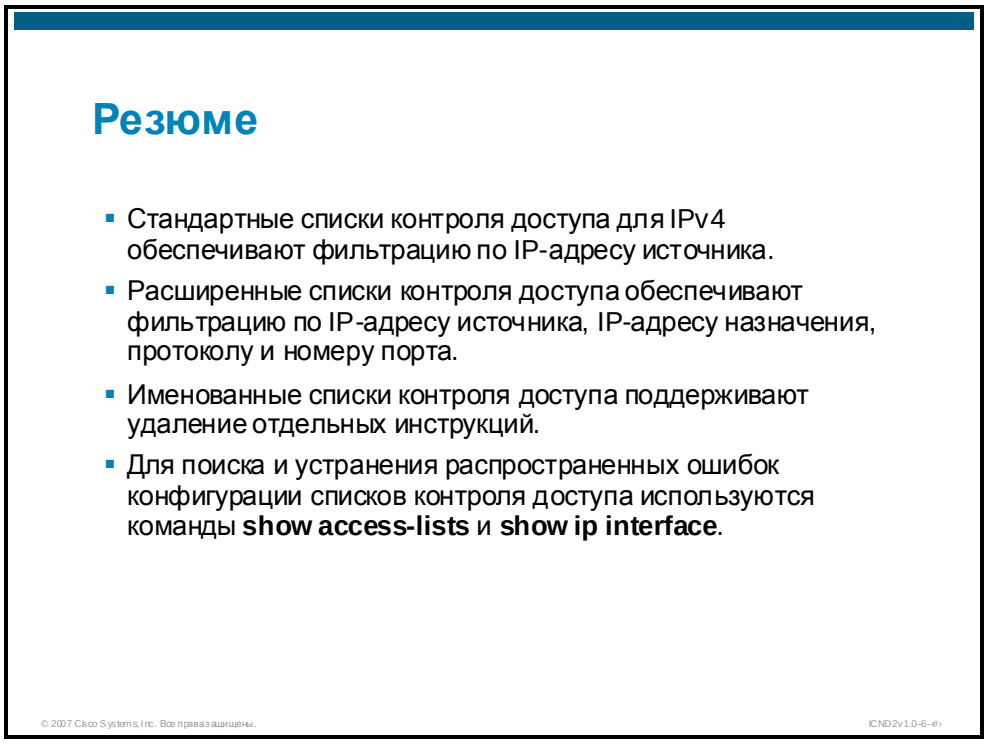
- **Проблема:** Хост 10.1.1.1 может подключаться к маршрутизатору B через Telnet, однако это подключение должно быть запрещено.

```
ERROR6# show access-lists 160
Extended IP access list 160
  10 deny tcp any host 10.160.22.33 eq telnet
  20 permit ip any any
```

- **Решение:** Хост 10.1.1.1 может подключиться к маршрутизатору B через Telnet, поскольку использование Telnet для подключения *к* маршрутизатору отличается от транзитного подключения Telnet к другому устройству *через* маршрутизатор. Инструкция 10 списка доступа 160 запрещает доступ через Telnet к адресу, назначенному интерфейсу S0 маршрутизатора B. Хост 10.1.1.1 все еще может использовать Telnet для подключения к маршрутизатору B через другой адрес интерфейса, например E0. Чтобы блокировать входящий и исходящий Telnet-трафик на маршрутизаторе, используйте команду **access-class** для активации списков контроля доступа на линиях VTY.

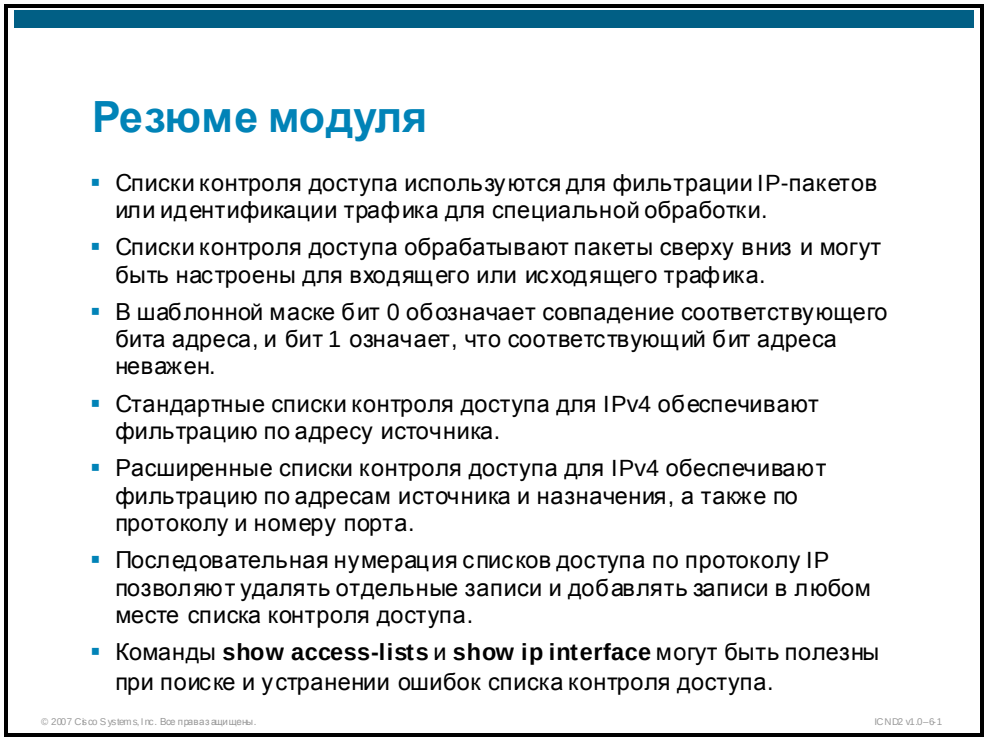
Резюме

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



Резюме модуля

В этом разделе приводится резюме вопросов, рассмотренных в модуле.



Стандартные и расширенные списки контроля доступа (ACL) ПО Cisco IOS используются для классификации IP-пакетов. Списки контроля доступа предлагают множество функций, таких как средства безопасности, шифрование, маршрутизация на основе политик и качество обслуживания (QoS). Эти функции активируются на интерфейсах маршрутизаторов и коммутаторов в определенном направлении (входящем или исходящем).

Нумерованные списки контроля доступа позволяют идентифицировать тип списка – стандартный или расширенный. Именованные списки контроля доступа дают администраторам больше гибкости при изменении отдельных записей.

Вопросы для самопроверки по модулю

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

В1) Что маршрутизатор Cisco делает с пакетом, соответствующим разрешающей инструкции списка контроля доступа? (Источник: введение в списки контроля доступа)

А) отбрасывает пакет
Б) возвращает пакет в источник
В) отправляет пакет в выходной буфер
Г) сохраняет пакет для дальнейшей обработки

В2) Что маршрутизатор Cisco делает с пакетом, соответствующим запрещающей инструкции списка контроля доступа? (Источник: введение в списки контроля доступа)

А) отбрасывает пакет
Б) возвращает пакет в источник
В) отправляет пакет в выходной буфер
Г) сохраняет пакет для дальнейшей обработки

В3) Список контроля доступа модно применить к нескольким интерфейсам. Сколько списков контроля доступа можно активировать на протокол, направление и интерфейс? (Источник: введение в списки контроля доступа)

А) 1
Б) 2
В) 4
Г) любое количество

В4) Какой термин используется для описания последней инструкции по умолчанию в конце каждого списка контроля доступа? (Источник: введение в списки контроля доступа)

А) инструкция «Отклонить все»
Б) инструкция «Отклонить хост»
В) инструкция «Разрешить все»
Г) инструкция « Разрешить хост»

В5) Какое утверждение наилучшим образом описывает разницу между стандартными и расширенными списками контроля доступа? (Источник: введение в списки контроля доступа)

А) Стандартные списки контроля доступа используют диапазон номеров 100 – 149, расширенные – диапазон 150 – 199.
Б) Стандартные списки контроля доступа используют фильтрацию по адресу источника и назначения, расширенный – фильтрацию по адресу источника.
В) Стандартные списки контроля доступа разрешают или запрещают доступ к определенному широко известному порту, расширенные списки выполняют фильтрацию по адресу источника и маске.
Г) Стандартные списки контроля доступа разрешают или запрещают весь пакет протоколов TCP/IP, расширенные позволяют выбрать конкретный протокол или номер порта.

В6) Какие два диапазона номеров используются для идентификации расширенных списков контроля доступа для IPv4 на маршрутизаторе Cisco? (Выберите два варианта.) (Источник: введение в списки контроля доступа)

А) 1 – 99
Б) 51 – 99
В) 100 – 199
Г) 200 – 299
Д) 1 300 – 1 999
Е) 2 000 – 1 699

В7) Списки контроля доступа обрабатываются сверху вниз. Какое из следующих утверждений описывает преимущество добавления более конкретных инструкций и инструкций, которым будет соответствовать значительная часть трафика, в начало списка контроля доступа? (Источник: введение в списки контроля доступа)

А) Снижение издержек на обработку.
Б) Списки контроля доступа можно использовать на других маршрутизаторах.
В) Списки контроля доступа проще редактировать.
Г) Добавление менее конкретных проверок упрощается.

В8) Системный администратор хочет настроить стандартный список контроля доступа для IPv4 на маршрутизаторе Cisco, разрешающий прием только для пакетов с хостов подсети 10.1.1.0/24 на интерфейсе маршрутизатора. Какая конфигурация списка контроля доступа позволит добиться этой цели? (Источник: настройка и устранение неполадок списков контроля доступа (ACL).)

А) **access-list 1 permit 10.1.1.0**
Б) **access-list 1 permit 10.1.1.0 host**
В) **access-list 99 permit 10.1.1.0 0.0.0.255**
Г) **access-list 100 permit 10.1.1.0 0.0.0.255**

В9) Какая команда Cisco IOS привязывает расширенный список контроля доступа для IPv4 к интерфейсу? (Источник: настройка и устранение неполадок списков контроля доступа (ACL).)

А) **ip access-list 101 e0**
Б) **access-group 101 e0**
В) **ip access-group 101 in**
Г) **access-list 101 permit tcp access-list 100 permit 10.1.1.0 0.0.0.255 eq 21**

В10) Как выглядит полная команда для создания записи списка контроля доступа со следующими параметрами? (Источник: настройка и устранение неполадок списков контроля доступа (ACL).)

- IP-адрес источника 172.16.0.0
- Маска источника 0.0.255.255
- Разрешить эту запись
- Номер списка контроля доступа 1

А) **access-list 1 deny 172.16.0.0 0.0.255.255**
Б) **access-list 1 permit 172.16.0.0 0.0.255.255**
В) **access-list permit 1 172.16.0.0 255.255.0.0**
Г) **access-list 99 permit 172.16.0.0 0.0.255.255**

В11) Ниже приводится список контроля доступа, введенный на маршрутизаторе Cisco.

```
access-list 135 deny tcp 172.16.16.0 0.0.15.255
172.16.32.0 0.0.15.255 eq telnet
access-list 135 permit ip any any
```

Если этот список доступа используется для контроля входящих пакетов на интерфейсе Ethernet 0, какие 3 утверждения будут верны? (Выберите три варианта.) (Источник: настройка и устранение неполадок списков контроля доступа (ACL).)

А) Адресу 172.16.1.1 будет запрещен доступ к адресу 172.16.37.5 через Telnet.
Б) Адресу 172.16.31.1 будет разрешен доступ к адресу 172.16.45.1 через FTP.
В) Адресу 172.16.1.1 будет разрешен доступ к адресу 172.16.32.1 через Telnet.
Г) Адресу 172.16.16.1 будет разрешен доступ к адресу 172.16.32.1 через Telnet.
Д) Адресу 172.16.16.1 будет разрешен доступ к адресу 172.16.50.1 через Telnet.
Е) Адресу 172.16.30.12 будет разрешен доступ к адресу 172.16.32.12 через Telnet.

В12) Какая команда активирует фильтрацию на основе стандартного списка контроля доступа для протокола IP на линияъ VTY для исходящих сеансов Telnet, запущенных на маршрутизаторе? (Источник: настройка и устранение неполадок списков контроля доступа (ACL).)

А) **access-vty 1 out**
Б) **access-class 1 out**
В) **ip access-list 1 out**
Г) **ip access-group 1 out**

В13) Какая команда используется на маршрутизаторах Cisco, чтобы определить, активированы ли списки контроля доступа по протоколу IP на интерфейсе Ethernet? (Источник: настройка и устранение неполадок списков контроля доступа (ACL).)

А) **show interfaces**
Б) **show ACL**
В) **show ip interface**
Г) **show ip access-list**

В14) С помощью какой команды можно узнать, настроен ли список доступа ACL 100 на маршрутизаторе Cisco? (Источник: настройка и устранение неполадок списков контроля доступа (ACL).)

А) **show interfaces**
Б) **show ip interface**
В) **show ip access-list**
Г) **show access-groups**

Ответы на вопросы для самопроверки по модулю

В1) В

В2) А

В3) А

В4) А

В5) Г

В6) В, Е

В7) А

В8) В

В9) В

В10) Б

В11) Б, В, Д

В12) Б

В13) В

В14) В

Модуль 7

Управление адресным пространством

Обзор

Один из главных недостатков IPv4 – ограниченное количество уникальных сетевых адресов, в настоящий момент в доступное адресное пространство Интернета заканчивается. Эту проблему можно решить двумя путями – преобразование сетевых адресов (NAT) и IPv6.

NAT предлагает краткосрочное решение проблемы, преобразуя частные адреса IPv4 в маршрутизируемые IP-адреса, уникальные в глобальном масштабе. IPv6 – долгосрочное решение. Увеличивая размер IP-адреса до 128 бит, IPv6 повышает общее число доступных адресов. В этом модуле рассматривается оба решения.

Задачи модуля

По окончании этого модуля вы сможете описывать ситуации, в которых следует внедрять NAT и PAT в сети среднего размера, а также настраивать NAT и PAT на маршрутизаторах. Кроме того, вы сможете объяснять принципы адресации IPv6 и настраивать протокол IPv6 на маршрутизаторах Cisco. Это значит, что вы сможете выполнять следующие задачи:

- настраивать и проверять статическое, динамическое и перегруженное преобразование NAT, определять основные параметры команд **show** и **debug**, необходимые для поиска и устранения неполадок NAT и PAT;
- описывать формат адресов IPv6 и компоненты, необходимые для запуска IPv6, настраивать IPv6 с маршрутизацией RIP и рассказывать о влиянии IPv6 на маршрутизацию в сети.

Занятие 1

Масштабирование сети с помощью NAT и PAT

Обзор

Две главные проблемы масштабируемости Интернета – нехватка адресного пространства IPv4 и масштабирование маршрутизации. Функции преобразования сетевых адресов (NAT) и преобразования адресов портов (PAT) ПО Cisco IOS позволяют экономить зарегистрированные адреса IPv4 в крупных сетях и упрощают управление адресами IPv4. NAT и PAT преобразуют адреса IPv4 в частных внутренних сетях в зарегистрированные адреса IPv4 для передачи через открытые сети, 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 номеров хостов и позволяет использовать один диапазон адресов IPv4 в нескольких интрасетях. В этом разделе описываются функции преобразования NAT и PAT, а также методы настройки NAT и PAT на маршрутизаторах Cisco.

Задачи

По окончании этого занятия вы сможете настраивать и проверять статическое, динамическое и перегруженное преобразование NAT, а также определять параметры команд **show** и **debug**, необходимые для поиска и устранения неполадок NAT и PAT. Это значит, что вы сможете выполнять следующие задачи:

- описывать функции и преимущества NAT и PAT;
- описывать статическое и динамическое преобразование внутренних адресов источника, а также настройку преобразования NAT;
- настраивать PAT путем перегрузки внутреннего глобального адреса;
- выявлять и устранять проблемы таблицы преобразования NAT;
- выявлять и устранять проблемы, связанные с использованием записи преобразования.

Общие сведения о NAT и PAT

В этом разделе описываются функции NAT и PAT.

Преобразование NAT поддерживается маршрутизатором Cisco и предназначено для экономии адресного пространства IPv4 и упрощения работы с ним. NAT позволяет частным интерсетям IPv4 использовать незарегистрированные адреса IPv4 для подключения к Интернету. Как правило, NAT соединяет две сети и преобразует частные (внутренние локальные) адреса внутренней сети в открытые (внутренние глобальные) адреса перед пересылкой пакетов в другую сеть. Эта функция позволяет NAT объявлять только один адрес для всей внешней сети. 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.

Список терминов NAT, используемых компанией Cisco, приводится ниже:

- **Внутренний локальный адрес.** Адрес IPv4, назначенный хосту во внутренней сети. Как правило, внутренний локальный адрес не является адресом IPv4, назначенным сетевым информационным центром (NIC) или поставщиком услуг.
- **Внутренний глобальный адрес.** Зарегистрированный адрес IPv4, назначенный центром NIC или поставщиком услуг. Представляет один или несколько внутренних локальных адресов IPv4 во внешних сетях.

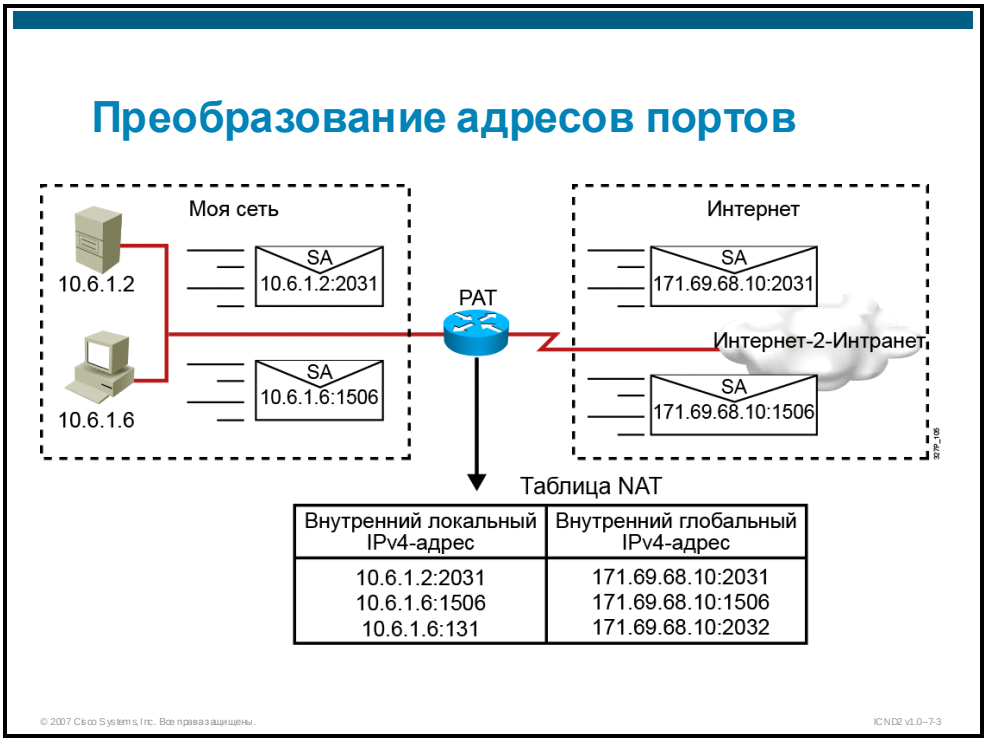
- **Внешний локальный адрес.** Адрес IPv4 внешнего хоста, под которым он отображается во внутренней сети. Внешний локальный адрес не обязательно должен быть зарегистрированным, он назначается из маршрутизируемого внутреннего адресного пространства.
- **Внешний глобальный адрес.** Адрес IPv4, назначенный хосту во внешней сети его владельцем. Внешний глобальный адрес выделяется из глобального маршрутизируемого адресного или сетевого пространства.

Преобразование NAT может работать в следующих режимах:

- **Статическое преобразование NAT.** Привязывает незарегистрированный адрес IPv4 к зарегистрированному адресу IPv4 (один к одному). Статическое преобразование NAT особенно полезно, если устройство должно быть доступно из внешней сети.
- **Динамическое преобразование NAT.** Привязывает незарегистрированный адрес IPv4 адресу из группы зарегистрированных адресов IPv4.
- **Перегрузка NAT.** Привязывает несколько незарегистрированных адресов IPv4 одному зарегистрированному адресу IPv4 (несколько к одному) с использованием нескольких портов. Перегрузка также называется преобразованием PAT и является формой динамического преобразования NAT.

Преобразование NAT предлагает следующие преимущества:

- Устраняет необходимость в переадресации всех хостов, нуждающихся в доступе к внешней сети, что обеспечивает экономию времени и денежных средств.
- Сокращает использование адресов благодаря мультиплексированию приложений на уровне портов. При использовании NAT внутренние хосты могут использовать один зарегистрированный адрес IPv4 для связи с внешними сетями. В конфигурации такого типа для поддержки множества внутренних хостов требуется относительно небольшое количество внешних адресов. Это позволяет экономить адреса IPv4.
- Повышение безопасности сети. Поскольку частные сети не объявляют свои адреса и внутреннюю топологию, они получают относительно высокий уровень безопасности при контролируемом обращении к внешним ресурсам в сочетании с NAT.

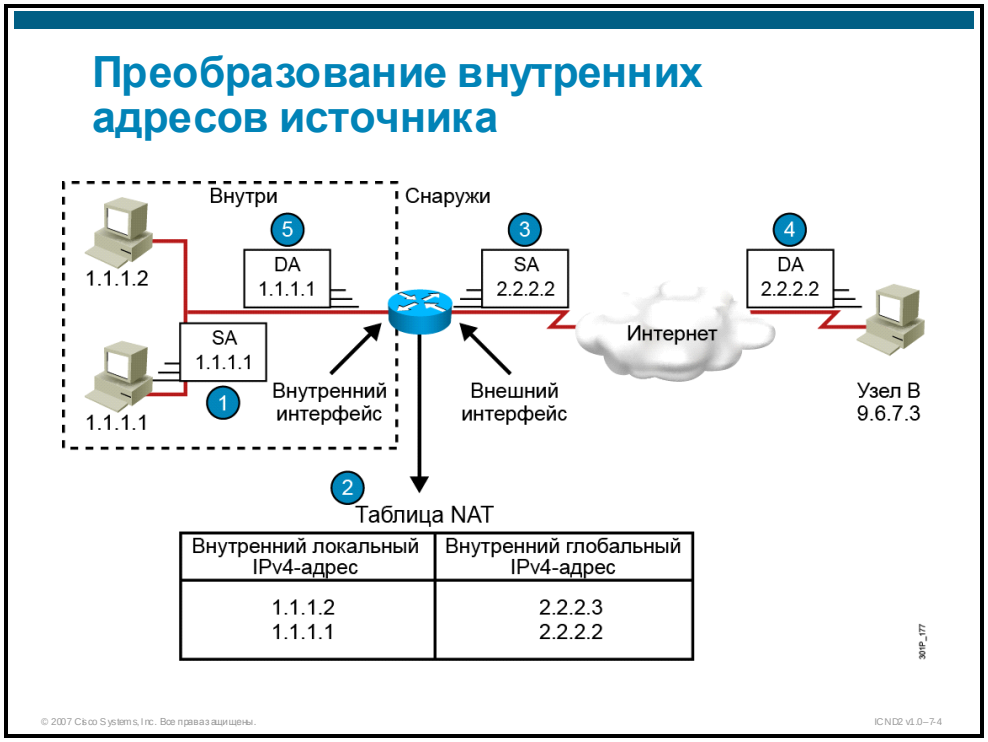


Одна из главных функций NAT – статическое преобразование PAT, которое также называется «перегрузкой» в конфигурации Cisco IOS. PAT преобразует несколько внутренних адресов в один внешний адрес, и позволяет им использовать этот адрес одновременно.

- Преобразование PAT использует уникальные номера портов источника, принадлежащих внутреннему глобальному адресу IPv4, 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 – 1 023 или 1 024 – 65 535. Если преобразование PAT не обнаруживает доступный порт в соответствующей группе портов, и настроено несколько внешних адресов IPv4, преобразование PAT переходит к следующему адресу IPv4 и пытается выделить исходный порт источника. Преобразование PAT продолжает попытки выделить исходный порт источника, пока не заканчиваются доступные порты и внешние адреса IPv4.

Преобразование внутренних адресов источника

В этом разделе описывается статическое и динамическое преобразование внутренних адресов источника, а также настройка преобразования NAT.



Вы можете преобразовать внутренние адреса IPv4 в адреса IPv4, 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.

Действие 1 Пользователь хоста 1.1.1.1 создает подключение к хосту B.

Действие 2 Первый пакет, полученный маршрутизатором от хоста 1.1.1.1 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 1.1.1.1 (SA 1.1.1.1) необходимо выполнить динамическое преобразование. Затем маршрутизатор выбирает глобальный, зарегистрированный адрес из динамического пула и создает запись преобразования (в нашем примере 2.2.2.2). Такая запись называется простой.

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

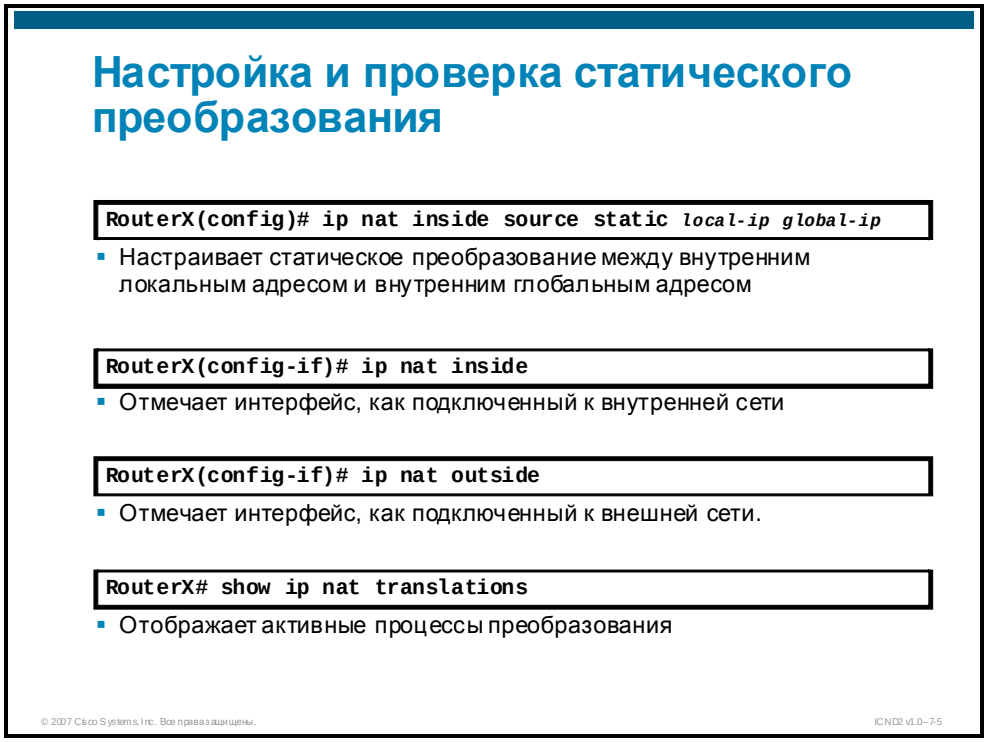
Действие 4 Хост B получает пакет и отвечает хосту 1.1.1.1, используя внутренний глобальный адрес назначения IPv4 2.2.2.2 (DA 2.2.2.2).

Действие 5 Когда маршрутизатор получает адрес IPv4, он выполняет поиск по таблице NAT, используя внутренний глобальный адрес в качестве критерия. Затем маршрутизатор выполняет обратное преобразование адреса во внутренний локальный адрес хоста 1.1.1.1 и пересылает пакет этому хосту.

Действие 6 Хост 1.1.1.1 получает пакет и продолжает диалог. Маршрутизатор выполняет действия 2 – 5 для каждого пакета.

Порядок, в котором маршрутизатор обрабатывает трафик, зависит от того, в какую сторону производится преобразование – глобальный-локальный или локальный-глобальный. В таблице ниже описывается порядок обработки трафика в зависимости от направления преобразования.

Локальный-глобальный	Глобальный-локальный
1. Если используется функция IP Security (IPsec), выполняется проверка входящего списка доступа.	1. Если используется функция IPsec, выполняется проверка входящего списка доступа.
2. Дешифрование – для Cisco Encryption Technology или IPsec.	2. Дешифрование – для Cisco Encryption Technology или IPsec
3. Проверка входящего списка доступа.	3. Проверка входящего списка доступа.
4. Проверка ограничений на входную скорость передачи данных.	4. Проверка ограничений на входную скорость передачи данных.
5. Учет входных данных.	5. Учет входных данных.
6. Маршрутизация на основе политик.	6. NAT-преобразование внешнего адреса во внутренний (глобального адреса в локальный)
7. Маршрутизация пакета.	7. Маршрутизация на основе политик.
8. Перенаправление в веб-кэш.	8. Маршрутизация пакета.
9. NAT-преобразование внутреннего адреса во внешний (локального адреса в глобальный)	9. Перенаправление в веб-кэш.
10. Проверка криптографической карты и, при необходимости, отметка пакета для шифрования.	10. Проверка криптографической карты и, при необходимости, отметка пакета для шифрования.
11. Проверка исходящего списка доступа.	11. Проверка исходящего списка доступа.
	12. Проверка контекстного контроля доступа CBAC.
	13. Перехват TCP.
	14. Шифрование.
	15. Постановка в очередь.

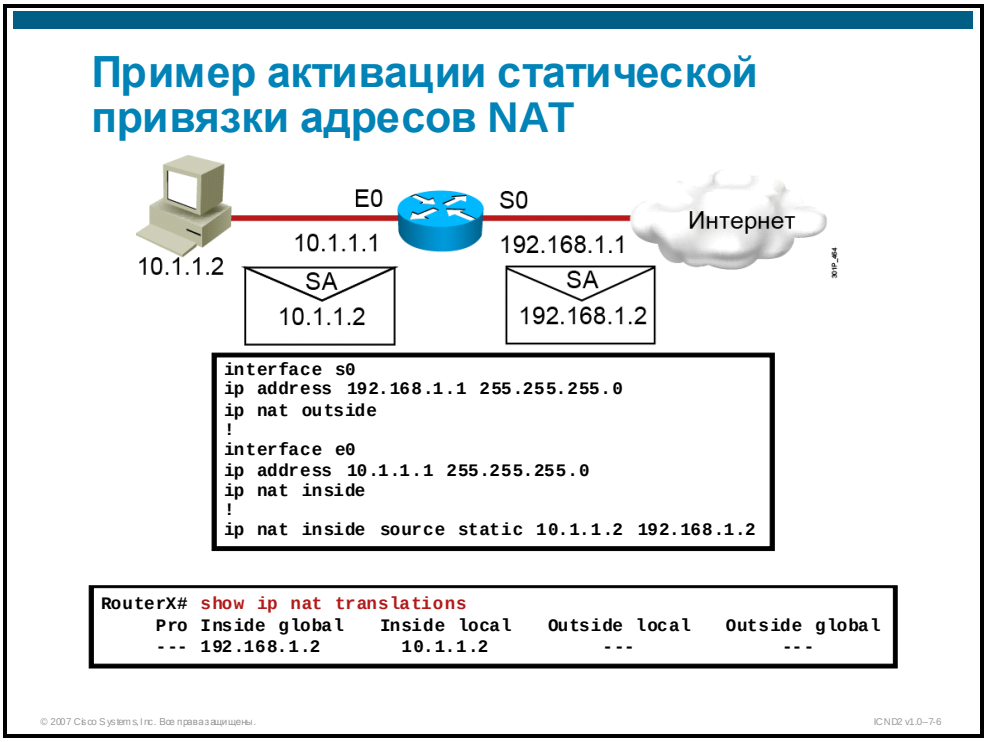


Чтобы настроить статическое преобразование внутренних адресов источника, выполните действия, описанные в таблице.

Процедура настройки статического преобразование адресов источника

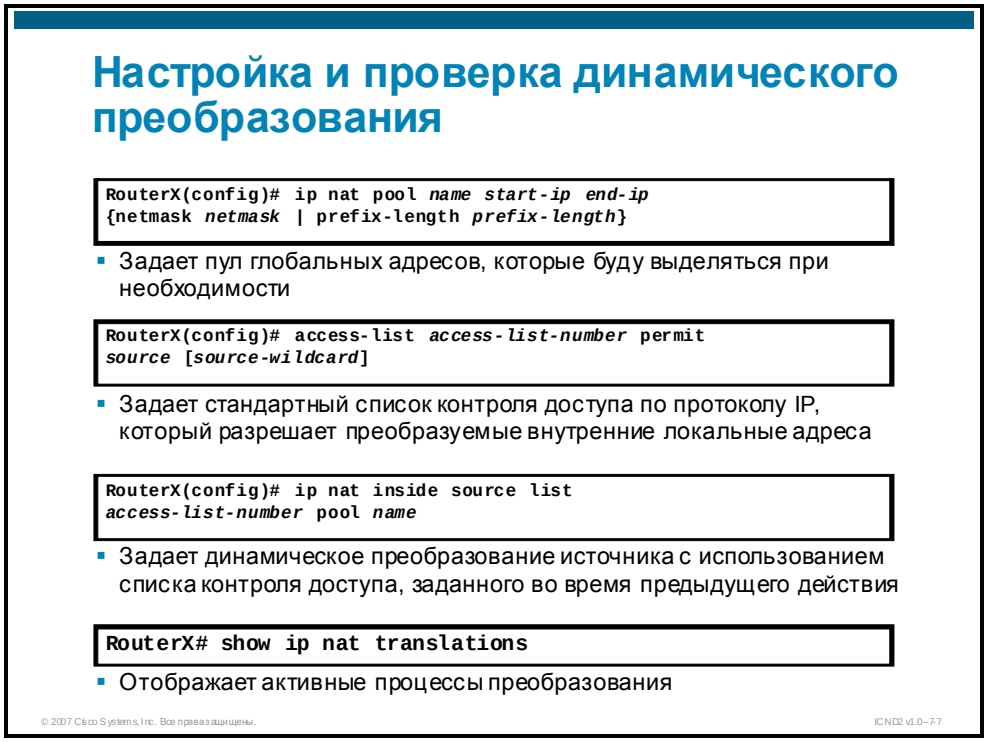
№	Действие	Примечания
1.	Настройте статическое преобразование между внутренним локальным адресом и внутренним глобальным адресом. `RouterX(config)# ip nat inside source static` *локальный ip-адрес глобальный ip-адрес*	Введите глобальную команду **no ip nat inside source static**, чтобы удалить статическое преобразование источника.
2.	Задайте внутренний интерфейс. `RouterX(config)# interface` *номер типа*	После ввода команды **interface** приглашение интерфейса командной строки изменится с (config)# на (config-if)#.
3.	Отметьте интерфейс, как подключенный к внутренней сети. `RouterX(config-if)# ip nat inside`	
4.	Задайте внешний интерфейс. `RouterX(config-if)# interface` *номер типа*	
5.	Отметьте интерфейс, как подключенный к внешней сети. `RouterX(config-if)# ip nat outside`	

Используйте команду **show ip nat translations** в режиме EXEC для вывода сведений об активных преобразованиях.



Пример: Статическая привязка адресов NAT

В примере ниже иллюстрируется использование дискретной привязки адресов для статического преобразования NAT. Маршрутизатор преобразует адрес пакетов хоста 10.1.1.2 в адрес 192.168.1.2.



Чтобы настроить динамическое преобразование внутренних адресов источника, выполните действия, описанные в таблице.

Процедура настройки динамического преобразование адресов источника

№	Действие	Примечания
1.	Задайте пул глобальных адресов, которые буду выделяться при необходимости. `RouterX(config)# ip nat pool` *имя начальный ip-адрес конечный ip-адрес* {**netmask** *маска сети* | **prefix-length** *длина префикса*}	Введите глобальную команду **no ip nat pool**, чтобы удалить пул глобальных адресов.
2.	Задайте стандартный список контроля доступа (ACL), разрешающий преобразуемые адреса. `RouterX(config)# access-list` *номер списка доступа* **permit** *источник* [*шаблон источника*]	Введите глобальную команду **no access-list** *номер списка доступа*, чтобы полностью удалить список контроля доступа.
3.	Задайте динамическое преобразование источника, указав список контроля доступа, заданный во время предыдущего действия. `RouterX(config)# ip nat inside source list` *номер списка доступа* **pool** *имя*	Введите глобальную команду **no ip nat inside source**, чтобы удалить динамическое преобразование источника.
4.	Задайте внутренний интерфейс. `RouterX(config)# interface` *номер типа*	После ввода команды **interface** приглашение интерфейса командной строки изменится с (config)# на (config-if)#.
5.	Отметьте интерфейс, как подключенный к внутренней сети. `RouterX(config-if)# ip nat inside`	

№	Действие	Примечания
6.	Задайте внешний интерфейс. `RouterX(config-if)# **interface** *номер типа*`	
7.	Отметьте интерфейс, как подключенный к внешней сети. `RouterX(config-if)# **ip nat outside**`	

Внимание Список контроля доступа должен разрешать только адреса, предназначенные для преобразования. Помните, что в конце каждого списка контроля доступа находится инструкция «Отклонить все». Список контроля доступа со слишком большим количеством разрешающих инструкций может привести к непредсказуемым результатам. Использование инструкции «Разрешить все» может спровоцировать потребление значительных ресурсов маршрутизатора преобразованием NAT, что в свою очередь может стать причиной проблем в сети.

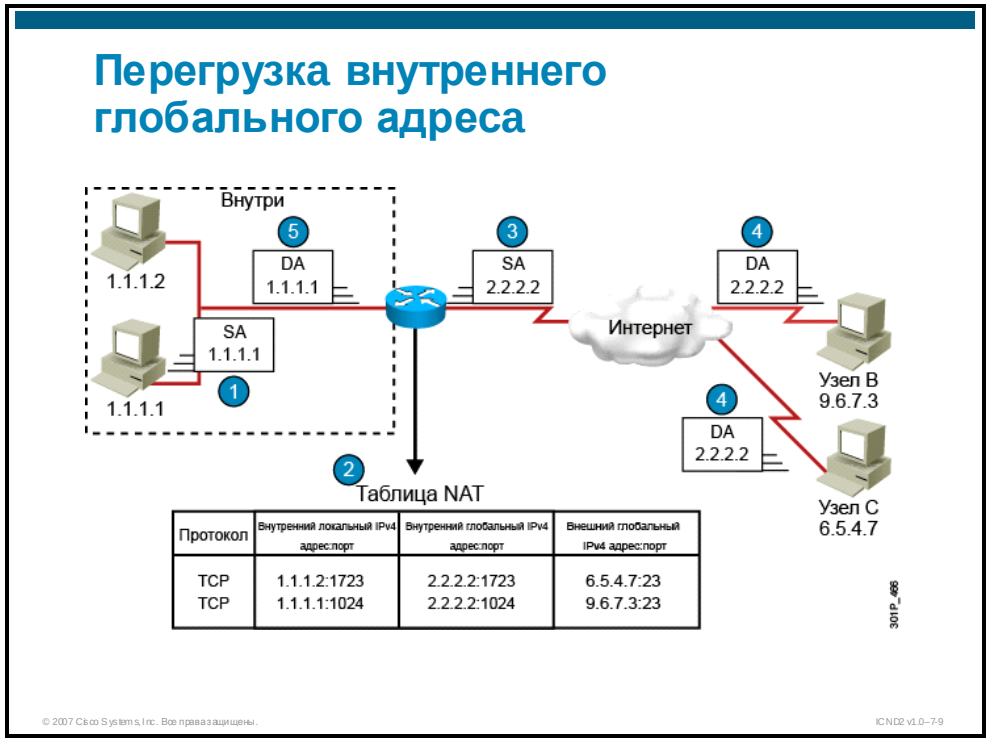
Используйте команду **show ip nat translations** в режиме EXEC для вывода сведений об активных преобразованиях.

Пример: Динамическое преобразование адресов

В этом примере преобразуются все адреса, проходящие через список ACL 1, т. е. Адрес источника из сети 192.168.1.0/24 преобразуется в адрес из пула net-208. Пул содержит адреса от 171.69.233.209/28 до 171.69.233.222/28.

Перегрузка внутреннего глобального адреса

В этом разделе описывается настройка преобразования PAT, которое реализуется путем перегрузки внутреннего глобального адреса.



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 от 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 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 дифференциаторов используются номера портов TCP. Хосты B и C считают, что они работают с одним хостом по адресу 2.2.2.2. На самом деле они работают с разными хостами, дифференциатором служит номер порта. Фактически, несколько хостов могут использовать один глобальный адрес IPv4 с помощью нескольких номеров портов.

Маршрутизатор выполняет следующий процесс при перегрузке внутреннего глобального адреса:

Действие 1 Пользователь хоста 1.1.1.1 создает подключение к хосту B.

Действие 2 Первый пакет, полученный маршрутизатором от хоста 1.1.1.1 заставляет его проверить свою таблицу NAT.

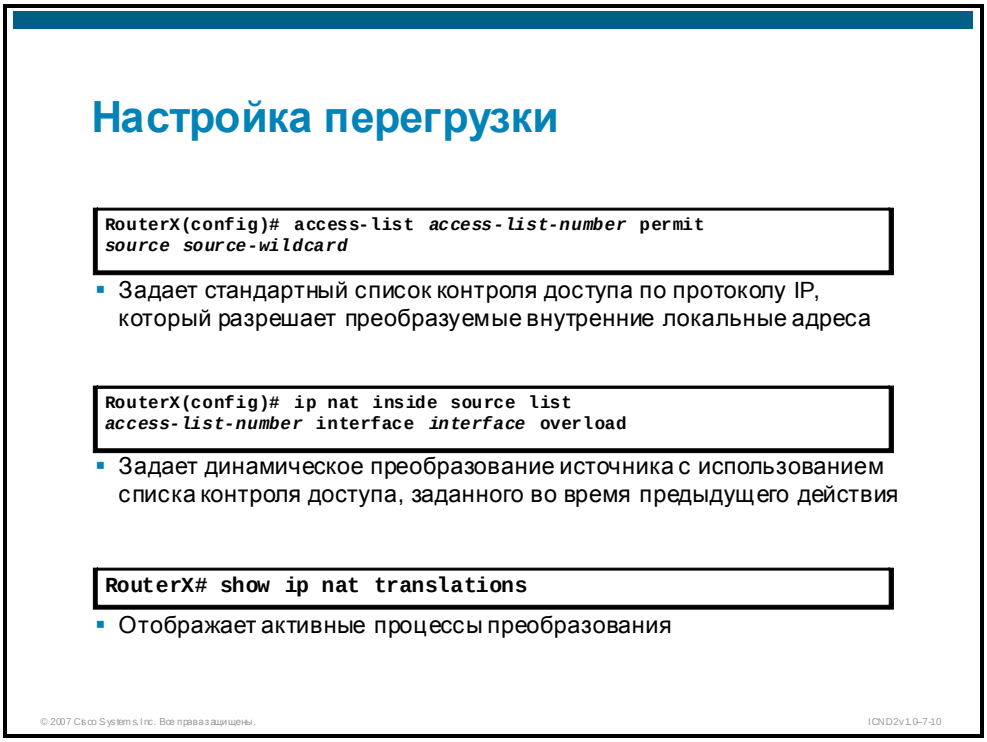
Если запись преобразования не задана, маршрутизатор определяет, что адрес 1.1.1.1 должен быть преобразован и устанавливает преобразование адреса 1.1.1.1 в зарегистрированный глобальный внутренний адрес. Если включена перегрузка и активно другое преобразование, маршрутизатор использует глобальный адрес этого преобразования и сохраняет достаточно информации для обратного преобразования. Такая запись называется расширенной.

Действие 3 Маршрутизатор заменяет внутренний локальный адрес источника 1.1.1.1 выбранным глобальным адресом в записи преобразования и пересылает пакет.

Действие 4 Хост B получает пакет и отвечает хосту 1.1.1.1, используя внутренний глобальный адрес назначения IPv4 2.2.2.2.

Действие 5 Когда маршрутизатор получает пакет с внутренним глобальным адресом IPv4, 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 1.1.1.1 и пересылает пакет хосту 1.1.1.1.

Действие 6 Хост 1.1.1.1 получает пакет и продолжает диалог. Маршрутизатор выполняет действия 2 – 5 для каждого пакета.

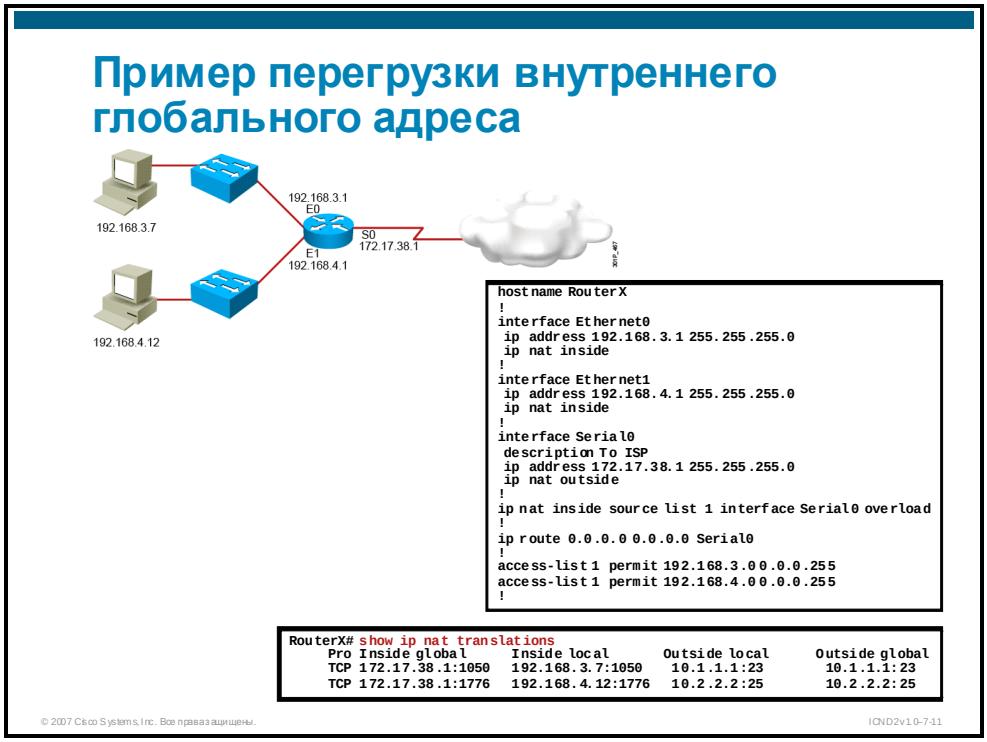


Чтобы настроить перегрузку внутренних глобальных адресов источника, выполните действия, описанные в таблице.

Процедура настройки перегрузки внутренних глобальных адресов источника

№	Действие	Примечания
1.	Задайте стандартный список контроля доступа (ACL), разрешающий преобразуемые адреса. `RouterX(config)# access-list` *номер списка доступа* `permit` *источник* [*шаблон источника*]	Введите глобальную команду **no access-list** *номер списка доступа*, чтобы полностью удалить список контроля доступа.
2.	Задайте динамическое преобразование источника, указав список контроля доступа, заданный во время предыдущего действия. `RouterX(config)# ip nat inside source list` *номер списка доступа* `interface` *интерфейс* `overload`	Введите глобальную команду **no ip nat inside source**, чтобы удалить динамическое преобразование источника. Ключевое слово **overload** включает преобразование PAT.
3.	Задайте внутренний интерфейс. `RouterX(config)# interface` *номер типа* `RouterX(config-if)# ip nat inside`	После ввода команды **interface** приглашение интерфейса командной строки изменится с (config)# на (config-if)#.
4.	Задайте внешний интерфейс. `RouterX(config-if)# interface` *номер типа* `RouterX(config-if)# ip nat outside`	

Используйте команду **show ip nat translations** в режиме EXEC для вывода сведений об активных преобразованиях.



Процесс NAT-преобразования внутреннего адреса во внешний состоит из следующих действий:

Действие 1 Входящий пакет попадает в таблицу маршрутизации, определяется следующий переход.

Действие 2 Инструкции NAT обрабатываются так, чтобы адрес IPv4 интерфейса serial 0 мог использоваться в режиме перегрузки. Преобразование PAT создает адрес источника.

Действие 3 Маршрутизатор инкапсулирует пакет и отправляет его из интерфейса serial 0.

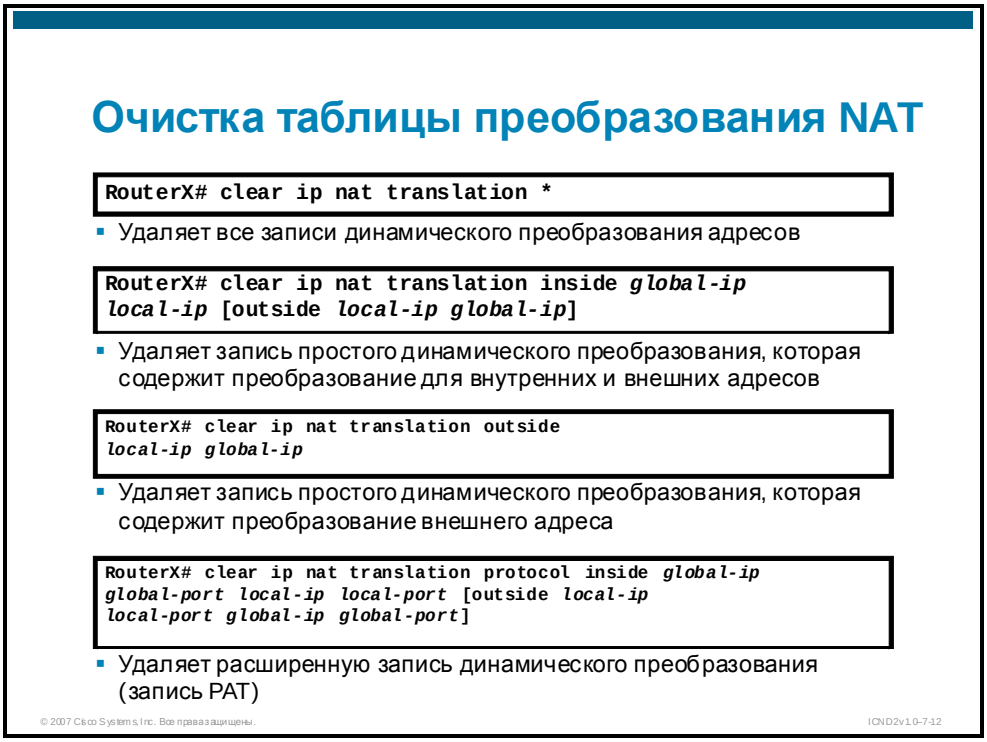
Действие 4 NAT-преобразование внешних адресов во внутренние выполняется последовательно.

Действие 5 Для инструкций NAT выполняется синтаксический разбор. Маршрутизатор ищет существующее преобразование и идентифицирует соответствующий адрес назначения.

Действие 6 Входящий пакет попадает в таблицу маршрутизации, определяется интерфейс на следующем переходе.

Действие 7 Пакет инкапсулируется и отправляется из локального интерфейса.

Во время этого процесса внутренние адреса невидимы. В результате хосты не имеют внешнего открытого адреса, что позволяет улучшить безопасность.



По умолчанию для динамического преобразования NAT и PAT задается период бездействия (время ожидания). Время ожидания по умолчанию меняется в зависимости от протокола. Периоды ожидания по умолчанию можно изменить с помощью команды **ip nat translation**. Синтаксис команды:

```
ip nat translation {timeout | udp-timeout | dns-timeout | tcp-timeout
| finrst-timeout | icmp-timeout | pptp-timeout | syn-timeout | port-
timeout} {seconds | never}
```

Параметры команды ip nat translation

Параметр	Описание
`timeout`	Время ожидания для всех динамических преобразований, кроме преобразования с перегрузкой. Значение по умолчанию – 86 400 сек (24 часа).
`udp-timeout`	Время ожидания для порта UDP. Значение по умолчанию – 300 сек (5 минут).
`dns-timeout`	Время ожидания для подключений к DNS. Значение по умолчанию – 60 секунд.
`tcp-timeout`	Время ожидания для порта TCP. Значение по умолчанию – 86 400 сек (24 часа).
`finrst-timeout`	Время ожидания для пакетов TCP Finish и Reset, закрывающих подключения. Значение по умолчанию – 60 секунд.
`icmp-timeout`	Время ожидания для потоков ICMP. Значение по умолчанию – 60 секунд.
`pptp-timeout`	Время ожидания для потоков PPTP. Значение по умолчанию – 86 400 сек (24 часа).

Параметр	Описание
`syn-timeout`	Время ожидания для потоков TCP сразу после сообщения синхронной передачи, которое состоит из цифровых сигналов, отправленных с точной синхронизацией. Значение по умолчанию – 60 секунд.
`port-timeout`	Время ожидания для порта TCP/UDP.
`seconds`	Время ожидания (в секундах), по истечении которого преобразование на указанном порте отключается. Значение по умолчанию – 0.
`never`	Для преобразования порта задается бесконечное время ожидания.

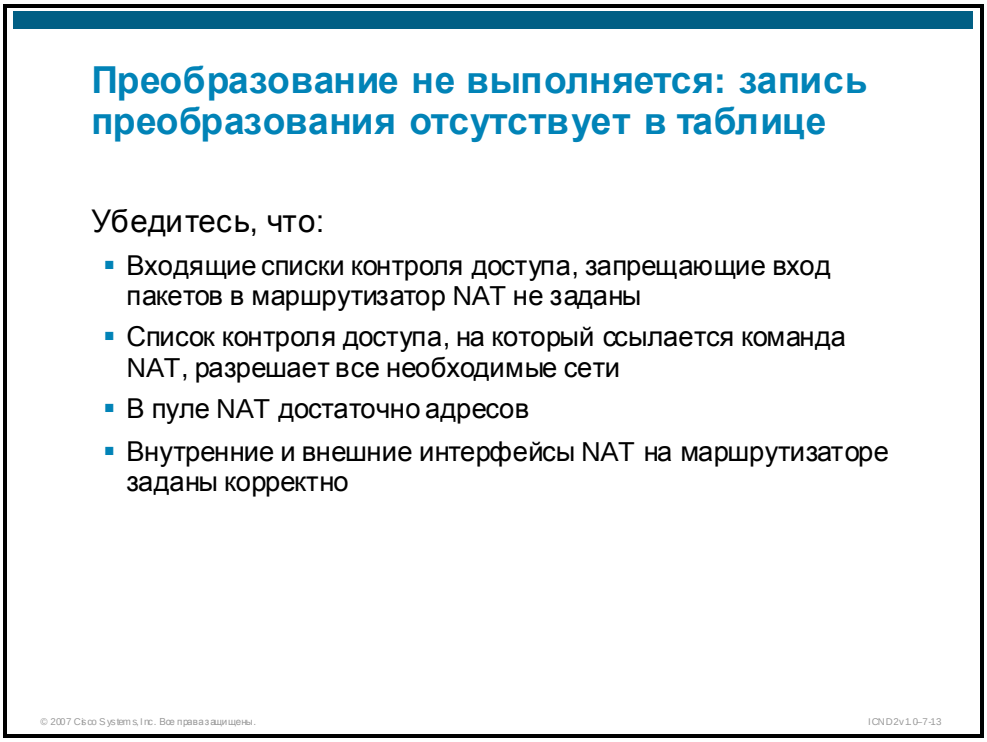
В таблице ниже перечислены команды, которые используются для удаления записей до того, как их время ожидания истечет.

Команды clear ip nat translation

Команда	Описание
`clear ip nat translation *`	Удаляет все записи динамического преобразования из таблицы преобразования NAT.
`clear ip nat translation inside` *`глобальный ip-адрес локальный ip-адрес`* **[`outside`** *`локальный ip-адрес глобальный ip-адрес`***]**	Удаляет запись простого динамического преобразования, которая содержит преобразование для внутренних и внешних адресов.
`clear ip nat translation outside` *`локальный ip-адрес глобальный ip-адрес`*	Удаляет запись простого динамического преобразования, которая содержит преобразование внешнего адреса.
`clear ip nat translation protocol inside` *`глобальный ip-адрес глобальный порт локальный ip-адрес локальный порт`* [**`outside`** *`локальный ip-адрес локальный порт глобальный ip-адрес глобальный порт`*]	Удаляет расширенную запись динамического преобразования (запись PAT).

Решение проблем таблицы преобразования

В этом разделе описывается решение проблем, мешающих выполнению преобразования в конфигурациях NAT и PAT.



Если в среде NAT возникают проблемы подключения IPv4, поиск причины этой проблемы часто бывает сложной задачей. Очень часто причиной считают преобразование NAT, хотя реальная проблема находится на более низком уровне. При определении причин проблем подключения IPv4 бывает полезно исключить NAT как возможный источник проблемы. Выполните следующие действия, чтобы убедиться, что NAT работает должным образом.

Действие 1 В зависимости от конфигурации четко определите цели и задачи NAT. Может выясниться, что источник проблемы в конфигурации NAT.

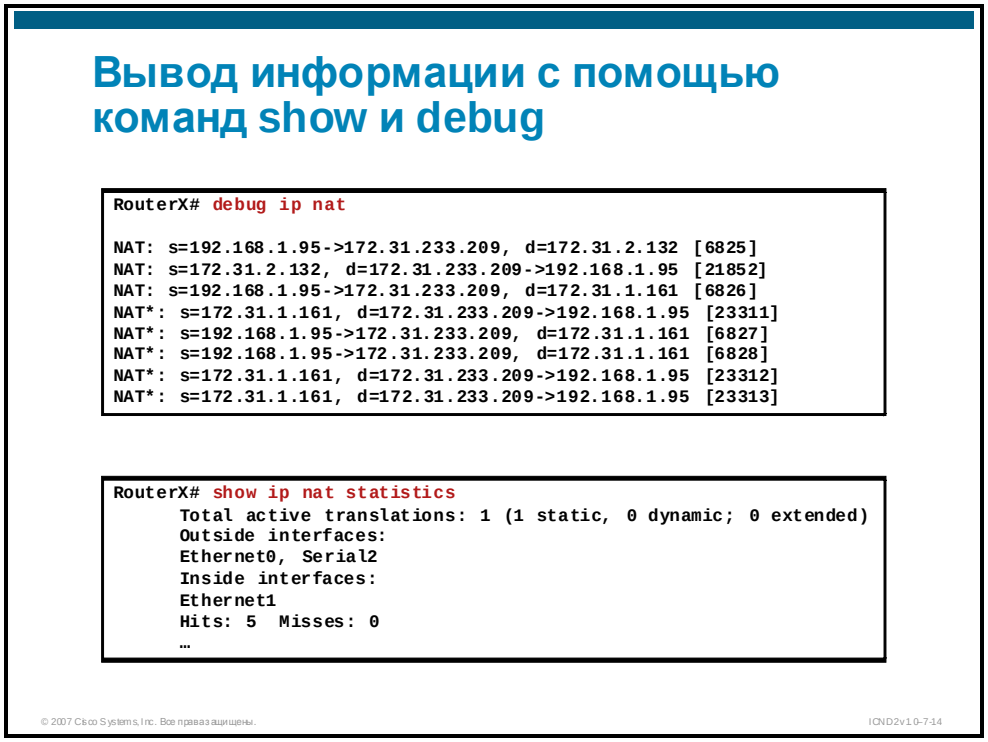
Действие 2 С помощью команды **show ip nat translations** определите, есть ли в таблице преобразования корректные записи преобразования.

Действие 3 Проверьте, выполняется ли преобразование с помощью команд **show** и **debug**.

Действие 4 Точно определите, что происходит с преобразованным пакетом и убедитесь, что маршрутизаторы имеют верные данные маршрутизации для преобразованного адреса и могут передавать пакет.

Если ожидаемые записи преобразования отсутствуют в таблице преобразования, проверьте следующее:

- входящие списки контроля доступа, запрещающие вход пакетов в маршрутизатор NAT не заданы;
- список контроля доступа, на который ссылается команда NAT, разрешает все необходимые сети;
- в пуле NAT достаточно адресов;
- внутренние и внешние интерфейсы NAT на маршрутизаторе заданы корректно.



В простой сети может быть целесообразно отслеживать статистику NAT с помощью команды **show ip nat statistics**. Однако в более сложных средах NAT с несколькими преобразованиями эта команда **show** будет бесполезна. В этом случае может потребоваться выполнение команд **debug** на маршрутизаторе.

Команда **debug ip nat** выводит сведения о каждом пакете, преобразованном маршрутизатором. Это помогает проверить работоспособность функции NAT. Команда **debug ip nat detailed** выводит описание каждого пакета, который рассматривается как кандидат на преобразование. Кроме того, эта команда выводит сведения об определенных ошибка и исключениях, таких как невозможность выделить глобальный адрес. Команда **debug ip nat detailed** выдает больше служебных данных, чем команда **debug ip nat**, но она предоставляет подробные сведения, которые могут быть необходимы для поиска и устранения проблемы NAT.

Пример: Использование команды debug ip nat

На рисунке приводится пример вывода команды **debug ip nat**. В этом примере в двух первых строках приводится вывод, созданный запросом и ответом DNS. Оставшиеся строки – отладочный вывод Telnet-подключения между хостом во внутренней сети и хостом во внешней сети.

Астериск (*) рядом с NAT обозначает, что преобразование выполняется на пути с быстрой коммутацией. Для первого пакета диалога всегда выполняется коммутация процессов. Оставшиеся пакеты проходят по пути с быстрой коммутацией если существует запись кэша.

Последняя запись каждой строки в квадратных скобках ([ ]), содержит идентификационный номер пакета. Эти сведения можно использовать для корреляции с другими данными трассировки от анализаторов протоколов.

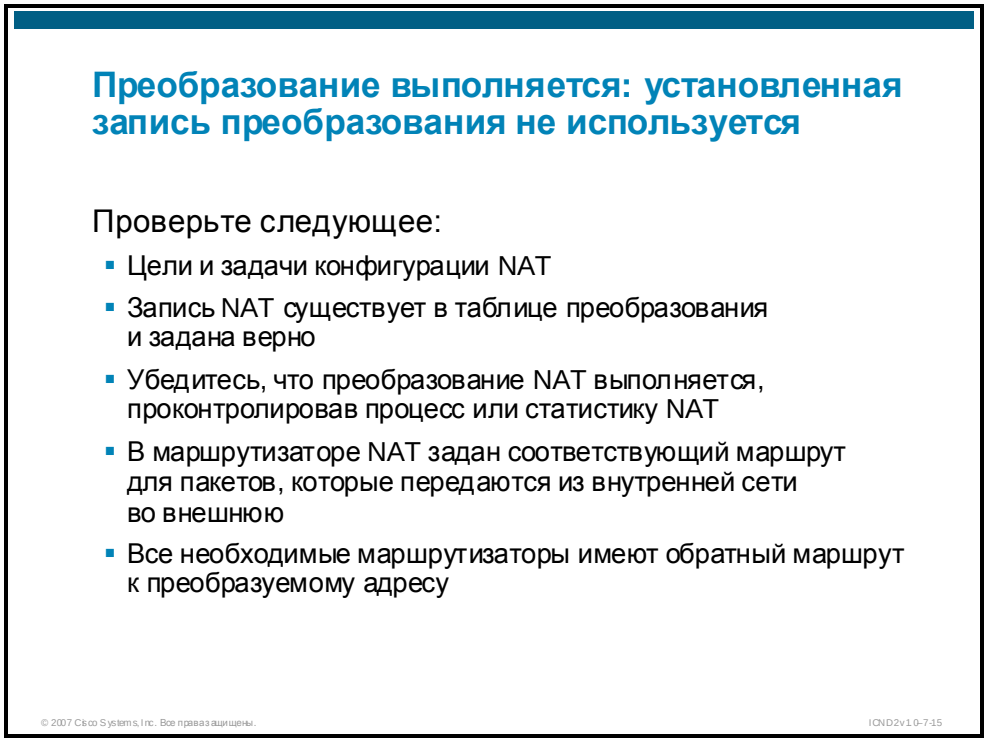
В таблице ниже описываются поля вывода команды **show ip nat statistics**.

Описание полей команды show ip nat statistics

Поле	Описание
Total translations	Количество активных преобразований в системе. Это число увеличивается при создании преобразования и уменьшается при удалении или истечении периода ожидания преобразования.
Outside interfaces	Список интерфейсов, отмеченных как внешние, с помощью команды **ip nat outside**.
Inside interfaces	Список интерфейсов, отмеченных как внутренние, с помощью команды **ip nat inside**.
Hits	Количество успешных операций поиска записи в таблице преобразования.
Misses	Количество неудачных операций поиска записи в таблице преобразования, в результате которых программное обеспечение создает новую запись.
Expired translations	Совокупное число преобразований, срок действия которых истек, с момента загрузки маршрутизатора.
Dynamic mappings	Сведения о динамических привязках.
Inside Source	Сведения о преобразовании внутренних адресов источника.
access-list	Номер списка контроля доступа, используемого в преобразовании.
pool	Имя пула (в нашем случае net-208).
refcount	Количество преобразований, использующих этот пул.
netmask	Маска сети IPv4, используемая пулом.
start	Первый адрес IPv4 в диапазоне адресов пула.
end	Последний адрес IPv4 в диапазоне адресов пула.
type	Тип пула. Возможные типы: обычный или ротационный.
total addresses	Количество адресов в пуле, доступных для преобразования.
allocated	Количество используемых адресов.
misses	Количество неудавшихся операций выделения адреса из пула.

Решение проблем, связанных с использованием записи преобразования

В этом разделе описывается выявление и устранение проблем, связанных с использованием записи преобразования.



Пример: Решение проблем, связанных с NAT

В соответствии с конфигурацией адрес источника (10.10.10.4) должен быть статически преобразован в 172.16.6.14. Чтобы проверить, существует ли преобразование в таблице преобразований, используйте команду **show ip nat translation**.

```
RouterX# show ip nat translation
Pro Inside global  Inside local  Outside local  Outside global
--- 172.16.6.14  10.10.10.4   ---    ---
```

Затем убедитесь, что преобразование выполняется. Это можно сделать двумя способами: выполнив команду NAT **debug** или отследив статистику NAT с помощью команды **show ip nat statistics**. Поскольку к командам **debug** следует прибегать в качестве последнего средства, начните с команды **show ip nat statistics**.

Чтобы определить, выполняется ли преобразование, отследите, увеличивается ли счетчик попаданий при прохождении трафика через маршрутизатор. Счетчик попаданий увеличивается каждый раз, когда запись в таблице преобразований используется для преобразования адреса. Сбросьте, а затем выведите статистику. Затем попытайтесь отправить эхо-запрос через маршрутизатор и выведите статистику снова.

```
RouterX# clear ip nat statistics
RouterX#
RouterX# show ip nat statistics
```

```
 Total active translations: 1 (1 static, 0 dynamic; 0 extended)
 Outside interfaces:
 Ethernet0, Serial2
 Inside interfaces:
 Ethernet1
 Hits: 0 Misses: 0
 Expired translations: 0
 Dynamic mappings:
 -- Inside Source
 access-list 7 pool test refcount 0
 pool test: netmask 255.255.255.0
 start 172.16.11.70 end 172.16.11.71
 type generic, total addresses 2, allocated 0 (0%), misses 0
```

После отправки эхо-запроса через маршрутизатор статистика NAT должна выглядеть следующим образом:

```
RouterX# show ip nat statistics
 Total active translations: 1 (1 static, 0 dynamic; 0 extended)
 Outside interfaces:
 Ethernet0, Serial2
 Inside interfaces:
 Ethernet1
 Hits: 5 Misses: 0
 Expired translations: 0
 Dynamic mappings:
 -- Inside Source
 access-list 7 pool test refcount 0
 pool test: netmask 255.255.255.0
 start 172.16.11.70 end 172.16.11.71
 type generic, total addresses 2, allocated 0 (0%), misses 0
```

В выводе команды **show**, отображается количество попаданий, которое увеличивается на 5 после сброса статистики NAT. При успешном запросе количество попаданий должно быть равно 10. Пять эхо-ответов ICMP, которые отправляются с преобразуемого адреса источника и пять пакетов эхо-ответа от места назначения, которые также должны быть преобразованы, всего 10 попаданий. Пять недостающих попаданий скорее всего связаны с тем, что эхо-ответы не преобразуются или не отправляются из маршрутизатора назначения.

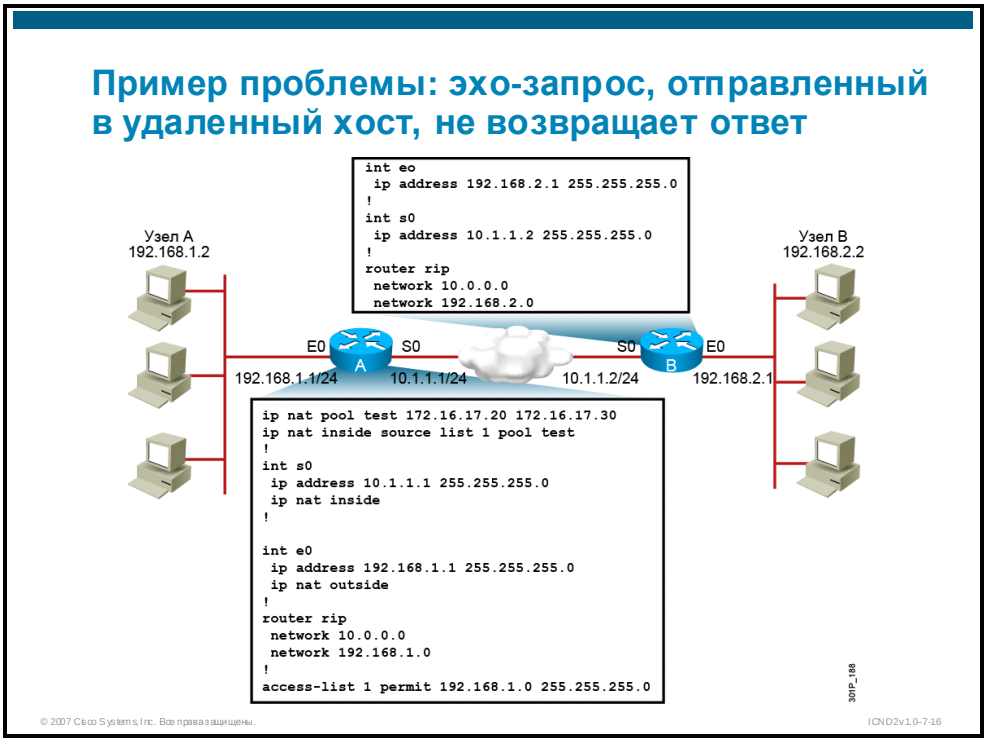
Чтобы определить, почему эхо-ответ не возвращается при отправке эхо-запроса, проверьте шлюз по умолчанию маршрутизатора, который служит шлюзом по умолчанию для обратного маршрута к преобразуемому адресу.

```
RouterY# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
  D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
  N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
  E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
  i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
are
  * - candidate default, U - per-user static route, o - ODR
  P - periodic downloaded static route

Gateway of last resort is not set
```



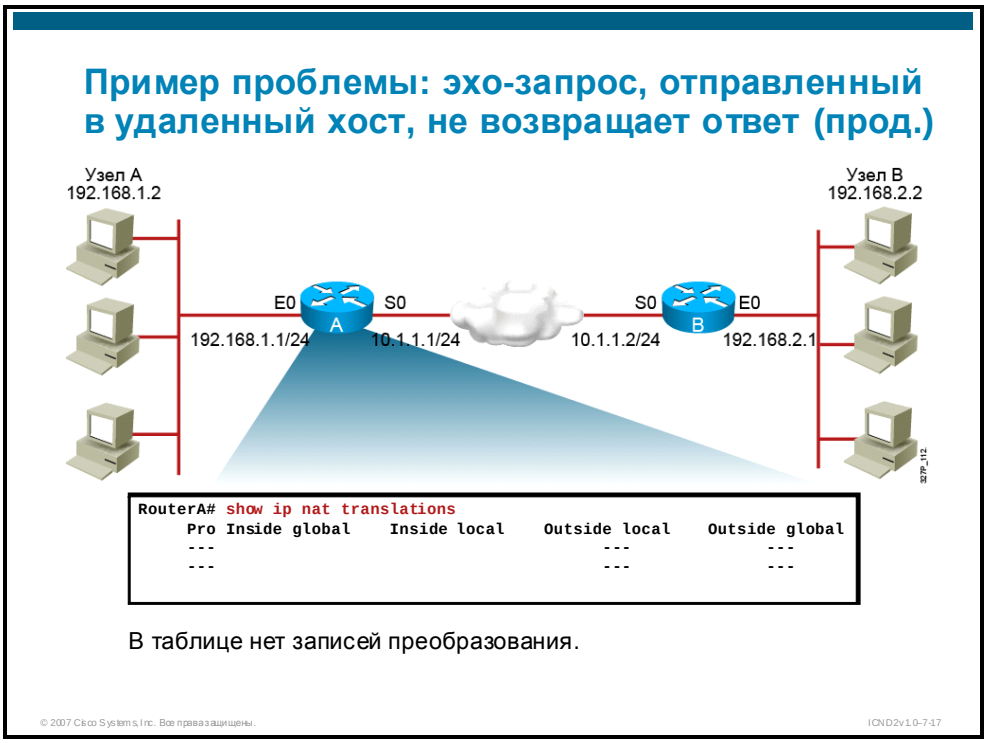
```
  172.16.0.0/24 is subnetted, 4 subnets
C  172.16.12.0 is directly connected, Serial0.8
C  172.16.9.0 is directly connected, Serial0.5
C  172.16.11.0 is directly connected, Serial0.6
C  172.16.5.0 is directly connected, Ethernet0
```

Таблица маршрутизации маршрутизатора B не содержит маршрута для 172.16.6.14 (преобразуемый адрес) . Поэтому эхо-ответы не генерируются при отправке эхо-запроса. После добавления обратного маршрута эхо-запрос сработает.



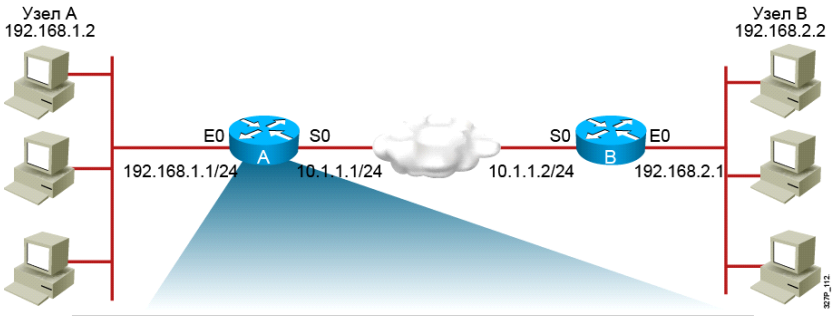
Пример: Эхо-запрос, отправленный в удаленный хост, не возвращает ответ

В сценарии на рисунке администратор столкнулся со следующим симптомом: хосту A (192.168.1.2) не удается отправить успешный эхо-запрос в хост B (192.168.2.2). На следующих рисунках описывается поиск и устранение этой проблемы.



Для поиска и устранения этой проблемы используйте команду **show ip nat translation**, чтобы определить, содержит ли таблица преобразования записи преобразования. Вы обнаружите, что в таблице нет записей.

Пример проблемы: эхо-запрос, отправленный в удаленный хост, не возвращает ответ (прод.)



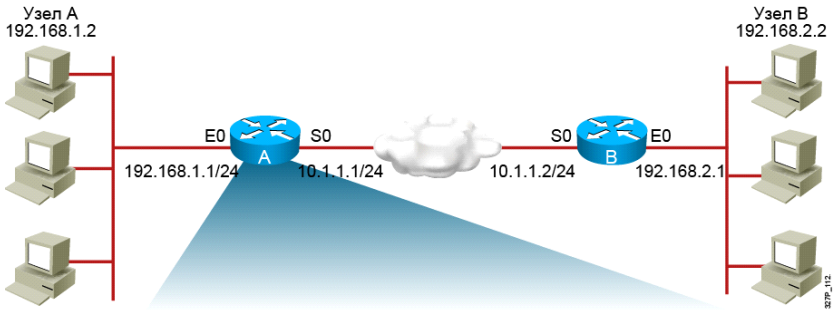

```
RouterA# show ip nat statistics
      Total active translations: 0 (0 static, 0 dynamic; 0 extended)
      Outside interfaces:
      Ethernet0
      Inside interfaces:
      Serial0
      Hits: 0  Misses: 0
      …
```

Внутренние и внешние интерфейсы NAT на маршрутизаторе заданы неверно.

Затем необходимо проверить, выполнялось ли преобразование, и определить интерфейсы, между которыми оно выполнялось. Для вывода этой информации используйте команду **show ip nat statistics**.

В данном примере вы определяете, что счетчики NAT имеют значение 0. Это значит, что преобразование не выполнялось. Кроме того, вы обнаружите, что внешние и внутренние интерфейсы NAT маршрутизатора заданы неверно.

Пример проблемы: эхо-запрос, отправленный в удаленный хост, не возвращает ответ (прод.)



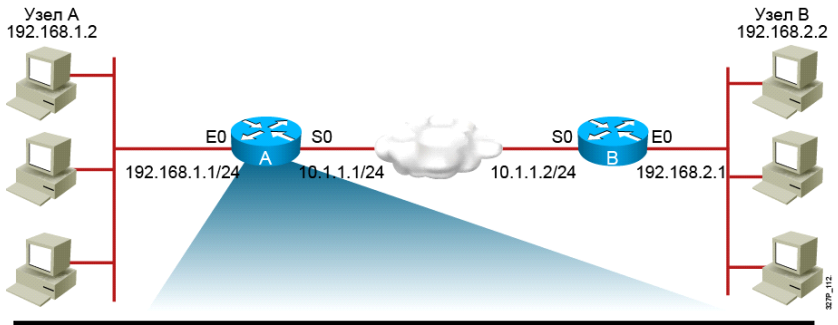

```
RouterA# show access-list

Standard IP access list 20
    10 permit 0.0.0.0, wildcard bits 255.255.255.0
```

- Эхо-запросы все еще не возвращают ответ и в таблице нет записей преобразования.
- В списке доступа, определяющем преобразуемые адреса, задана неверная шаблонная маска.

После того, как будут заданы верные внутренние и внешние интерфейсы NAT, отправьте еще один эхо-запрос с хоста A в хост B. В нашем примере этот также эхо-запрос не будет обработан. Выполните команды **show ip nat translations** и **show ip nat statistics** еще раз, чтобы выявить проблему. В данном примере вы обнаружите, что преобразование все еще не выполняется.

Затем вам следует использовать команду **show access-list**, чтобы убедиться, что список контроля доступа, на который ссылается команда NAT, разрешает все необходимые сети. В этом примере вы обнаружите, что в списке контроля доступа, определяющем преобразуемые адреса, задан неверный бит шаблонной маски.

Пример проблемы: эхо-запрос, отправленный в удаленный хост, не возвращает ответ (прод.)

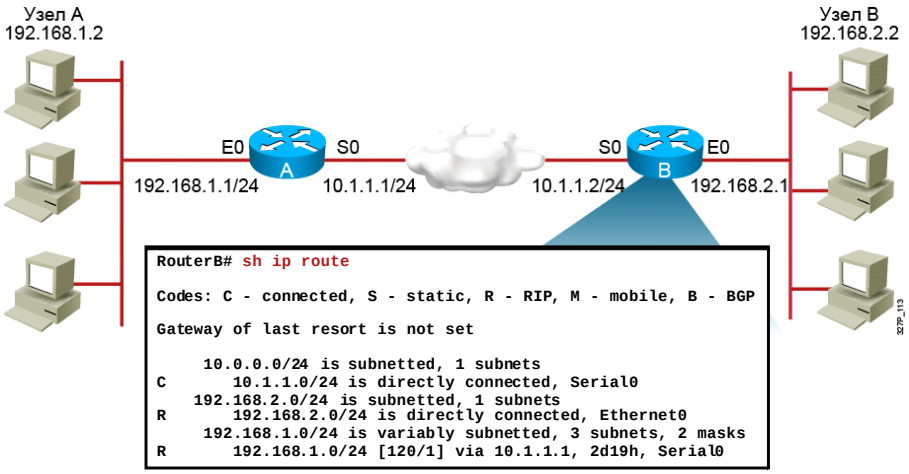



```
RouterA# show ip nat translations
     Pro Inside global      Inside local       Outside local      Outside global
     ---  172.16.17.20       192.168.1.2          ---                ---
```

- Преобразование выполняется.
- Эхо-запросы все еще не возвращают ответ.

После исправления бита шаблонной маски списка контроля доступа, отправьте еще один эхо-запрос с хоста A на хост B. Этот запрос также не будет обработан. Однако при повторном вводе команд **show ip nat translations** и **show ip nat statistics**, вы определите, что преобразование выполняется.

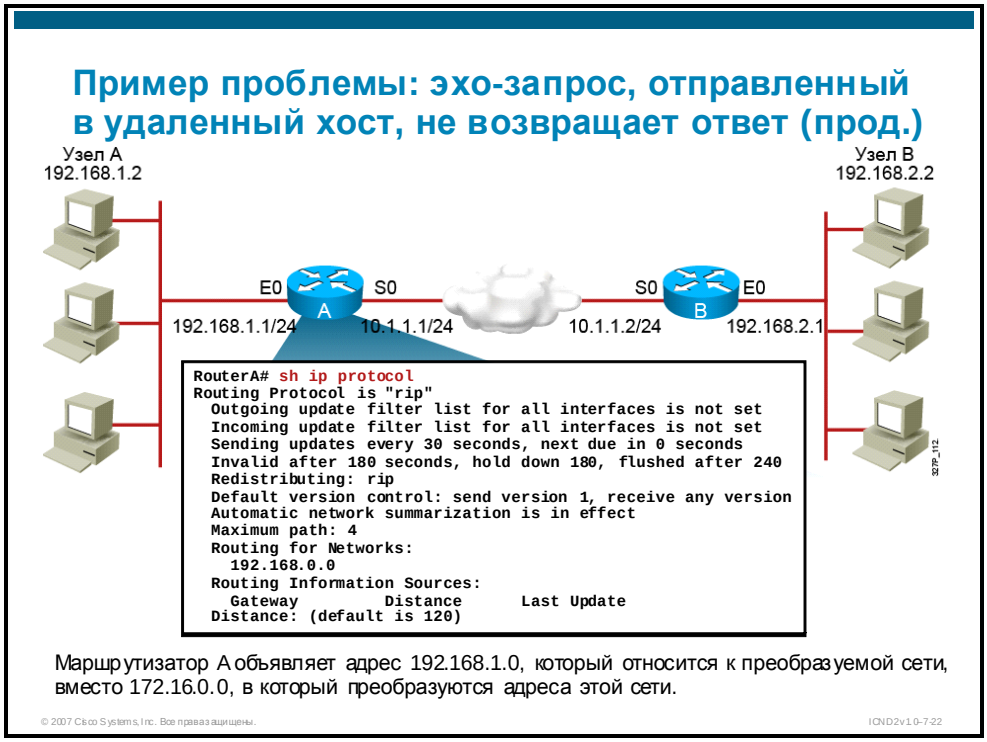
Пример проблемы: эхо-запрос, отправленный в удаленный хост, не возвращает ответ (прод.)



На маршрутизаторе B нет маршрута к преобразованному сетевому адресе 172.16.0.0.

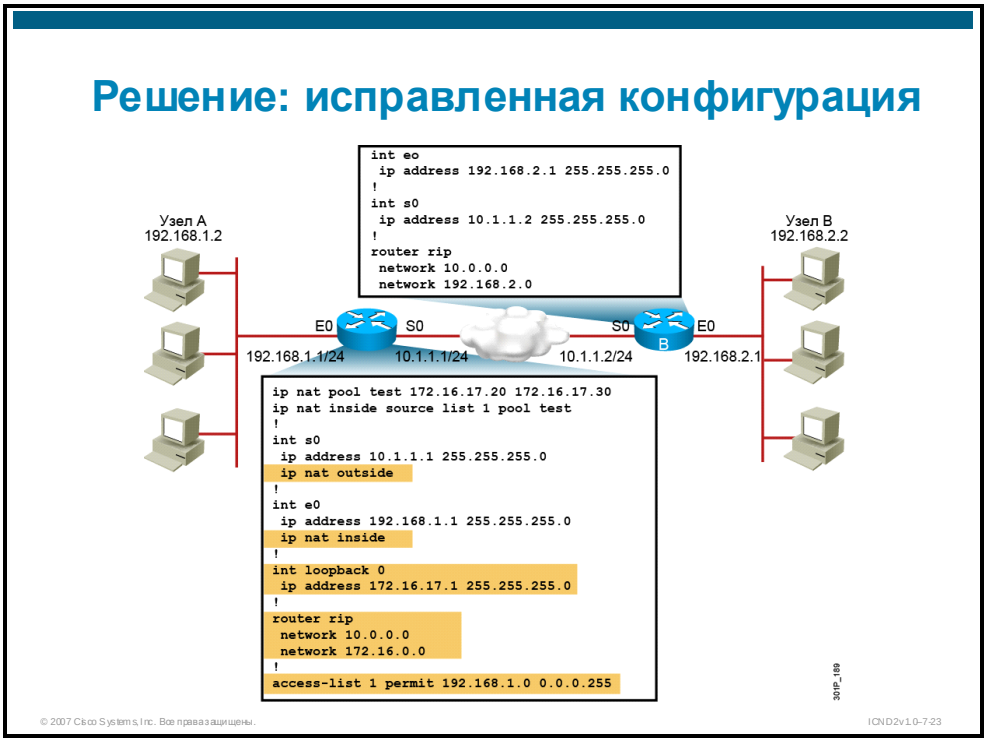
Затем вам следует ввести команду **show ip route** на маршрутизаторе B, чтобы убедиться, что для преобразуемого адреса существует обратный маршрут.

Вы обнаружите, что у маршрутизатора B нет маршрута к преобразованному сетевому адресу 172.16.0.0.



Вы должны вернуться к маршрутизатору A и ввести команду **show ip protocol**, чтобы проверить, объявляет ли маршрутизатор A преобразованный адрес 172.16.0.0.

Вы обнаружите, что маршрутизатор A объявляет адрес 192.168.1.0, который относится к преобразуемой сети, вместо сети 172.16.0.0, в которую преобразуются эти адреса.



Таким образом, чтобы исправить проблему, из-за которой хост A (192.168.1.2) не мог отправить эхо-запрос в хост B (192.168.2.2), вы изменили следующие параметры маршрутизатора A:

- Теперь интерфейс S0 назначен внешним интерфейсом, а не внутренним.
- Интерфейс E0 назначен внутренним интерфейсом, а не внешним.
- Шаблонная маска была изменена и принимает любой хост в сети 192.168.1.0. Раньше команда **access-list 1** не соответствовала ни одному из внутренних локальных адресов IPv4.
- Маршрутизатор A настроен на объявление сети 172.16.0.0. Раньше маршрутизатор B не знал, как получить доступ к сети 172.16.17.0/24. Конфигурация реализована путем создания интерфейса возвратной петли и изменения сетевых инструкций протокола RIP.

Резюме

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

Резюме

- Существует три типа преобразования NAT: статическое, динамическое и перегрузка (PAT).
- Статическое преобразование NAT – это привязка адресов один к одному. Динамические адреса NAT назначаются из пула.
- Перегрузка NAT (PAT) позволяет привязать несколько внутренних адресов к одному внешнему адресу.
- Используйте команду **show ip nat translation**, чтобы открыть таблицу преобразования и убедиться, что преобразование произошло.
- Чтобы определить, используется ли текущая запись преобразования, введите команду **show ip nat statistics**, чтобы проверить счетчик попаданий.

Занятие 2

Переход на IPv6

Обзор

Для наращивания сети в соответствии с будущими требованиями необходим неограниченный запас IP-адресов и улучшенная мобильность. Протокол IPv6 удовлетворяет все более сложные потребности иерархической адресации, которые не способен удовлетворить протокол IPv4. Протокол IPv6 использует несколько типов адресов, что делает его более эффективным, чем протокол IPv4. В этом занятии описываются различные типы адресов IPv6 и методы их назначения.

Для перехода с IPv4 на IPv6 используются различные методы, в том числе автоконфигурация. Механизм перехода выбирается в зависимости от потребностей сети. В этом занятии описываются различные механизмы перехода на сети IPv6.

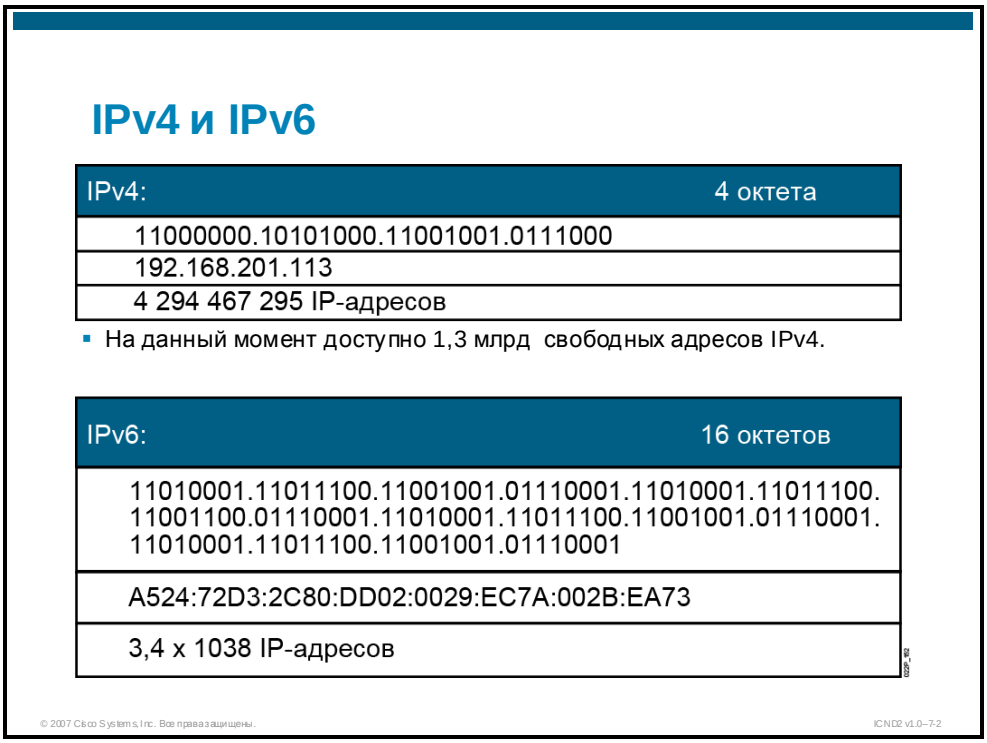
Задачи

По окончании этого занятия вы сможете описывать формат адресов протокола IPv6 и компоненты, необходимые для его внедрения, объяснять влияние IPv6 на сетевую маршрутизацию и настраивать основные параметры IPv6. Это значит, что вы сможете выполнять следующие задачи:

- рассказывать, почему протокол IPv6 необходим;
- описывать формат адреса IPv6;
- описывать методы назначения адресов IPv6;
- объяснять влияние IPv6 на распространенные протоколы маршрутизации и описывать изменения, которые необходимо внести в эти протоколы;
- объяснять стратегии перехода на среду IPv6;
- настраивать IPv6 с RIPng в сети IPv4.

Причины внедрения IPv6

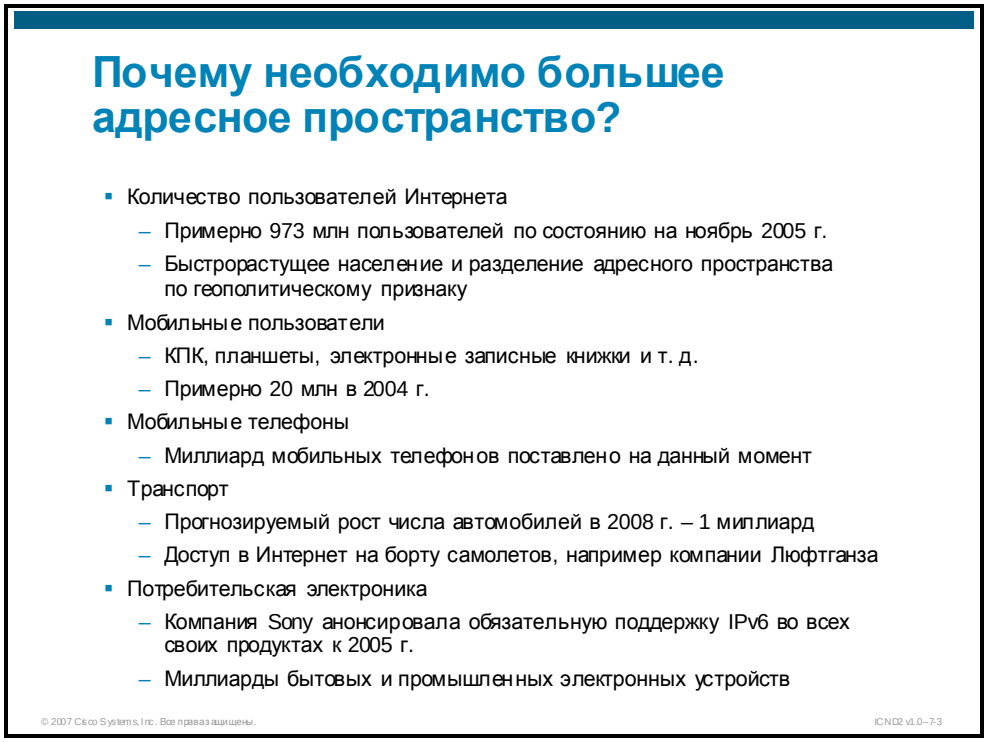
В этом разделе описываются причины внедрения IPv6.



Адресное пространство IPv4 обеспечивает примерно 4,3 млрд адресов. Из них только 3,7 млрд доступны для назначения, остальные зарезервированы для особых задач, таких как групповая рассылка, частное адресное пространство, проверка возвратной петли и исследования. По данным на 1 января 2007 г. 2,407 млрд из этих доступных адресов уже назначены конечным пользователям или поставщикам услуг Интернета (ISP). Таким образом, в адресном пространстве IPv4 остается примерно 1,3 млрд адресов.

Адрес IPv6 представляет собой двоичное значение с разрядностью 128 бит, которое можно представить 32-мя шестнадцатеричными цифрами (см. рисунок). Он поддерживает $3,4 * 10^{38}$ IP-адресов. Эта версия адресация IP обеспечивает достаточное количество адресов для поддержки будущего роста Интернета.

В дополнение к техническому и экономическому потенциалу, протокол IPv6 предлагает практически неограниченный запас IP-адресов. Благодаря обширному 128-битному адресному пространству, IPv6 поддерживает почти бесконечное число адресов, достаточное, чтобы выделить все адресное пространство IPv4 каждому жителю планеты.

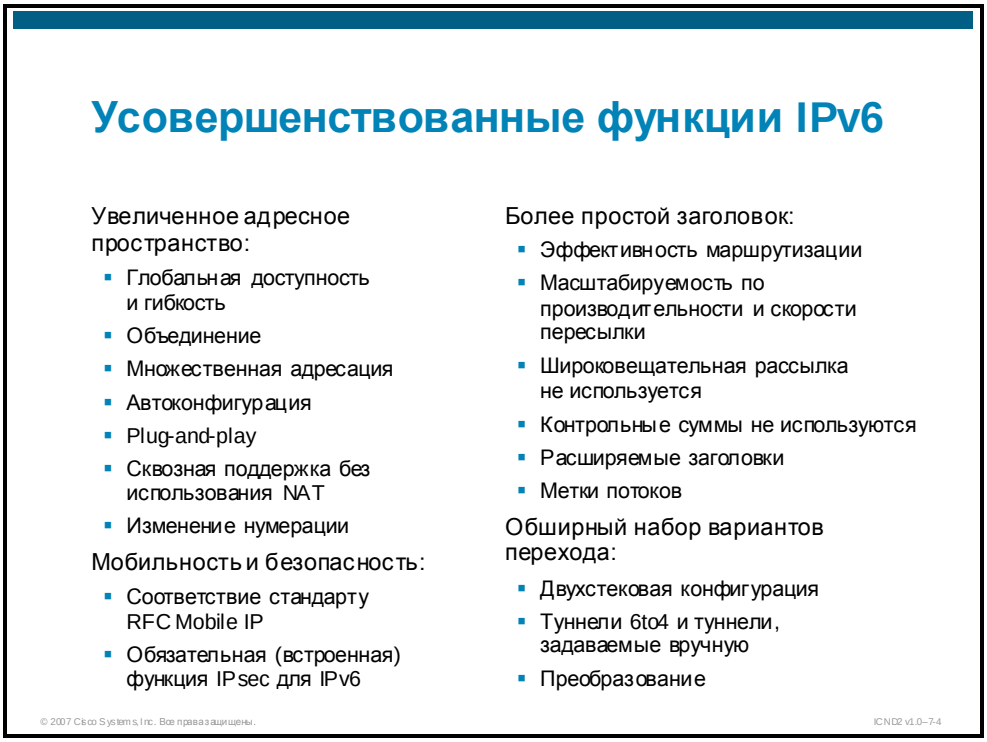


После полного перехода с IPv4 на IPv6 Интернет сильно изменится. Многие участники Интернет-сообщества проанализировали проблему нехватки адресов IPv4 и опубликовали отчеты. Однако прогнозы, когда именно адресное пространство IPv4 закончится, сильно расходятся. Некоторые называют 2008 или 2009 г., другие говорят, что это произойдет не раньше 2013 г. В любом случае, IPv4 не исчезнет за одну ночь. Скорее всего, переход на IPv6 будет постепенным.

Этот переход уже начался, особенно в Европе, Японии и Азиатско-Тихоокеанском регионе. Эти регионы почти исчерпали выделенные им адреса IPv4, и это увеличивает потребность в протоколе IPv6. Некоторые страны, такие как Япония, агрессивно внедряют IPv6. Другие, такие как Евросоюз, осуществляют медленный переход на IPv6, Китай рассматривает возможность создания новых сетей на основе IPv6.

Начиная с 1 октября 2003 г. министерство обороны США постановило, что все закупаемое оборудование должно поддерживать IPv6. Все правительственные агентства США должны внедрить IPv6 в свои основные сети к 2008 г., и они хотят уложиться в этот срок.

Эти примеры показывают, что внедрение IPv6 является серьезным отраслевым трендом.



Протокол IPv6 является результатом значительной модификации протокола IPv4. Некоторые функции IPv6 предлагают функциональные улучшения. На основе опыта, полученного разработчиками IP при использовании IPv4, были предложены изменения для удовлетворения текущих и потенциальных требований сетей.

- **Увеличенное адресное пространство:** Увеличенное адресное пространство предлагает следующие преимущества:
  - улучшение глобальной доступности и гибкости;
  - объединение префиксов, объявленных в таблице маршрутизации;
  - множественная адресация для использования нескольких поставщиков услуг Интернета;
  - автоконфигурация, которая поддерживает включение адресов канального уровня данных в адресное пространство;
  - решение Plug-and-play;
  - сквозная переадресация из частной сети в сеть общего доступа без преобразования адресов;
  - упрощенные механизмы смены нумерации и изменения адресов.
- **Упрощенный заголовок:** Более простой заголовок предлагает несколько преимущество по сравнению IPv4:
  - повышенная эффективность маршрутизации для масштабируемой производительности и скорости пересылки;
  - широковещательная рассылка не используется, что исключает возникновение широковещательных штормов;
  - обработка контрольных сумм не требуется;
  - более простые и эффективные механизмы расширения заголовка;
  - метки потоков для обработки отдельных потоков без необходимости в анализе пакета транспортного уровня для идентификации потока.

- **Мобильность и безопасность:** Мобильность и безопасность обеспечивается функциями стандарта Mobile IP и IP Security (IPsec). Мобильность позволяет пользователям мобильных сетевых устройств, как правило с беспроводным подключением, перемещаться между сетями.

  Mobile IP – стандарт IETF, доступный для протоколов IPv4 и IPv6. Он позволяет мобильным устройствам перемещаться между сетями без прерывания установленных сетевых соединений. Поскольку IPv4 не обеспечивает эту мобильность автоматически, ее необходимо добавлять с использованием дополнительных конфигураций.

  Функции мобильности встроены в протокол IPv6, что позволяет любому узлу IPv6 использовать их при необходимости. Заголовки маршрутизации протокола IPv6 делают Mobile IPv6 гораздо более эффективным, чем Mobile IPv4.

  IPsec – стандарт IETF, посвященный безопасности IP-сетей, доступный для протоколов IPv4 и IPv6. Хотя функции одинаковы для обоих сред, стандарт IPsec является обязательным в IPv6. Функции IPsec включены и доступны для использования на всех узлах IPv6, что делает Интернет на основе IPv6 более безопасным. Кроме того, IPsec требует наличия ключей у каждой стороны, а это означает глобальное развертывание и распространение ключей.

- **Обширный набор вариантов перехода:** Существует несколько способов добавить расширенные функции IPv6 к текущим возможностям IPv6.

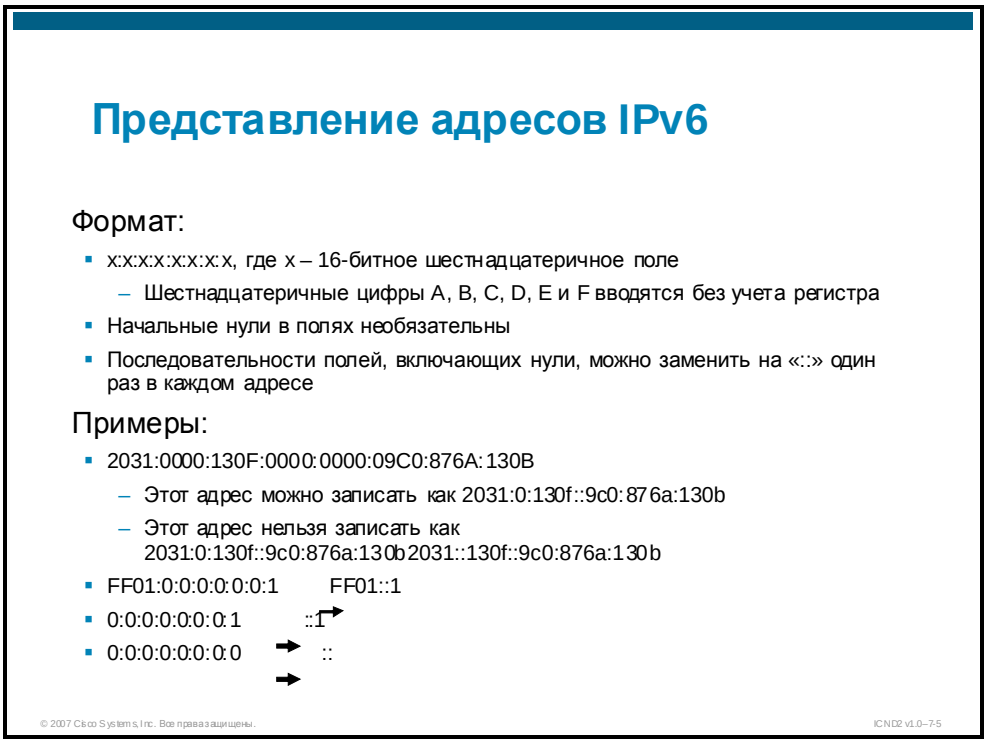
  — Один из подходов подразумевает внедрение двухстековой конфигурации, в которой IPv4 и IPv6 настраиваются на одном интерфейсе сетевого устройства.

  — Другой метод – туннелирование – становится все более распространенными с ростом количества сред IPv6. Существует множество методов туннелирования IPv6 поверх IPv4. Некоторые из них требуют ручной настройки, другие работают автоматически.

  — Версии Cisco IOS начиная 12.3(2)T поддерживают протокол NAT-PT для преобразования адресов между протоколами IPv6 и IPv4. Это преобразование обеспечивает прямое взаимодействие между хостами, использующими разные версии протокола IP.

Общие сведения об адресах IPv6

В этом разделе описывается формат адресов IPv6, а также методы их сокращения.



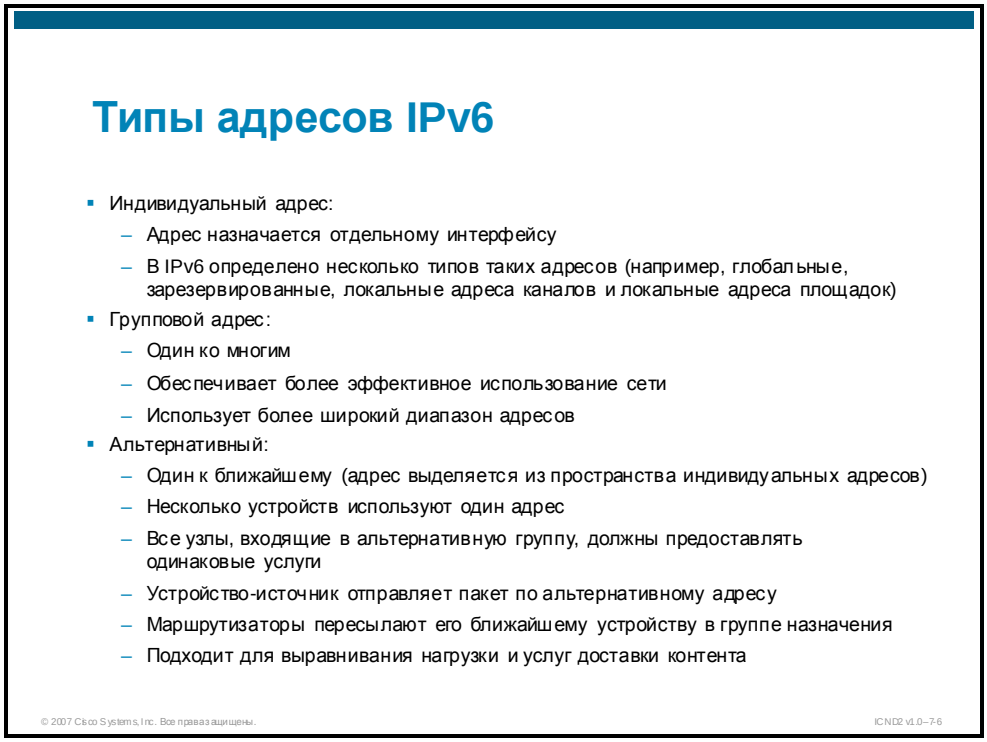
Для разделения записей в последовательности 16-битных полей, которая представляет адрес IPv6, используется двоеточие. Регистр шестнадцатеричных цифр A, B, C, D, E и F, входящих в адрес IPv6, не учитывается.

IPv6 не требует специальной номенклатуры записи адресной строки. Следуйте инструкциям ниже при вводе адресных строк IPv6:

- начальные нули в поле необязательны, 09C0 равняется 9C0 и 0000 равняется 0;
- последовательные поля из нулей можно заменить на «::», это сокращение можно вводить один раз для каждого адреса;
- неопределенный адрес записывается как «::», так как содержит только нули.

Использование записи «::» значительно уменьшает размер большинства адресов. Например, адрес FF01:0:0:0:0:0:0:1 можно записать как FF01::1.

Примечание	Синтаксический анализатор адресов определяет число недостающих нулей, разделяя две части и вводя нули до заполнения всех 128 бит. Если в адресе введено два сокращения «::», анализатор не сможет определить размер каждого из блоков нулей.



Широковещательная рассылка IPv4 является причиной многих проблем. Широковещательная рассылка инициирует несколько прерываний во всех компьютерах сети, а в отдельных случаях может вызвать неисправности, который остановят работу всей сети. Этот сбой называется широковещательным штормом.

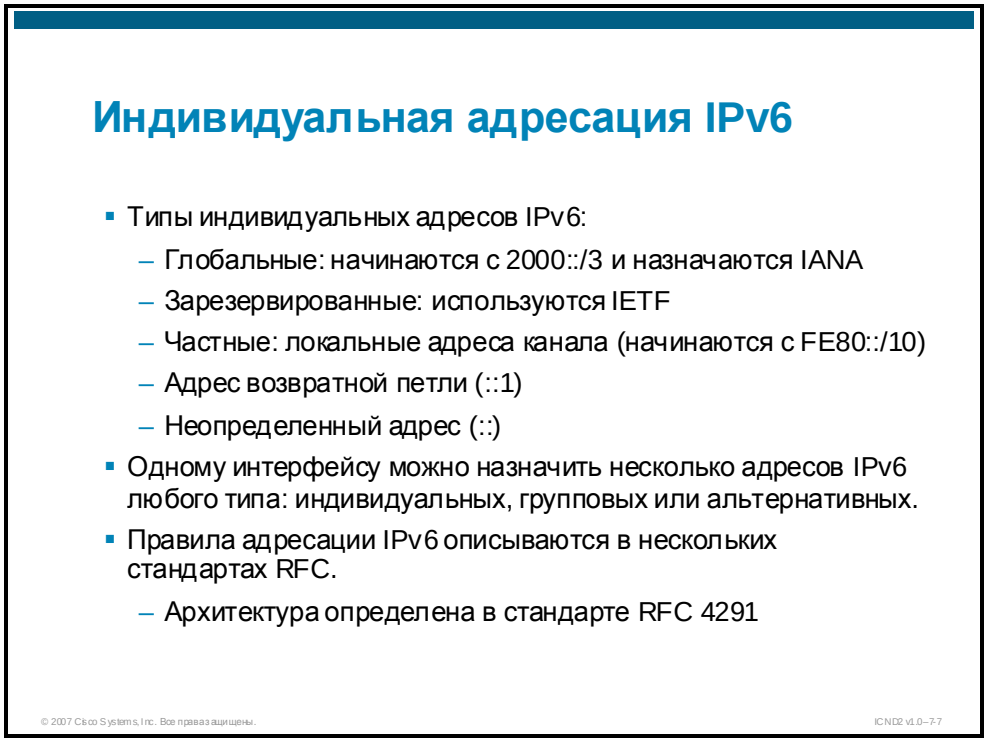
В сетях IPv6 широковещательная рассылка не используется. Вместо широковещательной рассылки IPv6 использует групповые рассылки и рассылки по альтернативным адресам. Групповая рассылка обеспечивает эффективную работу сети с помощью нескольких функциональных многоадресных групп, которые позволяют отправлять запросы ограниченному числу компьютеров в сети. Многоадресные группы исключают возникновение большинства проблем, связанных с широковещательными штормами в сетях IPv4.

Диапазон групповых адресов в IPv6 больше, чем в IPv4. В ближайшем будущем выделение групповых адресов ограничено не будет.

Кроме того, в IPv6 определен новый тип адреса, который называется альтернативным (адрес для отправки пакета любому из устройство группы). Альтернативный адрес идентифицирует список устройство или узлов, т. е. несколько интерфейсов. Альтернативные адреса являются компромиссом между индивидуальными и групповыми адресами. Индивидуальные пакеты отправляются определенному устройству с определенным IP-адресом, групповые – всем членам группы. Альтернативные пакеты отправляются любому из членов группы, которой назначен альтернативный адрес.

Для повышения эффективности, пакет, который отправляется по альтернативному адресу, доставляется ближайшему интерфейсу, который определяется используемым протоколом маршрутизации. Таким образом, альтернативную рассылку можно назвать «один к ближайшему». Синтаксически альтернативные адреса не отличаются от глобальных индивидуальных адресов, так как они выделяются из пула глобальных индивидуальных адресов.

Примечание На данный момент отрасль не накопила достаточного опыта глобального и произвольного применения альтернативных адресов. Кроме того, с широким использованием этих адресов связан ряд трудностей и угроз. До тех пор, пока разработчики не накопят достаточно опыта и не найдут решение этих проблем, на использование альтернативных адресов IPv6 налагаются следующие ограничения. (1) альтернативный адрес НЕЛЬЗЯ использовать как адрес источника пакета IPv6; (2) альтернативный адрес НЕЛЬЗЯ назначать хосту IPv6, только маршрутизатору.



Существует несколько основных типов индивидуальных адресов рассылки IPv6: глобальный, зарезервированный, частный (локальный для канала или площадки), возвратной петли и неопределенный.

Глобальные адреса

Глобальные индивидуальные адреса IPv6 аналогичны индивидуальным адресам IPv4. Глобальный индивидуальный адрес – это адрес IPv6 из глобального индивидуального префикса. Такая структура обеспечивает объединение префиксов маршрутизации, что ограничивает число записей в глобальной таблице маршрутизации. Глобальные индивидуальные адреса используются в объединенных восходящих каналах организаций, направленных к поставщикам услуг Интернета.

Зарезервированные адреса

IETF резервирует часть адресного пространства IPv6 для различных задач, текущих и будущих. Зарезервированные адреса представляют 1/256 адресного пространства IPv6. Адреса IPv6 других типов выделяются из этого блока.

Частные адреса

Блок адресов IPv6, выделенных под частные адреса, также, как в протоколе IPv4. Эти частные адреса действуют только внутри определенного канала или площадки и никогда не маршрутизируются за пределы сети компании. Первый октет частных адресов имеет значение «FE» в шестнадцатеричном счислении, следующее значение – цифра от 8 до F.

Эти адреса в свою очередь разделяются на два типа, в зависимости от области действия.

- Локальные адреса площадки, которые описываются ниже.
  - Эти адреса аналогичны адресам, определенным в стандарте RFC 1918, *Выделение адресов для частных интерсетей*, который используется в современных сетях IPv4. Эти адреса действуют в масштабе всей площадки или организации. Они обеспечивают адресацию внутри организации без необходимости в использовании частного префикса. Маршрутизаторы пересылают датаграммы внутри площадки, используя локальные адреса, но не за пределы площадки в сеть Интернет общего доступа.
  - Локальные адреса площадки начинаются с октета «FE», третья цифра адреса – «C» или «F». Таким образом эти адреса начинаются «FEC», «FED», «FEE» или «FEF».
- Локальные адреса канала, которые описываются ниже.
  - Локальные адреса уровня канала – новая концепция IPv6. Эти адреса имеют меньшую область действия, чем локальные адреса площадки. Они относятся только к одному физическому каналу (физической сети). Маршрутизаторы никогда не пересылают датаграммы с локальными адресами уровня канала, даже внутри организации. Они предназначены только для локального обмена внутри сегмента физической сети.
  - Эти адреса используются для операций обмена внутри канала, таких как автоматическая конфигурация адресов, обнаружение соседних узлов и обнаружение маршрутизаторов. Многие протоколы маршрутизации IPv6 также используют локальные адреса канала.
  - Локальные адреса площадки начинаются с октета «FE», третья цифра адреса – от 8 до B. Таким образом эти адреса начинаются «FE8», «FE9», «FEA» или «FEB».

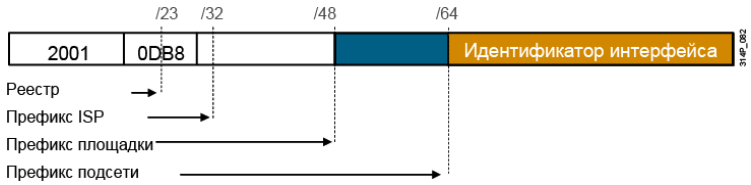
Адрес возвратной петли

Как и в протоколе IPv4, в IPv6 был назначен специальный адрес для тестирования. Датаграммы, переданные по этому адресу, возвращаются в устройство-отправитель. Однако в IPv6 для этой функции выделен только один адрес, а не целый блок. В качестве возвратной петли используется адрес 0:0:0:0:0:0:0:1, который, как правило, сокращается до «::1».

Неопределенный адрес

В протоколе IPv4 IP-адрес, состоящий из нулей, указывает на текущий хост и используется, если устройство не знает своего IP-адреса. В IPv6 эта концепция была формализована, и адрес из нулей (0:0:0:0:0:0:0:0) был назван неопределенным. Как правило, он используется в поле источника датаграммы, отправленной устройством, которое пытается настроить свой IP-адрес. Поскольку этот адрес состоит из нулей, его можно записать как «::».

Глобальные индивидуальные адреса IPv6 (а также адреса Anycast)



IPv6 использует один формат для глобальных индивидуальных и альтернативных адресов.

- Используется глобальный префикс маршрутизации, который обеспечивает восходящее объединение каналов, которое завершается у поставщика услуг Интернета.
- Одному интерфейсу можно назначить несколько адресов любого типа (глобальных индивидуальных и альтернативных).
- Любой интерфейс под управлением IPv6 включает хотя бы один адрес возвратной петли (::1/128) и один локальный адрес канала.
- Любому интерфейсу можно назначить несколько уникальных локальных и глобальных адресов.

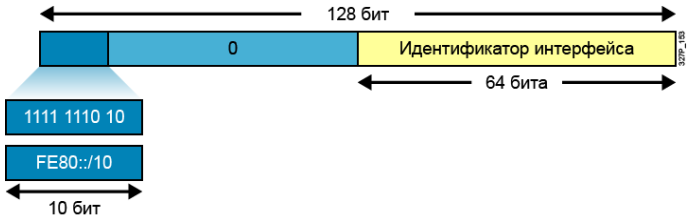
Глобальные индивидуальные адреса определяются глобальным префиксом маршрутизации, идентификатором подсети и идентификатором интерфейса. Пространство индивидуальных адресов IPv6 охватывает весь диапазон адресов IPv6, кроме блока FF00::/8 (1111 1111), который используется для групповых адресов. В настоящий момент пространство глобальных индивидуальных адресов, выделенное IANA, включает адреса, которые начинаются с двоичного числа 001 (2000::/3), что составляет 1/8 общего адресного пространства IPv6. Этот блок является самым крупным из выделенных блоков адресов.

Адреса с префиксами от 2000::/3 (001) до E000::/3 (111) должны включать 64-битный идентификатор интерфейса в формате расширенного универсального идентификатора (EUI)-64.

IANA выделяет адресное пространство IPv6 в диапазонах 2001::/16 реестрам.

Глобальный индивидуальный адрес, как правило, состоит из 48-битного глобального префикса маршрутизации и 16-битного идентификатора подсети. Отдельные организации могут использовать 16-битное поле подсети, которое называется идентификатором подсети, для создания собственной иерархии адресов и идентификации подсетей. Это поле позволяет организациям использовать до 65 535 отдельных подсетей. Дополнительные сведения см. в документации по стандарту RFC 3587, *формат глобальных индивидуальных адресов IPv6*, который заменяет RFC 2374.

Локальные адреса каналов



- Локальные адреса каналов используются в пределах канала и создаются динамически на всех интерфейсах IPv6 из локального префикса канала FE80::/10 и 64-битного идентификатора интерфейса.
- Локальные адреса канала используются для автоматической конфигурации адресов, обнаружения соседних узлов и обнаружения маршрутизаторов. Кроме того, локальные адреса каналов используются многими протоколами маршрутизации.
- Локальные адреса каналов служат для соединения устройств в одной локальной сети без использования глобальных адресов.
- При взаимодействии с локальным адресом канала необходимо указывать исходящий интерфейс, так как все интерфейсы подключаются к FE80::/10.

Работа IPv6 поверх протоколов канального уровня

IPv6 определен во всех актуальных протоколах канального уровня, в том числе:

- Ethernet*
- PPP*
- High-Level Data Link Control (HDLC)*
- FDDI
- Token Ring
- Attached Resource Computer network (ARCnet)
- Nonbroadcast multiaccess (NBMA)
- ATM**
- Frame Relay***
- IEEE 1394

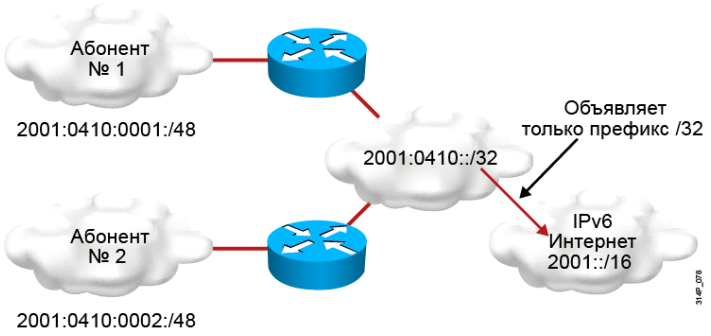
* Cisco поддерживает эти протоколы.

** Cisco поддерживает только постоянный виртуальный канал (PVC) ATM и не поддерживает коммутируемый виртуальный канал (SVC) и протокол ATM LAN Emulation (LANE).

*** Cisco поддерживает только Frame Relay PVC и не поддерживает SVC.

В стандарте RFC описывается работа IPv6 в каждом из этих протоколов канального уровня, но это не значит, что ПО Cisco IOS поддерживает их все. Протокол уровня передачи данных определяет, как создаются идентификаторы IPv6 и как процесс обнаружения соседних улов взаимодействует с распознаванием адресов канального уровня.

Более широкое адресное пространство обеспечивает объединение адресов



Объединение адресов предлагает следующие преимущества:

- Объединение префиксов, объявленных в глобальной таблице маршрутизации
- Эффективная и масштабируемая маршрутизация
- Улучшенная полоса пропускания и функциональные возможности сети для обработки пользовательского трафика

Более обширные адресные пространства обеспечивают выделения большего числа адресов поставщикам услуг Интернета и организациям. Поставщик услуг Интернета объединяет все префиксы своих клиентов в один и объявляет его в Интернете на базе IPv6. Кроме того, увеличенное адресное пространство достаточно велико, чтобы позволить организациям задавать один префикс для всей своей сети.

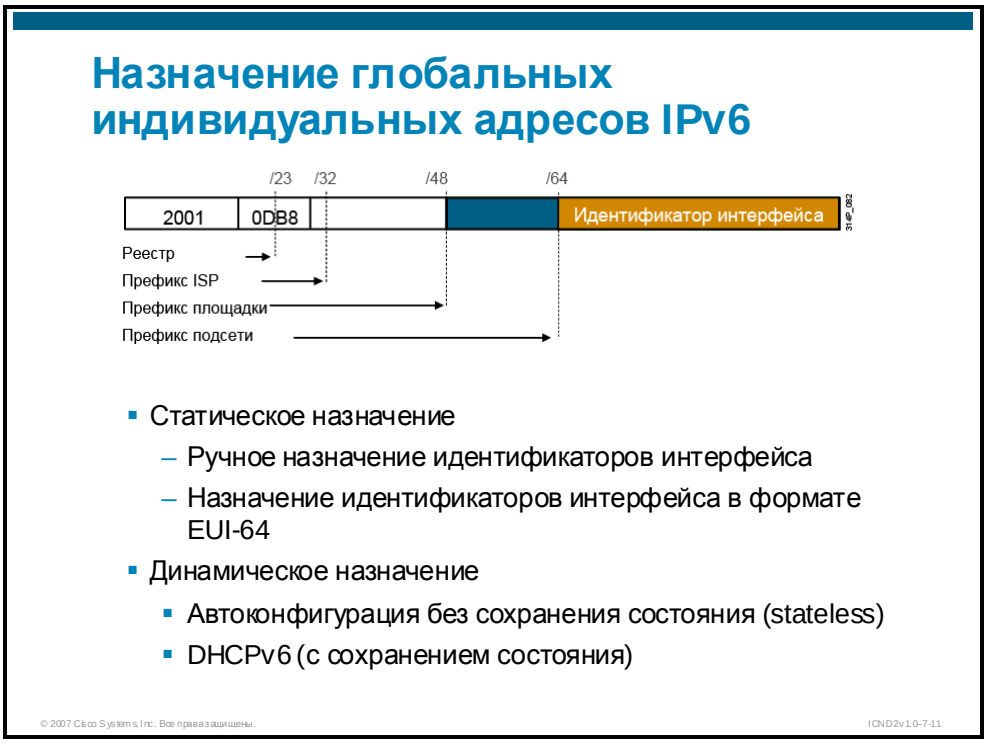
Объединение префиксов клиентов позволяет создать эффективную и масштабируемую таблицу маршрутизации. Масштабируемая маршрутизация необходима для более широкого распространения сетевых функций. Кроме того, масштабируемая маршрутизация улучшает полосу пропускания и функциональные возможности сети для обработки пользовательского трафика, объединяющего различные интерфейсы и приложения.

Применение Интернета, текущее и будущее, может включать следующие аспекты:

- значительное увеличение числа клиентов с широкополосным доступом и постоянным подключением к сети;
- пользователи, которые проводят больше времени в сети и готовы тратить больше денег на коммуникационные услуги (например на загрузку музыки) и дорогие товары и услуги, которые можно найти через поисковые системы;
- домашние сети с расширенными сетевыми приложениями, такими как Wireless VoIP, домашние системы наблюдения и расширенными услугами, такими как видео по требованию (VoD);
- масштабируемые компьютерные игры с участниками по всему миру и электронные средства обучения, насыщенные мультимедийными материалами, с удаленными лабораторными работами или моделями, вызываемыми по требованию.

Назначение адресов IPv6

В этом разделе описываются методы назначения адресов IPv6.



Идентификаторы интерфейсов IPv6 используются для идентификации интерфейсов в канале. Их можно рассматривать как «поле хоста» в адресе IPv6. Идентификаторы интерфейса должны быть уникальны в определенном канале. Идентификаторы интерфейса всегда имеют разрядность 64 и могут быть динамически получены от среды второго уровня или в результате инкапсуляции.

Существует несколько способов назначить устройству адрес IPv6:

- статическое назначение с использованием идентификатора интерфейса, заданного вручную;
- статическое назначение с использованием идентификатора интерфейса EUI-64;
- автоконфигурация без сохранения состояния (stateless);
- DHCP для IPv6 (DHCPv6).

Ручное назначение идентификаторов интерфейса

Один из способов статического назначения адресов IPv6 устройству – ручное назначение префикса (сети) и идентификатора интерфейса (хоста) в адресе IPv6. Чтобы настроить адрес IPv6 на интерфейсе маршрутизатора Cisco и включить обработку IPv6 на этом интерфейсе, введите команду **ipv6 address** *адрес ipv6/длина префикса* в режиме конфигурации интерфейса.

В примере ниже показано, как включить обработку IPv6 на интерфейсе и настроить адрес, указав нужные биты.

```
RouterX(config-if) ipv6 address 2001:DB8:2222:7272::72/64
```


Назначение идентификаторов интерфейса EUI-64

Другой способ статического назначение адреса IPv6 подразумевает ручную настройку префикса (сети) в адресе IPv6 и получение идентификатора интерфейса (хоста) из MAC-адреса устройства. Такой идентификатор называется идентификатором интерфейса EUI-64.

Чтобы настроить адрес IPv6 на интерфейсе маршрутизатора Cisco и включить обработку IPv6 на этом интерфейсе, используя идентификатор EUI-64 для младших 64 битов адреса (хоста), введите команду **ipv6 address** *префикс ipv6/длина префикса* **eui-64** на интерфейсе в режиме конфигурации.

В следующем примере адрес IPv6 2001:0DB8:0:1::/64 назначается интерфейсу Ethernet 0, при этом для младших 64 битов адреса используется идентификатор интерфейса EUI-64.

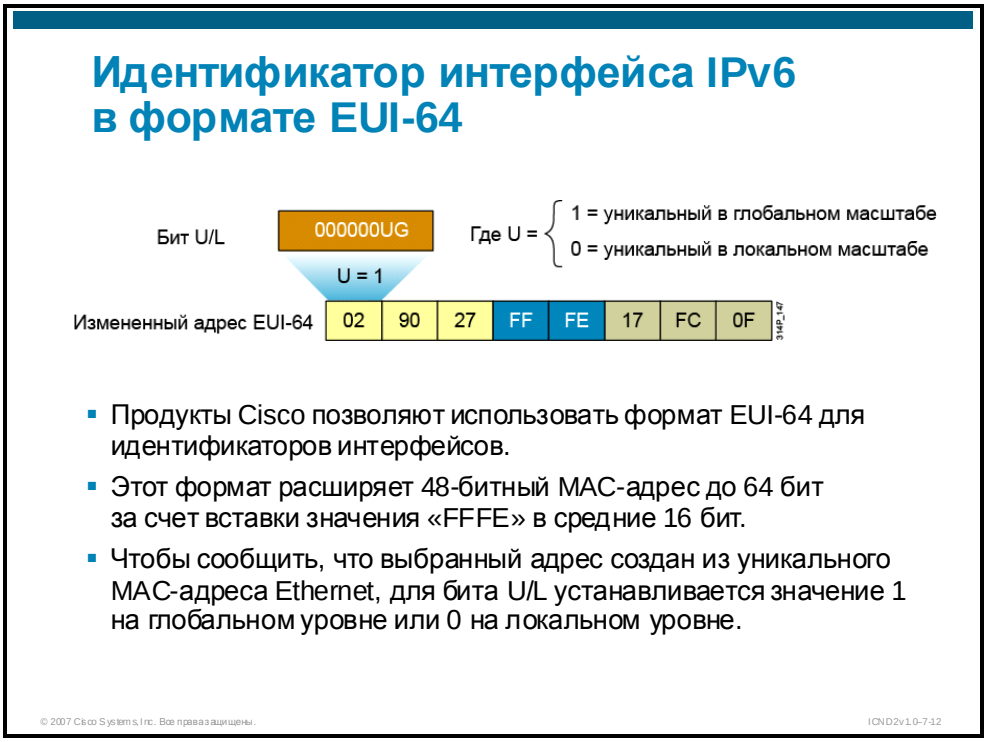
```
RouterX(config)# interface ethernet 0
RouterX(config-if)# ipv6 address 2001:0DB8:0:1::/64 eui-64
```

Автоконфигурация без сохранения состояния

Служба автоконфигурации, как следует из ее названия, автоматически настраивает адрес IPv6 узла. В IPv6 предполагается, что компьютерные терминалы и устройства, не относящиеся к ПК, будут подключены к сети. Механизм автоконфигурации был представлен, чтобы обеспечить добавление таких устройств в сеть по методу Plug-and-play и снизить затраты на администрирование.

DHCPv6 (с сохранением состояния)

DHCP для IPv6 позволяет DHCP-серверам передавать параметры конфигурации, такие как сетевой адрес IPv6, узлам IPv6. Эта функция обеспечивает автоматическое выделение многоразовый сетевых адресов и предлагает дополнительную гибкость конфигурации. Этот протокол является аналогом автоконфигурации адресов IPv6 (RFC 2462), но работает с сохранением состояния. Его можно использовать параллельно с автоконфигурацией IPv6 для получения параметров конфигурации, а также независимо от нее.



Использование формата EUI-64 в адресах IPv6

64-битный идентификатор интерфейса в адресе IPv6 идентифицирует уникальный интерфейс в канале. Канал – это сетевая среда, которую узлы используют для взаимодействия на канальном уровне. Идентификатор интерфейса может быть уникален в более крупной среде. Во многих случаях идентификатор интерфейса равен MAC-адресу интерфейса или получен из MAC-адреса. Как и в IPv4, префикс подсети в IPv6 привязывается к одному каналу.

Идентификаторы интерфейсов в глобальных индивидуальных адресах IPv6 и адресах других типов имеет длину 64 бита и может быть сформирован в формате EUI-64. Идентификатор интерфейса в формате EUI-64 получается из 48-битного адреса канального уровня (MAC-адреса). Для этого между тремя старшими байтами (поле уникального идентификатора организации [OUI]) и тремя младшими байтами (серийный номер) адреса канального уровня вставляется шестнадцатеричное число FFFE. Чтобы сообщить, что выбранный адрес создан из уникального MAC-адреса Ethernet MAC, седьмому биту старшего байта присваивается значение 1 (эквивалент бита IEEE G/L), чтобы указать на уникальность 48-битного адреса.

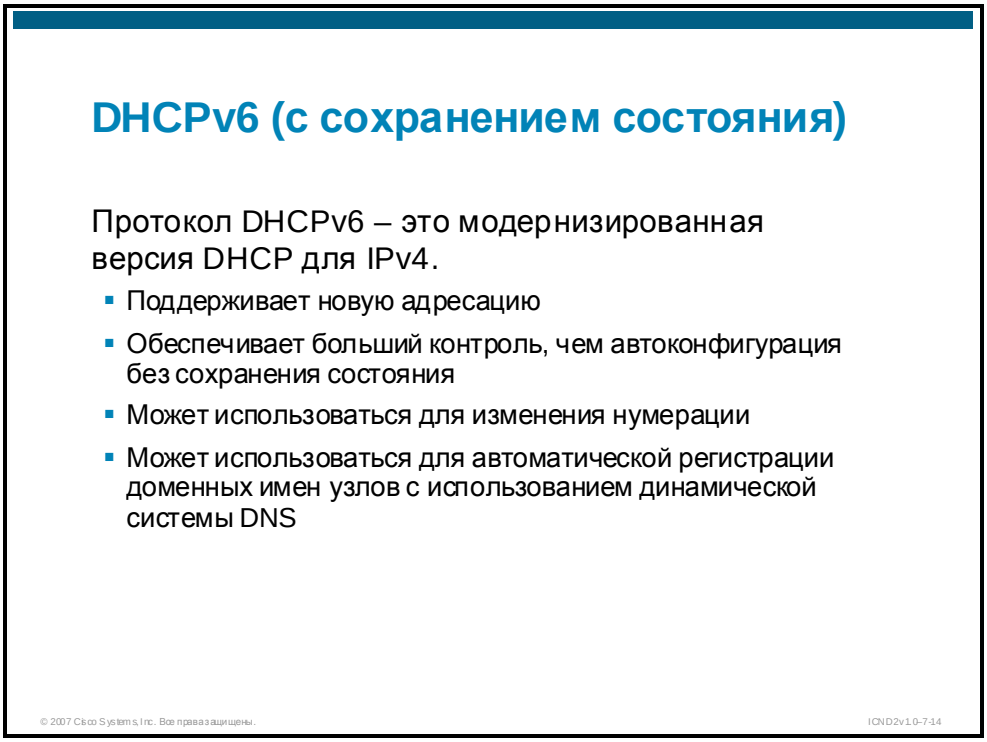
Автоконфигурация без сохранения состояния – одна из ключевых функций IPv6. Она обеспечивает базовую настройку узлов без использования серверов, а также простое изменение нумерации.

Автоконфигурация без сохранения состояния использует данные объявлений маршрутизатора для настройки узла. Префикс объявления маршрутизации используется в адресе узла качестве префикса /64. Остальные 64 бита получаются путем генерации динамического идентификатора интерфейса. Для Ethernet используется измененный идентификатор в формате EUI-64.

Маршрутизаторы рассылают объявления маршрутизации периодически. Узел нуждается в адресе на ранних этапах загрузки. Ожидание следующего объявления маршрутизации для настройки интерфейса было бы слишком долгим. Вместо этого узел отправляет маршрутизаторам запрос на немедленную отправку объявления маршрутизации, что позволяет узлу немедленно настроить адрес IPv6. Все маршрутизаторы отправляют обычное объявление маршрутизации с групповым адресом в качестве адреса назначения.

Автоконфигурация выполняет настройку устройств IPv6 по методу Plug-and-play, что обеспечивает автоматическое подключение устройств к сети без настройки администратором и без необходимости в серверах, таких как DHCP-серверы. Эта функция делает возможным развертывание в Интернете новых устройств, таких как сотовые телефоны, беспроводные устройства, бытовые приборы и домашние сети.

Примечание	DHCP без сохранения состояния – это концепция (представленная в феврале 2004 г.), которая объединяет функции автоконфигурации без сохранения состояния и метод «широких» клиентов DHCP с сохранением состояния. DHCP без сохранения состояния для IPv6 также называется «DHCP-lite». См. стандарт RFC 3736 служба *DHCP без сохранения состояния для IPv6*.



Протокол DHCPv6 – это обновленная версия протокола DHCP для IPv4. Он поддерживает модель адресации IPv6 и использует преимущества новых функций IPv6. Характеристики DHCPv6:

- предлагает больше контроля, чем автоконфигурация без серверов и без сохранения состояния;
- может использоваться в среде, включающей серверы и не включающей маршрутизаторы;
- может использоваться одновременно с автоконфигурацией без сохранения состояния;
- может использоваться для изменения нумерации;
- может использоваться для автоматической регистрации доменных имен хостов с использованием динамической системы DNS.

Принцип работы DHCPv6

DHCPv6 работает также, как DHCPv4 за исключением следующих особенностей:

- Первым делом клиенты определяют наличие маршрутизаторов в канале.
- Если маршрутизатор обнаружен, система проверяет его объявление, чтобы определить, можно ли использовать DHCP.
- Если маршрутизатор не найден или допускает использование DHCP:
  - По групповому адресу all-DHCP-agents отправляется сообщение запроса DHCP.
  - Клиент использует локальный адрес канала в качестве адреса источника.

Процесс получения данных конфигурации клиентами DHCPv6 похож на аналогичный процесс для IPv4, однако имеется ряд отличий. Первым делом клиент должен обнаружить маршрутизаторы в канале с помощью сообщений обнаружения соседних узлов. Если обнаруживается хотя бы один маршрутизатор, клиент проверяет объявления маршрутизатора, чтобы определить, следует ли использовать DHCPv6. Если объявления маршрутизатора позволяют использовать DHCPv6 в данном канале или если маршрутизатор не найден, клиент переходит в фазу запроса DHCP и находит DHCP-сервер.

DHCPv6 использует групповую рассылку для многих сообщений. Клиент отправляет сообщение с запросом по групповому адресу ALL-DHCP-Agents на уровне канала. Агенты включают как серверы, так и повторители.

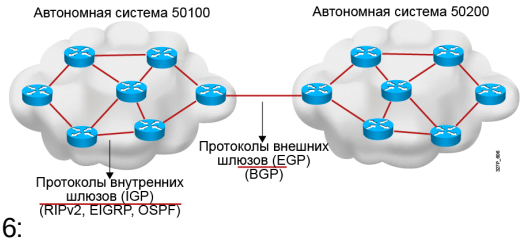
Повторитель DHCP пересылает сообщение по групповому адресу All-DHCP-Servers на уровне локальной площадки. Это значит, что администратору не требуется настраивать на повторителе все статические адреса DHCP-серверов, как в протоколе IPv4. Если вы хотите, чтобы только заданные DHCP-серверы получали сообщения или если с пересылкой группового трафика во все сегменты сети с DHCP-серверами возникают проблемы, вы можете задать статический список DHCP-серверов на повторителе.

Вы можете настроить разные серверы DHCPv6 или один сервер в разных контекстах для назначения адресов на основе разных политик. Например, один сервер DHCPv6 может назначать глобальные адреса на основе ограничительной политики, например «не назначать адреса принтерам». Другой сервер DHCPv6 или тот же сервер в другом контексте может назначать локальные адреса площадки на основе более свободной политики, например «назначать адреса всем».

Принципы маршрутизации в IPv6

В этом разделе описывается влияние протокола IPv6 на стандартные протоколы маршрутизации, а также модификации, которые необходимо внести в эти протоколы для поддержки IPv6.

Протоколы маршрутизации IPv6



- Типы маршрутизации IPv6:
  - Статическая
  - RIPng (RFC 2080)
  - OSPFv3 (RFC 2740)
  - IS-IS для IPv6
  - MP-BGP4 (RFC 2545/2858)
  - EIGRP для IPv6
- Перед настройкой протокола маршрутизации для IPv6 необходимо ввести команду **ipv6 unicast-routing**.

IPv6 использует совпадение наилучшего префикса, аналогично бесклассовой междоменной маршрутизации IPv4 (CIDR). Многие из стандартных протоколов маршрутизации были модифицированы для поддержки адресов IPv6 и новой структуры заголовка. На рисунке приводятся протоколы маршрутизации, модернизированные на сегодняшний день.

Статическая маршрутизация IPv6 настраивается так же, как в IPv4. В соответствии со стандартом RFC 2461 для протокола IPv6 существует дополнительное требование, маршрутизатор должен определять локальный адрес канала каждого соседнего маршрутизатора, чтобы сообщение перенаправления могло определить соседний маршрутизатор по локальному адресу канала. Это значит, что использование глобального индивидуальные адреса в качестве адреса следующего перехода не рекомендуется для маршрутизации IPv6.

Для включения IPv6 используется глобальная команда Cisco IOS **ipv6 unicast-routing**. Индивидуальную маршрутизацию IPv6 необходимо активировать до протокола маршрутизации с поддержкой IPv6 или статического маршрута IPv6.

Протокол обмена информацией о маршрутизации следующего поколения (RIPng) (RFC 2080) – протокол вектора расстояния с ограничением на 15 переходов и поддержкой методов Split horizon и Poison reverse для защиты от петель маршрутизации. Особенности протокола RIPng:

- основывается на протоколе RIPv2 и близок к нему;
- использует протокол IPv6 в качестве транспорта;
- включает префикс IPv6 и адрес IPv6 следующего перехода;
- использует многоадресную группу FF02::9, которая включает все маршрутизаторы RIP, в качестве адреса назначения для обновлений RIP;
- рассылает обновления из порта UDP 521;
- поддерживается в версии Cisco IOS 12.2(2)T и выше.

Стратегии внедрения IPv6

В этом разделе описываются механизмы перехода, которые используются для транзита трафика IPv6 через сети IPv4.

Переход с IPv4 не требует одновременной модернизации всех узлов. Многие механизмы перехода обеспечивают прозрачную интеграцию IPv4 и IPv6. Другие механизмы позволяют узлам IPv4 и IPv6 взаимодействовать друг с другом. Все эти механизмы применяются в тех или иных ситуациях.

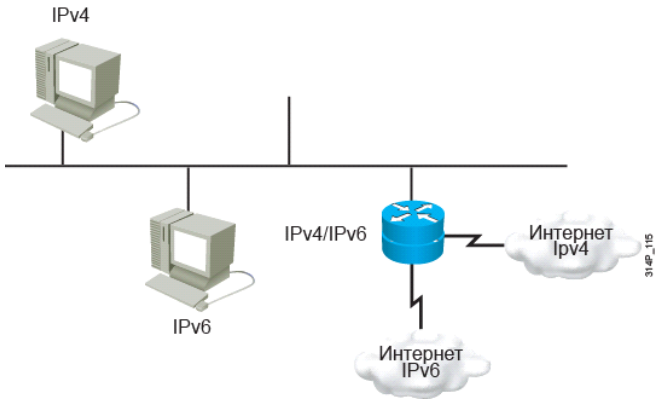
Три самых распространенных метода перехода с IPv4 на IPv6 перечислены ниже.

- **Двухстековая конфигурация:** Двухстековая конфигурация – метод интеграции, который подразумевает внедрение на узлах средств подключения для обеих сетей – IPv4 и IPv6. Таким образом узел и соответствующие маршрутизаторы используют два стека протоколов.
- **Туннелирование:** Доступно несколько методов туннелирования.
  - **Ручное туннелирование IPv6 поверх IPv4:** Метод интеграции, в котором пакет IPv6 инкапсулируется в протоколе IPv4. Этот метод требует двухстековых маршрутизаторов.
  - **Динамическое туннелирование 6to4:** Этот метод подразумевает автоматическое соединение островов IPv6 с помощью сети IPv4, как правило через Интернет. Туннелирование 6to4 динамически применяет уникальный префикс IPv6 к каждому острову IPv6. Это обеспечивает быстрое развертывание протокола IPv6 в корпоративной сети без необходимости в получении адреса от поставщика услуг Интернета или из реестра.

- **Туннелирование по протоколу ISATAP (протокол автоматической адресации туннелей):** Автоматический механизм туннелирования с наложением, использующий существующую сеть IPv4 в качестве канального уровня для IPv6. Туннели ISATAP позволяют отдельным двухстековым хостам IPv4 или IPv6 на площадке взаимодействовать с другими подобными узлами через виртуальный канал, создавая сеть IPv6 на основе инфраструктуры IPv4.
- **Туннелирование Teredo:** Технология перехода на IPv6, которая использует автоматическое туннелирование между хостами, вместо туннелирования через шлюз. Она используется для передачи индивидуального трафика IPv6, если двухстековые хосты (узлы под управлением обоих протоколов – IPv6 и IPv4), расположены за одним или несколькими преобразователями сетевых адресов IPv4.

- **Прокси и преобразование адресов (NAT-PT):** Механизм преобразования, который располагается между сетями IPv6 и IPv4. Преобразует пакеты IPv6 в пакеты IPv4 и обратно.

Двухстековая конфигурация Cisco IOS



Двухстековая конфигурация – метод интеграции, который подразумевает внедрение на узлах средств подключения для обеих сетей – IPv4 и IPv6.

Двухстековая конфигурация – это метод интеграции, который подразумевает внедрение на узлах средств подключения для обеих сетей – IPv4 и IPv6. Таким образом, узлы работают под управлением обоих стеков. Эту конфигурацию можно внедрить на одном или нескольких интерфейсах. Функции двухстекового метода описываются ниже.

- Двухстековый узел выбирает, какой стек использовать, основываясь на адресе назначения. Двухстековый узел отдает предпочтение протоколу IPv6, если он доступен. Двухстековый подход к интеграции IPv6, который подразумевает работу узлов под управлением обоих стеков – IPv4 и IPv6, будет одним из самых распространенных методов интеграции. Старые приложения, поддерживающие только IPv4, будут работать как и раньше. Новые и модифицированные приложения получат преимущества обоих уровней IP.
- Для поддержки адресов IPv4 и IPv6 и запросов DNS обоих стеков был представлен новый прикладной программный интерфейс (API). В этом интерфейсе вызовы gethostbyname и gethostbyaddr заменены. Преобразованное приложение может использовать как IPv4, так и IPv6. Приложение можно перевести на новый API, и продолжать использовать его только для IPv4.
- Опыт портирования приложений IPv4 на IPv6 показывает, что для большинства приложений будет достаточно небольшого изменения в отдельных фрагментах исходного кода. Этот метод широко известен и применялся в прошлом для перехода между протоколами. Он обеспечивает постепенную модернизацию приложений для использования IPv6.

Двухстековая конфигурация Cisco IOS (прод.)

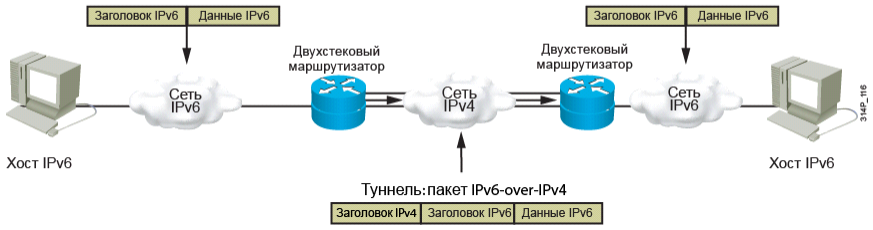
Когда на интерфейсе настроены протоколы IPv4 и IPv6, он считается двухстековым.

ПО Cisco IOS версии 12.2(2)T и выше готовы к использованию IPv6. Как только администратор настраивает базовые функции IPv4 и IPv6 на интерфейсе, этот интерфейс становится двухстековым и начинает пересылать трафик IPv4 и IPv6.

Для использования IPv6 маршрутизаторе Cisco IOS необходимо ввести команду глобальной конфигурации **ipv6 unicast-routing**. Эта команда включает пересылку датаграмм IPv6 на интерфейсе.

Примечание	Необходимо назначить адрес IPv6 всем интерфейсам, пересылающим трафик IPv6, с помощью команды **ipv6 address** *адрес IPv6* [*/длина префикса*].

Туннелирование IPv6



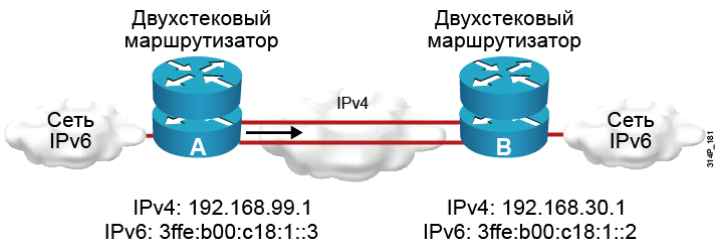
Туннелирование – метод интеграции, подразумевающий инкапсуляцию пакетов IPv6 другим протоколом, например IPv4. В качестве метода инкапсуляции используется IPv4.

- Включает 20-байтный заголовок IPv4 без параметров, заголовок IPv6 и полезную часть пакета
- Требует двухстековых маршрутизаторов

Туннелирование – метод интеграции, подразумевающий инкапсуляцию пакетов IPv6 другим протоколом, например IPv4. При использовании протокола IPv4 для инкапсуляции пакета IPv6, в заголовке IPv4 указывается тип протокола 41. Пакет имеет следующие характеристики:

- включает 20-байтный заголовок IPv4 без параметров, заголовок IPv6 и полезную часть пакета;
- требует двухстековых маршрутизаторов, этот процесс обеспечивает соединение островов IPv6 без необходимости в переводе на IPv6 промежуточных сетей; с туннелированием связано две проблемы:
  - размер MTU сокращается на 20 октетов, если заголовок IPv4 не содержит дополнительных полей;
  - поиск и устранение неполадок в туннелированных сетях может быть сложной задачей. Туннелирование – промежуточный метод интеграции и перехода, его не следует рассматривать как окончательное решение. Конечной целью должна быть «родная» архитектура IPv6.

Туннель IPv6, настроенный вручную



Настроенные туннели требуют:

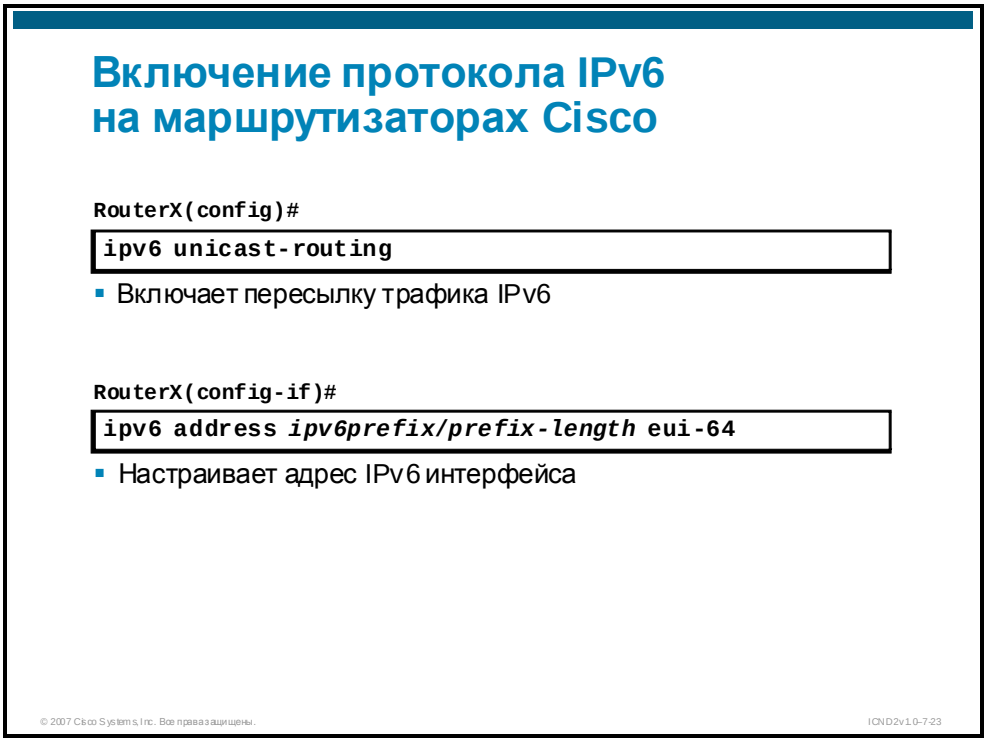
- Двухстековых конечных точек
- Адресов IPv4 и IPv6, настроенных на каждой стороне

В туннеле, настроенном вручную, можно статически задать как адреса IPv4, так и адреса IPv6. Это действие необходимо выполнить на маршрутизаторах на обеих сторонах туннеля. Маршрутизаторы должны быть двухстековыми. Такая конфигурация не может меняться динамически с изменением потребности сети и маршрутизации. Кроме того, необходимо настроить маршрутизацию для пересылки пакетов между двумя сетями IPv6.

Конечные точки туннеля могут быть ненумерованными, однако это усложнит поиск и устранение неполадок. Сохранение адресов для туннелей, которое было необходимо в IPv4, не требуется для IPv6.

Настройка IPv6

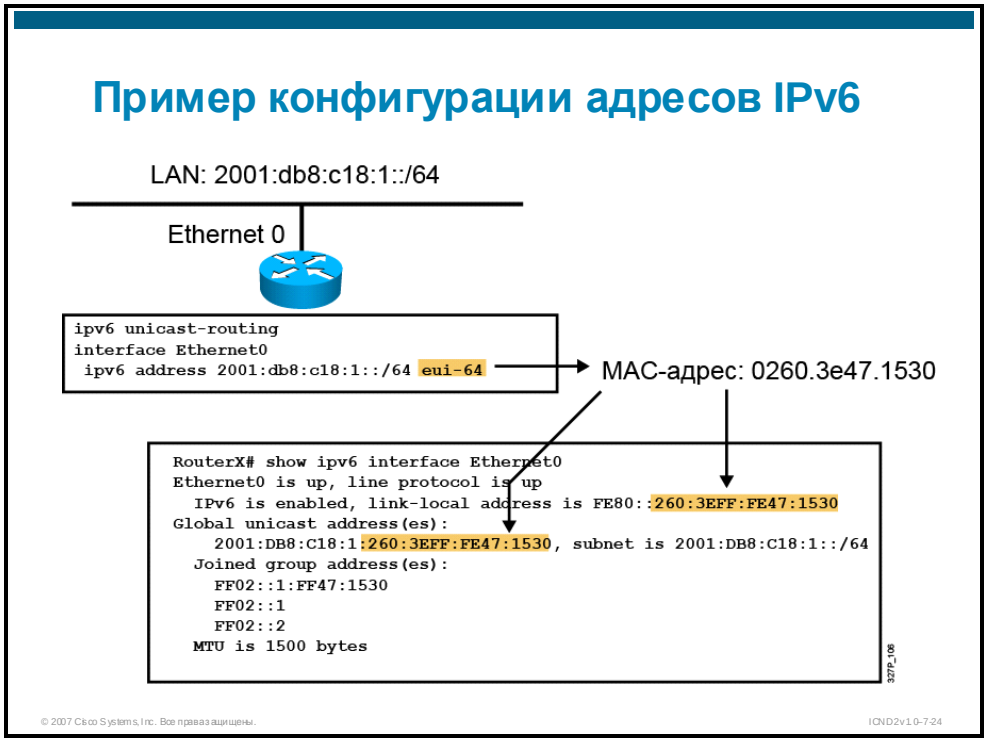
В этом разделе описывается настройка IPv6, включение RIPng и туннелирование трафика IPv6 через сеть IPv4.



Активация протокола IPv6 на маршрутизаторе состоит из двух основных этапов. Во-первых необходимо активировать пересылку трафика IPv6 на маршрутизаторе, во-вторых – настроить все интерфейсы, для которых необходим протокол IPv6.

По умолчанию пересылка IPv6 отключена на маршрутизаторах Cisco. Чтобы активировать пересылку трафика IPv6 между интерфейсами, необходимо ввести команду глобальной конфигурации **ipv6 unicast-routing**. Эта команда включает пересылку индивидуального трафика IPv6.

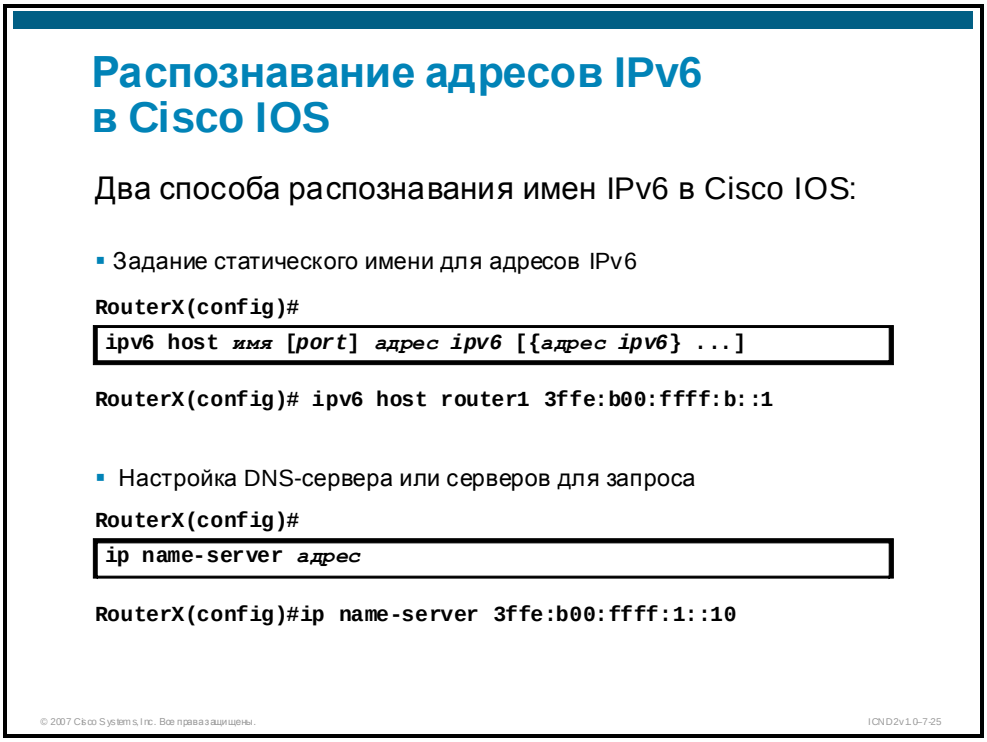
Команда **ipv6 address** используется для настройки глобального адреса IPv6. Локальный адрес канала автоматически настраивается при назначении адреса интерфейсу. Необходимо указать полный 128-битный адрес IPv6 или включить использование 64-битного префикса с помощью параметра **eui-64**.



Вы можете указать адрес IPv6 полностью или вычислить идентификатор хоста (правые 64 бита) на основе идентификатора интерфейса в формате EUI-64. В этом примере адрес IPv6 интерфейса настроен в формате EUI-64.

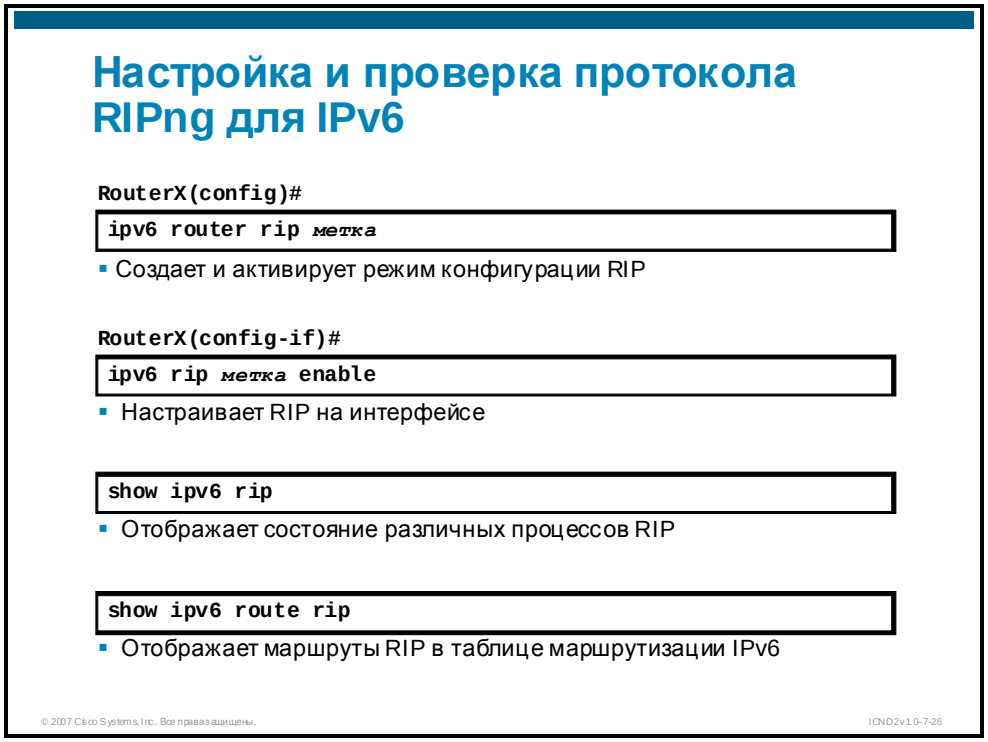
Кроме того, адрес IPv6 можно назначить интерфейсу маршрутизатора с помощью команды **ipv6 address** *адрес ipv6/длина префикса* в режиме конфигурации интерфейса.

Примечание	При настройке адреса IPv6 на интерфейсе выполняется автоматическая настройка локального адреса канала для этого интерфейса.



Процесс Cisco IOS поддерживает три способа распознавания имен.

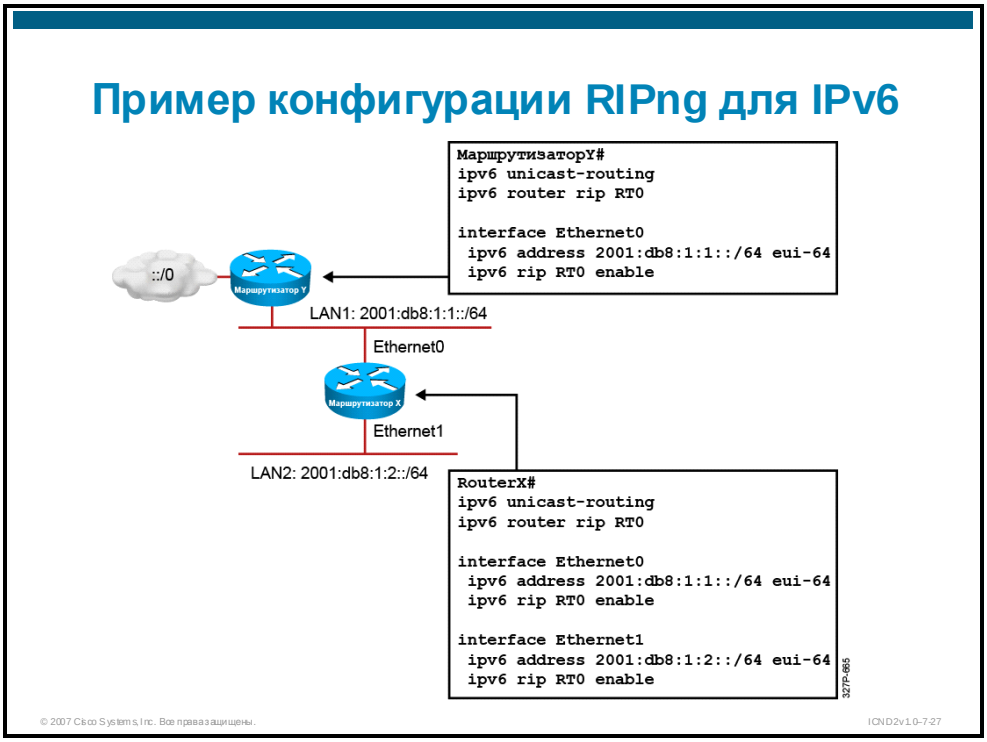
- Для адресов IPv6 можно задать статические имена с помощью команды **ipv6 host** *имя* [*порт*] *адрес ipv61* [*адрес ipv6 2...адрес ipv6 4*]. Одно имя хоста можно назначить максимум четырем адресам IPv6. Параметр *порт* обозначает порт Telnet, который следует использовать для соответствующего хоста.
- Чтобы указать DNS-сервер для маршрутизатора используется команда **ip name-server** *адрес*. В качестве параметра *адрес* можно вводить адрес IPv4 или IPv6. С помощью этой команды можно задать до шести DNS-серверов.



Настройка и проверка протокола RIPng для IPv6

На рисунке приводится пример синтаксиса команд, используемых для настройки протокола RIPng. Синтаксис близок к синтаксису аналогичных команд для IPv4. В протоколе RIPng вместо команды **network** для определения интерфейсов, которые должны управляться RIPng, следует использовать команду **ipv6 rip** *метка* **enable** в режиме конфигурации интерфейса. Эта команда включает RIPng на соответствующем интерфейсе. Параметр *метка* команды **ipv6 rip enable** должен совпадать с аналогичным параметром команды **ipv6 router rip**.

Примечание	При динамическом включении протокола RIP на интерфейсе динамически создается процесс «router rip».

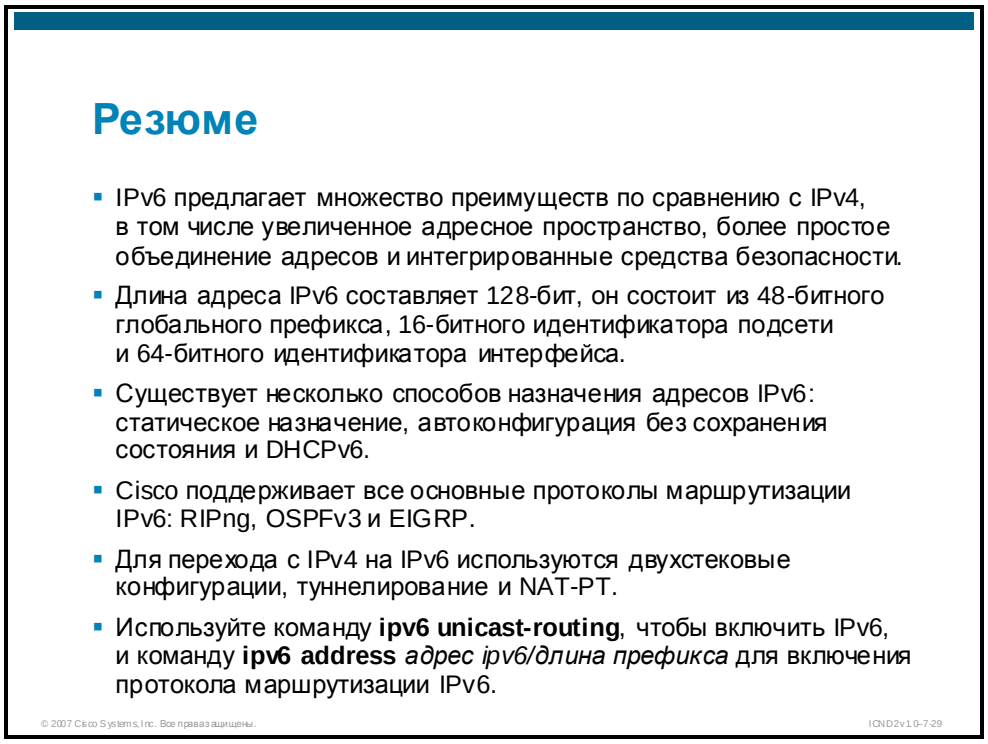


Пример: Конфигурация протокола RIPng для IPv6

В примере выше используется сеть с двумя маршрутизаторами. Маршрутизатор Y подключен к сети по умолчанию. На маршрутизаторах X и Y для идентификации процесса RIPng используется метка «RT0». Протокол RIPng включен на первом Ethernet-интерфейсе маршрутизатора Y с помощью команды **ipv6 rip RT0 enable**. Маршрутизатор X сообщает, что протокол RIPng включен на обоих интерфейсах Ethernet с помощью команды **ipv6 rip RT0 enable**.

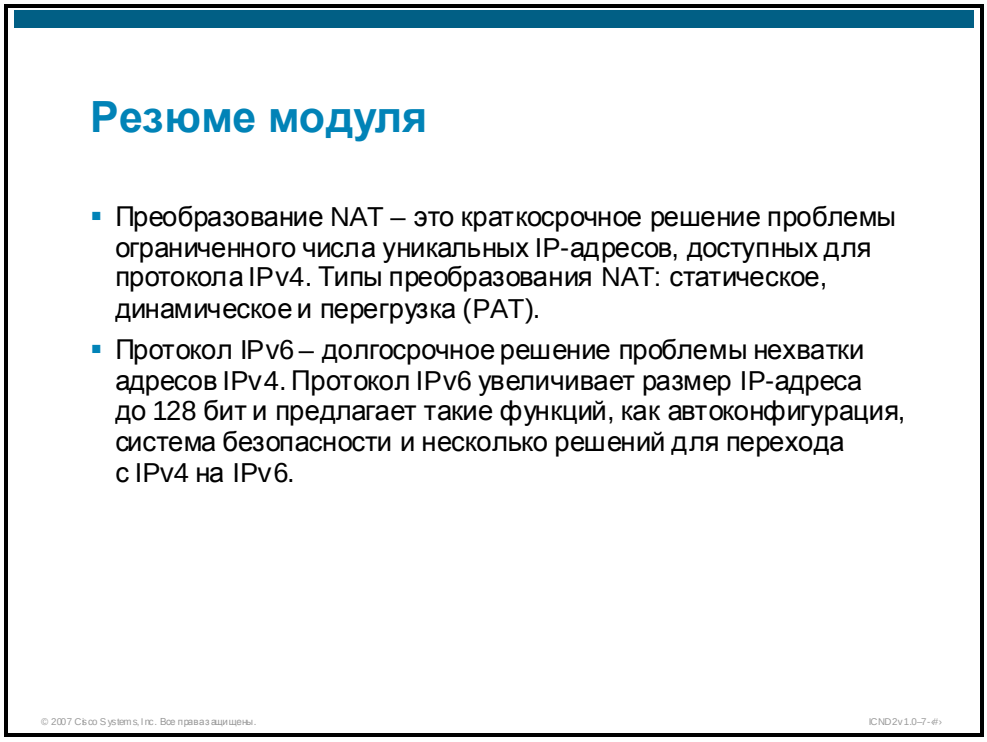
Резюме

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



Резюме модуля

В этом разделе приводится резюме вопросов, рассмотренных в модуле.



Для экономии адресного пространства IPv4 используются три типа преобразования сетевых адресов (NAT): статическое преобразование NAT, динамическое преобразование NAT и преобразование адресов портов (PAT). Статическое преобразование NAT обеспечивает привязку внутреннего локального адреса к внутреннему глобальному адресу по принципу «один к одному». При использовании динамического преобразования NAT внутренние глобальные адреса автоматически выделяются из пула. Преобразование PAT, также известное как перегрузка NAT, позволяет преобразовать большое число внутренних адресов в один или несколько внутренних глобальных адресов.

Протокол IPv6 устраняет потребность в NAT. Увеличение размера IP-адреса до 128 бит обеспечивает практически бесконечное адресное пространство. Переход с IPv4 на IPv6 не произойдет за одну ночь. Методы перехода, такие как двухстековые конфигурации, туннели IPv6-IPv4 и преобразования NAT-PT предлагают различные варианты перехода с IPv4 на IPv6.

Вопросы для самопроверки по модулю

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

B1) Сопоставьте термины NAT и их определения. (Источник: масштабирование сети с помощью NAT и PAT)

_____ 1. статическое преобразование NAT

_____ 2. динамическое преобразование NAT

_____ 3. внутренний локальный адрес

_____ 4. внутренний глобальный адрес

А) адрес, который преобразуется NAT
Б) адрес внутреннего хоста, который используется для взаимодействия с внешней сетью
В) привязывает незарегистрированный адрес IPv4 к зарегистрированному адресу IPv4 по принципу «один к одному»
Г) привязывает незарегистрированный адрес IPv4 к адресу из группы зарегистрированных адресов IPv4

B2) Какая команда Cisco IOS используется для задания пула глобальных адресов, которые могут выделяться при необходимости? (Источник: масштабирование сети с помощью NAT и PAT)

А) **ip nat pool**
Б) **ip nat inside pool**
В) **ip nat outside pool**
Г) **ip nat inside source static**

B3) Что делает команда **ip nat inside source static**? (Источник: масштабирование сети с помощью NAT и PAT)

А) выбирает внутренний статический интерфейс
Б) отмечает интерфейс, как подключенный к внешней сети
В) задает пул глобальных адресов, которые будут выделяться при необходимости
Г) настраивает статическое преобразование между внутренним локальным адресом и внутренним глобальным адресом

B4) Сопоставьте команды, используемые для настройки перегрузки NAT, и их функции. (Источник: масштабирование сети с помощью NAT и PAT)

_____ 1. **ip nat inside**

_____ 2. **ip nat outside**

_____ 3. **access-list 1 permit 10.1.1.0 0.0.0.255**

_____ 4. **ip nat inside source list 1 pool nat-pool overload**

_____ 5. **ip nat pool nat-pool 192.1.1.17 192.1.1.20 netmask 255.255.255.240**

А) отмечает интерфейс, как подключенный к внутренней сети
Б) отмечает интерфейс, как подключенный к внешней сети
В) задает пул внутренних глобальных адресов, которые будут выделяться при необходимости
Г) создает динамическое преобразование адреса порта с использованием заданного списка контроля доступа
Д) задает стандартный список контроля доступа, разрешающий преобразуемые адреса.

В5) Какая команда удаляет выбранную запись динамического преобразования из таблицы преобразования NAT? (Источник: масштабирование сети с помощью NAT и PAT)

А) **clear ip nat translation ***
Б) **clear ip nat translation inside**
В) **clear ip nat translation outside**
Г) **clear ip nat translation protocol inside**

В6) Вывод какой команды содержит активные преобразования таблицы преобразования NAT? (Источник: масштабирование сети с помощью NAT и PAT)

А) **show ip nat statistics**
Б) **show ip nat translations**
В) **clear ip nat translation ***
Г) **clear ip nat translation outside**

В7) 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: масштабирование сети с помощью NAT и PAT)

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 адреса IPv4.

В8) Вывод какой команды содержит сведения об определенных ошибках и исключениях, таких как невозможность выделить глобальный адрес? (Источник: масштабирование сети с помощью NAT и PAT)

А) **debug ip nat**
Б) **debug ip nat detailed**
В) **show ip nat statistics**
Г) **show ip nat translations**

В9) Каковы преимущества IPv6 по сравнению с IPv4? (Источник: переход на IPv6)

А) увеличенное адресное пространство
Б) более короткий заголовок
В) более простой заголовок
Г) поддержка IPsec на всех каналах

В10) Почему преобразование NAT не требуется для IPv6? (Источник: переход на IPv6)

А) Преобразование NAT недоступно для IPv6.
Б) Адреса IPv6 не поддерживают частное адресное пространство.
В) IPv6 позволяет всем пользователям предприятия использовать глобальный адрес.
Г) Шестнадцатеричные адреса нельзя преобразовать.

В11) Как IPv6 уменьшает таблицы маршрутизации на маршрутизаторах Интернета? (Источник: переход на IPv6)

А) путем задания точек объединения в адресном пространстве
Б) за счет использования нового протокола
В) с помощью автоконфигурации
Г) с помощью локальных адресов площадки

В12) Как можно сократить последовательность наборов нулей в адресе IPv6? (Источник: переход на IPv6)

А) с помощью символов «:::»
Б) путем исключения начальных нулей
В) путем замены 4-х последовательных нулей одним
Г) с помощью символов «::»

В13) К какому типу адресов IPv6 принадлежит глобальный индивидуальный адрес, назначенный нескольким интерфейсам? (Источник: переход на IPv6)

А) альтернативный
Б) индивидуальный
В) групповой
Г) широковещательный

В14) Какой тип адресов IPv4 был исключен в IPv6? (Источник: переход на IPv6)

А) индивидуальный
Б) групповой
В) широковещательный
Г) глобальный

В15) Какое утверждение о формате системных идентификаторов EUI-64, используемом в автоконфигурации Cisco без сохранения состояния, верно? (Источник: переход на IPv6)

А) Это MAC-адрес с аггрегатором уровня площадки.
Б) Это MAC-адрес с полем ISO OUI.
В) Этот формат расширяет 48-битный MAC-адрес до 64 бит, за счет вставки значения «FFFE» в средние 16 бит.
Г) Он не соответствует стандартам IEEE по уникальности адреса.
Д) Он используется только компанией Cisco.

В16) Какой термин обозначает ситуацию, в которой маршрутизатор IPv6 используется для предоставления адреса IPv6 запрашивающему хосту? (Источник: переход на IPv6)

А) автоадресация
Б) локальный адрес канала
В) IPv6 NAT
Г) стандартная автоконфигурация без сохранения состояния
Д) автоконфигурация DHCP

В17) Какие из нижеперечисленных протоколов *не* являются протоколами маршрутизации IPv6? (Выберите два варианта.) (Источник: переход на IPv6)

А) IGRP6
Б) OSPFv3
В) EIGRP for IPv6
Г) RIPng
Д) ODR
Е) MP-BGP4

В18) Выберите два наиболее распространенных метода перехода с IPv4 на IPv6? (Выберите два варианта.) (Источник: переход на IPv6)

А) IPv6 NAT
Б) двухстековая конфигурация
В) туннелирование 6to4
Г) IPv6 Mobile

В19) Какая глобальная команда активирует IPv6 или двухстековую конфигурацию на маршрутизаторе Cisco? (Источник: переход на IPv6)

А) **ipv6 routing**
Б) **ipv6 unicast-routing**
В) **ipv6 address**
Г) **ipv6 dual stack**

В20) Выберите два верных утверждения о двухстековой конфигурации? (Выберите два варианта.) (Источник: переход на IPv6)

А) В новом API заменены вызовы gethostbyname и gethostbyaddr.
Б) Туннелирование выполняется автоматически.
В) В двухстековой конфигурации протокол IPv4 имеет приоритет над IPv6.
Г) Протокол IPv4 нельзя использовать при переходе на IPv6.
Д) Используемый стек выбирается в зависимости от адреса назначения.

Ответы на вопросы для самопроверки по модулю

В1) 1 = В, 2 = Г, 3 = А, 4 = Б

В2) А

В3) Г

В4) 1 = А, 2 = Б, 3 = Д, 4 = Г, 5 = В

В5) Г

В6) Б

В7) А, Г, Д

В8) Б

В9) Б

В10) В

В11) А

В12) Г

В13) А

В14) В

В15) В

В16) Г

В17) А, Д

В18) Б, В

В19) Б

В20) А, Д

Модуль 8

Расширение локальной сети в глобальную сеть

Обзор

Глобальные сети предоставляют пользователям доступ к ресурсам обширного географического региона, как правило, за плату. Некоторые сервисы рассматриваются как подключения 2-го уровня между удаленными площадками, и предоставляются телефонными компаниями с использованием коммутаторов глобальной сети. В числе таких технологий последовательный канал «точка-точка» (выделенная линия) и подключения Frame Relay.

Другие подключения используют инфраструктуру Интернета, альтернативу третьего уровня, для соединения удаленных площадок организации. Чтобы обеспечить безопасный доступ через общедоступную сеть Интернет, можно внедрить виртуальную частную сеть (VPN).

В этом занятии описываются компоненты решения VPN для подключения через глобальные сети, настройка соединения PPP, а также принцип работы, настройку и устранение неполадок Frame Relay.

Задачи модуля

По окончании этого занятия в научитесь определять и внедрять подходящую технологию ГВС в соответствии с требованиями сети. Это значит, что вы сможете выполнять следующие задачи:

- описывать использование VPN для соединения площадок и удаленного пользовательского доступа;
- подключаться к поставщику услуг через сеть, описывать принцип работы и настройку PPP;
- подключаться к поставщику услуг через сеть и описывать принцип работы и настройку Frame Relay;
- определять методы выявления распространенных проблем Frame Relay и предлагать решения этих проблем.

Занятие 1

Общие сведения о решениях VPN

Обзор

Решения Cisco для виртуальных частных сетей (VPN) обеспечивают инфраструктуру глобальной сети на основе Интернета для соединения офисов, домашних офисов, площадок бизнес-партнеров и удаленных работников в единую корпоративную сеть. Экономичное широкополосное Интернет-подключение, защищенное зашифрованными VPN-туннелями, позволяет снизить затраты на полосу пропускания глобальной сети и повысить скорость подключения.

Интегрируя передовые средства сетевого анализа и маршрутизацию, виртуальные частные сети Cisco обеспечивают надежную передачу сложного, критически-важного трафика, например голосовых данных или трафика приложений «клиент-сервер», не подвергая риску качество связи и безопасность.

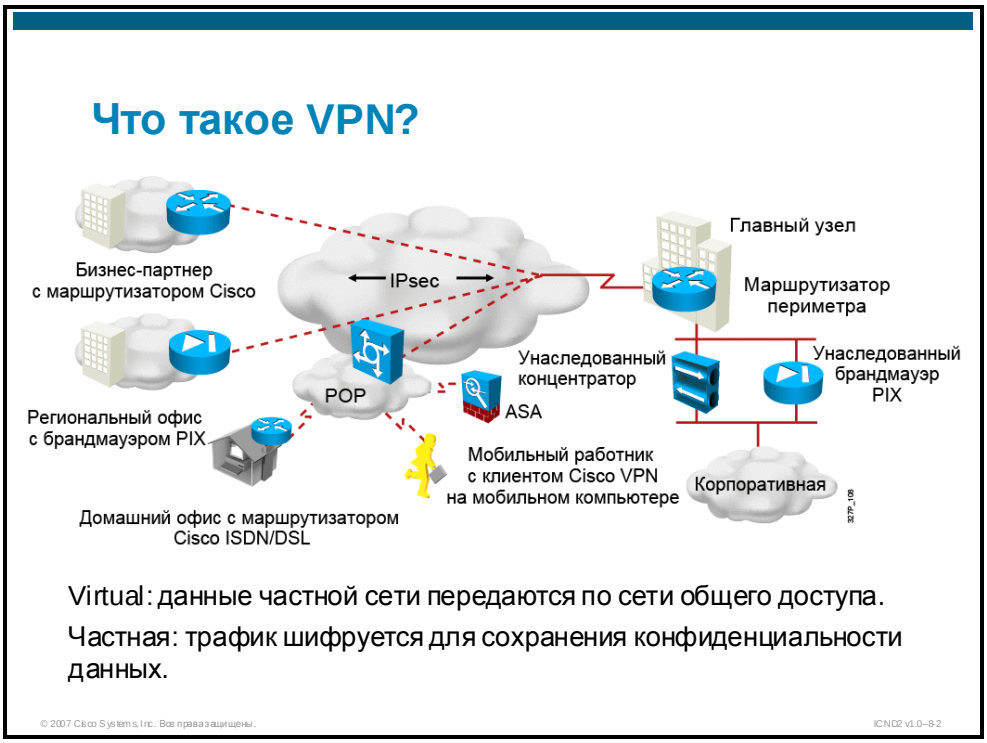
Задачи

По окончании этого занятия вы сможете описывать использование VPN для соединения площадок и удаленного пользовательского доступа. Вы узнаете о преимуществах сред VPN, а также оборудовании, ПО и протоколах, необходимых для настройки решения VPN. Это значит, что вы сможете выполнять следующие задачи:

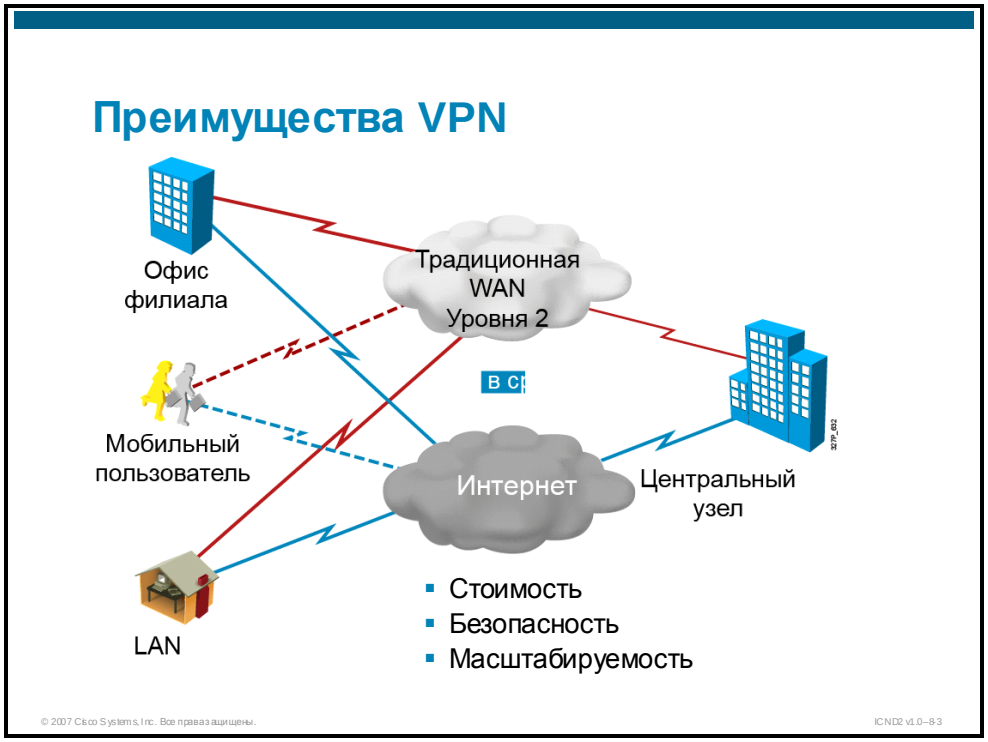
- давать определение VPN;
- давать определение различных типов VPN и описывать сценарии их использования;
- описывать компоненты VPN;
- описывать функцию IPsec и ее компоненты;
- описывать активацию шифрования, средств безопасности и аутентификации для пакета протоколов Ipsec.

Сети VPN и их преимущества

В этом решении описывается решение VPN и его преимущества.



VPN – это зашифрованное соединение между частными сетями через сеть общего доступа, например Интернет. V значит Virtual (виртуальная), N – Network (сеть). Данные частной сети безопасно передаются через сеть общего доступа (Интернет), формируя виртуальный канал. Буква P обозначает Private. Для сохранения конфиденциальности трафик шифруется. Вместо выделенной линии второго уровня VPN использует виртуальные подключения, которые маршрутизируются из частной сети компании к удаленной площадке или хосту служащего компании.

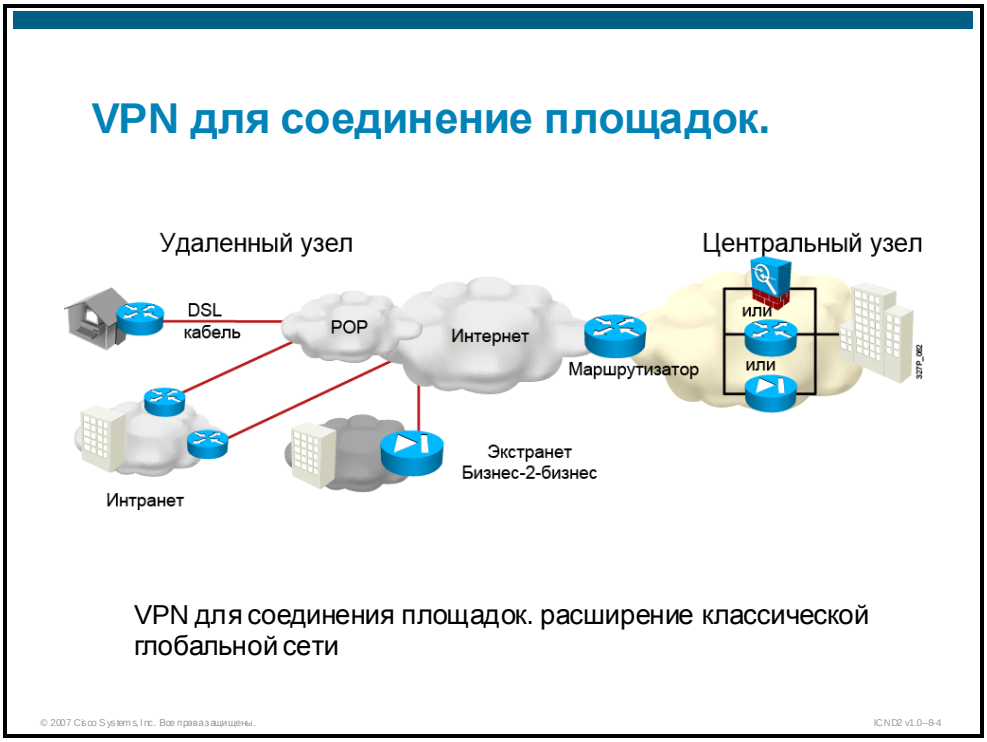


Преимущества VPN приводятся ниже:

- **Сокращение затрат:** VPN позволяет организациям использовать экономичный сторонний транспорт – сеть Интернет – для подключения удаленных офисов и пользователей к главной корпоративной площадке и устраняет потребность в дорогих выделенных каналах ГВС и модемных пулах. Более того, с появлением экономичных технологий широкополосного доступа, таких как DSL, организации могут использовать VPN для снижения затрат на связь и повышения полосы пропускания удаленных подключений.
- **Безопасность:** VPN обеспечивают самый высокий уровень безопасности благодаря передовым протоколам шифрования и аутентификации, которые защищают данные от несанкционированного доступа.
- **Масштабируемость:** VPN позволяют корпорациям использовать инфраструктуру и устройства поставщиков услуг Интернета, что упрощает добавление новых пользователей. Таким образом, корпорации могут значительно увеличивать полосу пропускания без наращивания инфраструктуры.
- **Совместимость с технологией широкополосного доступа:** VPN позволяет мобильным работникам, удаленным работникам и людям, которые хотят продлить свой рабочий день, получить доступ к корпоративной сети, воспользовавшись широкополосным подключением, например DSL или кабельным модемом, что обеспечивает значительную гибкость и эффективность. Более этого, высокоскоростные широкополосные каналы предлагают экономичное решение для соединения удаленных офисов.

Типы VPN

В этом разделе описывается два типа VPN.



Существует два типа виртуальных частных сетей:

- VPN для соединения площадок.
- VPN удаленного доступа, которая реализуется двумя типами решений VPN:
  - Cisco Easy VPN;
  - Cisco IOS IP IPsec/SSL VPN, другое название – WebVPN.

VPN для соединения площадок – расширение классической глобальной сети. Такие VPN используются для соединения полноценных сетей. Например они могут служить для подключения сети филиала к сети штаб-квартиры компании. В прошлом для соединения площадок использовались арендованные каналы и каналы Frame Relay. Теперь, когда у большинства компаний есть доступ в Интернет, эти каналы можно заменить на VPN для соединения площадок.

В VPN для соединения площадок хосты не используют ПО Cisco VPN Client, они отправляют и принимают обычный трафик TCP/IP через «шлюз» VPN. В качестве шлюза может использоваться маршрутизатор, брандмауэр VPN-концентратор Cisco и адаптивное устройство безопасности Cisco ASA 5500. Шлюз VPN выполняет инкапсуляцию и шифрование всего исходящего трафика площадки и отправляет его через туннель VPN в сети Интернет в аналогичный шлюз VPN на площадке назначения. При получении трафика шлюз VPN отделяет заголовки, расшифровывает контент и передает пакеты в узел назначения внутри частной сети.

VPN удаленного доступа

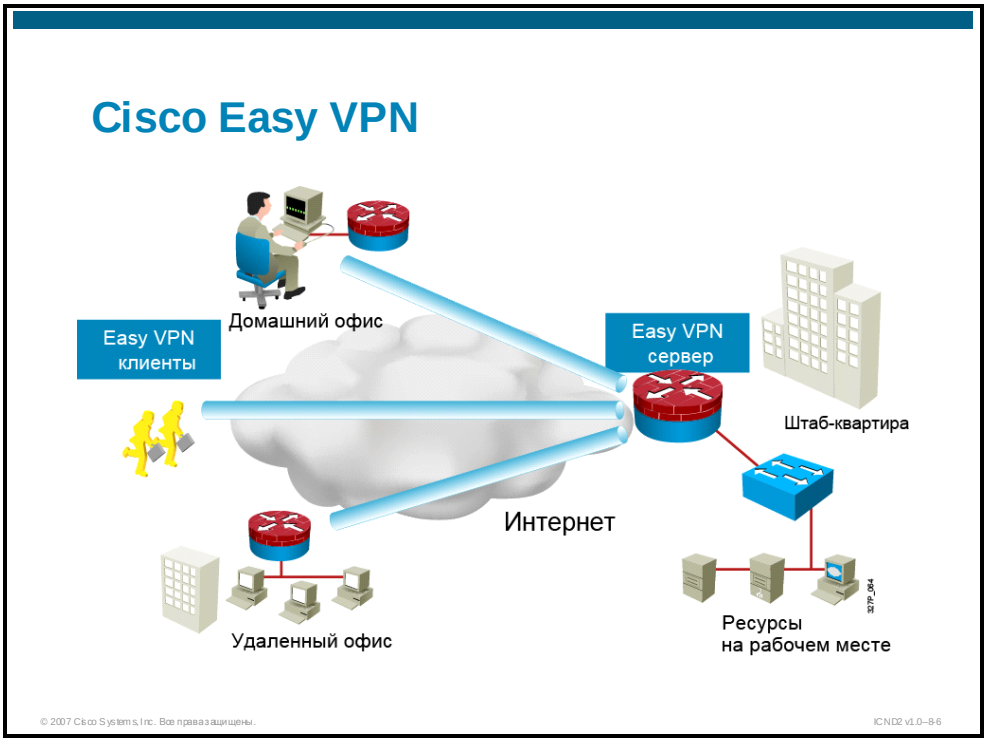
VPN удаленного доступа: развитие сетей коммутируемого доступа и ISDN

ICND2 v1.0—8-5

Удаленный доступ представляет собой усовершенствование сетей с коммутацией каналов, таких как аналоговая телефонная линия или ISDN. VPN удаленного доступа предназначены для удаленных работников, мобильных пользователей и обмена данными между потребителем и организацией. VPN удаленного доступа обеспечивают безопасное подключение отдельных хостов к корпоративной сети через Интернет.

В прошлом корпорации работали с удаленными пользователями с помощью коммутируемого доступа через телефонную сеть и ISDN. С появлением VPN мобильные пользователи нуждаются только в доступе в Интернет для подключения к центральному офису. Удаленные работники, как правило, используют широкополосное соединение, DSL или кабельный модем для доступа в Интернет.

В VPN удаленного доступа каждый хост работает под управлением ПО Cisco VPN Client. Каждый раз, когда хост пытается передать трафик, ПО Cisco VPN Client инкапсулирует и шифрует его перед отправкой через Интернет в шлюз VPN на периферии сети назначения. При получении трафика шлюз VPN выполняет те же действия, что аналогичный шлюз в VPN соединения площадок.



При внедрении VPN для удаленных работников и малых офисов, простота развертывания крайне важна. Решение Cisco Easy VPN упрощает развертывание VPN в сетях малых, средних и крупных предприятий, включающих продукты Cisco. Cisco Easy VPN – экономичное решение, идеальное для удаленных офисов с низким уровнем ИТ-поддержки.

Cisco Easy VPN состоит из двух компонентов:

- **Cisco Easy VPN Server:** в качестве сервера может служить специализированный шлюз VPN, например VPN-концентратор Cisco, брандмауэр Cisco PIX, адаптивное устройство безопасности Cisco ASA или маршрутизатор Cisco IOS. Шлюз VPN, использующий ПО Cisco Easy VPN Server, может завершать туннели VPN, инициированные мобильными и удаленными пользователями с компьютерами под управлением ПО Cisco VPN Client. Кроме того, шлюз VPN может завершать туннели VPN с удаленных устройств, работающих в качестве узлов Cisco Easy VPN Remote в сети VPN для соединения площадок.
- **Cisco Easy VPN Remote:** Cisco Easy VPN Remote позволяет маршрутизаторам Cisco IOS, брандмауэрам PIX, адаптивным устройствам безопасности Cisco ASA и аппаратным клиентам Cisco VPN получать политики от Cisco Easy VPN Server. Это сводит к минимуму требования к настройке VPN на удаленном объекте. Cisco Easy VPN обеспечивает принудительную передачу таких параметров VPN, как внутренние IP-адреса, внутренние маски подсети, адреса DHCP-серверов, адреса WINS-серверов и флаги разделения туннелей, с Cisco Easy VPN Server в удаленные устройства.

Преимущества

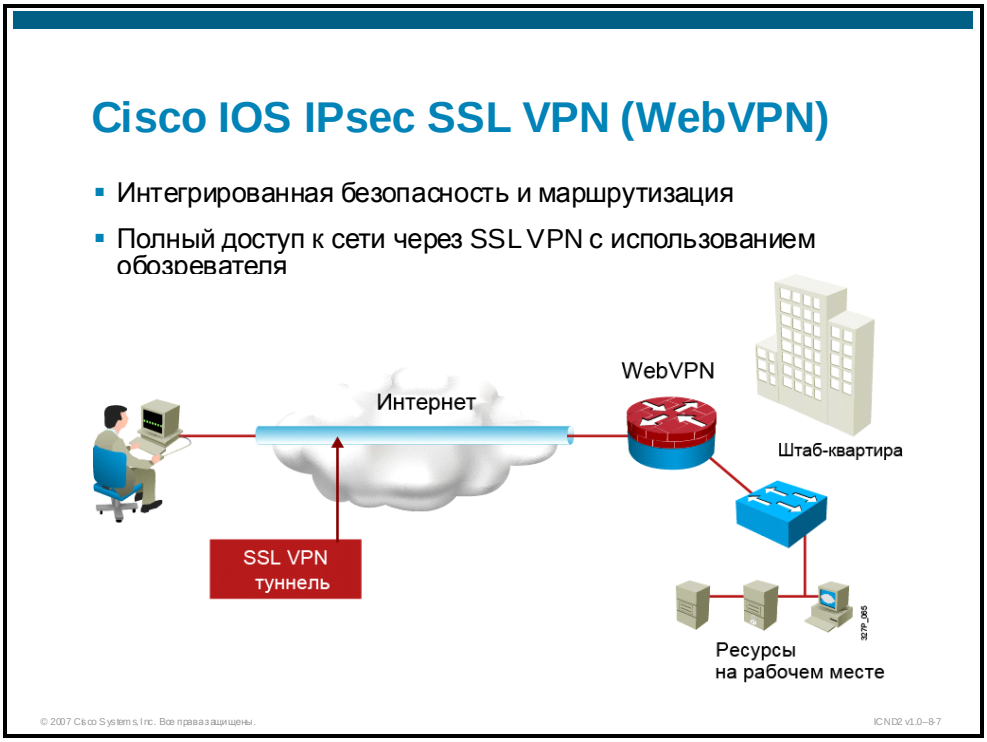
Преимущества Cisco Easy VPN:

- Централизованное хранение конфигураций обеспечивает динамическую настройку политик конечных пользователей и снижает потребность в ручной настройке.
- Локальная конфигурация VPN не зависит от IP-адреса удаленного узла. Эта функция позволяет поставщику услуг изменять конфигурации оборудования и сети с минимальной перенастройкой оборудования конечных пользователей или вообще без нее.
- Cisco Easy VPN обеспечивает централизованное управление политиками безопасности.
- Cisco Easy VPN обеспечивает развертывание в больших масштабах с быстрым добавлением пользователей.
- Cisco Easy VPN не требует установки и настройки ПО Cisco Easy VPN Remote конечными пользователями.

Ограничения

Для решения Cisco Easy VPN характерны следующие ограничения:

- Ручная настройка преобразования NAT и PAT не допускается.
  - Cisco Easy VPN Remote автоматически создает необходимые конфигурации NAT и PAT для туннеля VPN.
- Поддерживается только один узел назначения.
  - Cisco Easy VPN Remote поддерживает конфигурации только с одним узлом назначения и туннельным подключением.
  - Если приложение требует создания нескольких туннелей VPN, необходимо вручную настроить параметры IPsec VPN, NAT и PAT на сервере и удаленном клиенте.
- Cisco Easy VPN требует серверов назначения.
  - Для работы Cisco Easy VPN Remote необходимо, что узел назначения был сервером удаленного доступа Cisco Easy VPN.
- Цифровые сертификаты не поддерживаются.
  - Поддерживается аутентификация на основе предварительных общих ключей (PSK).
  - Расширенную аутентификацию (XAUTH) можно использовать в дополнение к PSK для обеспечения аутентификации на уровне пользователей в дополнение к аутентификации на уровне устройств.
- На серверах IPsec поддерживается только группа политик 2 протокола ISAKMP.
  - Cisco VPN Client и Cisco VPN Server поддерживает политики ISAKMP, использующие согласование группы 2 (1024-битный алгоритм Диффи-Хеллмана [DH]).
- Некоторые наборы преобразований не поддерживаются.
  - Функция Cisco Easy VPN Remote не поддерживает наборы преобразований, обеспечивающие шифрование без аутентификации (ESP-DES и ESP-3DES) и наборы преобразований, обеспечивающих аутентификацию без шифрования (ESP-NULL, ESP-SHA-HMAC и ESP-NULL ESP-MD5-HMAC).
  - Cisco VPN Client и Cisco VPN Server не поддерживают протокол AH, но поддерживают протокол ESP.



Решение Cisco IOS IPsec/SSL VPN, также известное как WebVPN, – новая технология, которая обеспечивает удаленный доступ практически с любого узла, имеющего доступ в Интернет. Для этого достаточно веб-обозревателя и шифрования SSL, встроенного в этот веб-обозреватель. WebVPN обеспечивает гибкость для поддержки безопасного доступа всех пользователей, независимо от конечного хоста, с которого они подключаются. Если приложение предъявляет умеренные требования к доступу, WebVPN может работать без предварительной установки клиентского ПО на конечный хост. Это позволяет компаниям включить в защищенные корпоративные сети любого авторизованного пользователя, обеспечивая удаленный доступ к корпоративным ресурсам с любого узла, имеющего доступ в Интернет.

В настоящий момент WebVPN предлагает два режима доступа к SSL VPN: бесклиентный и тонкий клиент. WebVPN позволяет пользователям обращаться к веб-страницам и сервисам. Сюда входит доступ к файлам, отправка и получение электронной почты и запуск TCP-приложений без использования ПО IPsec VPN Client. WebVPN можно применять для групп пользователей, которые нуждаются в контроле доступа на уровне отдельных серверов или приложений или в доступе с рабочих станций, не принадлежащих предприятию.

Во многих случаях IPsec и WebVPN дополняют друг друга, так как решают разные проблемы. Этот подход позволяет одному устройству удовлетворять все требования пользователей к удаленному доступу.

Преимущества

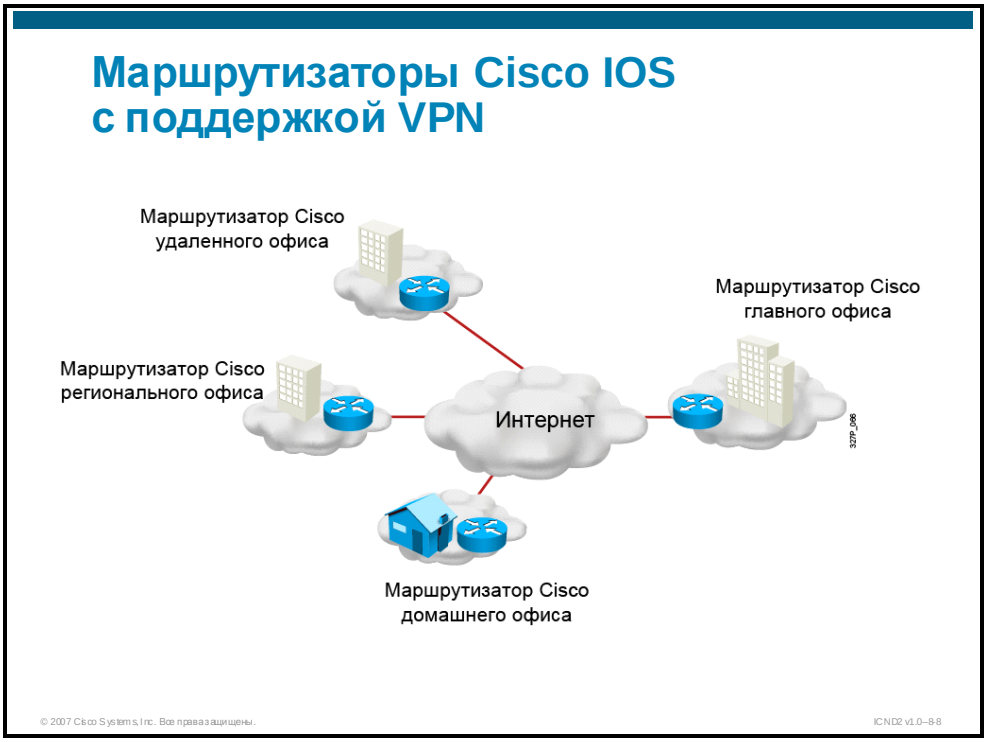
Главное преимущества WebVPN – совместимость с динамическими многоточечными VPN (DMVPN), брандмауэрами Cisco IOS, IPsec, системами предотвращения вторжений (IPS), Cisco Easy VPN и NAT.

Ограничения

Главное ограничение решения WebVPN заключается в том, что оно поддерживается только в программном обеспечении. Подключения WebVPN обрабатываются ЦП маршрутизатора. Встроенное ускорение VPN, доступное в маршрутизаторах интегрированных услуг, применяется только к подключениям IPsec.

Компоненты VPN

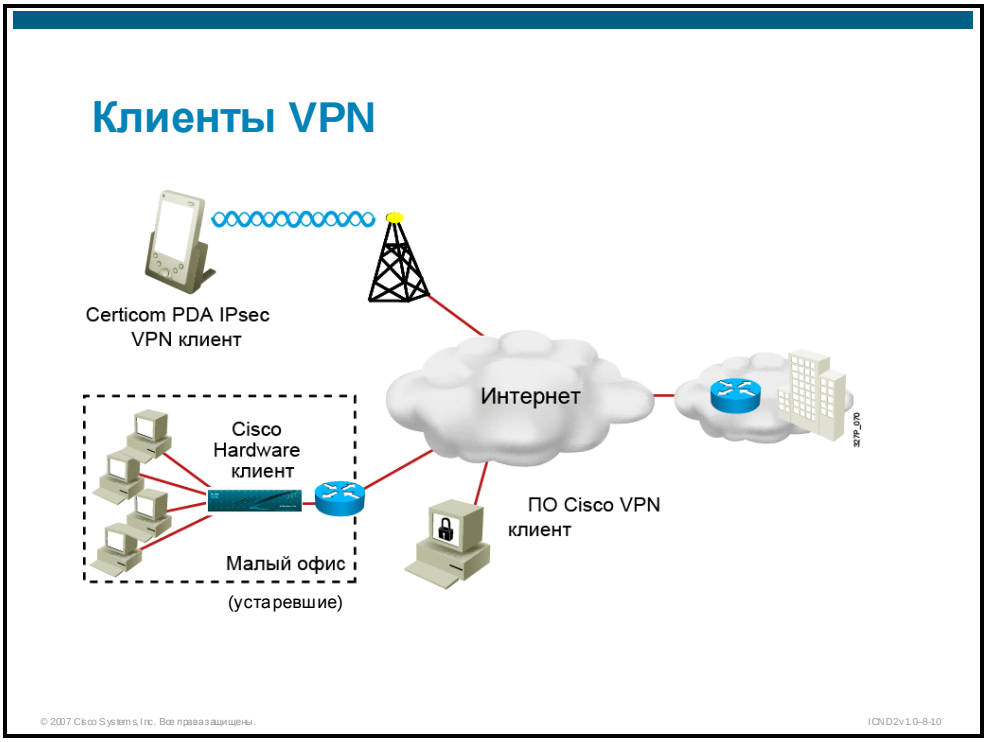
В этом разделе описываются программные и аппаратные компоненты, из которых состоит среда VPN.



Cisco предлагает портфель маршрутизаторов, оптимизированных для VPN. ПО Cisco IOS, работающее на маршрутизаторах Cisco, объединяет многофункциональные службы VPN и ведущую в отрасли маршрутизацию в единое комплексное решение. ПО Cisco VPN обеспечивает высокий уровень безопасности за счет шифрования и аутентификации. Маршрутизаторы Cisco VPN поддерживают высокую производительность решений VPN для интрасетей, экстрасетей и соединения площадок.

Адаптивные устройства безопасности Cisco ASA 5500 предлагают гибкие технологии для создания специализированных решений, удовлетворяющих различным требованиям к удаленному доступу и соединению площадок. Адаптивные устройства безопасности ASA 5500 предоставляют простой в управлении удаленный доступ через IPsec и соединение площадок через VPN, учитывающее особенности сети. Это позволяет организациям создавать безопасные подключения для мобильных пользователей, удаленных площадок и бизнес-партнеров.

ASA 5500 предлагает функции IPsec и SSL VPN в одной платформе, устраняя потребность в параллельных решениях. Помимо служб VPN ASA 5500 предлагает брандмауэр для анализа приложений и службы предотвращения вторжений.



VPN удаленного доступа Cisco поддерживают три клиента IPsecs: Certicom IPsec, программный клиент Cisco VPN Client и аппаратный клиент Cisco VPN 3002.

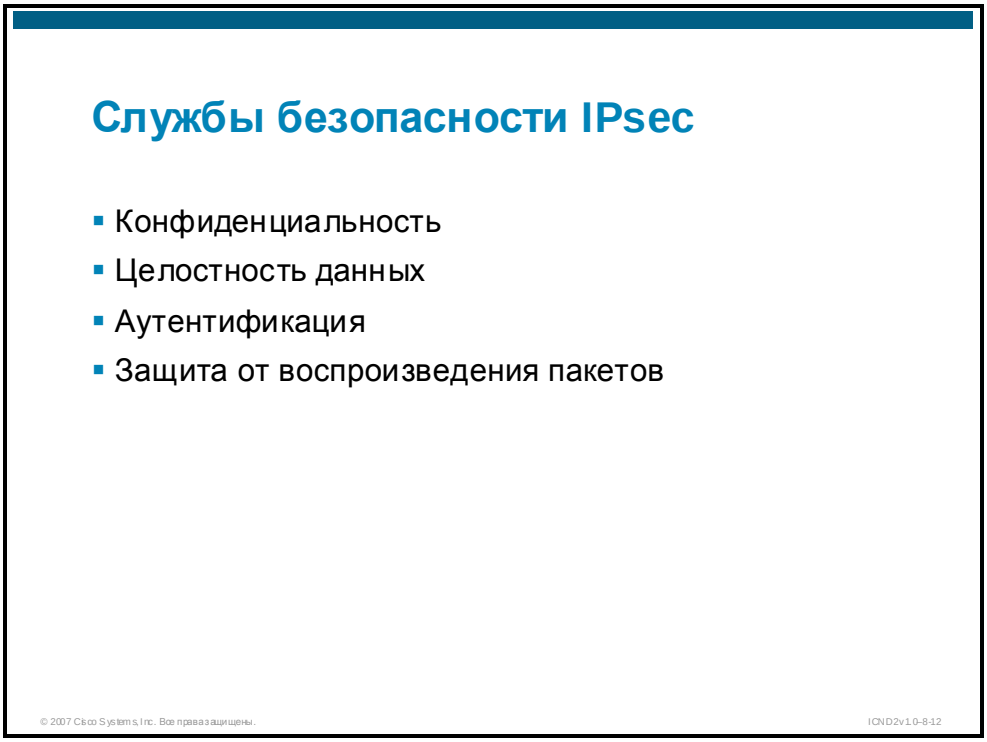
- **Клиент Certicom:** Беспроводной клиент, загружаемый на беспроводные КПК под управлением ОС Palm или Microsoft Windows Mobile. Беспроводное клиентское ПО Certicom позволяет компаниям сделать важные корпоративные приложения, такие как электронная почта и управление связями с клиентами (CRM), доступными мобильным работникам. Это обеспечивается за счет подключения переносных устройств к корпоративным шлюзам VPN для получения безопасного беспроводного доступа.
- **Аппаратный клиент Cisco VPN 3002 (устаревшее оборудование):** Сетевое устройство, используемое для подключения локальных сетей малых и домашних офисов к VPN. Устройство поставляется с однопортовым или восьмипортовым коммутаторам. Аппаратный клиент VPN 3002 заменяет традиционные приложения Cisco VPN Client на отдельных компьютерах малых и домашних офисов.
- **Программный клиент Cisco VPN Client:** Программное обеспечение, загружаемое на ПК или лэптоп пользователя. Cisco VPN Client позволяет организациям создавать сквозные, зашифрованные туннели VPN для безопасного подключения мобильных и удаленных работников. Функция Cisco Easy VPN позволяет ПО Cisco VPN Client получать политики безопасности от устройства VPN на центральной площадке (Cisco Easy VPN Server) при создание туннельного подключения VPN. Это позволяет свести к минимуму требования к настройке на удаленном объекте.

Общие сведения об IPsec

В этом разделе описывается структура IPsec, которая обеспечивает безопасность VPN.

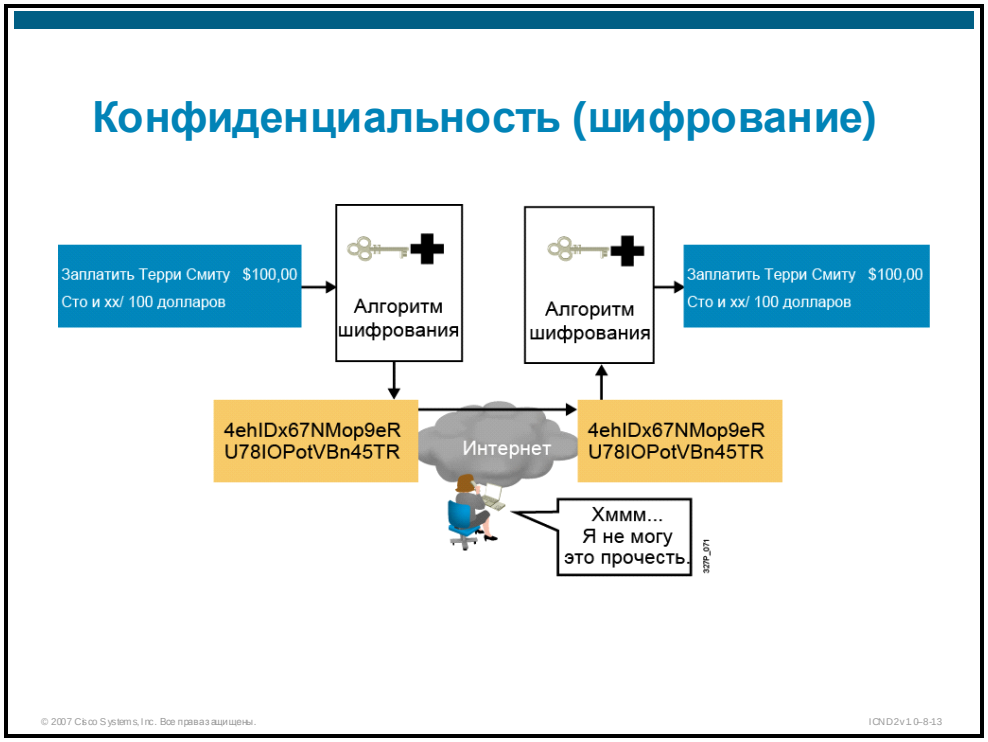
IPsec действует как протокол сетевого уровня, защищая и аутентифицируя IP-пакеты между устройствами IPsec, участвующими в соединении (узлами). IPsec не привязан к конкретным алгоритмам шифрования, аутентификации и безопасности, а также технологиям генерации ключей. IPsec – это структура открытых стандартов.

Отсутствие привязки протокола IPsec к определенным алгоритмам позволяет внедрять новые и более эффективные алгоритмы без необходимости в исправлении существующих стандартов IPsec. IPsec обеспечивает конфиденциальность и целостность данных, а также аутентификацию их источника перед соединением узлов на уровне IP. IPsec защищает путь между двумя шлюзами, двумя хостами или шлюзом и хостом.



Службы безопасности IPsec выполняют 4 важные функции.

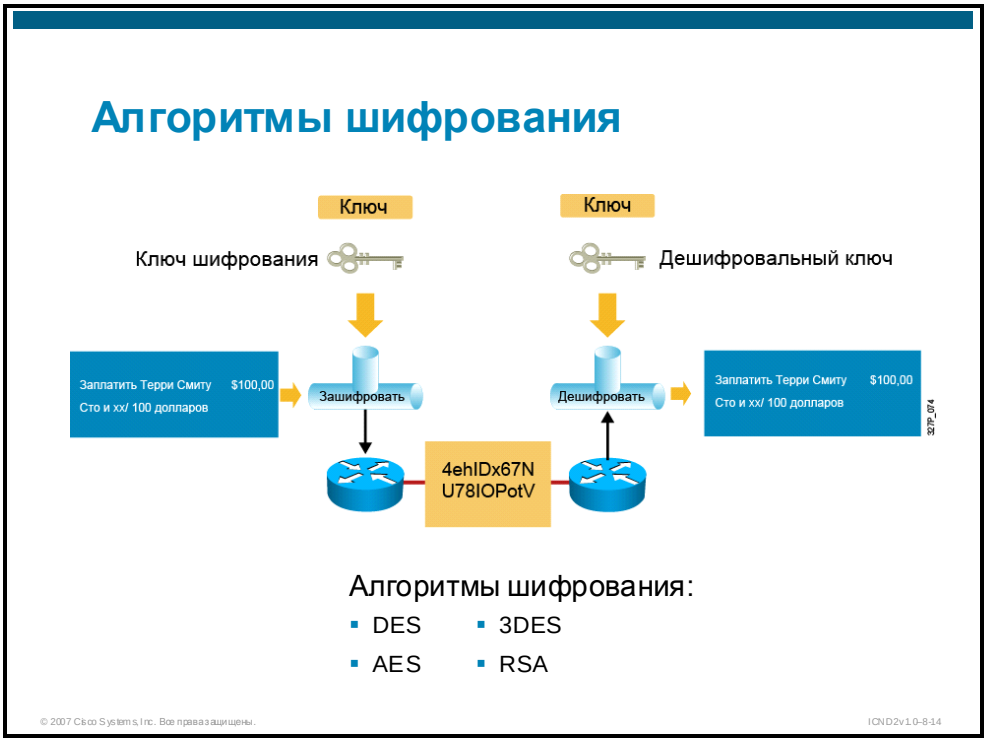
- **Конфиденциальность (шифрование):** Отправитель шифрует пакеты перед тем, как передать их через сеть. Это предотвращает возможность перехвата сообщений. Если сообщение перехвачено, злоумышленник не сможет прочитать его.
- **Целостность данных:** Получатель может проверить, были ли данные изменены во время передачи через Интернет. IPsec гарантирует целостность данных с помощью контрольных сумм, простой проверке по избыточности.
- **Аутентификация:** Аутентификация гарантирует, что соединение установлено с нужным партнером по связи. Получатель может аутентифицировать источник пакета, гарантируя и сертифицируя подлинность источника информации.
- **Защита от воспроизведения пакетов:** Защита от воспроизведения гарантирует, что каждый пакет уникален и не дублируется. Защита пакетов IPsec обеспечивается за счет сравнения последовательных номеров полученных пакетов со скользящим окном хоста назначения или шлюза безопасности. Пакет с последовательным номером ниже скользящего окна считается запоздавшим или дублированным. Запоздавшие и дублированные пакеты отбрасываются.



Незашифрованный текст, передаваемый через сеть Интернет общего доступа, может быть перехвачен и прочитан злоумышленником. Для сохранения конфиденциальности данные необходимо шифровать. Цифровое скремблирование данных делает невозможным их несанкционированное прочтение.

Чтобы шифрование работало, отправитель и получатель должны знать правила преобразования исходного сообщения в закодированную форму. Правила основываются на алгоритме и ключе. Алгоритм – это математическая функция, которое комбинирует сообщение, текст, цифры или все вышеперечисленное со строкой из цифр, которая называется ключом. В результате получается нечитаемое зашифрованное сообщение. Расшифровка такого сообщения крайне сложна и невозможна без ключа.

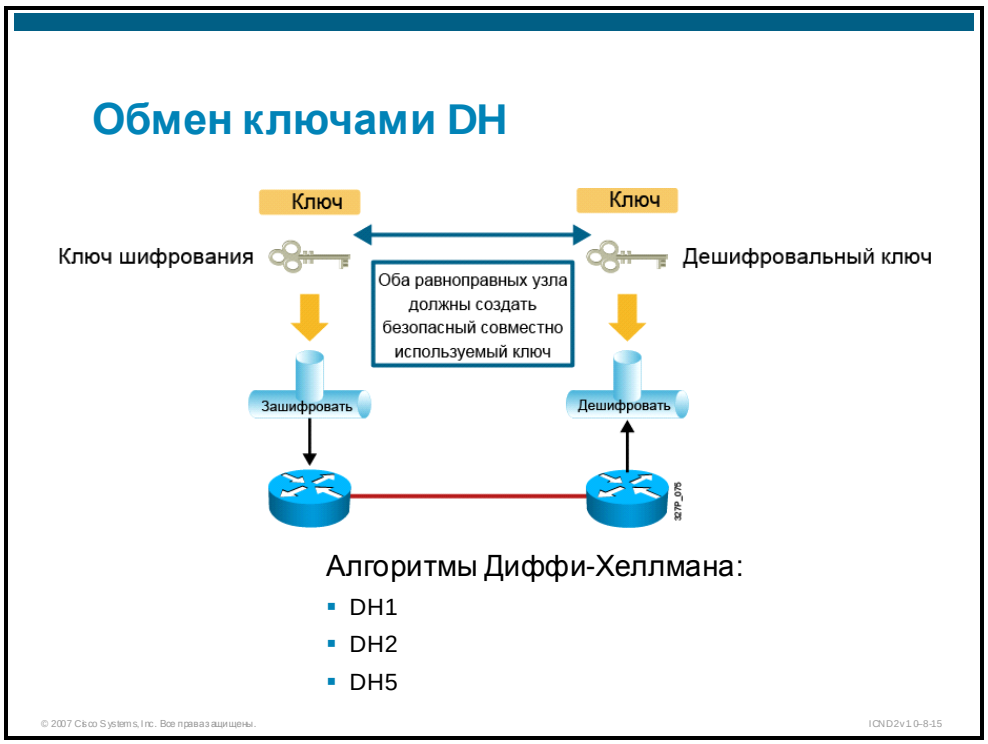
В примере ниже пользователь хочет отправить финансовый документ через Интернет. На локальной стороне документ комбинируется с ключом и пропускается через алгоритм шифрования. В результате получается зашифрованный текст, не поддающийся расшифровке. Затем зашифрованный текст отправляется через Интернет. На удаленной стороне сообщение повторно комбинируется с ключом и снова пропускается через алгоритм шифрования. В результате получается исходный финансовый документ.



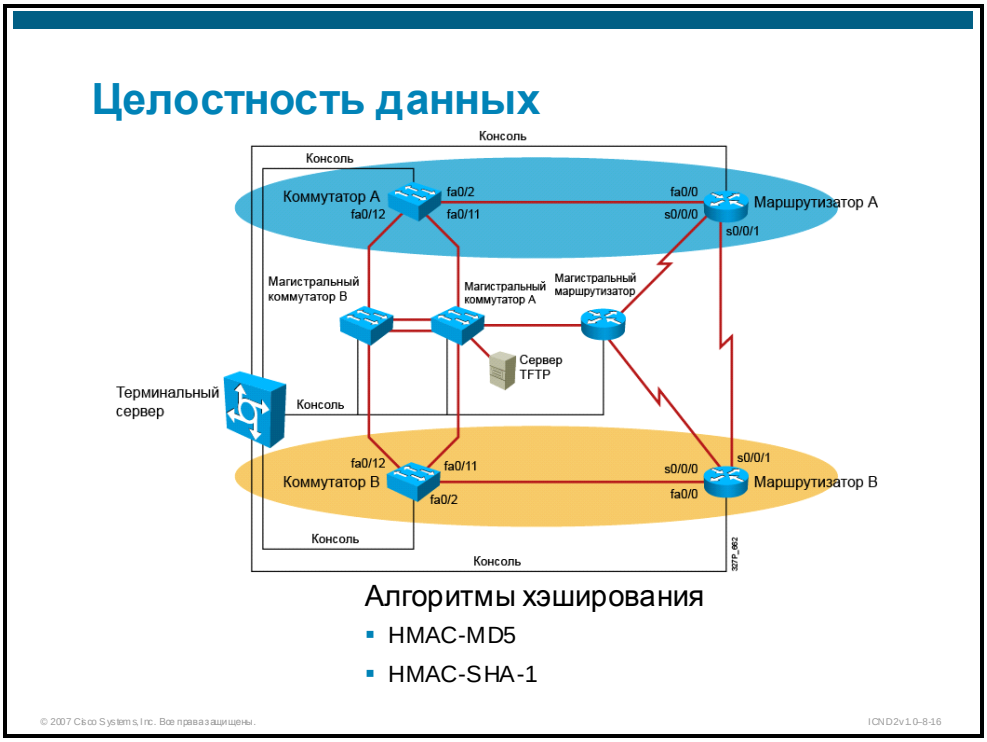
Степень безопасности зависит от длины ключа и алгоритма шифрования. Время, необходимое для прогона всех вариантов, зависит от вычислительной мощности компьютера. Поэтому чем короче ключ, тем проще его взломать.

Некоторые алгоритмы шифрования и длины ключей, которые они используют, приводятся ниже:

- **Алгоритм Data Encryption Standard (DES):** Алгоритм DES разработан компанией IBM. Он использует 56-битный ключ, который обеспечивает высокопроизводительное шифрование. DES представляет собой криптосистему с симметричным ключом.
- **Алгоритм Triple DES (3DES):** Алгоритм 3DES является вариантом 56-битного алгоритма DES. 3DES работает также, как DES, разбивая данные на 64-битные блоки. Затем 3DES трижды обрабатывает каждый блок, используя независимые 56-битные ключи. 3DES предлагает значительное увеличение криптографической сложности по сравнению с 56-битным алгоритмом DES. DES представляет собой криптосистему с симметричным ключом.
- **Advanced Encryption Standard (AES):** Национальный институт стандартов и технологии (NIST) недавно принял AES в качестве замены существующего шифрования DES в криптографических устройствах. AES обеспечивает более высокий уровень безопасности, чем DES и расходует вычислительную мощность более эффективно, чем 3DES. AES предлагает три варианта длины ключа. 128, 192 и 256 бит.
- **Rivest, Shamir, and Adleman (RSA):** RSA – асимметричная криптосистема. Она использует ключи длиной 512, 768, 1024 бит или выше. IPsec не использует алгоритм RSA для шифрования данных. Протокол IKE использует шифрование RSA только на этапе аутентификации узлов.



Алгоритмы шифрования, такие как DES и 3DES требуют общего симметричного ключа для шифрования и дешифрования. Для отправки общих секретных ключей администраторам устройств используется электронная почта, услуги курьера или ночной экспресс. Но самый простой метод обмена – обмен открытыми ключами между шифрующим и дешифрующим устройствами. Метод обмена открытыми ключами, который называется согласованием ключей DH, позволяет двум узлам сформировать общий секретный ключ, даже если для связи между ними используется небезопасный канал.



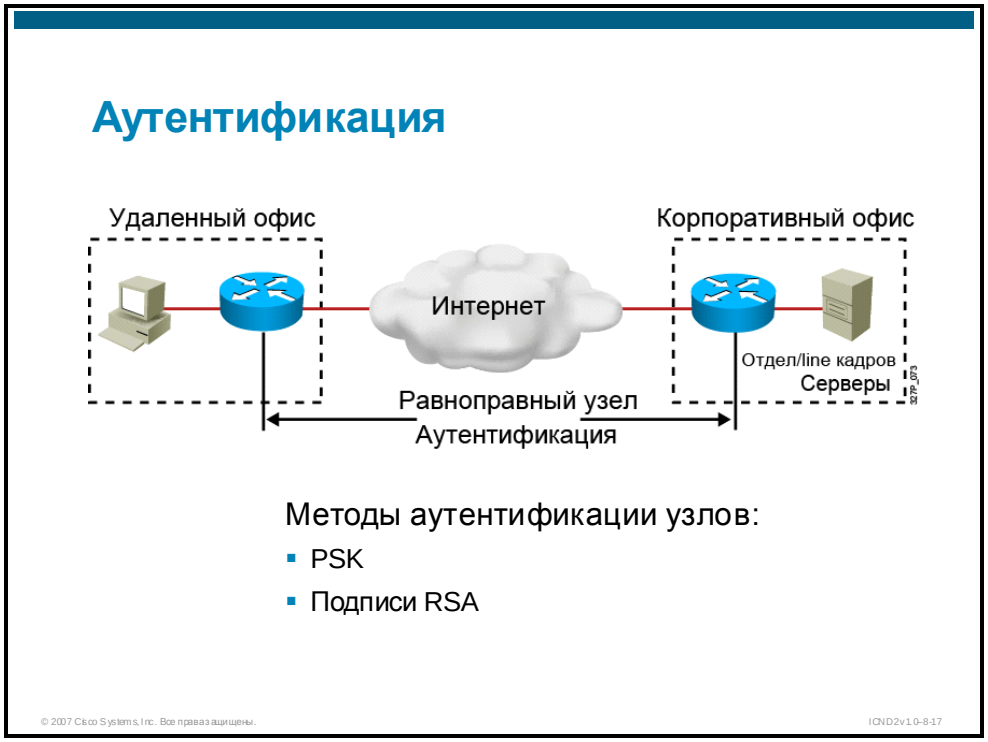
Данные VPN передаются через сеть Интернет общего доступа. Существует вероятность, что они будут перехвачены и изменены. Для решения этой проблемы можно использовать алгоритм защиты целостности данных. Алгоритм целостности данных добавляет хэш в сообщение. Хэш гарантирует целостность исходного сообщения. Если передаваемый хэш совпадает с полученным хэшем, значит в сообщение не были внесены несанкционированные изменения. Однако, если значения хэша не совпадают, значит сообщение было изменено.

В примере выше некто пытается отправить Терри Смиту чек на 100 долларов. На удаленной стороне Алекс Джонс пытается обналичить чек на 1 000 долларов. При передаче через Интернет чек был модифицирован. Было изменено имя получателя и сумма в долларах. В этом случае, если был использован алгоритм для защиты целостности данных, хэши не совпадут и транзакция будет признана недействительной.

Keyed Hashed Message Authentication Codes (HMAC) – это алгоритм, гарантирующий целостность сообщения. На локальной стороне сообщение и общий секретный ключ пропускаются через алгоритм хэширования, который генерирует значение хэша. Затем сообщение и хэш передаются через сеть.

Существует два стандартных алгоритма HMAC:

- **HMAC- Message Digest 5 (MD5):** Использует 128-битный общий секретный ключ. Сообщение переменны длиной и 128-битный общий ключ комбинируются и пропускаются через алгоритм хэширования HMAC-MD5. В результате получается 128-битный хэш. Хэш добавляется к исходному сообщению и передается в удаленный узел.
- **HMAC- Secure Hash Algorithm 1 (SHA-1):** HMAC-SHA-1 использует 160-битный секретный ключ. Сообщение переменной длины и 160-битный общий ключ комбинируются и пропускаются через алгоритм хэширования HMAC-SHA-1. В результате получается 160-битный хэш. Хэш добавляется к исходному сообщению и передается в удаленный узел.



При ведении бизнеса на больших расстояниях важно знать, кто находится на другой стороне телефонной линии, принимает электронное сообщение или факс. Это правило относится и к сетям VPN. Устройство на другой стороне туннеля VPN должно быть аутентифицировано, прежде чем канал будет признан безопасным. Существует два метода аутентификации узлов:

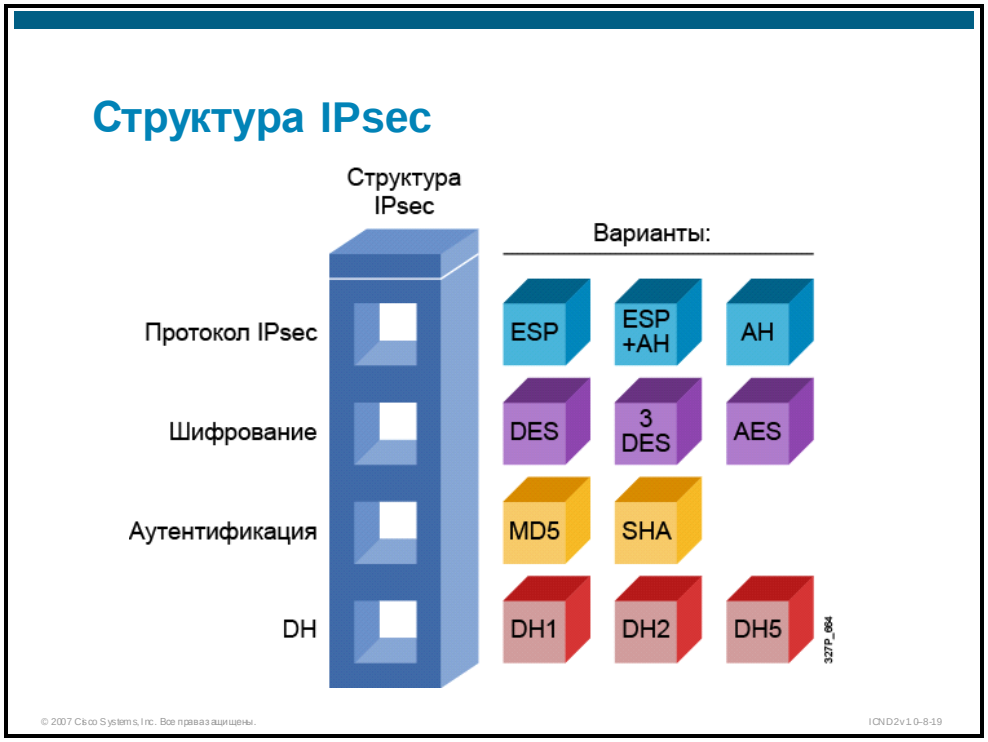
- **PSK:** Секретный ключ, который вручную вводится на всех узлах и используется для их аутентификации. На каждой из сторон PSK комбинируется с другими данными для формирования ключа аутентификации.
- **Подписи RSA:** Используют обмен цифровыми сертификатами для аутентификации узлов. Локальное устройство получает хэш и шифрует его с использованием закрытого ключа. Зашифрованный хэш (цифровая подпись) прилагается к сообщению и пересылается удаленному узлу. На удаленном узле зашифрованный хэш расшифровывается с использованием открытого ключа локальной стороны. Если расшифрованный хэш совпадает с повторно вычисленным хэшем, подпись считается подлинной.

Структура протоколов IPsec

В этом разделе описывается активация шифрования, средств безопасности и аутентификации для пакета протоколов IPsec.

IPsec – это структура открытых стандартов. IPsec определяет обмен сообщениями для защиты каналов связи, но использует существующие протоколы. Существует два основных протокола IPsec.

- **AH:** AH – это протокол, который следует использовать, когда конфиденциальность не требуется или не разрешена. Он обеспечивает аутентификацию и целостность IP-пакетов, передаваемых между двумя системами. Протокол включает методы, которые позволяют проверить, были ли сообщения, передаваемые из маршрутизатора A в маршрутизатор B, изменены во время передачи. Протокол проверяет источник данных, в данном примере это должен быть маршрутизатор A или B. AH не обеспечивает конфиденциальности (шифрования) пакетов. Весь текст передается в незашифрованном виде. Сам по себе протокол AH обеспечивает слабую защиту. Поэтому протокол AH используется совместно протоколом ESP для обеспечения шифрования и защиты от несанкционированного изменения.
- **ESP:** Протокол безопасности с поддержкой конфиденциальности (шифрование) и аутентификации. ESP обеспечивает конфиденциальность путем шифрования IP-пакетов. Шифрование IP-пакетов скрывает полезную часть пакета, а также удостоверения источника и места назначения. ESP выполняет аутентификацию внутреннего IP-пакета и заголовка ESP. Аутентификация подразумевает проверку подлинности источника данных и защиту целостности данных. Хотя использование шифрования и аутентификации в протоколе ESP необязательно, необходимо выбрать хотя бы одну из этих функций.



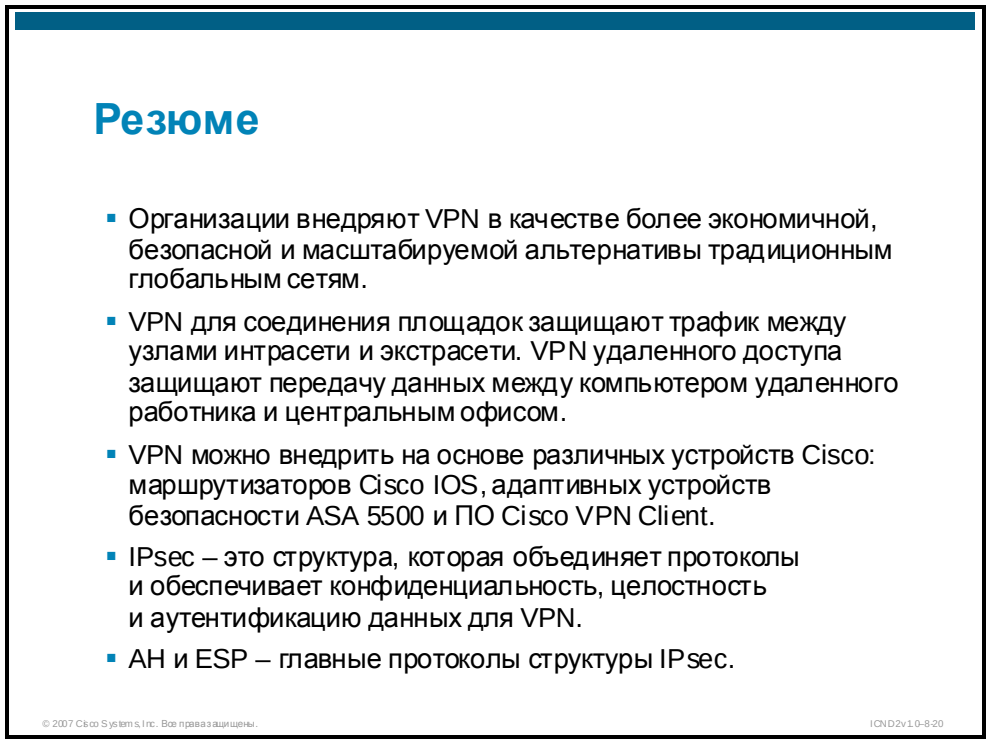
IPsec – это структура открытых стандартов, которая определяет правила безопасной связи. IPsec использует существующие алгоритмы шифрования, аутентификации и обмена ключами. Некоторые из стандартных алгоритмов, используемых IPsec, перечислены ниже:

- **DES:** Выполняет шифрование и расшифровку данных.
- **3DES:** Предлагает значительное увеличение криптографической сложности по сравнению с 56-битным алгоритмом DES.
- **AES:** Обеспечивает бОльшую сложность шифрования в зависимости от используемой длины ключа, а также более высокую производительность.
- **MD5:** Аутентифицирует данные пакета с использованием 128-битного общего секретного ключа.
- **SHA-1:** Аутентифицирует данные пакета с использованием 160-битного общего секретного ключа.
- **DH:** Позволяет двум сторонам формировать общий секретный ключ, используемый для алгоритмов шифрования и хэширования DES и MD5, через небезопасный канал связи.

В примере на рисунке приводятся элементы структуры IPsec, которые заполняются протоколами. При настройке служб безопасности шлюза IPsec сначала следует выбрать протокол IPsec. Доступные варианты: ESP и ESP с AH. Второе поле – алгоритм шифрования. Выберите алгоритм шифрования, соответствующий необходимому уровню безопасности: DES, 3DES или AES. Третье поле – аутентификация. Выберите алгоритм аутентификации для защиты целостности данных: MD5 или SHA. Последнее поле – группа алгоритма DH. Выберите группу DH: DH1 или DH2. IPsec предоставляет структуру, администратор выбирает алгоритмы, на базе которых реализуются службы безопасности в рамках этой структуры.

Резюме

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



Занятие 2

Создание подключения типа «точка-точка» к ГВС с помощью протокола PPP

Обзор

Службы глобальной сети, как правило, предоставляются поставщиком услуг на условиях аренды. Некоторые службы глобальной сети рассматриваются как подключения 2-го уровня между удаленными площадками, и предоставляются телефонными компаниями с использованием коммутаторов ГВС.

PPP – это протокол инкапсуляции, используемый для передачи IP-трафика через последовательные подключения типа «точка-точка» (арендованные каналы). В этом занятии описывается принцип работы, настройка и проверка протокола PPP.

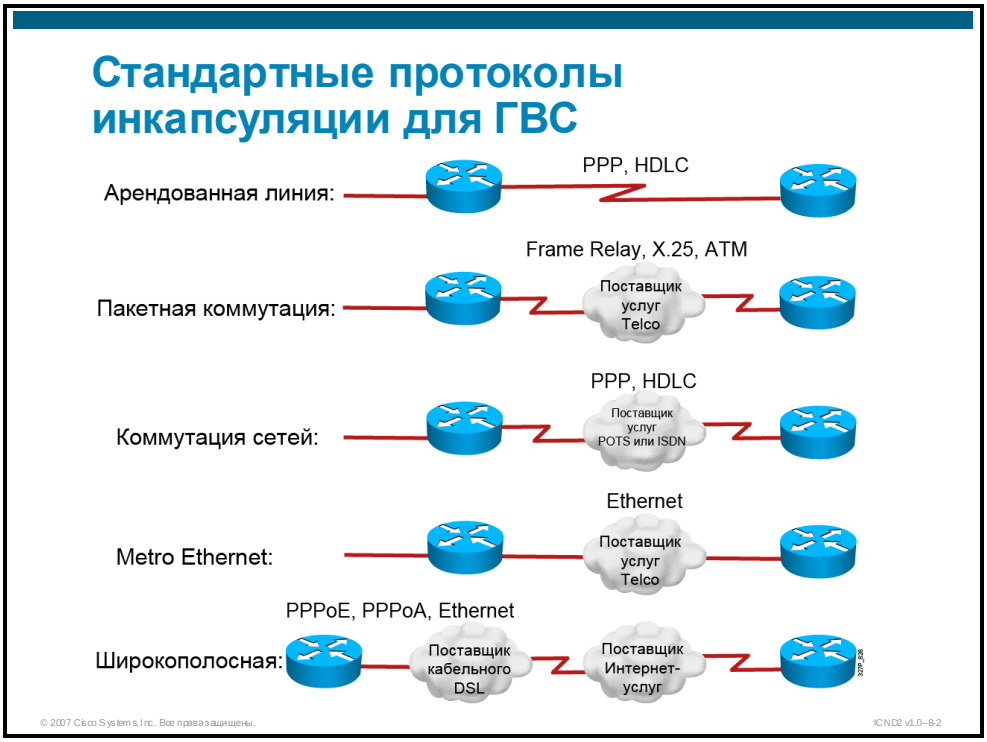
Задачи

По окончании этого занятия вы сможете подключаться к поставщику услуг через сеть и описывать принцип работы и настройку протокола PPP. Это значит, что вы сможете выполнять следующие задачи:

- описывать типы инкапсуляции, доступные для маршрутизаторов Cisco;
- описывать функции и возможности протокола PPP;
- настраивать и проверять VTP.

Общие сведения об инкапсуляции для глобальной сети

В этом разделе описываются различные протоколы инкапсуляции, используемые для соединения удаленных площадок.



Перед передачей через канал ГВС данные инкапсулируются в кадры. Чтобы система выбрала верный протокол, необходимо настроить соответствующий тип инкапсуляции второго уровня. Выбор протокола второго уровня зависит от технологии ГВС и коммуникационного оборудования. Ниже описываются стандартные протоколы ГВС.

- **High-Level Data Link Control (HDLC):** Тип инкапсуляции, который по умолчанию используется продуктами Cisco для подключений «точка-точка», выделенных каналов и подключений с коммутацией каналов. Как правило, протокол HDLC используется, когда устройства Cisco взаимодействуют через соединение «точка-точка». HDLC – это битовый синхронный протокол канального уровня.
- **PPP:** Обеспечивает соединение между маршрутизаторами и соединение между хостом и сетью через синхронные и асинхронные каналы. Протокол PPP предназначен для работы с несколькими протоколами сетевого уровня, включая IP. PPP поддерживает встроенные механизмы обеспечения безопасности, такие как Password Authentication Protocol (PAP) и Challenge Handshake Authentication Protocol (CHAP).
- **X.25 и Link Access Procedure, Balanced (LAPB):** Стандарты ITU-T определяют методы обслуживания соединений между DTE и DCE для удаленного терминального доступа и передачи данных между компьютерами в сетях общего доступа. Стандарт X.25 определяет LAPB, протокол канального уровня, который управляет передачей данных между DTE и DCE, в том числе инкапсуляцией пакетов в кадры, классификацией и выявлением ошибок. Протокол X.25 – предшественник Frame Relay.

- **Frame Relay:** Протокол, заменивший X.25. Стандартный коммутируемый протокол канального уровня, обрабатывающий несколько виртуальных каналов (VC). Frame Relay оптимизирован для исключения некоторых длительных процессов, таких как исправление ошибок и управление потоками, которые использовались в X.25 для компенсации недостатков старых ненадежных каналов связи.
- **ATM:** Этот протокол является международным стандартом передачи ячеек. Для различных служб, таких как голос, видео и данные, используются ячейки фиксированной длины (53 байта). Технология коммутации ячеек ATM, использует ячейки фиксированной длины. Это позволяет выполнять обработку на аппаратном уровне, что в свою очередь уменьшает задержки передачи. Протокол ATM разработан, чтобы реализовать преимущества высокоскоростных сред передачи данных, таких как T3, E3 и SONET.
- **Широкополосные технологии:** В телекоммуникациях термин «широкополосный», как правило, относится к каналу, в котором несколько фрагментов данных передаются одновременно для повышения эффективной скорости передачи, независимо от фактической скорости. В сетевом проектировании этот термин относится к методам передачи, в которых два или более сигналов используют одну среду передачи. Некоторые из таких технологий перечислены ниже.
  - **DSL-PPP поверх Ethernet (PPPoE) и PPP поверх ATM (PPPoA):** Семейство технологий, обеспечивающее передачу цифровых данных по проводам местной телефонной сети. Как правило, скорость загрузки потребительских служб DSL составляет от 256 до 24 000 Кбит/с, в зависимости от технологии DSL, состояния линии и уровня обслуживания. Реализации DSL часто используют PPPoE и PPPoA. Оба исполнения поддерживают стандартные функции PPP, такие как аутентификация, шифрование и сжатие. PPPoE – это сетевой протокол для инкапсуляции кадров PPP в кадры Ethernet. PPPoA – это сетевой протокол для инкапсуляции кадров PPP в ATM Adaptation Layer 5 (AAL5).
  - **Кабельный Ethernet:** Кабельный модем обеспечивает доступ к цифровому сигналу, переданному через телевизионную кабельную инфраструктуру. Кабельные модемы, как правило, применяются для широкополосного доступа в Интернет на базе неиспользуемой полосы пропускания телевизионной кабельной сети. Полоса пропускания кабельных модемов бизнес-класса, как правило, составляет от 3 Мбит/с до 30 Мбит/с. Современные кабельные модемы используют формат кадров Ethernet для передачи данных через восходящие и нисходящие каналы передачи данных. Каждый из нисходящих каналов передачи данных и связанных с ними восходящих каналов в кабельной сети формирует глобальную сеть Ethernet.
- **Metro Ethernet:** Metro Ethernet, метод предоставления многоточечных сервисов и сервисов «точка-точка» был создан в связи с распространением новых оптических сред в инфраструктурах организаций. Корпоративные заказчики, использующие Ethernet в комплексах зданий в течение многих лет, достигли высокого уровня уверенности в этой технологии и просят своих поставщиков услуг предоставлять Ethernet в качестве варианта подключения. Возможно, Ethernet является самой масштабируемой транспортной технологией – полоса пропускания составляет от 10 Мбит/с до 10 Гбит/с, запланирована полоса пропускания 40 Гбит/с. Существует несколько методов передачи данных Ethernet по метросетям:
  - передача Ethernet через «темное» оптоволокно;
  - передача Ethernet через сети SONET и синхронной цифровой иерархии (SDH);
  - передача данных Ethernet с использованием технологии Resilient Packet Ring (RPR).

Обзор PPP

В этом разделе описываются функции и возможности протокола PPP.

Протокол PPP был разработан для поддержки каналов типа «точка-точка». Протокол PPP описывается в стандартах RFC 1661 и 1332 и инкапсулирует данные протокола сетевого уровня в каналы «точка-точка». RFC 1661 модифицирован в стандарте RFC 2153, *расширения PPP для производителей*.

Протокол PPP можно настроить на следующих типах физических интерфейсов.

- **Асинхронный последовательный интерфейс:** Коммутируемый доступ через обычную аналоговую телефонную линию.
- **Синхронный последовательный интерфейс:** ISDN или арендованные каналы «точка-точка».

Протокол управления каналом (LCP), входящий в PPP, используется для создания и настройки функций контроля канала ГВС. PPP предлагает обширный набор служб. Эти службы реализуются протоколом LCP и, как правило, используются для согласования и проверки кадров. Они позволяют внедрять элементы управления, которые администратор выбрал для подключения.

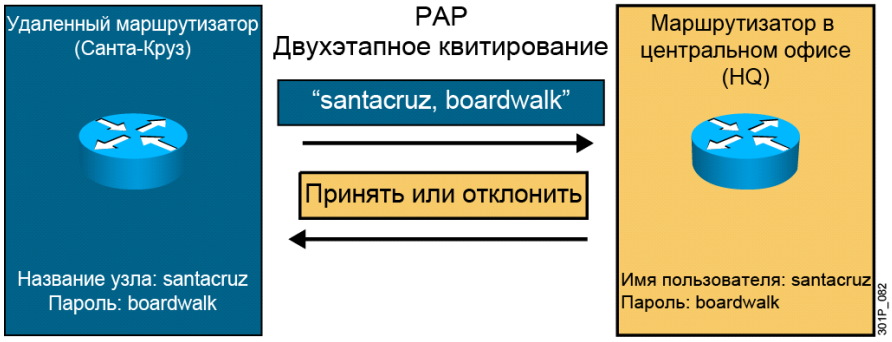
Благодаря функциям верхнего уровня PPP может переносить пакеты нескольких протоколов сетевого уровня с помощью протоколов управления сетью (NCP). Протоколы NCP используют функциональные поля, которые содержат стандартизированные коды. Эти коды указывают, какой тип протокола инкапсулирован в кадре PPP.

Создание сеанса PPP состоит из трех этапов. В таблице ниже приводится описание этих этапов.

Этапы создания сеанса PPP

	Этап	Описание
1.	Этап формирования канала	Во время этого этапа каждое устройство PPP отправляет пакеты LCP для проверки канала передачи данных. Пакеты LCP содержат поле конфигурации, которое позволяет устройствам согласовать используемые параметры, такие как максимальный размер принимаемого блока, сжатие отдельных полей PPP и протокол аутентификации канала. Если поле конфигурации не входит в пакет LCP, применяются параметры конфигурации по умолчанию.
2.	Этап аутентификации (необязательный)	После создания канала и выбора протокола аутентификации узел переходит к этапу аутентификации. Если аутентификация используется, она выполняется *до* этапа протокола сетевого уровня. PPP поддерживает два протокола аутентификации: PAP и CHAP. Оба протокола описываются в стандарте RFC 1334, *протоколы аутентификации PPP*. Однако с появлением стандарта RFC 1994, *протокол CHAP для PPP*, стандарт RFC 1334 вышел из употребления.
3.	Этап протокола сетевого уровня	Во время этого этапа устройства PPP отправляют пакеты NCP, чтобы выбрать и настроить один или несколько протоколов сетевого уровня, таких как IP. После настройки каждого из протоколов сетевого уровня датаграммы этого протокола можно передавать через канал.

Протоколы аутентификации PPP: PAP

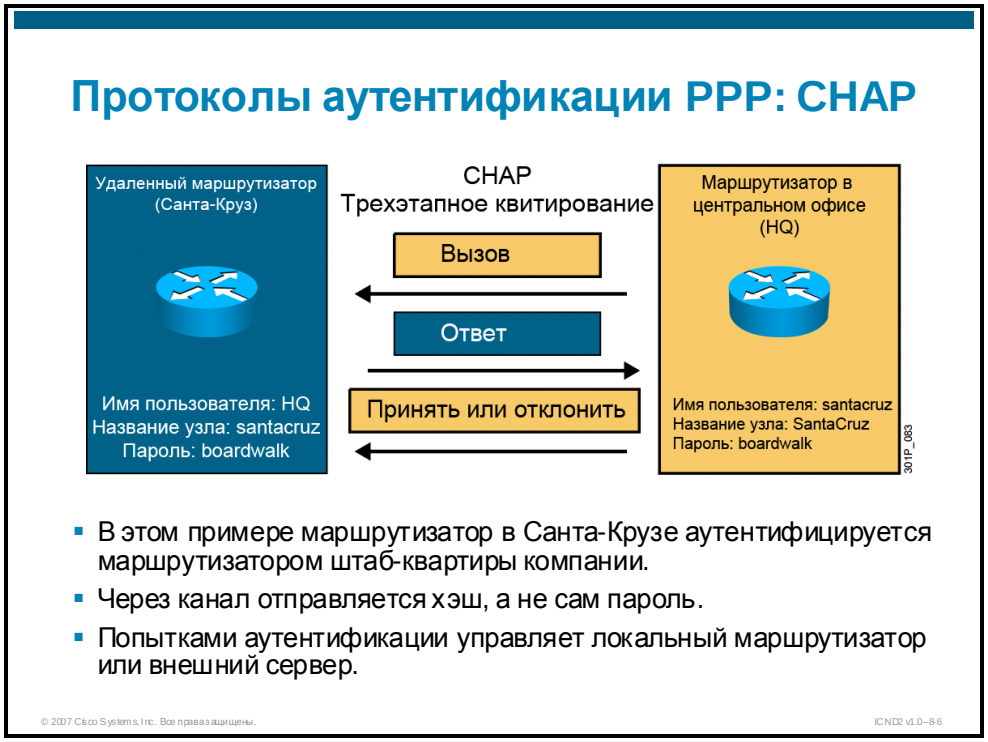


- Пароли аутентификации отправляются в незашифрованном виде
- Попытками аутентификации управляется удаленный узел

PAP – это двусторонний протокол установления соединения, который предоставляет простой метод создания удостоверения хоста. Процесс PAP выполняется после первоначального формирования канала.

По окончании этапа создания канала PPP удаленный узел несколько раз посылает имя пользователя и пароля в маршрутизатор, пока не получит подтверждение аутентификации или пока подключение не будет разорвано.

PAP не является сильным протоколом аутентификации. Пароли отправляются через канал в виде незашифрованного текста. Это может быть нормально в средах, использующих маркерные пароли, которые меняются при каждой аутентификации, но в большинстве сред использование этого протокола будет небезопасно. Кроме того, протокол не поддерживает защиту от воспроизведения пакетов и атак по методу проб и ошибок – частотой и временем попыток входа в систему управляет удаленный узел.



Протокол CHAP, основанный на трехсторонней процедуре установления соединения, выполняется сразу после создания канала и периодически во время его работы, проверяя удостоверение удаленного хоста с использованием трехсторонней процедуры установления соединения.

По окончании этапа создания канала PPP локальный маршрутизатор отправляет сообщение вызова в удаленный узел. Удаленный узел возвращает значение, которое, как правило, рассчитывается с помощью односторонней функции кэширования, чаще всего используется алгоритм Message Digest 5 (MD5). В качестве входных данных для расчета используется пароль и сообщение вызова. Локальный маршрутизатор сравнивает ответ с собственным расчетом ожидаемого значения. Если значения совпадают, аутентификация подтверждается. В противном случае подключение немедленно разрывается.

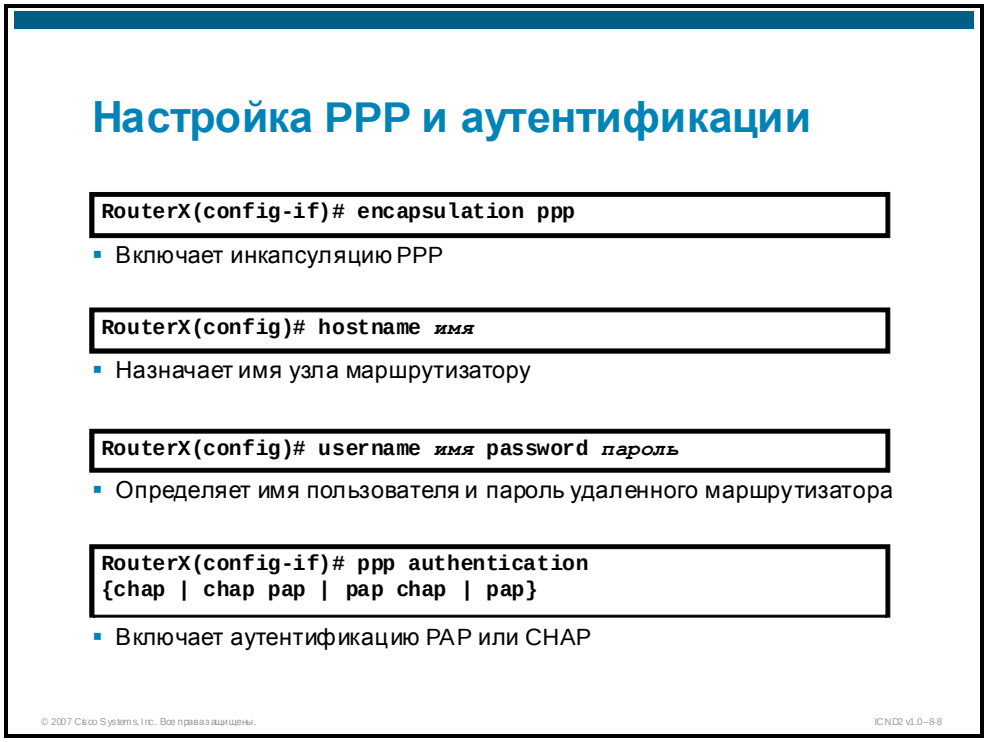
Протокол CHAP обеспечивает защиту от воспроизведения пакетов за счет переменного, уникального и непредсказуемого сообщения вызова. Поскольку сообщение вызова уникально и случайно, значение хэша также будет уникальным и случайным. Использование повторных сообщений вызова позволяет ограничить степень воздействия отдельных атак. Частота и время отправки сообщений вызова определяется локальным маршрутизатором или сервером аутентификации стороннего производителя.

Настройка и проверка PPP

В этом разделе описывается настройка и проверка протокола инкапсуляции PPP.

Чтобы включить инкапсуляцию PPP с аутентификацией PAP или CHAP на интерфейсе, выполните следующие действия:

- Включите инкапсуляцию PPP в качестве протокола второго уровня на интерфейсе.
- (Необязательно) Включите аутентификацию PPP, выполнив следующие действия:
  1. настройте имя хоста маршрутизатора в качестве его идентификатора;
  2. настройте имя пользователя и пароль для аутентификации узла PPP;
  3. выберите метод аутентификации для канала PPP: PAP или CHAP.



Чтобы включить инкапсуляцию PPP, введите команду **encapsulation ppp** в режиме конфигурации интерфейса.

Перед настройкой аутентификации PPP на интерфейсе необходимо настроить инкапсуляцию PPP. Выполните следующие действия, чтобы настроить аутентификацию PAP или CHAP.

Действие 1 Убедитесь, что каждому маршрутизатору назначено имя хоста. Для назначения имени хоста введите команду **hostname** *имя* в режиме конфигурации интерфейса. Это имя должно совпадать с именем, которое ожидает аутентифицирующий маршрутизатор на другой стороне канала.

Действие 2 На каждом из маршрутизаторов настройте имя пользователя и пароль, которые следует ожидать от удаленного маршрутизатора, с помощью команды глобальной конфигурации **username** *имя* **password** *пароль*.

В таблице ниже описываются параметры команды **username**.

Параметры команды username

Параметр	Описание
имя	Имя хоста удаленного маршрутизатора. При вводе имени хоста учитывается регистр.
пароль	Пароль должен быть одинаковым на обоих маршрутизаторах Cisco. В версиях ПО Cisco IOS, предшествующих 11.2, этот пароль был зашифрован. Начиная с версии 11.2, пароль хранится в незашифрованном виде. Чтобы зашифровать пароли маршрутизатора Cisco IOS, введите команду **service password-encryption** в режиме глобальной конфигурации.

Добавьте имя пользователя для всех аутентифицируемых удаленных систем, с которыми работает локальный маршрутизатор. Обратите внимание, что на удаленном устройстве должно быть настроено имя пользователя для локального маршрутизатора и такой же пароль.

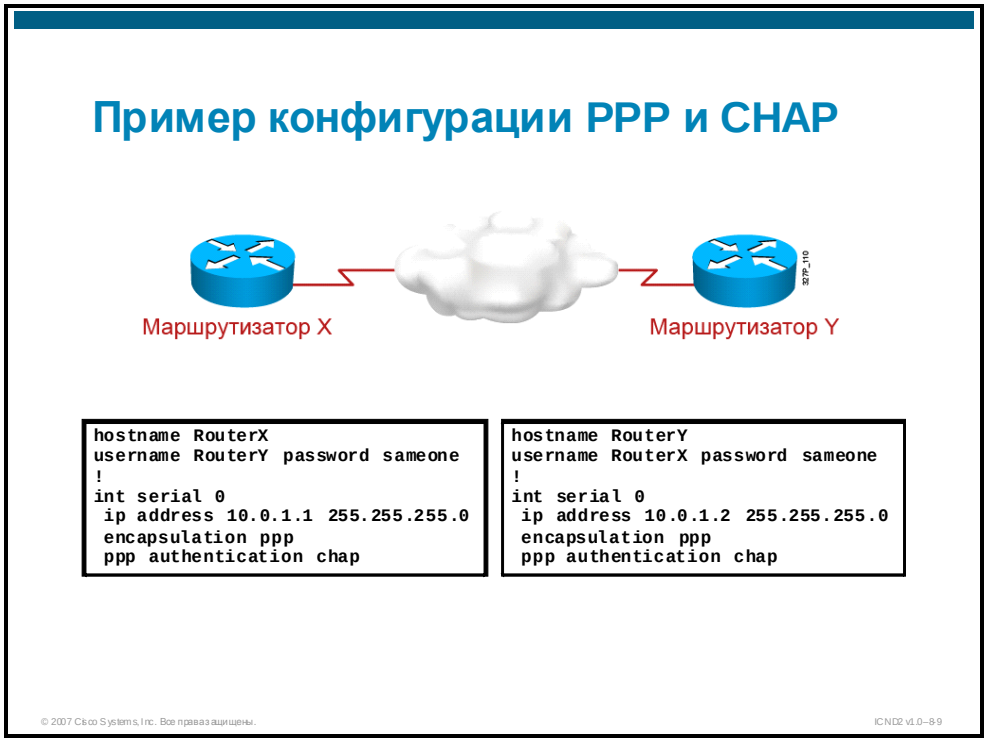
Действие 3 Настройте аутентификацию PPP с помощью команды конфигурации интерфейса **ppp authentication** {**chap** | **chap pap** | **pap chap** | **pap**}.

Если вы введете команду **ppp authentication chap** для интерфейса, все входящие сеансы PPP на этом интерфейсе будут аутентифицироваться по методу CHAP. Аналогично, если вы введете команду **ppp authentication pap** для интерфейса, все входящие сеансы PPP на этом интерфейсе будут аутентифицироваться по методу PAP.

При вводе команды **ppp authentication chap pap** маршрутизатор попытается аутентифицировать все входящие сеансы PPP с помощью CHAP. Если удаленное устройство не поддерживает CHAP, маршрутизатор попытается аутентифицировать сеанс PPP с помощью PAP. Если удаленное устройство не поддерживает ни CHAP ни PAP, аутентификация считается неудачной и сеанс PPP отбрасывается.

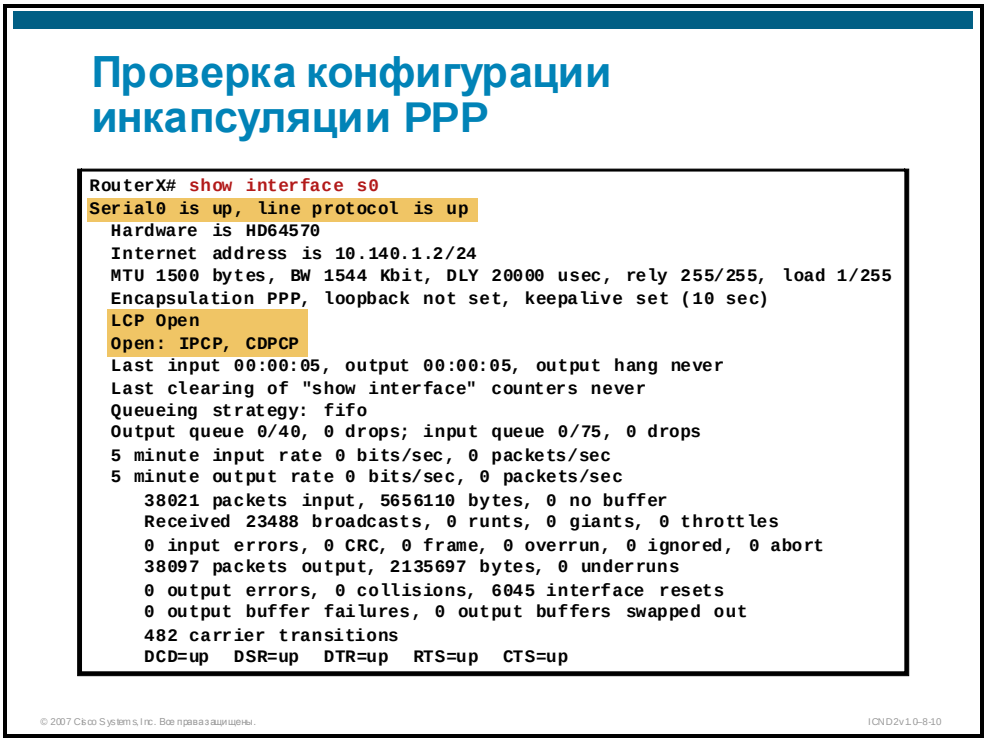
При вводе команды **ppp authentication pap chap** маршрутизатор попытается аутентифицировать все входящие сеансы PPP с помощью PAP. Если удаленное устройство не поддерживает PAP, маршрутизатор попытается аутентифицировать сеанс PPP с помощью CHAP. Если удаленное устройство не поддерживает ни один из протоколов, аутентификация считается неудачной и сеанс PPP отбрасывается.

Примечание Если активированы оба метода, при согласовании канала запрашивается метод, указанный первым. Если удаленный узел предлагает использовать второй метод или отказывается от первого метода, предпринимается попытка применить второй метод.



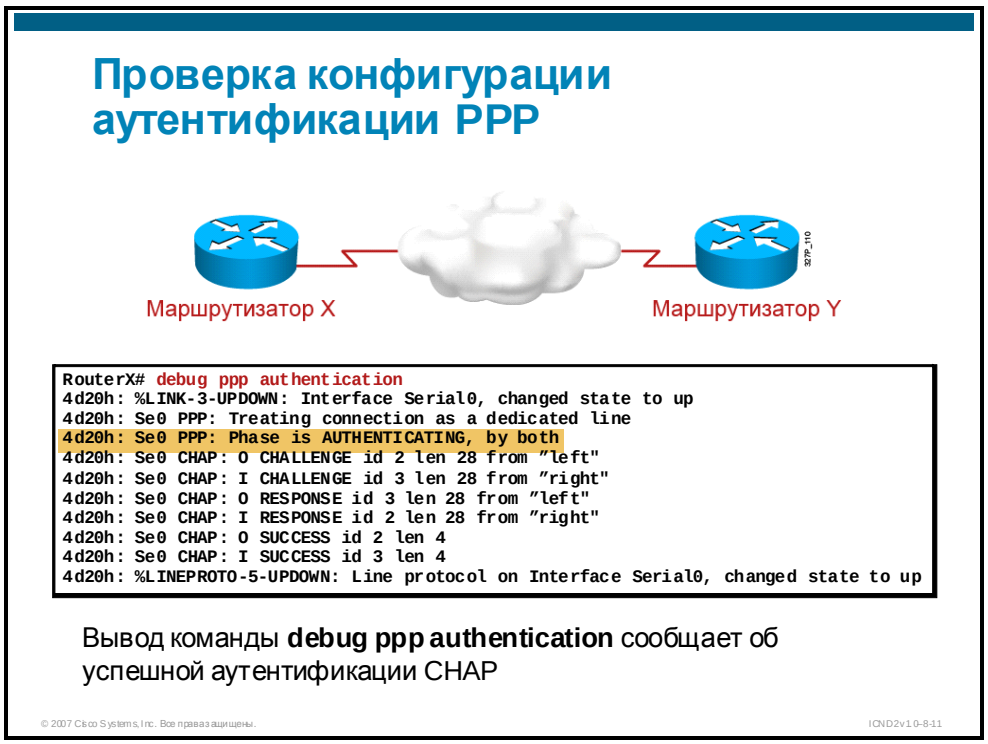
Пример: Конфигурация PPP и CHAP

На рисунке описывается процедура двухстороннего вызова. Имя хоста маршрутизатора должно совпадать с именем пользователя, настроенным на другом маршрутизаторе. Пароли должны быть одинаковы.



Пример: Проверка конфигурации инкапсуляции PPP

Для проверки правильности конфигурации используется команда **show interface**. На рисунке показано, что инкапсуляция PPP задана и протокол LCP установил соединение. На это указывает строка «LCP Open» в выводе команды.



Пример: Проверка конфигурации аутентификации PPP

На рисунке приводится вывод маршрутизатора во время аутентификации CHAP. Поскольку настроена двусторонняя аутентификация (каждый маршрутизатор аутентифицирует сообщения другого маршрутизатора), сообщения отражают процессы аутентификации локального маршрутизатора удаленным маршрутизатором и удаленного маршрутизатора локальным маршрутизатором. Для отображения последовательности операций обмена по мере их выполнения введите команду **debug ppp authentication**.

Чтобы определить, какую аутентификацию CHAP выполняет маршрутизатор – одностороннюю или двустороннюю – найдите одно из следующих сообщений в выводе команды **debug ppp authentication**. Эти сообщения обозначают, что выполняется двухсторонняя аутентификация:

```
Se0 PPP: Phase is AUTHENTICATING, by both
```

Любое из следующих сообщений будет обозначать, что маршрутизаторы выполняют одностороннюю аутентификацию:

```
Se0 PPP: Phase is AUTHENTICATING, by the peer
Se0 PPP: Phase is AUTHENTICATING, by this end
```

Вывод ниже обозначает двустороннюю аутентификацию PAP:

```
Se0 PPP: Phase is AUTHENTICATING, by both       (Двусторонняя
аутентификация)
Se0 PAP: O AUTH-REQ id 4 len 18 from «RouterX»  (Исходящий запрос на
аутентификацию)
Se0 PAP: I AUTH-REQ id 1 len 18 from «RouterY»  (Входящий запрос на
аутентификацию)
Se0 PAP: Authenticating peer RouterY   (Аутентификация входящего
сообщения)
```

```
Se0 PAP: O AUTH-ACK id 1 len 5          (Исходящее подтверждение)
Se0 PAP: I AUTH-ACK id 4 len 5          (Входящее подтверждение)
```

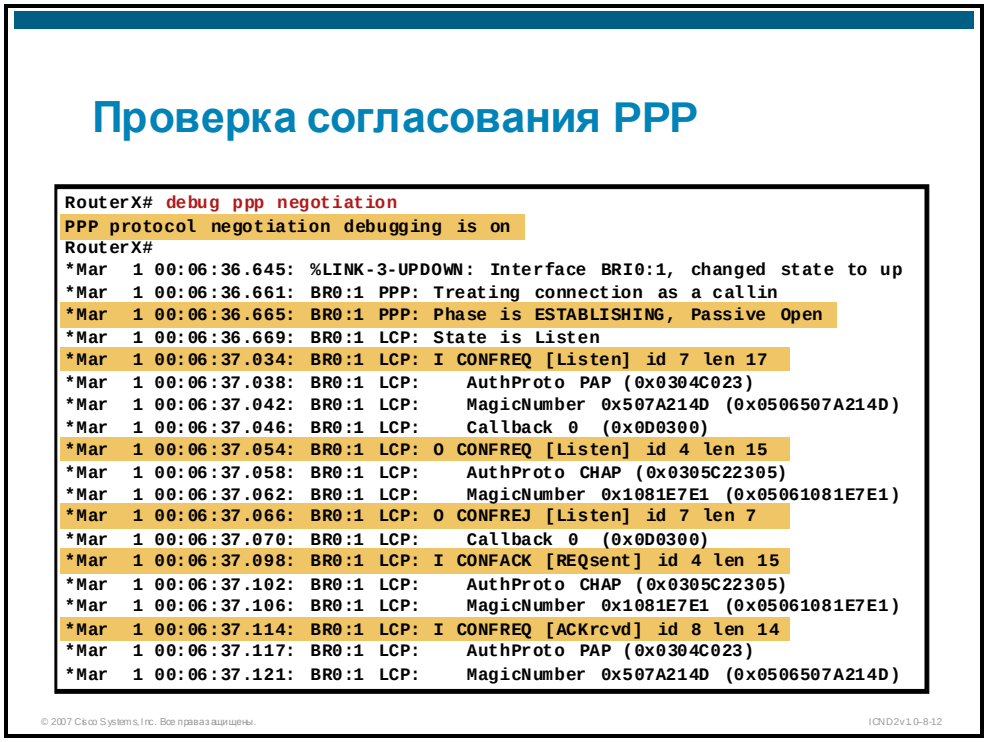
Чтобы определить, выполняет ли маршрутизатор аутентификацию CHAP или PAP, найдите следующие строки в выводе команды **debug ppp authentication**:

- Найдите слово CHAP разделе этапа AUTHENTICATING, см. пример ниже:

```
*Mar 7 21:16:29.468: BR0:1 PPP: Phase is AUTHENTICATING, by
this end
*Mar 7 21:16:29.468: BR0:1 CHAP: O CHALLENGE id 5 len 33 from
«maui-soho-03»
```

- Найдите слово PAP в разделе этапа AUTHENTICATING, см. пример ниже:

```
*Mar 7 21:24:11.980: BR0:1 PPP: Phase is AUTHENTICATING, by
both
*Mar 7 21:24:12.084: BR0:1 PAP: I AUTH-REQ id 1 len 23 from
«maui-soho-01»
```

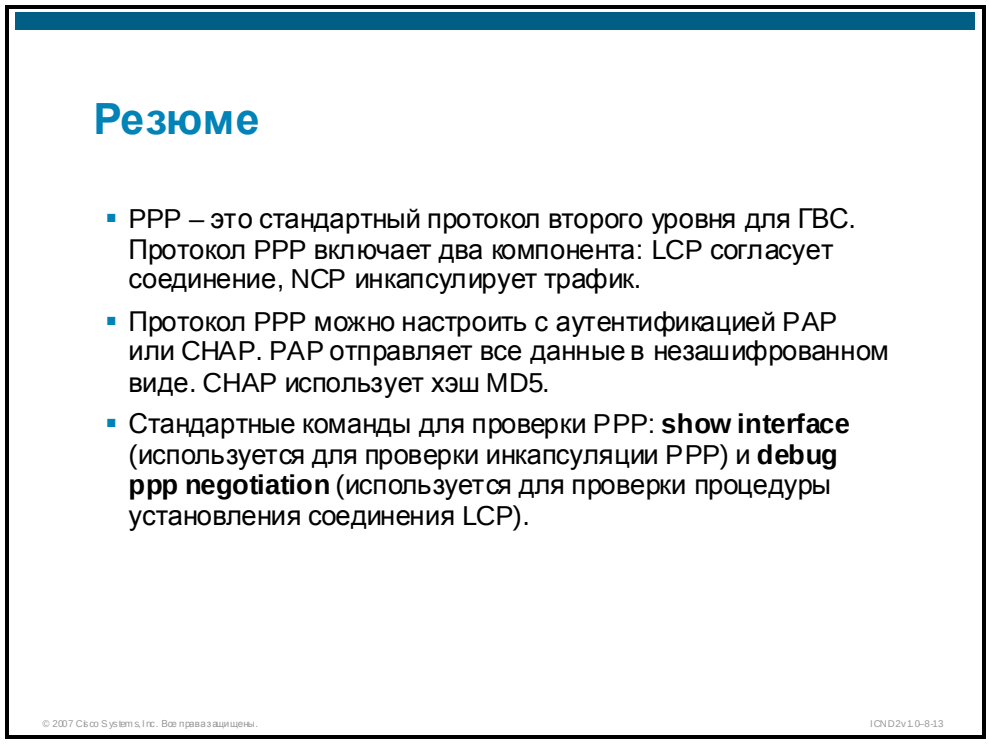
Типовой вывод команды **debug ppp negotiation** описывается ниже:

- **Временная метка:** Полезны временные метки в миллисекундах.
- **Интерфейс и номер интерфейса:** Это поле полезно при поиске и устранении неполадок нескольких соединений или если соединение проходит через несколько интерфейсов.
- **Тип сообщения PPP:** Это поле обозначает тип сообщения в строке – общее сообщение PPP, LCP, CHAP, PAP или IP Control Protocol (IPCP).
- **Направление сообщения:** Буква «I» обозначает входящий пакет, буква «O» – исходящий. Это поле позволяет определить, было ли сообщение создано или получено маршрутизатором.
- **Сообщение:** Это поле обозначает операцию, для которой выполняется согласование.
- **Идентификатор:** Это поле привязывает сообщения запроса и соответствующие сообщения ответа. Поле идентификатора можно использовать для сопоставления ответа входящему сообщению.
- **Длина:** Поле длины обозначает длину информационного поля. Это поле неважно для обычной процедуры поиска и устранения неполадок.

Последнее поле может не отображаться для некоторых сообщений PPP, в зависимости от их назначения.

Резюме

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



Занятие 3

Создание подключения к ГВС с помощью Frame Relay

Обзор

Frame Relay – высокопроизводительный протокол ГВС, стандартизированный ITU-T и широко используемый в США. В этом занятии описывается принцип работы, настройка и устранение неполадок Frame Relay.

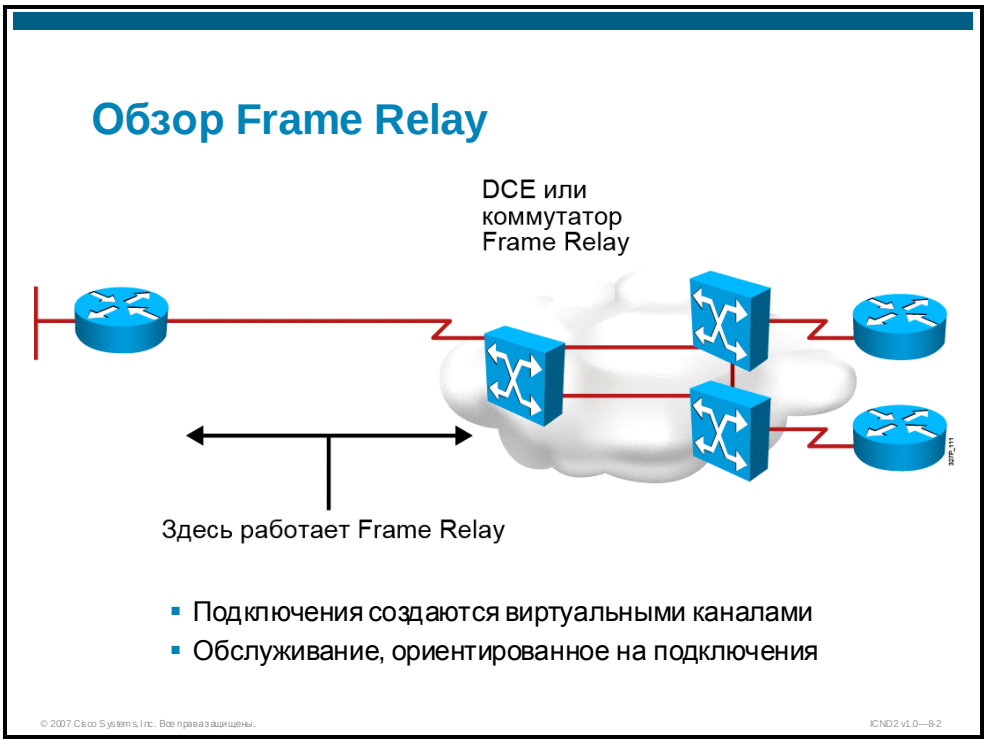
Задачи

По окончании этого занятия вы сможете подключаться к поставщику услуг через сеть и описывать принцип работы и настройку протокола Frame Relay. Это значит, что вы сможете выполнять следующие задачи:

- описывать функции и особенности Frame Relay;
- настраивать Frame Relay;
- проверять соответствие работы протокола Frame Relay параметрам конфигурации.

Общие сведения о Frame Relay

В этом разделе описываются основные функции Frame Relay.



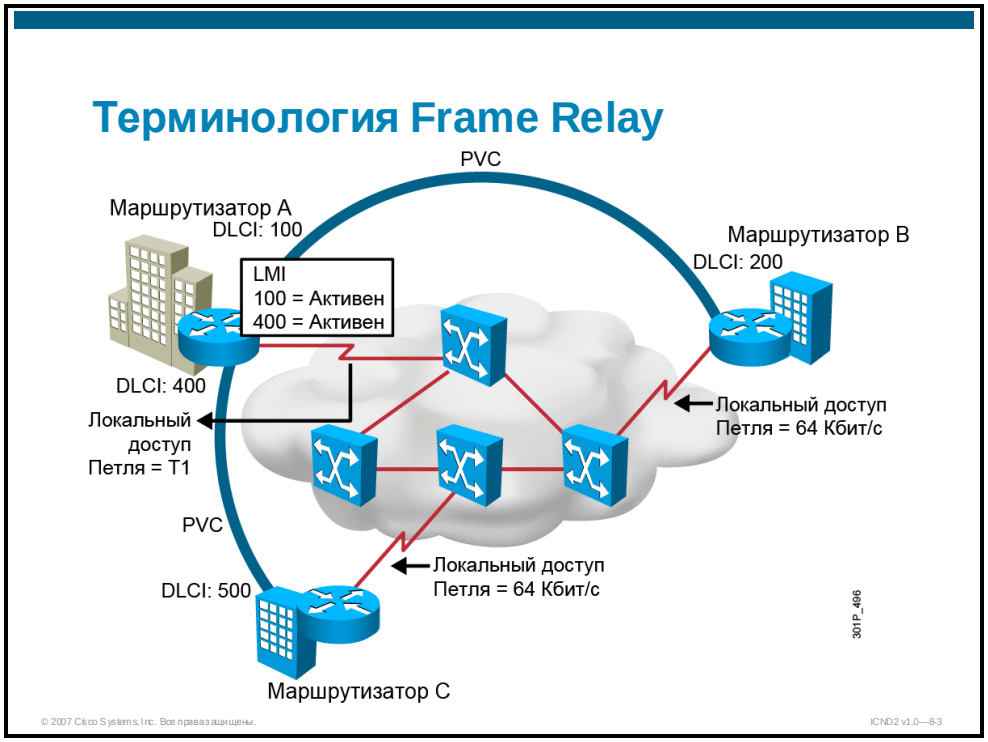
Frame Relay – это технология канального уровня, ориентированная на подключения и оптимизированная для высокой производительности и эффективности. Для защиты от ошибок технология использует протоколы верхнего уровня и надежные цифровые и оптические сети.

Технология Frame Relay определяет процесс соединения между маршрутизатором и коммутационным оборудованием локального доступа, принадлежащим поставщику услуг. Она *не* определяет передачу данных внутри облака Frame Relay поставщика услуг.

Устройства, подключенные к ГВС Frame Relay, можно разделить на две категории:

- **DTE:** Как правило, является оконечным оборудованием. Устройства DTE часто располагаются на площадке заказчика и могут принадлежать ему. Примеры устройств DTE: устройства доступа Frame Relay (FRAD), маршрутизаторы и мосты.
- **DCE:** Устройства для объединения сетей, принадлежащие поставщику услуг. Устройства DCE обеспечивают коммутацию и синхронизацию, а также передают данные через ГВС. В большинстве случаев в качестве коммутаторов ГВС используются коммутаторы Frame Relay.

Технология Frame Relay поддерживает методы статистического мультиплексирования нескольких логических диалогов, которые называются виртуальным каналами (VC), в одном физическом канале, назначая идентификатор подключения каждой паре устройств DTE. Коммутационное оборудование поставщика услуг создает таблицу коммутации, которая сопоставляет идентификаторы подключения и исходящие порты. При получении кадра коммутирующее устройство анализирует идентификатор подключения и передает его в соответствующий исходящий порт. Полный путь к месту назначения формируется до передачи первого кадра.



В обсуждении Frame Relay часто используются следующие термины, они могут немного отличаться от терминов, используемых вашим поставщиком услуг Frame Relay.

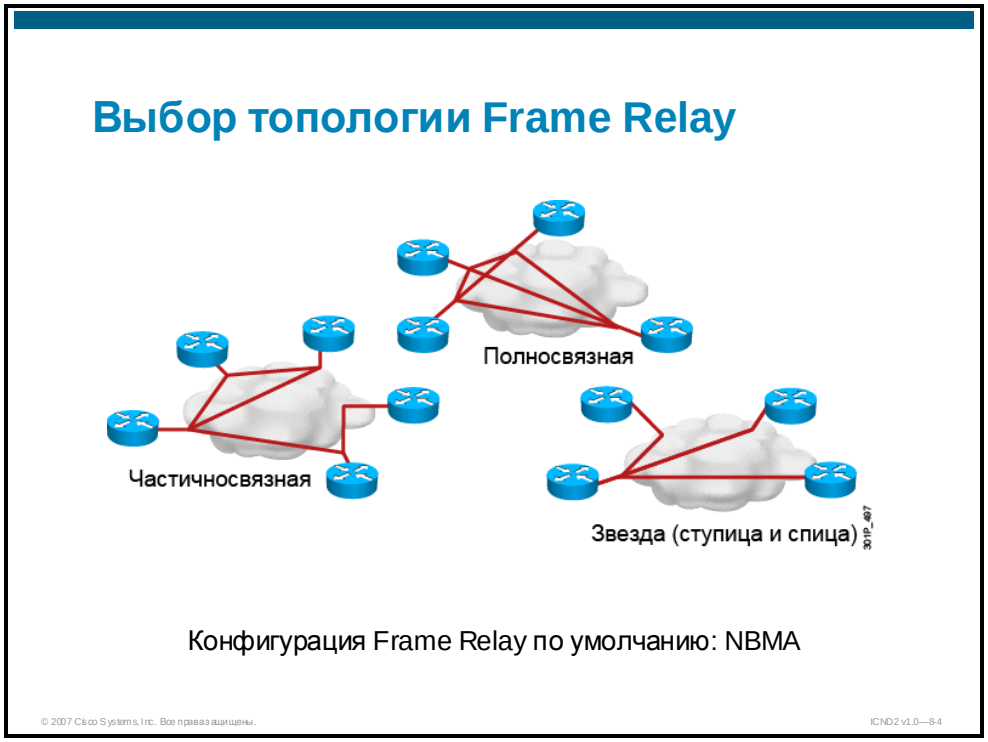
- **Скорость локального доступа:** Тактовая частота (скорость порта) подключения (локального шлейфа) к облаку Frame Relay. Скорость локального доступа – это скорость, с которой данные передаются в сеть и из сети, независимо от других параметров.
- **Виртуальный канал (VC):** Логическому каналу присваивается уникальный идентификатор DLCI, который обеспечивает двустороннюю связь между устройствами DTE. Несколько виртуальных каналов мультиплексируются в один физический канал для передачи через сеть. Эта функция часто упрощает архитектуру оборудования и сети, необходимую для соединения нескольких устройств DTE. Виртуальный канал может проходить через любое количество промежуточных устройств DCE (коммутаторов Frame Relay). Виртуальный канал может быть постоянным (PVC) или коммутируемым (SVC).
- **PVC:** Обеспечивает постоянные подключения, которые используются для частой и регулярной передачи данных между устройствами DTE через сеть Frame Relay. Связь через PVC не требует процедур установки и разрыва вызова, используемых в SVC.
- **SVC:** Обеспечивает временные подключения для редкой передачи данных между устройствами DTE через сеть Frame Relay. Каналы SVC создаются динамически (по требованию) и разрываются после завершения передачи.

Примечание	С появлением стандартов ANSI T1.617 и ITU-T Q.933 (уровень 3), а также Q.922 (уровень 2), в технологии Frame Relay введена поддержка SVC. Версии Cisco IOS 11.2 и выше поддерживают каналы Frame Relay SVC. Каналы Frame Relay SVC не рассматриваются в этом курсе.

- **Идентификатор DLCI:** 10-битное число в поле адреса заголовка кадра Frame Relay, который идентифицирует виртуальный канал. Идентификаторы DLCI значимы в локальном масштабе, так как указывают на точку между локальным маршрутизатором и локальным коммутатором Frame Relay, к которому подключено устройство с DLCI. Поэтому устройства на противоположной стороне подключения могут использовать другие значения DLCI для того же виртуального канала.
- **Гарантированная скорость передачи данных (CIR):** Определяет максимальную среднюю скорость передачи данных, которая гарантируется сетью при нормальных условиях. При подписке на услуги Frame Relay вы указываете скорость локального доступа, например 56 Кбит/с или T1. Как правило, скорость CIR указывается для каждого идентификатора DLCI. Если вы передаете данные со скоростью, превышающей CIR для того или иного идентификатора DLCI, сеть отмечает соответствующую часть кадров битом DE (подлежит отбрасыванию). Сеть делает все возможное для доставки всех пакетов, но отбрасывает пакеты DE при перегрузке. Во многих недорогих услугах Frame Relay используется нулевая скорость CIR. Нулевая скорость CIR означает, что все кадры имеют атрибут DE и сеть может отбрасывать их при необходимости. Бит DE находится в поле адреса заголовка кадра Frame Relay.
- **Протокол Inverse ARP:** Метод динамического сопоставления локального идентификатора DLCI и адреса сетевого уровня удаленного маршрутизатора. Inverse ARP позволяет маршрутизатору автоматически обнаруживать сетевой адрес удаленного устройства DTE, связанного с виртуальным каналам.
- **Протокол LMI (Local Management Interface):** Стандарт сигнализации между маршрутизатором (устройством DTE) и локальным коммутатором Frame Relay (устройством DCE), управляющий подключением и состоянием подключения между маршрутизатором и коммутатором Frame Relay.
- **Бит FECN (Forward explicit congestion notification):** Бит в поле адреса заголовка Frame Relay. Механизм FECN применяется, когда устройство DTE отправляет кадры Frame Relay в сеть. Если сеть перегружена, устройства DCE (коммутаторы Frame Relay) устанавливают значение 1 для бита FECN. Когда эти кадры достигают DTE-устройства назначения, адрес с битом FECN сообщает, что пройденный путь от источника к месту назначения, перегружен. Устройство DTE может передать эту информацию для обработки протоколами более высокого уровня. В зависимости от среды, будет запущен механизм управления потоком или индикатор будет проигнорирован.
- **Бит BECN (Backward explicit congestion notification):** Бит в поле адреса заголовка Frame Relay. Устройства DCE устанавливают значение 1 для бита BECN в кадрах, которые передаются в направлении, противоположном передаче кадров с битом FECN. Установка значения 1 для бита BECN сообщает принимающему устройству DTE, что путь через сеть перегружен. Устройство DTE может передать эту информацию для обработки протоколами более высокого уровня. В зависимости от среды, будет запущен механизм управления потоком или индикатор будет проигнорирован.

Пример: Терминология Frame Relay – DLCI

Как показано на рисунке, маршрутизатор A имеет два виртуальных канала, настроенных на одном физическом интерфейсе. DLCI 100 идентифицирует виртуальный канал, подключенный к маршрутизатору B. DLCI 400 идентифицирует виртуальный канал, подключенный к маршрутизатору C. На другой стороне для идентификации виртуального канала будет использоваться другое значение DLCI.

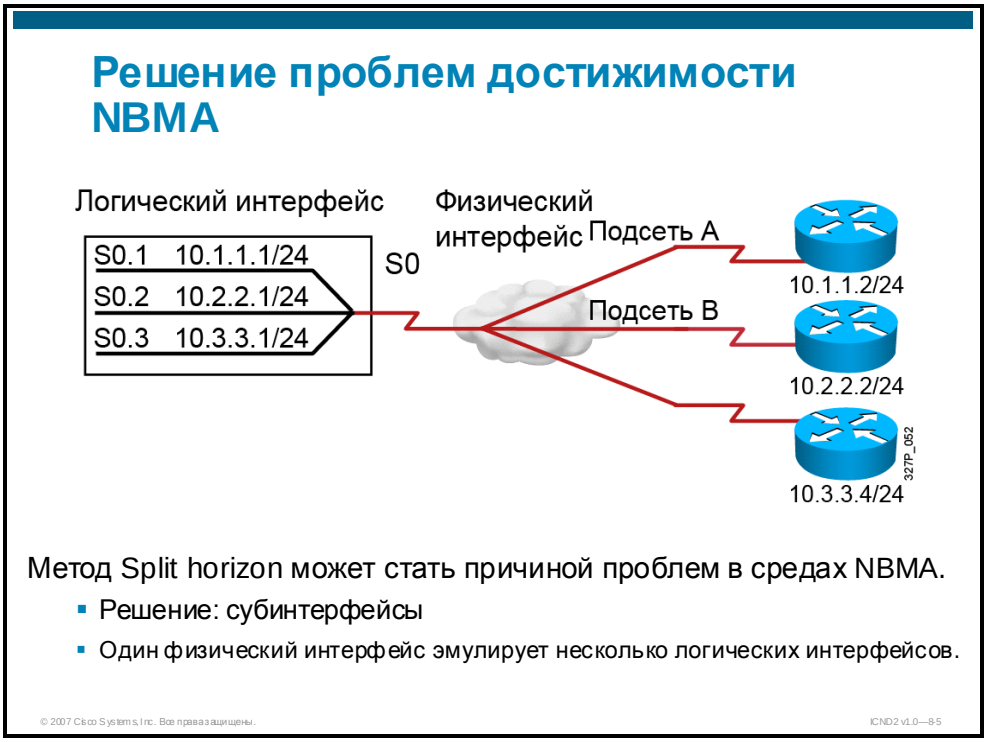


Frame Relay позволяет объединять удаленные площадки в различные топологии, см. ниже:

- **Топология «Звезда»:** Удаленные площадки подключаются к центральной площадке, на которой, как правило, предоставляется доступ к услуге или приложению. Топология «Звезда» также известна как конфигурация «Ступица и спица» и является самой популярной сетевой топологией Frame Relay. Эта топология – самая экономичная, так как требует минимального числа каналов PVC. На рисунке центральный маршрутизатор предоставляет многоточечное подключение, так как использует один интерфейс для соединения нескольких каналов PVC.
- **Полносвязная ячеистая топология:** Все маршрутизаторы имеют виртуальные каналы ко всем прочим местам назначения. Полносвязная ячеистая топология стоит дорого, но обеспечивает прямое подключение каждой площадки ко всем остальным площадкам, что в свою очередь обеспечивает резервирование. Когда канал становится недоступным, маршрутизатор может перенаправить трафик через другую площадку. С увеличением числа узлов такая топология может стать чрезмерно дорогой. Общее число каналов, необходимых для реализации полносвязной ячеистой топологии, рассчитывается по формуле $n\ (n-1)\ /\ 2$, где n – количество узлов. Например, для полносвязной сети из 10 узлов необходимо 45 каналов: $10\ (10-1)\ /\ 2$.
- **Частичносвязная ячеистая топология:** Отдельные площадки имеют подключения ко всем остальным площадкам. В зависимости от режима трафика в сети, могут потребоваться дополнительные каналы PVC для удаленных узлов, через которые проходят плотные потоки трафика.

По умолчанию сеть Frame Relay предоставляет соединение NBMA (нешироковещательный множественный доступ) между удаленными площадками. Среда NBMA обрабатывается как любая другая широковещательная среда Ethernet, в которой все маршрутизаторы находятся в одной подсети.

Однако для сокращения затрат облака NBMA, как правило, создаются по топологии «Звезда». При использовании топологии «Звезда» физическая топология обеспечивает множественный доступ, который предлагает среда Ethernet, поэтому маршрутизаторы могут не иметь отдельных каналов PVC ко всем удаленным маршрутизаторам подсети. Метод Split horizon – одна из главных проблем, которые возникают в среде Frame Relay, когда несколько каналов PVC работают на одном интерфейсе.

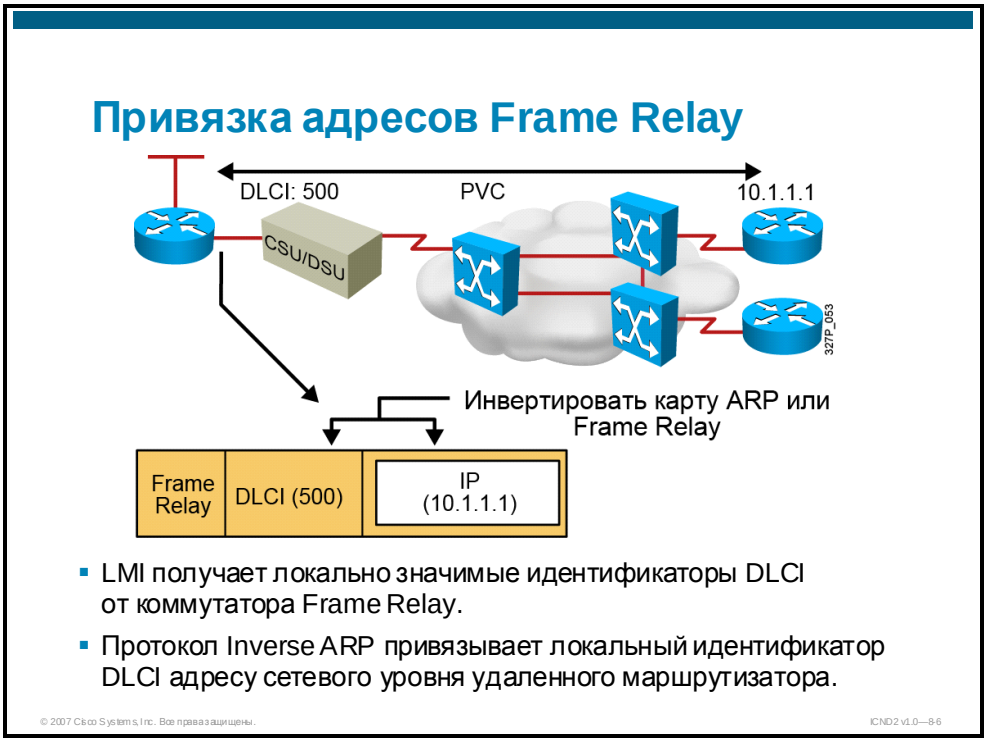


В любой топологии Frame Relay, в которой один интерфейс используется для соединения нескольких площадок, могут возникнуть проблемы, связанные с тем, что Frame Relay является средой NBMA. Топология Frame Relay NBMA является причиной двух проблем.

- **Достижимость обновлений маршрутизации:** Обновления Split horizon исключают петли маршрутизации, предотвращая пересылку обновлений, полученных на интерфейсе, с этого интерфейса. В сети Frame Relay с топологией «ступица и спицы» (звезда) удаленный маршрутизатор (спица) отправляет обновление в маршрутизатор штаб-квартиры (ступица), который использует один физический интерфейс для соединения нескольких PVC. Маршрутизатор штаб-квартиры получает широковещательное обновление маршрутизации на физическом интерфейсе, но не может переслать обновление другим удаленным маршрутизаторам (спицам) через этот физический интерфейс. Метод Split horizon не является проблемой, если на интерфейсе настроен один канал PVC, так как такое подключение аналогично подключению «точка-точка».
- **Широковещательная репликация:** При использовании маршрутизаторов с поддержкой многоточечных подключений на одном интерфейсе, который завершает несколько каналов PVC, маршрутизатор должен реплицировать широковещательные пакеты, такие как обновления маршрутизации, на всех каналах PVC к удаленным маршрутизаторам. Эти реплицированные широковещательные пакеты потребляют значительную полосу пропускания и вызывают значительные колебания задержки при передаче пользовательского трафика.

Для решения проблемы достижимости обновлений маршрутизации используется несколько методов.

- Один из способов решения проблем функции Split horizon – отключить эту функцию. Однако с таким решением связаны две проблемы. Во-первых, хотя большинство протоколов сетевого уровня, таких как IP, позволяют отключить Split horizon, не все протоколы предлагают эту возможность. Во-вторых, отключение Split horizon повышает вероятность образования петель маршрутизации.
- Другой способо – использование полносвязной ячеистой топологии, но такая топология означает повышение затрат.
- Последний способов – применение субинтерфейсов. Чтобы включить пересылку широковещательных обновлений маршрутизации в сети Frame Relay с топологией «Звезда», можно настроить на маршрутизаторе логические интерфейсы (субинтерфейсы), которые представляют собой логические разделы физического интерфейса. В средах маршрутизации, использующих метод Split horizon, обновления маршрутизации, полученные на одном субинтерфейсе, могут быть отправлены из другого субинтерфейса. В конфигурации субинтерфейсов каждый виртуальный канал настраивается как подключение «точка-точка», что позволяет каждому субинтерфейсу работать аналогично арендованному каналу. Каждый субинтерфейс Frame Relay «точка-точка» находится в отдельной подсети.



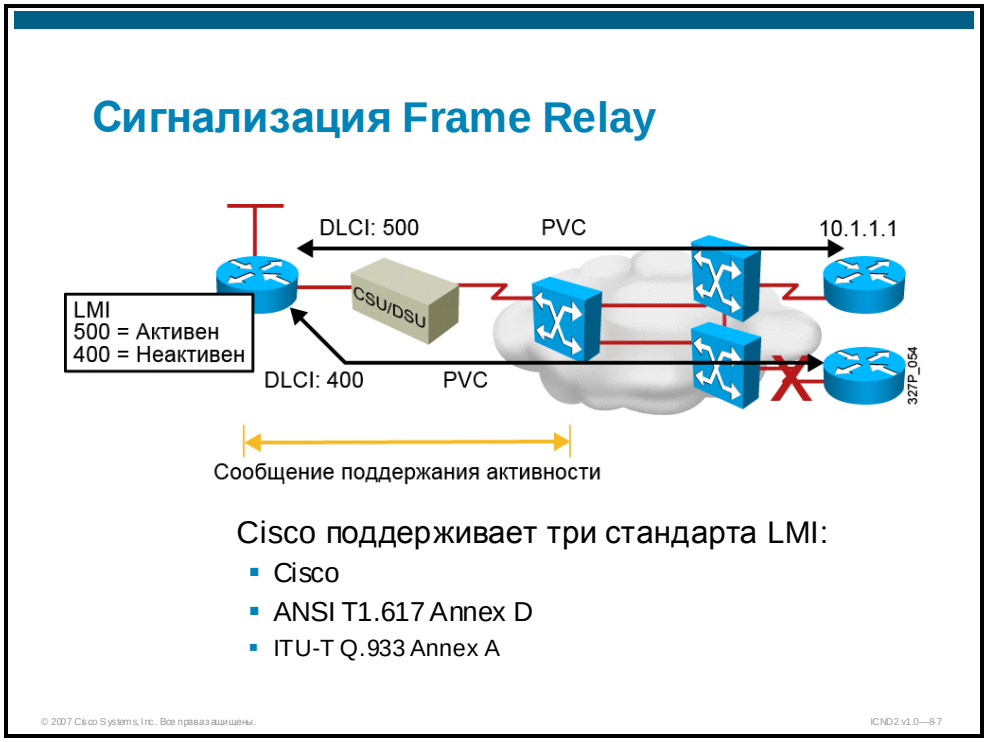
Для подключения Frame Relay необходимо, чтобы локальный идентификатор DLCI в виртуальном канале был привязан к адресу назначения сетевого уровня, например IP-адресу. Маршрутизаторы могут автоматически извлекать локальный идентификатор DLCI из локального коммутатора Frame Relay с помощью протокола LMI.

На маршрутизаторах Cisco локальный идентификатор DLCI может динамически привязываться к адресу сетевого уровня удаленного маршрутизатора с помощью протокола Inverse ARP. Протокол Inverse ARP назначает идентификатор DLCI адресу сетевого уровня маршрутизатора на следующем переходе. Протокол Inverse ARP описывается в стандарте RFC 1293.

Пример: Привязка адресов Frame Relay

Как показано на рисунке, с помощью протокола Inverse ARP маршрутизатор слева может автоматически обнаруживать IP-адрес удаленного маршрутизатора, а затем привязывать его к локальному маршрутизатору DLCI. В этом случае локальный DLCI 500 привязан к IP-адресу 10.1.1.1. Поэтому, когда маршрутизатор отправляет данные по адресу 10.1.1.1, используется DLCI 500.

В качестве альтернативы автоматической привязке локальных идентификаторов DLCI адресам сетевого уровня удаленных маршрутизаторов с помощью Inverse ARP, можно настроить статическую привязку Frame Relay в таблице соответствия.



LMI – это стандарт сигнализации между маршрутизатором и коммутатором Frame Relay. LMI управляет подключением и поддерживает статус подключения между устройствами.

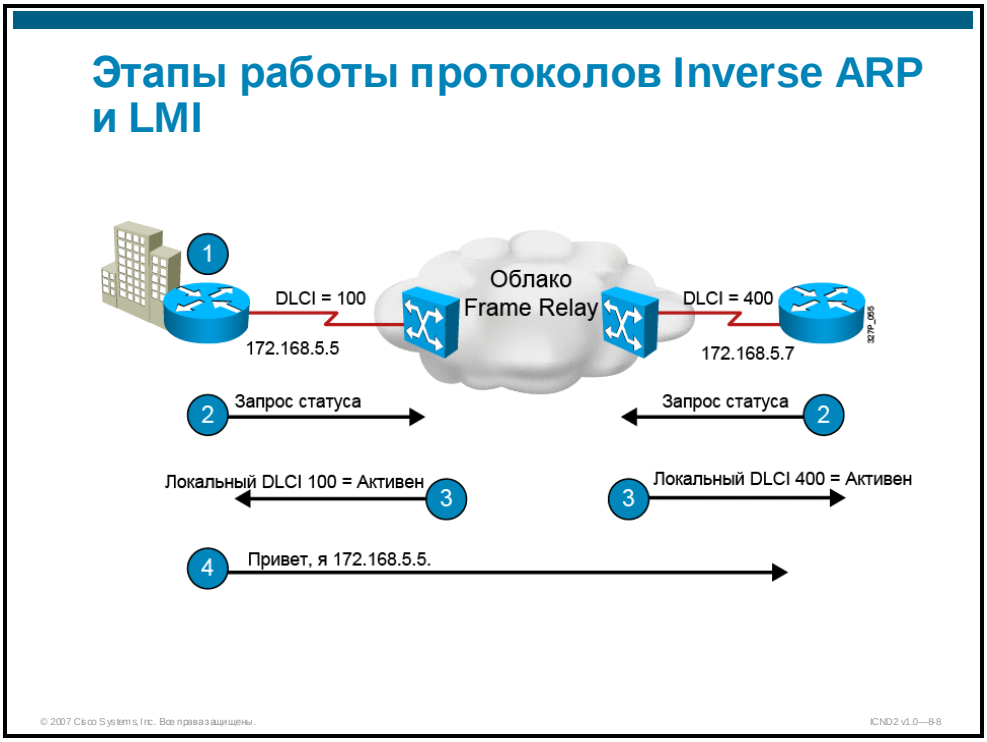
Хотя протокол LMI можно настраивать вручную, начиная с версии Cisco IOS 11.2 маршрутизатор Cisco пытается автоматически определить тип LMI, используемый коммутатором Frame Relay. Маршрутизатор отправляет несколько полных запросов состояния LMI коммутатору Frame Relay. Коммутатор Frame Relay возвращает один или несколько типов LMI, и маршрутизатор настраивается в соответствии с последним полученным типом. Маршрутизаторы Cisco поддерживает три типа LMI:

- **Cisco:** Тип LMI, совместно заданный компаниями Cisco, StrataCom, Northern Telecom (Nortel) и Digital Equipment Corporation.
- **ANSI:** ANSI T1.617 Annex D.
- **Q.933A:** ITU-T Q.933 Annex A.

Кроме того, нужный тип LMI можно выбрать вручную для гарантии правильной работы Frame Relay.

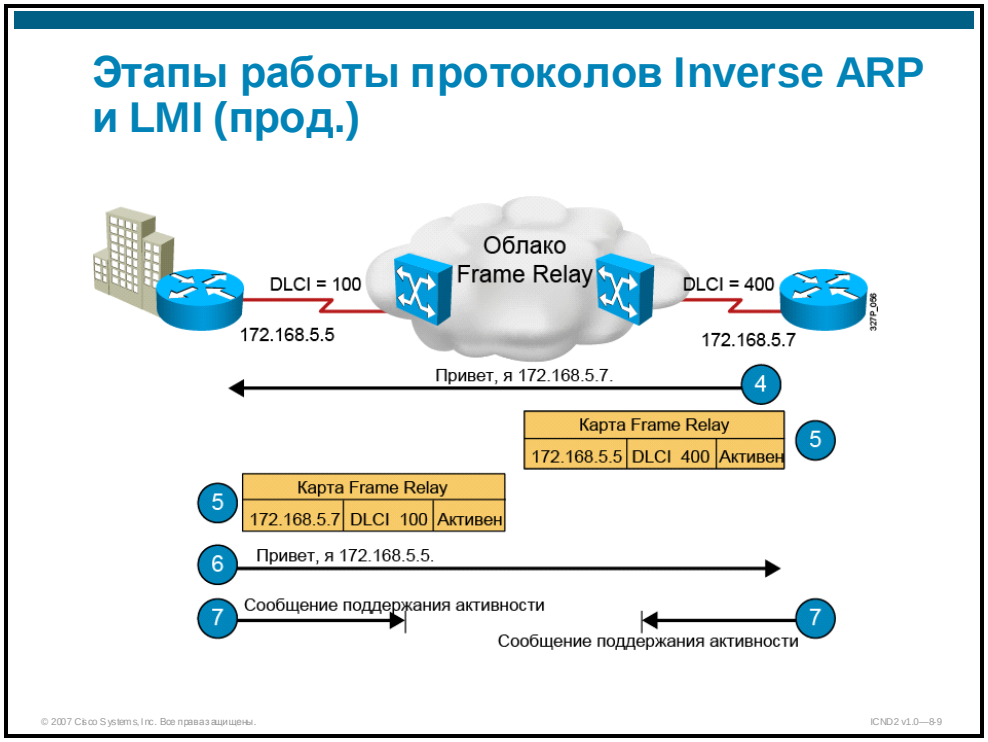
Когда маршрутизатор получает данные LMI, он переводит свой виртуальный канал в одно из следующих состояний:

- **Active:** Указывает, что виртуальный канал активен и маршрутизаторы могут обмениваться данными через сеть Frame Relay.
- **Inactive:** Указывает, что локальное подключение к коммутатору Frame Relay активно, но подключение удаленного маршрутизатора к удаленному коммутатору Frame Relay не работает.
- **Deleted:** Указывает, что тип LMI не получен от коммутатора Frame Relay или что между маршрутизатором и локальным коммутатором Frame Relay нет соединения.



Ниже приводится общее описание работы протокола Inverse ARP и сигнализации LMI в подключении Frame Relay.

1. Каждый маршрутизатор подключается к коммутатору Frame Relay через CSU/DSU.
2. При настройке Frame Relay на интерфейсе маршрутизатор отправляет сообщение запроса состояния LMI коммутатору Frame Relay. Это сообщение оповещает коммутатор о состоянии маршрутизатора и запрашивает у коммутатора данные о состоянии подключения виртуальных каналов маршрутизатора.
3. В ответ на запрос коммутатор Frame Relay отправляет сообщение о состоянии LMI, которое включает локальные идентификаторы DLCI каналов PVC к удаленным маршрутизаторам, которым локальный маршрутизатор может передавать данные.
4. Для каждого активного DLCI каждый маршрутизатор отправляет пакет Inverse ARP, чтобы объявить о себе.



5. Когда маршрутизатор получает сообщение Inverse ARP, он создает запись привязки в таблице соответствия Frame Relay, которая включает идентификатор DLCI и адрес сетевого уровня удаленного маршрутизатора. Обратите внимание, что в качестве DLCI маршрутизатора используется локальный DLCI, а не DLCI удаленного маршрутизатора. В таблице Frame Relay может отображаться любое из трех состояний подключения.

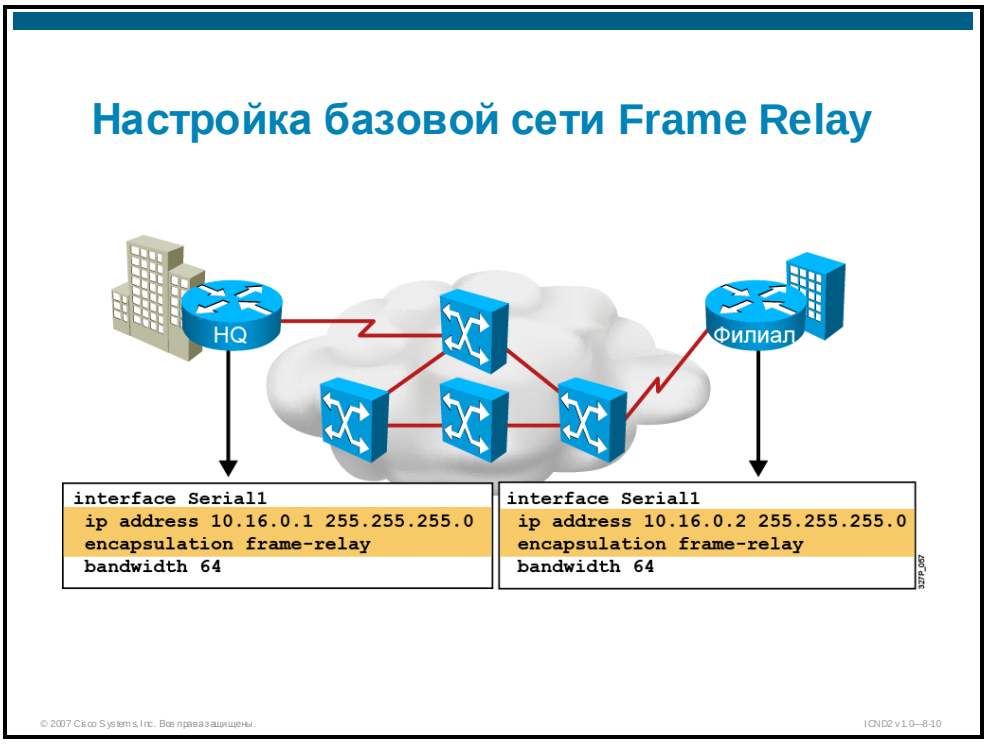
Примечание	Если протокол Inverse ARP не работает или не поддерживается на удаленном маршрутизаторе, необходимо вручную настроить статические таблицы Frame Relay, сопоставляющие локальные идентификаторы DLCI и удаленные адреса сетевого уровня.

6. Каждые 60 секунд маршрутизаторы отправляют сообщения Inverse ARP по всем активным идентификаторам DLCI. Каждые 10 секунд маршрутизатор обменивается данными LMI с коммутатором (сообщения Keepalive).

7. Маршрутизатор изменяет состояние каждого идентификатора DLCI на «Active», «Inactive» или «Deleted», в зависимости от сообщения ответа LMI, полученного от коммутатора Frame Relay.

Настройка Frame Relay

В этом разделе описывается настройка базового канала Frame Relay PVC.



Базовая конфигурация Frame Relay предполагает настройку Frame Relay на одном или нескольких физических интерфейсах, а также поддержки протоколов LMI и Inverse ARP на маршрутизаторах.

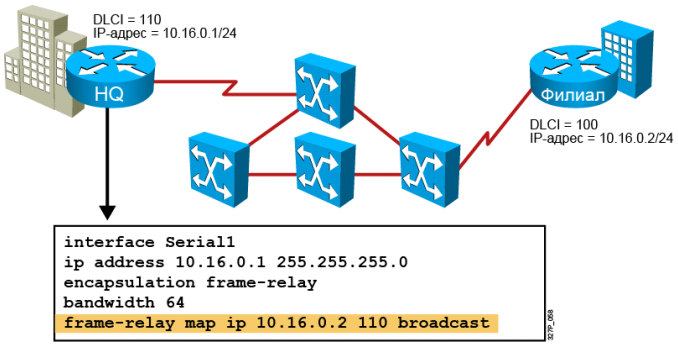
В таблице ниже описываются действия по настройкн базовой сети Frame Relay.

Действия по настройке базовой сети Frame Relay

№	Действие	Примечания
1.	Выберите интерфейс, на котором необходимо настроить Frame Relay. Используйте режим конфигурации интерфейса. `RouterX(config)# interface serial1`	После перехода в режим конфигурации интерфейса приглашение командной строки изменится с (config) # на (config-if) #.
2.	Настройте адрес сетевого уровня, например IP-адрес. `RouterX(config-if)# ip address 10.16.0.1 255.255.255.0`	

№	Действие	Примечания
3.	Выберите тип инкапсуляции Frame Relay, который будет применяться для инкапсуляции сквозного трафика данных. Используйте команду конфигурации интерфейса **encapsulation frame-relay**. `RouterX(config-if)# encapsulation frame-relay [cisco|ietf]`	Параметр **cisco** активирует инкапсуляцию Cisco. Используйте этот параметр, если подключение выполняется к другому маршрутизатору Cisco. Это значение по умолчанию. Параметр **ietf** активирует инкапсуляцию по стандарту IETF (RFC 1490). Выберите этот параметр, если выполняется подключение к маршрутизатору другого производителя.
4.	Создайте подключение LMI с помощью команды конфигурации интерфейса **frame-relay lmi-type**. `RouterX(config-if)# frame-relay lmi-type {ansi | cisco | q933a}`	Эта команда необходима только в версиях Cisco IOS 11.1 и ниже. В версии Cisco IOS 11.2 и выше тип LMI определяется автоматически и его настройка не требуется. По умолчанию используется параметр **cisco**. Тип LMI выбирается для каждого интерфейса, данные о выбранном типе можно вывести с помощью команды EXEC **show interfaces**.
5.	Настройте полосу пропускания интерфейса с помощью команды конфигурации интерфейса **bandwidth** [**kilobits**]. `RouterX(config-if)# bandwidth 64`	Эта команда влияет на операции маршрутизации, выполняемые такими протоколами, как IGRP, EIGRP и OSPF, а также на другие расчеты.
6.	Включите протокол Inverse ARP, если он отключен на маршрутизаторе. Используйте команду конфигурации интерфейса **frame-relay inverse-arp** [*протокол*] [*dlci*]. `RouterX(config-if)# frame-relay inverse-arp ip 16`	*протокол:* Поддерживаемые протоколы: IP, IPX, AppleTalk, DECnet, Banyan VINES и XNS. *dlci*: идентификатор DLCI на локальном интерфейсе, с которым будет производиться обмен сообщениями Inverse ARP. Inverse ARP включен по умолчанию и не отображается в выводе конфигурации.

Настройка статической таблицы соответствия Frame Relay



Статическую таблицу соответствия Frame Relay следует настраивать в следующих случаях:

- Удаленный узел Frame Relay не поддерживает Inverse ARP
- Необходим контроль над широковещательным трафиком в канале PVC
- Необходимо использовать разные типы инкапсуляции Frame Relay для каналов PVC

Если удаленный маршрутизатор не поддерживает Inverse ARP, узлы Frame Relay будут использовать разные типы инкапсуляции Frame Relay. Если вы хотите контролировать широковещательный и групповой трафик канала PVC, необходимо статически привязать идентификатор DLCI к адресу сетевого уровня удаленного маршрутизатора. Такие записи называются статическими записями таблицы соответствия Frame Relay.

Используйте следующую команду, чтобы статически привязать удаленный адрес сетевого уровня локальному идентификатору DLCI.

```
RouterX(config-if)# frame-relay map протокол адрес протокола
dlci [broadcast] [ietf | cisco | payload-compress packet-by-
packet]
```


Параметры команды frame-relay map

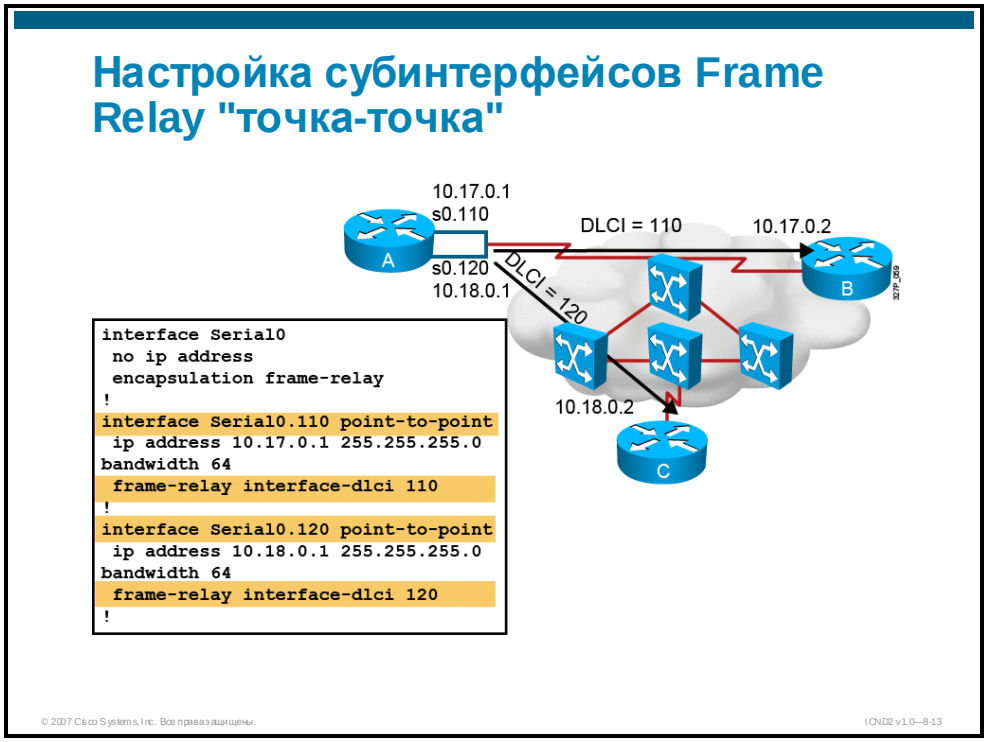
Параметр	Описание
протокол	Задает поддерживаемый протокол (моста или LLC). Доступные варианты AppleTalk, DECnet, DLSW, IP, IPX, LLC, LLC2, RSRB, Banyan VINES и XNS.
адрес протокола	Задает адрес сетевого уровня интерфейса целевого маршрутизатора.
dlci	Задает локальный идентификатор DLCI, который используется для подключения к удаленному адресу протокола.
broadcast	(Необязательно) Разрешает широковещательные и групповые рассылки в виртуальном канале. Это позволяет использовать протоколы динамической маршрутизации в виртуальном канале.
ietf | cisco	Включает инкапсуляцию IETF или Cisco.
payload-compress packet-by-packet	(Необязательно) Включает сжатие полезной части пакетов с помощью метода Stacker. Это проприетарный метод сжатия компании Cisco.

Настройка субинтерфейсов Frame Relay

- "Точка-точка"
  - Субинтерфейсы работают как арендованные каналы.
  - Для каждого субинтерфейса "точка-точка" требуется отдельная подсеть.
  - Режим "точка-точка" применяется в топологиях "Звезда".
- Многоточечные
  - Субинтерфейсы действуют как сети NBMA и не решают проблем, связанных с методом Split horizon.
  - Многоточечные субинтерфейсы позволяют экономить адресное пространство, так как используют одну подсеть.
  - Многоточечные интерфейсы применяются в полносвязной и частичносвязной ячеистой топологии.

Субинтерфейсы можно настроить в одном из двух режимов:

- **«Точка-точка»:** Один субинтерфейс «точка-точка» используется для создания одного канала PVC к физическому интерфейсу или субинтерфейсу удаленного маршрутизатора. В этом случае каждая пара маршрутизаторов, участвующих в соединении «точка-точка», находится в отдельной подсети, и каждому субинтерфейсу присваивается один идентификатор DLCI. В среде «точка-точка» трафик обновлений не подчиняется правилу Split horizon, так как каждый субинтерфейс работает как интерфейс «точка-точка».
- **Многоточечный:** Один многоточечный субинтерфейс используется для создания нескольких каналов PVC к нескольким субинтерфейсам или физическим интерфейсам удаленных маршрутизаторов. В этом случае все интерфейсы, участвующие в соединении, находятся в одной подсети. В этой среде субинтерфейс действует как стандартный интерфейс NBMA Frame Relay, поэтому трафик обновлений подчиняется правилу Split horizon.



Пример: Настройка субинтерфейсов Frame Relay «точка-точка»

На этом рисунке маршрутизатор A имеет два субинтерфейса «точка-точка». Субинтерфейс s0.110 подключается к маршрутизатору B, субинтерфейс s0.120 подключается к маршрутизатору C. Каждый субинтерфейс находится в отдельной подсети.

Выполните следующие действия, чтобы настроить субинтерфейсы на физическом интерфейсе.

Действие 1 Выберите интерфейс, на котором необходимо настроить субинтерфейсы, и перейдите в режим конфигурации интерфейса.

Действие 2 Удалите адреса сетевого уровня, назначенные физическому интерфейсу, назначьте адрес сетевого уровня субинтерфейсу.

Действие 3 Настройте инкапсуляцию Frame Relay.

Действие 4 С помощью команды ниже выберите субинтерфейс, который необходимо настроить, сделайте его субинтерфейсом «точка-точка».

```
RouterX(config-if)# interface serial номер.номер
субинтерфейса point-to-point}
```

Параметры команды interface serial

Параметры команды interface serial	Описание
.номер субинтерфейса	Номера субинтерфейса выбираются из диапазона 1 – 4 294 967 293. Номер перед точкой (.) – это номер интерфейса, к которому принадлежит субинтерфейс.
point-to-point	Выберите этот параметр, если необходимо, чтобы каждая пара маршрутизаторов, участвующих в подключении «точка-точка» имела собственную подсеть.

Примечание Необходимо указать параметр **multipoint** или **point-to-point**, значение по умолчанию не определено.

Действие 5 Если интерфейс настроен в режиме «точка-точка», для него необходимо настроить локальный идентификатор DLCI, чтобы отличать субинтерфейс от физического интерфейса. Команда для настройки локального идентификатора DLCI на субинтерфейсе приводится ниже.

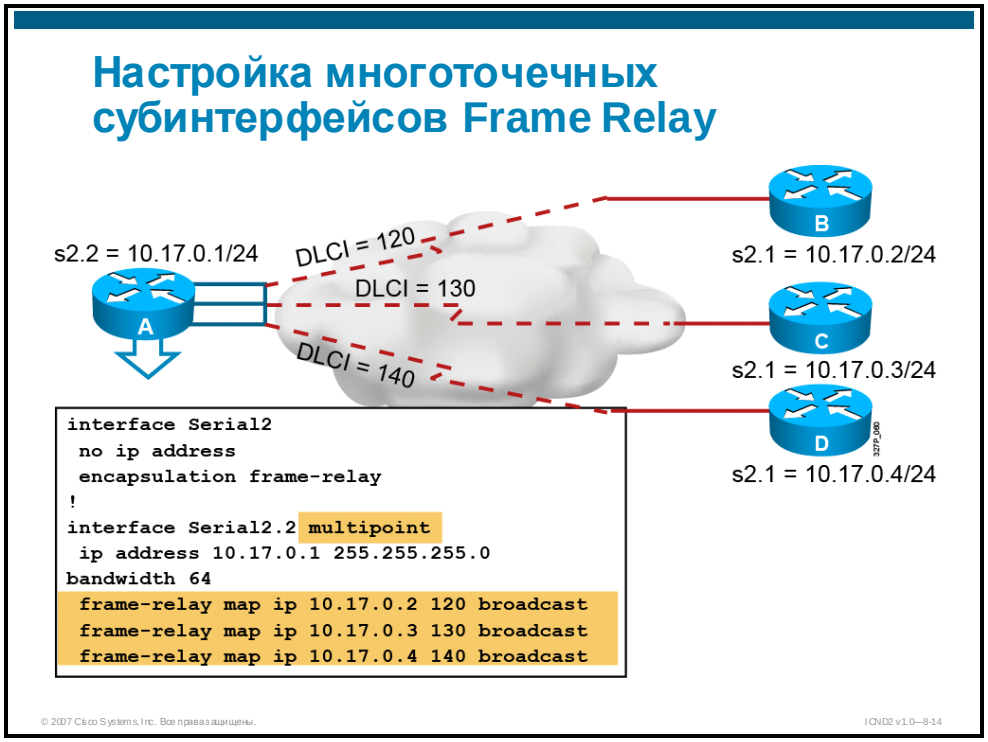
```
RouterX(config-subif)# frame-relay interface-dlci номер dlci
```

Параметры команды frame-relay interface-dlci

Параметр команды frame-relay interface-dlci	Описание
номер ***dlci***	Задает локальный номер DLCI для субинтерфейса. Других методов назначения идентификаторов DLCI, полученных от LMI, не существует, так как LMI не распознает субинтерфейсы.

Не используйте команду **frame-relay interface-dlci** на физических интерфейсах.

Примечание Если субинтерфейс настроен в режиме «точка-точка», вы не сможете переназначить его номер субинтерфейсу в многоточечном режиме без перезагрузки маршрутизатора. Вместо этого следует использовать другой номер субинтерфейса.



Пример: Настройка многоточечных субинтерфейсов Frame Relay

На рисунке все маршрутизаторы находятся в подсети 10.17.0.0/24. На маршрутизаторе A настроен многоточечный субинтерфейс с тремя каналами PVC. Канал PVC с идентификатором DLCI 120 используется для подключения к маршрутизатору B, канал PVC с идентификатором DLCI 130 используется для подключения к маршрутизатору C и канал PVC с DLCI 140 используется для подключения к маршрутизатору D.

По умолчанию метод Split horizon отключен на основных многоточечных интерфейсах Frame Relay и включен на многоточечных субинтерфейсах Frame Relay. На рисунке с конфигурацией, включающей многоточечный субинтерфейс, метод Split horizon необходимо вручную отключить на маршрутизаторе A, чтобы решить проблему Split horizon на этом маршрутизаторе.

Выполните следующие действия, чтобы настроить субинтерфейсы на физическом интерфейсе.

Действие 1 Выберите интерфейс, на котором необходимо настроить субинтерфейсы, и перейдите в режим конфигурации интерфейса.

Действие 2 Удалите адреса сетевого уровня, назначенные физическому интерфейсу, назначьте адрес сетевого уровня субинтерфейсу.

Действие 3 Настройте инкапсуляцию Frame Relay.

Действие 4 С помощью команды ниже выберите субинтерфейс, который необходимо настроить, и переведите его в многоточечный режим.

```
RouterX(config-if)# interface serial номер.номер субинтерфейса multipoint
```

Параметры команды interface serial

Параметры команды interface serial	Описание
.номер субинтерфейса	Номера субинтерфейса выбираются из диапазона 1 – 4 294 967 293. Номер перед точкой (.) – это номер интерфейса, к которому принадлежит субинтерфейс.
multipoint	Выберите этот параметр, если необходимо, чтобы все маршрутизаторы работали в одной подсети.

Примечание Необходимо указать параметр **multipoint** или **point-to-point**, значение по умолчанию отсутствует.

Действие 5 Если интерфейс настроен в многоточечном режиме, для него необходимо настроить локальный идентификатор DLCI, чтобы отличать субинтерфейс от физического интерфейса. Эта конфигурация не требуется для многоточечных интерфейсов, настроенных со статическими таблицами маршрутов. Команда для настройки локального идентификатора DLCI на субинтерфейсе приводится ниже.

```
RouterX(config-subif)# frame-relay interface-dlci номер dlci
```

Параметры команды frame-relay interface-dlci

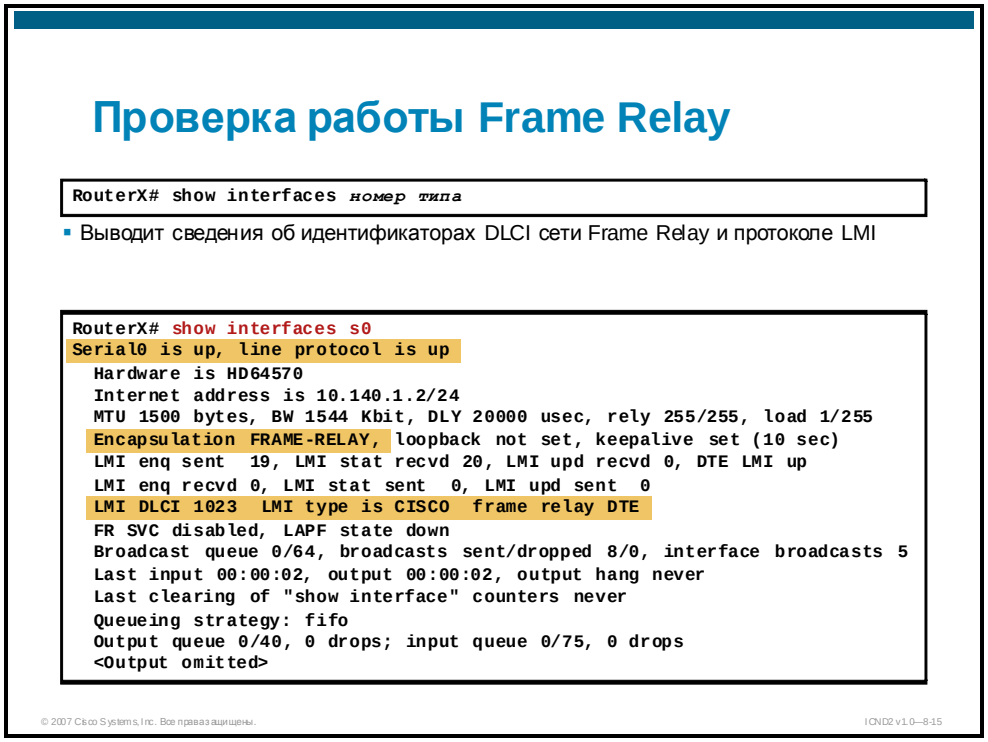
Параметр команды frame-relay interface-dlci	Описание
номер ***dlci***	Задает локальный номер DLCI для субинтерфейса. Других методов назначения идентификаторов DLCI, полученных от LMI, не существует, так как LMI не распознает субинтерфейсы.

Не используйте команду **frame-relay interface-dlci** на физических интерфейсах.

Примечание Если субинтерфейс настроен в режиме «точка-точка», вы не сможете переназначить его номер субинтерфейсу в многоточечном режиме без перезагрузки маршрутизатора. Вместо этого следует использовать другой номер субинтерфейса.

Проверка сети Frame Relay

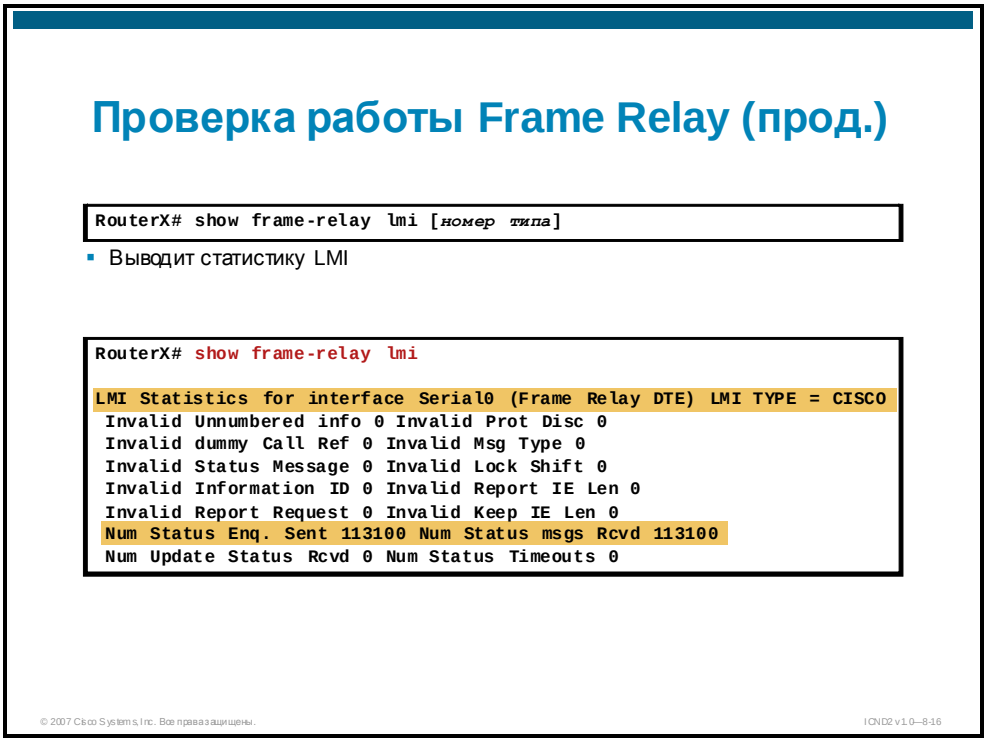
В этом разделе описываются команды Frame Relay **show** и **debug**, которые используются для проверки работы Frame Relay.



Команда **show interfaces** отображает сведения об инкапсуляции и состоянии интерфейсов на 1-м и 2-м уровнях. Убедитесь, что выбрана инкапсуляция Frame Relay.

Кроме того, эта команда выводит сведения о типе LMI и идентификаторе LMI DLCI. Идентификатор LMI DLCI отличается от идентификатора DLCI, который относится к каналу PVC, используемому для передачи данных.

Кроме того, в выводе приводится тип устройств Frame Relay – DTE или DCE. Как правило, маршрутизатор будет иметь тип DTE. Однако маршрутизатор Cisco можно настроить как коммутатор Frame Relay, в этом случае его тип будет DCE.

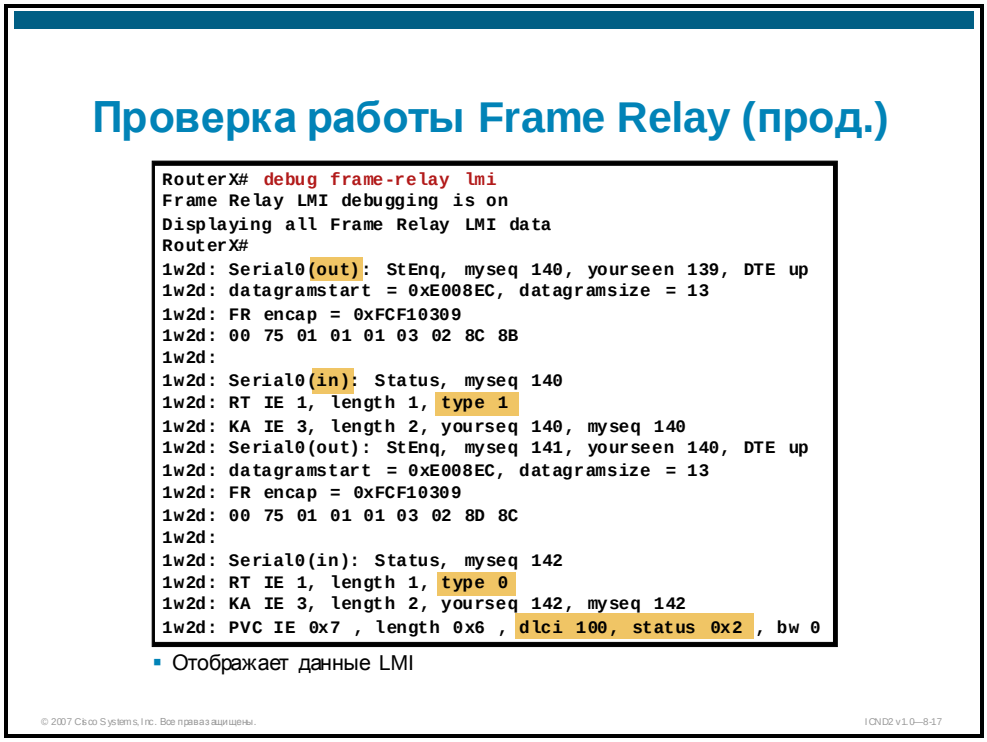


Используйте команду **show frame-relay lmi**, чтобы вывести статистику трафика LMI. В частности эта команда отображает количество сообщений состояния, переданных между локальным маршрутизатором и коммутатором Frame Relay.

В таблице ниже описываются некоторые поля входных данных команды **show frame-relay lmi**.

Поля вывода команды show frame-relay lmi

Поле	Описание
LMI Type	Спецификация сигнализации или LMI, варианты: Cisco, ANSI и ITU-T
Num Status Enq. Sent	Количество отправленных сообщений запроса состояния LMI
Num Status Msgs Rcvd	Количество полученных сообщений состояния LMI



Используйте команду **debug frame-relay lmi**, чтобы проверить отправку и получение пакетов LMI коммутатором Frame Relay и маршрутизатором.

В первых четырех строках описывается обмен данными LMI. В первой строке описывается запрос LMI, отправленный маршрутизатором в коммутатор Frame Relay. Во второй строке описывается ответ LMI, полученный маршрутизатором от коммутатора Frame Relay. В третьей и четвертой строке описывается ответ на этот запрос от коммутатора. После этого обмена данными LMI выполняются две аналогичных операции. Последние шесть строк содержат полное сообщение о состоянии LMI, которое включает описание двух каналов PVC маршрутизатора.

В таблице ниже описываются значимые поля, приведенные на рисунке.

Поля вывода команды debug frame-relay lmi

Поле	Описание
Serial0(out)	Указывает, что запрос LMI был отправлен из интерфейса serial 0
StEnq	Командный режим сообщения, возможные варианты: ■ StEnq: запрос состояния ■ Status: ответ на запрос состояния
myseq 140	Счетчик Myseq, привязанный к счетчику CURRENT SEQ маршрутизатора
yourseen 139	Счетчик Yourseen, привязанный к счетчику LAST RCVD SEQ
DTE up	Состояние канального протокола («up» или «down») для порта устройства DTE (пользовательского)
RT IE 1	Значение информационного элемента (IE) типа отчета (RT)

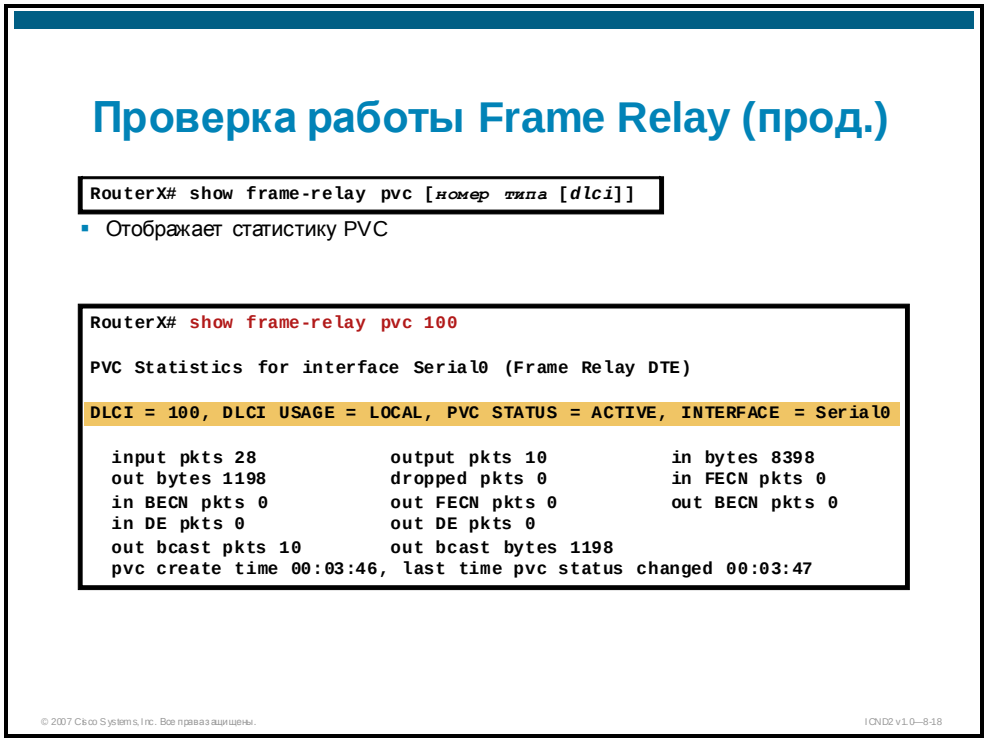
Поле	Описание
length 1	Длина информационного элемента типа отчета в байтах
type 1	Тип отчета – RT IE
KA IE 3	Значение информационного элемента Keepalive
length 2	Длина информационного элемента Keepalive в байтах
yourseq 142	Счетчик Yourseq, привязанный к счетчику CURRENT SEQ коммутатора
myseq 142	Счетчик Myseq, привязанный к счетчику CURRENT SEQ маршрутизатора
PVC IE 0x7	Значение типа информационного элемента PVC
length 0x6	Длина информационного элемента PVC в байтах
dlci 100	Значение DLCI в десятичном счислении для данного PVC
status 0x2	Значение состояния, возможные значения: ■ **0x00:** Added/inactive ■ **0x02:** Added/active ■ **0x04:** Deleted ■ **0x08:** New/inactive ■ **0x0a:** New/active
bw 0	Скорость CIR для DLCI

Раздел вывода «(out)» – это сообщение состояния LMI, отправленное маршрутизатором. Раздел вывода «(in)» – это сообщение, полученное от коммутатора Frame Relay.

Раздел вывода «type 0» – это полное сообщение состояния LMI. Раздел вывода «type 0» указывает на обмен данными LMI.

Строка «dlci 100, status 0x2» означает, что состояние DLCI 100 – «Active». Стандартные значения поля состояния DLCI приводятся ниже.

- **0x0:** Состояние «Added» и «Inactive» значит, что этот DLCI запрограммирован, но по каким-то причинам не используется, например, из-за того, что другая сторона канала PVC недоступна.
- **0x2:** Состояние «Added» и «active» означает, что коммутатор Frame Relay имеет идентификатор DLCI и система работает должным образом. Можно начать передачу трафика с этим DLCI в заголовке.
- **0x4:** «Deleted» означает, что на коммутаторе Frame Relay не запрограммирован DLCI для этого маршрутизатора, однако он был запрограммирован в прошлом. Это состояние может быть вызвано инверсией DLCI на маршрутизаторе или удалением канала PVC из облака Frame Relay поставщиком услуг.



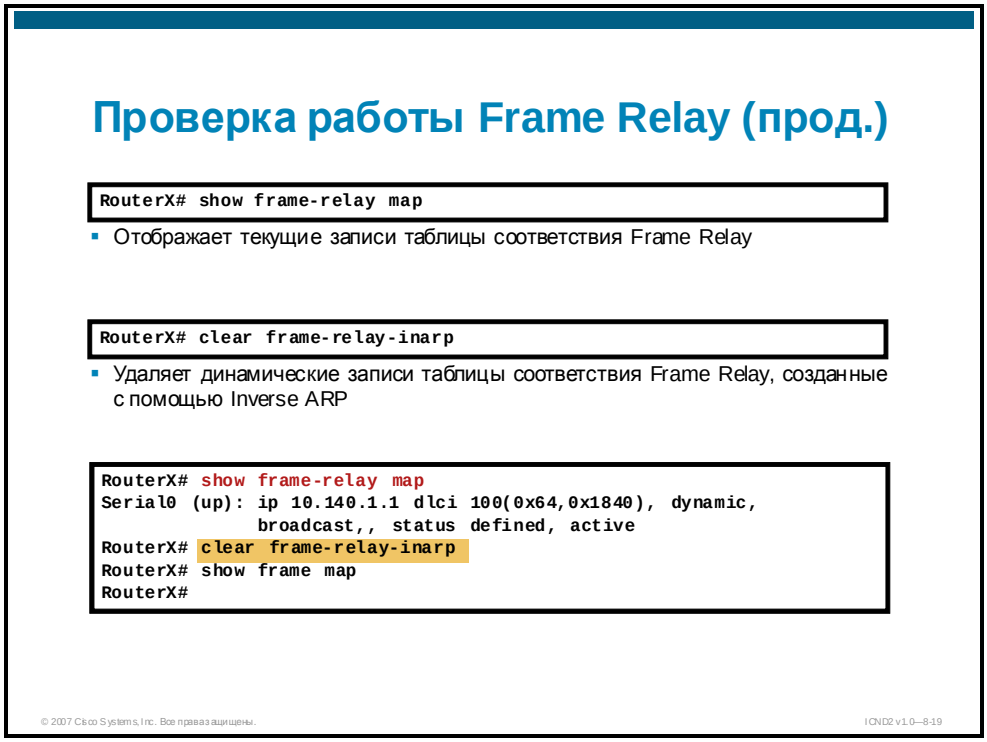
Используйте команду **show frame-relay pvc** [**interface** *интерфейс*] [*dlci*], чтобы вывести данные о состоянии всех настроенных каналов PVC, а также статистику трафика.

В таблице ниже описываются поля команды **show frame-relay pvc**.

Поля вывода команды show frame-relay pvc

Поле	Описание
DLCI	Один из номеров DLCI для данного канала PVC.
DLCI USAGE	Принимает значение «SWITCHED», если маршрутизатор или сервер доступа используется в качестве коммутатора, или значение «LOCAL», если маршрутизатор или сервер доступа используется в качестве DTE.
PVC STATUS	Состояние канала PVC. Устройство DCE передает данные о состоянии и устройство DTE получает эти данные. Если механизм LMI отключен на интерфейсе с помощью команды **no keepalive**, канал PVC будет находиться в состоянии STATIC. В противном будет выполняться обмен данными о состоянии PVC с помощью протокола LMI. ■ **STATIC:** протокол LMI отключен на интерфейсе. ■ **ACTIVE:** канал PVC находится в рабочем режиме и может передавать пакеты. ■ **INACTIVE:** канал PVC настроен, но отключен. ■ **DELETED:** канал PVC отсутствует (только для устройств DTE), т. е. данные о состоянии не получены от протокола LMI. Если используется команда **frame-relay end-to-end keepalive**, в дополнение к состоянию LMI передается состояние EEK. Два примера приводятся ниже: ■ **ACTIVE (EEK UP):** канал PVC функционирует в соответствии с данными Keepalive протоколов LMI и EEK. ■ **ACTIVE (EEK DOWN):** канал PVC функционирует в соответствии с данными Keepalive протокола LMI, но протокол EEK вернул ошибку.

Поле	Описание
INTERFACE	Субинтерфейс, связанный с данным идентификатором DLCI.
LOCAL PVC STATUS	Состояние канала PVC, настроенного локально на межсетевом интерфейсе NNI.
NNI PVC STATUS	Состояние канала PVC, полученного через канал NNI.
input pkts	Количество пакетов, полученных через этот канал PVC.
output pkts	Количество пакетов, полученных через этот канал PVC.
in bytes	Количество байт, полученных через этот канал PVC.
out bytes	Количество байт, отправленных через этот канал PVC.
dropped pkts	Количество входящих и исходящих пакетов, отброшенных маршрутизатором на уровне Frame Relay.
in pkts dropped	Количество отброшенных входящих пакетов. Входящие пакеты могут отбрасываться по нескольким причинам: ■ неактивный канал PVC; ■ политики; ■ пакеты, превышающие уровень отбрасывания DE; ■ отброшенные проблемы; ■ ошибки при выделении памяти; ■ проблемы конфигурации.
out pkts dropped	Количество отброшенных исходящих пакетов, в том числе из-за запаздывания и ограничения трафика.
out bytes dropped	Объем отброшенных исходящих пакетов (в байтах).
late-dropped out pkts	Количество исходящих пакетов, отброшенных в соответствии с политикой качества обслуживания (QoS), таких как очередь виртуального канала и ограничение трафика Frame Relay. Поле не отображается, если его значение 0.
late-dropped out bytes	Объем исходящих пакетов (в байтах), отброшенных в соответствии с политикой качества обслуживания (QoS), таких как очередь виртуального канала и ограничение трафика Frame Relay Поле не отображается, если его значение 0.
in FECN pkts	Количество полученных пакетов с битом FECN.
in BECN pkts	Количество полученных пакетов с битом BECN.
out FECN pkts	Количество отправленных пакетов с битом BECN.
out BECN pkts	Количество отправленных пакетов с битом BECN.
in DE pkts	Количество полученных пакетов DE.
out DE pkts	Количество отправленных пакетов DE.
out bcast pkts	Количество исходящих широковещательных пакетов.
out bcast bytes	Количество входящих широковещательных пакетов.



Используйте команду **show frame-relay map**, чтобы вывести текущие записи таблицы соответствия и сведения о подключениях.

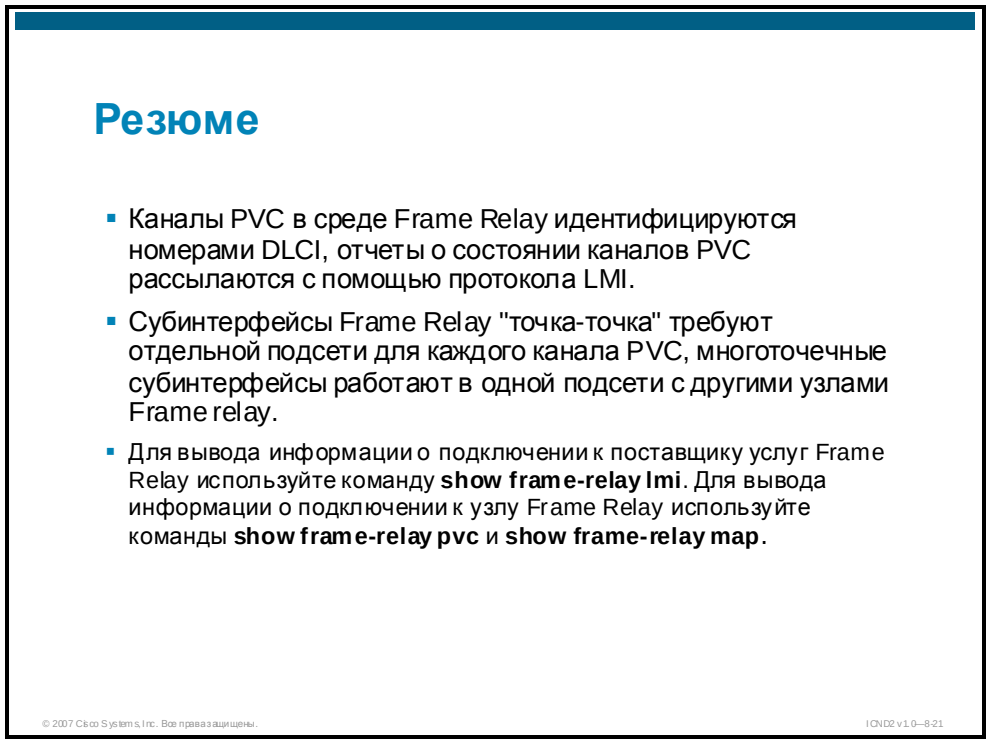
Ниже приводится объяснение вывода команды **show frame-relay map** на рисунке.

- «100» – это локальный номер DLCI в десятичном счислении.
- «0x64» – это номер DLCI, преобразованный в шестнадцатеричную форму (0x64 = 100 в десятичном счислении).
- «0x1840» – фактическое значение, которое будет передано в канал DLCI (значение преобразуется из-за распределения битов DLCI в поле адреса кадра Frame Relay).
- «10.140.1.1» – это IP-адрес удаленного маршрутизатора (динамическая запись, полученная от процесса Inverse ARP).
- На канале PVC включена широковещательная и групповая рассылка.
- Состояние PVC – «Active».

Чтобы удалить динамические записи таблицы соответствия Frame Relay, созданные с помощью Inverse ARP, используйте команду **clear frame-relay-inarp** привилегированного режима EXEC.

Резюме

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



Занятие 4

Устранение неполадок в глобальных сетях на базе Frame Relay

Обзор

Сеть Frame Relay предлагает несколько дополнительных преимуществ по сравнению с арендованными каналами. Но эти преимущества увеличивают сложность среды. С добавлением таких концепций, как NBMA, LMI, Inverse ARP и таблицы соответствия Frame Relay, администратор должен обладать базовыми знаниями по этим концепциям для более эффективного поиска и устранения проблем подключения, которые могут возникнуть в сети.

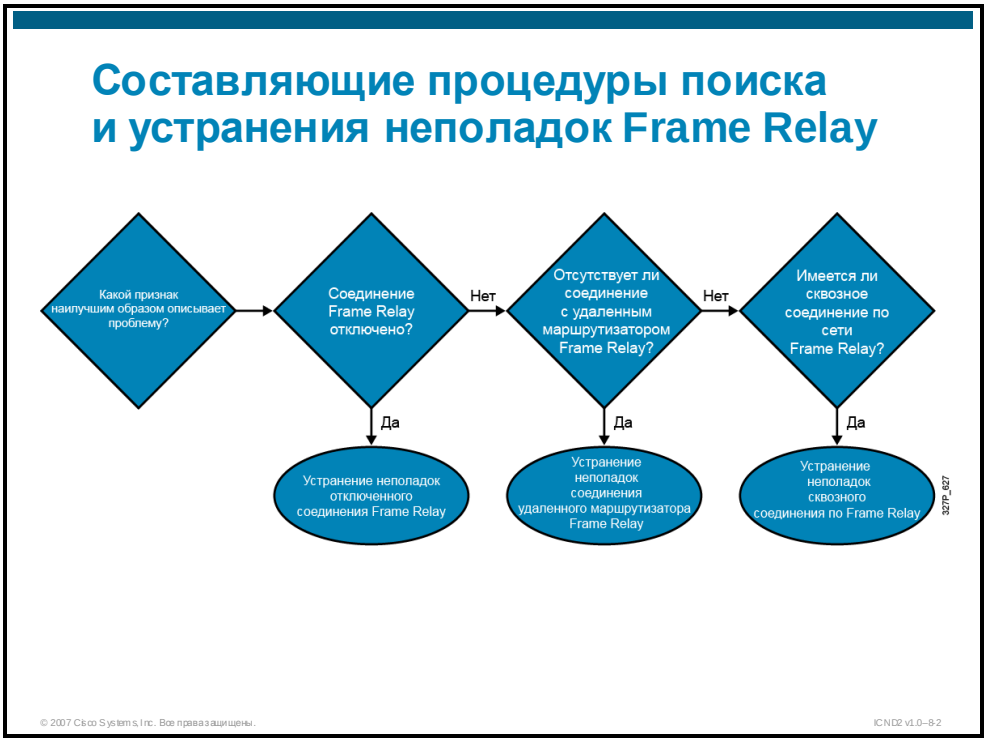
Задачи

По окончании этого занятия вы сможете определять методы поиска и устранения распространенных проблем Frame Relay, а также предлагать решения этих проблем. Это значит, что вы сможете выполнять следующие задачи:

- описывать базовый набор действий по поиску и устранению неполадок в глобальной сети на базе Frame Relay;
- выявлять и устранять распространенные проблемы подключения Frame Relay.

Составляющие процедуры поиска и устранения неполадок Frame Relay

В этом разделе описывается базовый набор действий по поиску и устранению неполадок в глобальной сети на базе Frame Relay.

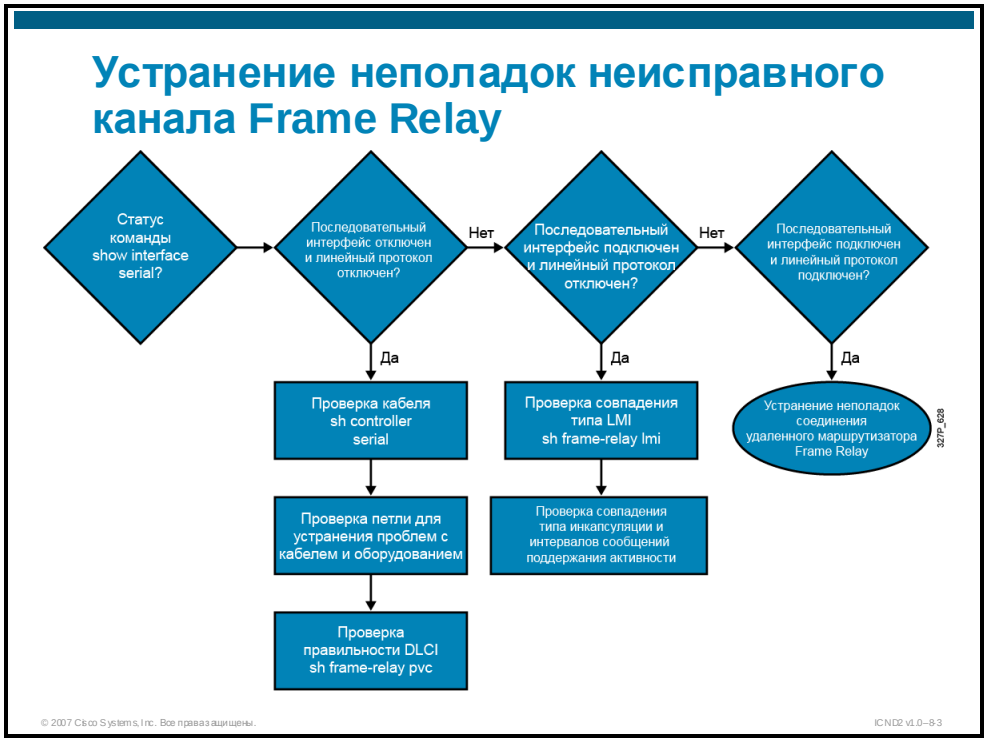


Основные составляющие процедуры поиска и устранения Frame Relay описываются ниже:

- поиск и устранение неполадок недоступного канала Frame Relay, это может быть вызвано проблемой 1-го или 2-го уровня;
- поиск и устранение неполадок подключений удаленного маршрутизатора Frame Relay, т. е. подключений между одноранговыми маршрутизаторами Frame Relay;
- поиск и устранение сквозных подключений Frame Relay, т. е. подключений между рабочими станциями через сеть Frame Relay.

Поиск и устранение проблем подключения Frame Relay

В этом разделе описывается поиск и устранение наиболее распространенных проблем подключения Frame Relay.



Первое действие, которое следует выполнить при поиске и устранении неполадок подключения Frame Relay, – проверить состояние интерфейса Frame Relay. Для проверки состояния интерфейса Frame Relay используется команда **show interface serial** *номер*[/*номер*].

Если в выводе команды **show interface serial** отображается состояние «interface down/line protocol down», это, как правило, указывает на проблему 1-го (физического) уровня. Такой вывод указывает на проблему кабеля, устройства CSU/DSU или последовательной линии.

Сначала убедитесь, что кабель подключен и распознается маршрутизатором с помощью команды **show controllers serial** [*слот/порт*].

После этого для поиска и устранения проблемы может потребоваться проверка возвратной петли.

Выполните следующие действия для проверки возвратной петли.

Действие 1 Установите инкапсуляцию HDLC для последовательного канала и выберите период Keepalive 10 секунд. Для этого введите команды **encapsulation hdlc** и **keepalive 10** в режиме конфигурации интерфейса, для которого выполняется процедура поиска и устранения неполадок.

Действие 2 Переведите устройство CSU/DSU или в режим локального шлейфа. Сведения о том, как это сделать, можно найти в документации по устройству. Если канальный протокол переходит в рабочее состояние, когда устройство CSU/DSU или модем находится в режиме локального шлейфа, что обозначается сообщением «line protocol is up (looped)», скорее всего проблема возникла не в локальном устройстве CSU/DSU. Если строка состояния не изменяется, источником проблемы может быть маршрутизатор, соединительный кабель, устройство CSU/DSU или модем. В большинстве случаев проблема возникает в устройстве CSU/DSU или модеме.

Действие 3 Выполните команду **ping** для IP-адреса интерфейса, для которого выполняется поиск и устранение неполадок, когда устройство CSU/DSU или модем находится в режиме локального шлейфа. Необработанных эхо-запросов быть не должно. Расширенный эхо-запрос, использующий комбинацию данных 0x0000, помогает в решении проблем канала, так как каналы T1 и E1 синхронизируются по данным и требуют битов перехода через каждые 8 бит. Комбинация данных с большим числом нулей помогает понять, применяются ли биты перехода в транковом подключении. Комбинация данных с большим числом единиц используется для эмуляции интенсивного потока нулей, если на пути прохождения данных присутствуют инверторы. Переменная комбинация (0x5555) представляет «обычный» трафик. Если эхо-запросы обрабатываются неудачно или система возвращает ошибки CRC, необходимо получить тестер частоты ошибочных битов (BERT) с соответствующим анализатором от телефонной компании.

Действие 4 Завершив проверку, обязательно верните интерфейс к инкапсуляции Frame Relay.

Неверный идентификатор DLCI, статически заданный на субинтерфейсе, также может перевести его в состояние «down/down». В этом случае будет отображаться состояние PVC «deleted». Чтобы убедиться, что настроен правильный номер DLCI, используйте команду **show frame-relay pvc**.

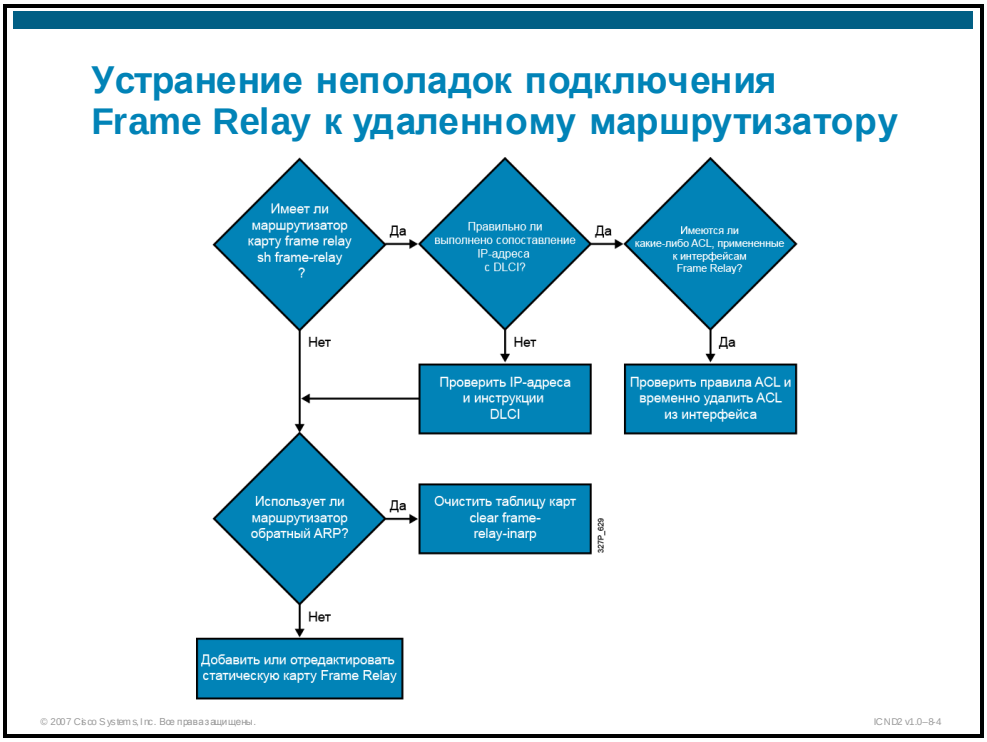
```
RouterX#sh frame-relay pvc

PVC Statistics for interface Serial0/0/0 (Frame Relay DTE)

             Active     Inactive      Deleted       Static
  Local         0            0            1            0
  Switched      0            0            0            0
  Unused        0            0            0            0

DLCI = 100, DLCI USAGE = LOCAL, PVC STATUS = DELETED, INTERFACE = Serial0/0/0

  input pkts 9             output pkts 8            in bytes 879
  out bytes 1024           dropped pkts 0           in pkts dropped 0
  out pkts dropped 0       out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 2         out bcast bytes 138
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 00:00:27, last time pvc status changed 00:00:27
```

В этом выводе номер DLCI имеет значение «100» и состояние «deleted». Это может означать, что настроен неверный DLCI.

Если в выводе команды **show interface serial** отображается состояние «interface up/line protocol down», это, как правило, указывает на проблему 2-го (канального) уровня. В этом случае последовательный интерфейс может не получать сообщения LMI Keepalive от поставщика услуг Frame Relay. Чтобы убедиться, что сообщения LMI отправляются и принимаются, и что тип LMI маршрутизатора совпадает с типом LMI поставщика услуг, введите команду **show frame-relay lmi**.

```
RouterX#sh frame-relay lmi

LMI Statistics for interface Serial0/0/0 (Frame Relay DTE) LMI TYPE = CISCO
  Invalid Unnumbered info 0             Invalid Prot Disc 0
  Invalid dummy Call Ref 0              Invalid Msg Type 0
  Invalid Status Message 0              Invalid Lock Shift 0
  Invalid Information ID 0              Invalid Report IE Len 0
  Invalid Report Request 0              Invalid Keep IE Len 0
  Num Status Enq. Sent 236              Num Status msgs Rcvd 31
  Num Update Status Rcvd 0              Num Status Timeouts 206
  Last Full Status Req 00:00:38         Last Full Status Rcvd 00:00:38
```

Вывод показывает, что было отправлено 236 сообщений запроса состояния LMI (Num Status Enq. Sent) и было получено 31 сообщение состояния LMI (Num Status msgs Rcvd), тип LMI – «Cisco».



Чтобы получить доступ к одноранговому маршрутизатору через сеть Frame Relay, маршрутизатор Frame Relay должен привязать IP-адрес этого маршрутизатора к локальному идентификатору DLCI, который будет использоваться для получения доступа к этому IP-адресу. Команда **show frame-relay map** отображает IP-адреса и привязанные к ним идентификаторы DLCI, а также сведения о том, была ли привязка введена статически или получена динамически с помощью протокола Inverse ARP.

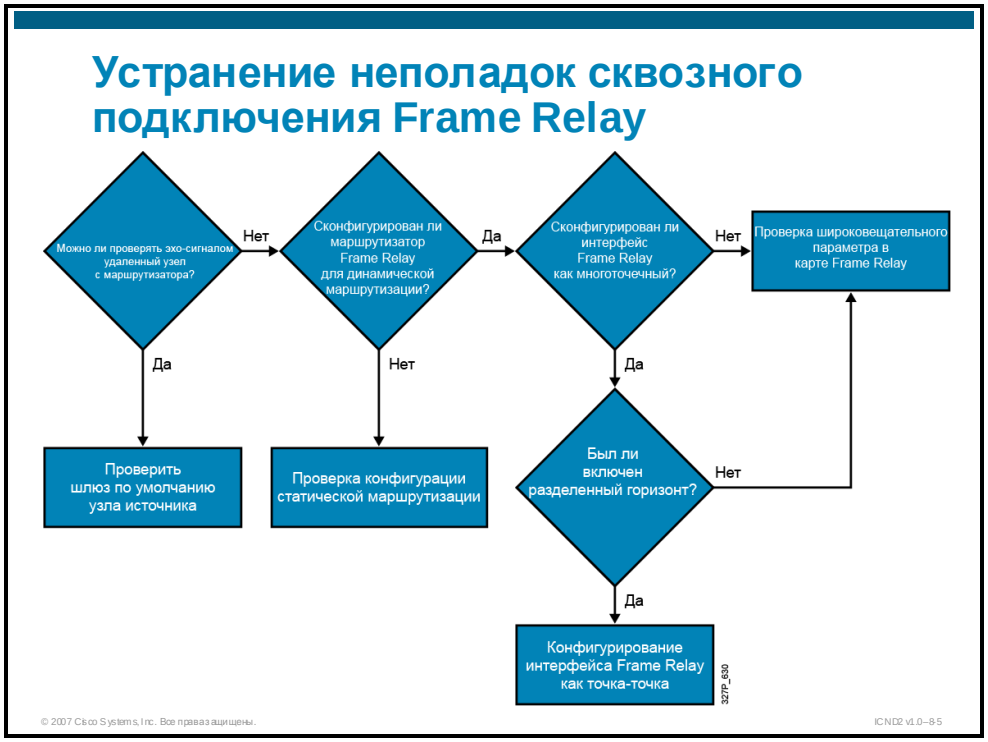
```
RouterX#sh frame-relay map
Serial0/0/0 (up): ip 10.140.1.1 dlci 100(0x64,0x1840), dynamic,
              broadcast,
              CISCO, status defined, active
```

Если вы недавно изменили адрес интерфейса удаленного маршрутизатора Frame Relay, может потребоваться использование команды **clear frame-relay-inarp** для очистки таблицы соответствия Frame Relay локального маршрутизатора. При этом протокол Inverse ARP выполнит повторную привязку нового адреса к DLCI.

Если IP-адрес однорангового маршрутизатора не появляется в таблице соответствия Frame Relay, возможно, удаленный маршрутизатор не поддерживает Inverse ARP. Попробуйте привязать IP-адрес к идентификатору DLCI статически с помощью команды **frame-relay map** *протокол адрес протокола dlci* [**broadcast**].

Кроме того, на интерфейсах Frame Relay могут быть активированы списки контроля доступа (ACL), влияющие на подключение. Чтобы проверить, активирован ли список ACL на интерфейсе, введите команду **show ip interface**.

Чтобы временно удалить список ACL с интерфейса и проверить, влияет ли он на подключение, введите команду **no ip access-group** *номер acl* **{in|out}** в режиме конфигурации интерфейса.



Существование сквозного подключения между рабочими станциями через сеть Frame Relay зависит от того, удовлетворены ли общие требования к маршрутизации. Если в сети Frame Relay возникли проблемы сквозного подключения, проверьте таблицы маршрутизации, чтобы определить, имеют ли маршрутизаторы маршрут к месту назначения, подключение к которому неисправно. Для проверки таблицы маршрутизации используйте команду **show ip route**.

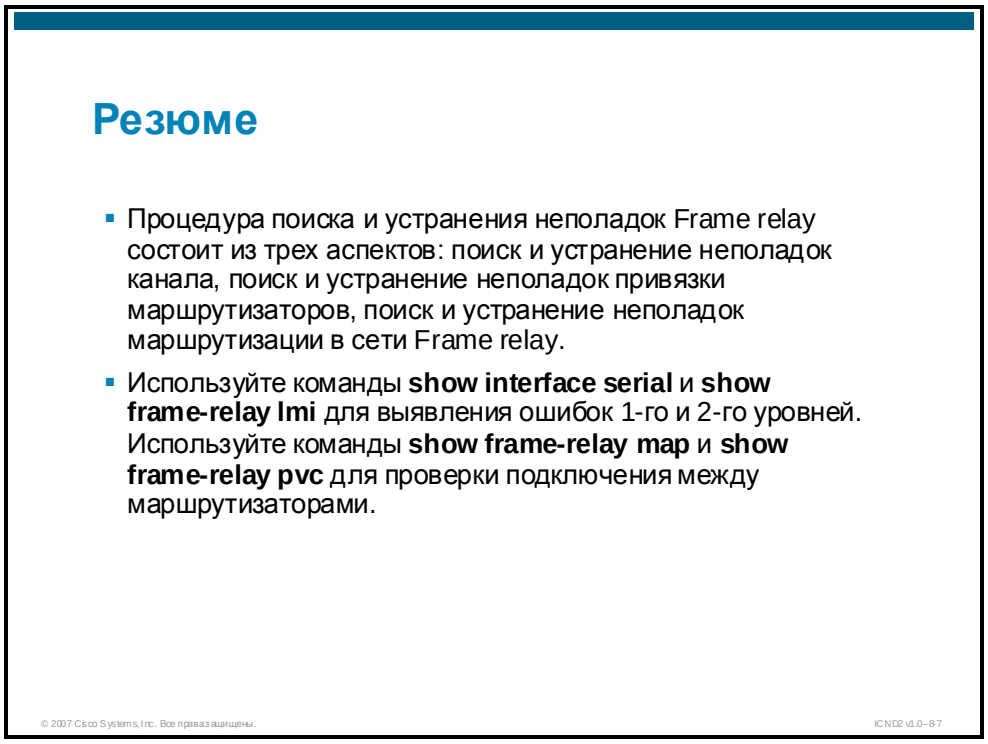
```
RouterX#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.2.0 is directly connected, Loopback1
     10.0.0.0/24 is subnetted, 3 subnets
C       10.23.23.0 is directly connected, Serial0/0/1
C       10.2.2.0 is directly connected, FastEthernet0/0
     192.168.1.0/24 is variably subnetted, 3 subnets, 3 masks
C       192.168.1.64/28 is directly connected, Loopback0
```

Если в таблице маршрутизации присутствуют только маршруты с прямым подключением, возможно, в сети Frame Relay возникла проблема, которая мешает объявлению обновлений маршрутизации. Поскольку сеть Frame Relay является средой NBMA, необходимо настроить протокол маршрутизации на передачу групповых и широковещательных пакетов через сеть Frame Relay. При использовании Inverse ARP эта возможность активируется автоматически. При использовании статической таблицы соответствия Frame Relay, необходимо явно настроить поддержку широковещательного трафика. Команда show **frame-relay map** показывает, включена ли поддержка широковещательного трафика, которая обеспечивает передачу обновлений маршрутизации по сети Frame Relay.

```
RouterX#sh frame-relay map
Serial0/0/0 (up): ip 10.140.1.1 dlci 100(0x64,0x1840), dynamic,
              broadcast,
              CISCO, status defined, active
```

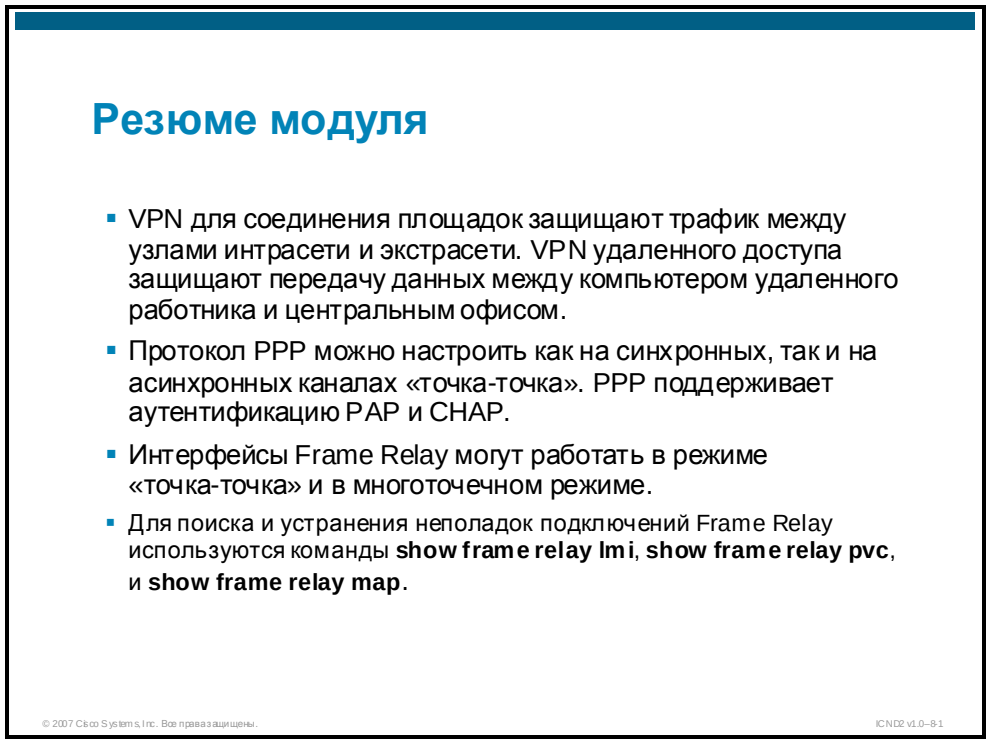

Резюме

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



Резюме модуля

В этом разделе приводится резюме вопросов, рассмотренных в модуле.



Существует множество способов подключения пользователей к удаленным службам, каждый из них имеет свои преимущества и недостатки. Широко используются традиционные технологии ГВС 2-го уровня, такие как Frame Relay и арендованные каналы. Однако в отрасли существует новый тренд, который подразумевает использование Интернета для соединения площадок и удаленного доступа с использованием решений на базе виртуальных частных сетей (VPN), более простых, безопасных и масштабируемых, чем традиционные решения.

Вопросы для самопроверки по модулю

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

B1) Какой компонент используется протоколом PPP для инкапсуляции нескольких протоколов? (Источник: создание подключения типа «точка-точка» к ГВС с помощью протокола PPP)

А) NCP
Б) LCP
В) IPCP
Г) IPXCP

B2) Каково назначение LCP? (Источник: создание подключения типа «точка-точка» к ГВС с помощью протокола PPP)

А) аутентификация
Б) согласование элементов управления
В) инкапсуляция нескольких протоколов
Г) указание асинхронного или синхронного режима

B3) Какой тип пакета используется на этапе формирования канала PPP? (Источник: создание подключения типа «точка-точка» к ГВС с помощью протокола PPP)

А) LCP
Б) PAP
В) NCP
Г) CHAP

B4) Какие два утверждения наилучшим образом описывают протокол CHAP? (Выберите два варианта.) (Источник: создание подключения типа «точка-точка» к ГВС с помощью протокола PPP)

А) CHAP выполняется периодически.
Б) CHAP использует двустороннюю процедуру установления соединения.
В) CHAP использует трехстороннюю процедуру установления соединения.
Г) CHAP использует двустороннее хэширование.
Д) Пароли CHAP отправляются в незашифрованном виде.

B5) Как удаленный узел отвечает на сообщение вызова при использовании протокола CHAP? (Источник: создание подключения типа «точка-точка» к ГВС с помощью протокола PPP)

А) значением хэша
Б) ответным сообщением вызова
В) незашифрованным паролем
Г) зашифрованным паролем

В6) Какое имя пользователя необходимо настроить на маршрутизаторах для аутентификации PPP? (Источник: создание подключения типа «точка-точка» к ГВС с помощью протокола PPP)

А) Имя должно совпадать с именем хоста локального маршрутизатора.
Б) Имя должно совпадать с именем хоста удаленного маршрутизатора.
В) Имя не должно совпадать ни с одним из имен хоста.
Г) На имя пользователя не налагается ограничений.

В7) Какой вывод команды **show interface** указывает на верную настройку PPP? (Источник: создание подключения типа «точка-точка» к ГВС с помощью протокола PPP)

А) Encaps = PPP
А) PPP encapsulation
Б) Encapsulation PPP
В) Encapsulation HDLC using PPP

В8) Сопоставьте каждый из компонентов процесса Frame Relay и его определение. (Источник: создание подключения к ГВС с помощью Frame Relay)

_____ 1. скорость локального доступа.

_____ 2. SVC

_____ 3. CIR

_____ 4. LMI

_____ 5. Inverse ARP

А) максимальная средняя скорость передачи данных
Б) тактовая частота подключения к облаку Frame Relay
В) метод динамической привязки адреса сетевого уровня к локальному идентификатору DLCI
Г) виртуальный канал динамически создается по требованию и разрывается после завершения передачи
Д) стандарт сигнализации между маршрутизатором и коммутатором Frame Relay, который используется для управления подключением и состоянием подключения между устройствами.

В9) Чем идентифицируется логический канал между маршрутизатором и локальным коммутатором Frame Relay? (Источник: создание подключения к ГВС с помощью Frame Relay)

А) идентификатором DLCI
Б) сигналом LMI
В) пакетом FECN
Г) пакетом BECN

В10) Сопоставьте каждый из типов топологии Frame Relay и его описание. (Источник: создание подключения к ГВС с помощью Frame Relay)

_____ 1. звезда

_____ 2. полносвязная

_____ 3. частичносвязная

А) Все маршрутизаторы имеют виртуальные каналы ко всем остальным местам назначения.

Б) Многие, но все, маршрутизаторы имеют доступ ко всем остальным площадкам.

В) Удаленные площадки подключаются к центральной площадке, на которой, как правило, предоставляется доступ к услуге или приложению.

В11) Какая из характеристик Frame Relay может вызвать проблемы достижимости в ситуациях, когда один интерфейс используется для соединения нескольких площадок? (Источник: устранение неполадок в глобальных сетях на базе Frame Relay)

А) неустойчивость
Б) «точка-точка»
В) коррекция ошибок
Г) NBMA

В12) Какая альтернатива методу Inverse ARP доступна для привязки идентификатора DLCI адресу сетевого уровня в сети Frame Relay? (Источник: создание подключения к ГВС с помощью Frame Relay)

А) ARP
Б) RARP
В) DHCP
Г) команды статической привязки Frame Relay

В13) Какие три типа LMI поддерживаются в продуктах Cisco? (Выберите три варианта.) (Источник: создание подключения к ГВС с помощью Frame Relay)

А) DEC
Б) ANSI
В) Cisco
Г) Q.931
Д) Q.933A
Е) Q.921

В14) Какой адрес привязывается к локальному идентификатору DLCI в виртуальном канале Frame Relay? (Источник: устранение неполадок в глобальных сетях на базе Frame Relay)

А) адрес порта
Б) адрес порта источника
В) адрес сетевого уровня
Г) адрес канального уровня

В15) Какое состояние виртуального канала на маршрутизаторе Cisco указывает, что локальное подключение коммутатору Frame Relay работает, а подключение удаленного маршрутизатора к коммутатору Frame Relay – нет? (Источник: устранение неполадок в глобальных сетях на базе Frame Relay)

А) состояние LMI
Б) состояние «active»
В) состояние «deleted»
Г) состояние «inactive»

В16) Каковы два типа VPN? (Выберите два варианта.) (Источник: общие сведения о решениях VPN)

А) Удаленный доступ
Б) Удаленный-площадка
В) Удаленный-удаленный
Г) Соединение площадок.

В17) Какой вариант ответа не является преимуществом VPN? (Источник: общие сведения о решениях VPN)

А) они дешевле глобальных сетей 2-го уровня
Б) они обеспечивают масштабируемость
В) не требуют телекоммуникационного оборудования
Г) обеспечивают безопасность

В18) Какой вариант ответа не является компонентом сети IPsec? (Источник: общие сведения о решениях VPN)

А) ESP
Б) MD5
В) AES
Г) RSMAC

В19) Какой компонент безопасности предотвращает несанкционированное изменение данных? (Источник: общие сведения о решениях VPN)

А) аутентификация
Б) целостность
В) конфиденциальность
Г) защита от воспроизведения пакетов

В20) Какие два алгоритма используются для проверки целостности данных? (Выберите два варианта.) (Источник: общие сведения о решениях VPN)

А) AES
Б) SHA
В) 3DES
Г) MD5

Ответы на вопросы для самопроверки по модулю

В1) А

В2) Б

В3) А

В4) А, В

В5) А

В6) Б

В7) В

В8) 1 = Б, 2 = Г, 3 = А, 4 = Д, 5 = В

В9) А

В10) 1 = В, 2 = А, 3 = Б

В11) Г

В12) Г

В13) Б, В, Д

В14) В

В15) Г

В16) А, Г

В17) В

В18) Г

В19) Б

В20) Б, Г

