Глава 6

Маршрутизирующие протоколы IP

В этой главе представлены основные сведения и рекомендации по настройке конфигурации следующих протоколов маршрутизации IP.

- 6.1. Протокол маршрутной информации (Routing Information Protocol — RIP)
- 6.2. Протокол маршрутной информации (RIP) для IPv6
- 6.3. Расширенный протокол маршрутизации внутреннего шлюза (Enhanced Interior Gateway Routing Protocol — EIGRP)
- 6.4. Расширенный протокол маршрутизации внутреннего шлюза (EIGRP) для IPv6
- 6.5. Открытый протокол предпочтительного выбора кратчайшего пути (Open Shortest Path First — OSPF)
- 6.6. Открытый протокол предпочтительного выбора кратчайшего пути (OSPF) версии 3 (для IPv6)
- 6.7. Интегрированный протокол IS-IS
- 6.8. Интегрированный протокол IS-IS для IPv6
- 6.9. Протокол граничного шлюза (Border Gateway Protocol — BGP)
- 6.10. Протокол граничного мультипротокольного шлюза (BGP) для IPv6

6.1. Протокол маршрутной информации (Routing Information Protocol — RIP)

- RIP — это дистанционно-векторный протокол маршрутизации, в котором в качестве метрики используется количество транзитных переходов.
- Протокол RIP имеет две версии: протокол RIP версии 1 (RIP-1), который определен документом RFC 1058, и протокол RIP версии 2 (RIP-2), который определен

документом RFC 2453. RIP-1 — это применяемая по умолчанию версия протокола RIP.

- В протоколе RIP-1 для рассылки маршрутной информации через все определенные сетевые интерфейсы используются широковещательные сообщения. В протоколе RIP-2 для отправки анонсов маршрутизации во все определенные сети используются многоадресатные рассылки.
- Протокол RIP-1 является протоколом с поддержкой классов, не допускающим применение масок подсети переменной длины (Variable Length Subnet Mask — VLSM). Протокол RIP-2 — это протокол без поддержки классов, обеспечивающий использование VLSM.
- Максимальное количество транзитных переходов для любой версии составляет 15 транзитных переходов. Маршрут с количеством транзитных переходов, которое достигло 16, рассматривается как недостижимый.
- При перераспределении маршрутов должна быть определена применяемая по умолчанию метрика, так как в противном случае в качестве значения по умолчанию будет использоваться 15, и любой перераспределенный маршрут окажется недоступным.
- В протоколе RIP полная таблица маршрутизации анонсируется через каждые 30 с. Маршруты отмечаются как неприменимые, если для них в течении 180 с не происходит получение никаких обновлений. Маршруты удаляются, если по истечении 240 с не происходит никаких обновлений.

НА ЗАМЕТКУ

В протоколе RIP для обмена данными служит порт 520 протокола UDP. Протокол RIP-1 предусматривает рассылку широковещательных сообщений для участвующих интерфейсов с применением определенного широковещательного адреса (по умолчанию определенным адресом является 255.255.255.255). В протоколе RIP-2 предусмотрена отправка многоадресатных сообщений по стандартному адресу 224.0.0.9 в участвующих интерфейсах. Если определено соседнее устройство, то в версиях 1 и 2 происходит отправка сообщения как одноадресатного по адресу соседнего устройства.

Настройка конфигурации

1. Ввод в действие процесса маршрутизации RIP:

   ```
   (global) router rip
   ```

   Эта команда активизирует процесс маршрутизации RIP и обеспечивает переход устройства в режим настройки конфигурации маршрутизатора. Если не назначены никакие сети как участвующие в процессе, протокол RIP не функционирует.

2. Связывание сети с процессом RIP:

   ```
   (router) network network-number
   ```

   Команда `network` позволяет указать сети с поддержкой классов, которые должны анонсироваться с помощью процесса маршрутизации. Если задана подсеть, то в конфигурации она обозначается как относящаяся к адресу глав-

ного класса. Поэтому, если в конфигурации не задано иное, то любой интерфейс маршрутизатора, которому назначен адрес в сети главного класса, становится активным интерфейсом RIP.

3. (Необязательно.) Определение применяемой версии RIP:

```
(router) version { 1 | 2 }
```

Эта команда определяет конфигурацию маршрутизатора таким образом, чтобы он отправлял и получал только пакеты RIP с указанной версией.

НА ЗАМЕТКУ

По умолчанию после ввода в действие протокола RIP маршрутизатор отправляет пакеты версии 1, а получает и обрабатывает пакеты обеих версий, RIP-1 и RIP-2. После применения команды `version` маршрутизатор отправляет и получает пакеты только указанной версии. Это поведение можно изменить отдельно для каждого интерфейса, как описано в пп. 4 и 5.

4. (Необязательно.) Изменение параметров отправки пакетов RIP для данного интерфейса:

```
(interface) ip rip send version [ 1 | 2 | 1 2]
```

В режиме настройки конфигурации интерфейса можно настроить маршрутизатор на отправку только обновлений версии 1 с помощью параметра `1`, только обновлений версии 2 с помощью параметра `2` или обновлений обеих версий, 1 и 2, с помощью параметра `1 2`. Эта команда переопределяет и поведение по умолчанию, и глобальное поведение, которое было определено с помощью команды `version` маршрутизатора.

5. (Необязательно.) Изменение параметров получения пакетов RIP для данного интерфейса:

```
(interface) ip rip receive version [ 1 | 2 | 1 2]
```

В режиме настройки конфигурации интерфейса можно настроить маршрутизатор на получение только обновлений версии 1 с помощью параметра `1`, только обновлений версии 2 с помощью параметра `2` или обновлений обеих версий, 1 и 2, с помощью параметра `1 2`. Эта команда переопределяет и поведение по умолчанию, и глобальное поведение, которое было определено с помощью команды `version` маршрутизатора.

6. (Необязательно.) Определение в конфигурации RIP отправки одноадресатных обновлений:

```
(router) neighbor ip-address
```

Эта команда задает в конфигурации маршрутизатора, что должны передаваться одноадресатные обновления RIP указанному соседнему устройству.

7. (Необязательно.) Задание в конфигурации интерфейса, что не должны передаваться обновления RIP:

```
(router) passive-interface type number
```

Эта команда, выполняемая в режиме настройки конфигурации маршрутизатора, указывает, что через интерфейс не должны передаваться никакие широковещательные или многоадресатные обновления RIP. Выполнение этой

команды не отражается на способности маршрутизатора получать или отправлять одноадресатные обновления.

8. (Необязательно.) Корректировка таймеров маршрутизирующего протокола:

```
(router) timers basic update invalid hold-down flush [sleeptime]
```

Данная команда, применяемая в режиме настройки конфигурации маршрутизатора, позволяет отрегулировать частоту обновлений маршрутизации и может использоваться для достижения более быстрой сходимости. Параметр `update` устанавливает периодичность в секундах, с которой происходит отправка обновлений (значение по умолчанию — 30 с). Это — фундаментальный параметр синхронизации протокола маршрутизации. Параметр `invalid`, который имеет значение по умолчанию 180 с, устанавливает интервал времени в секундах, по истечении которого маршрут объявляется как недопустимый; его значение должно быть по меньшей мере в три раза больше значения параметра `update`. Параметр *`hold-down`* (который равен по умолчанию 180 с) устанавливает интервал в секундах, в течение которого происходит подавление передачи маршрутной информации о лучших маршрутах. Его значение должно превышать значение параметра *`update`* по меньшей мере в три раза. Параметр `flush`, значение по умолчанию которого равно 240 с, определяет продолжительность времени в секундах, которое должно пройти, прежде чем маршрут будет удален из таблицы маршрутизации; указанный интервал должен быть не меньше суммы значений параметров `invalid` и `hold-down`. Если его значение меньше этой суммы, то не может вовремя закончиться надлежащий интервал удержания. Это приводит к принятию нового маршрута еще до истечения интервала удержания (`hold-down`). Параметр *`sleeptime`* устанавливает интервал в миллисекундах, позволяющий отложить ввод в действие обновлений маршрутизации в том случае, если происходит обновление содержимого флэш-памяти. Значение *`sleeptime`* должно быть меньше по сравнению со значением времени *`update`*. Если значение *`sleeptime`* больше значения времени *`update`*, то таблицы маршрутизации становятся несинхронизированными.

9. (Необязательно.) Введение задержки между пакетами отправляемых обновлений RIP:

```
(router) output-delay delay
```

Маршрутизатор разделяет исходящие пакеты обновлений, состоящих из нескольких пакетов, на величину интервала в миллисекундах, определяемого параметром `delay`. Значение задержки может быть задано равным от 8 до 50 мс (значение по умолчанию — 0). Необходимость в использовании этого параметра может возникнуть, если маршрутизатор-отправитель является намного более быстродействующим, чем маршрутизатор-получатель. Если обнаруживается, что в медленно действующем маршрутизаторе происходит уничтожение входящих обновлений RIP, то в конфигурации можно задать значение задержки, определив его экспериментальным путем. Начните со значения 10 мс и увеличивайте его до достижения приемлемой производительности.

ВНИМАНИЕ!

При корректировке значений таймеров маршрутизации необходимо соблюдать исключительную осторожность. Если значения этих таймеров в соседних устройствах становятся несогласованными, то может происходить самопроизвольное изменение маршрута (route flapping).

10. (Необязательно.) Запрет на проверку правильности IP-адресов отправителя для входящих обновлений:

```
(router) no validate-update-source
```

Эта команда используется для предотвращения отбрасывания маршрутизатором полученных обновлений с адресом отправителя, находящимся вне сети; под этим подразумевается устройство с адресом отправителя, который не находится в таблице маршрутизации.

11. (Необязательно.) Запрещение разделения диапазона:

```
(interface) no ip split-horizon
```

Будучи дистанционно-векторным протоколом маршрутизации, RIP реализует разделение диапазона. Для запрета применения этого средства отдельно для каждого интерфейса используется команда `no ip split-horizon`. Необходимость в этом может возникнуть при работе с протоколом типа X.25 или при использовании многоточечного соединения Frame Relay.

12. (Необязательно.) Ввод в действие активизированных обновлений:

```
(interface) ip rip triggered
```

13. В медленно действующих каналах распределенной сети, ориентированных на соединение, издержки, связанные с периодической передачей пакетов RIP, могут составить значительную часть пропускной способности канала и отрицательно повлиять на передачу данных. В каналах, ориентированных на соединение, могут быть разрешены расширения протокола RIP с применением активизации передачи обновлений (см. документ RFC 2091) в целях подавления передачи периодических обновлений и отправки обновлений только при обнаружении изменений в таблице маршрутизации.

Команды, относящиеся только к версии RIP-2

1. (Необязательно.) Запрещение автоматического суммирования:

```
(router) no auto-summary
```

Суммирование маршрутов разрешено по умолчанию. Анонсированные маршруты к подсетям суммируются в сетевые маршруты с поддержкой классов. Если для смежных подсетей назначены разные интерфейсы, то суммирование маршрутов должно быть запрещено.

2. (Необязательно.) Ввод в действие аутентификации RIP.

a) Ввод в действие аутентификации пакетов RIP:

```
(interface) ip rip authentication key-chain name-of-chain
```

Эта команда позволяет ввести в действие средства аутентификации применительно к указанному интерфейсу с использованием заданной цепочки

ключей. Благодаря этому появляется возможность проверять обновления до их обработки маршрутизатором.

б) Выбор режима аутентификации:

```
(interface) ip rip authentication mode {text | md5}
```

Эта команда указывает режим шифрования, используемый в процессе маршрутизатора для отправки ключа. Шифрование открытого текста не происходит, а применение параметра `md5` приводит к тому, что используется шифрование по протоколу MD5 (Message Digest 5).

в) Определение цепочки ключей:

```
(global) key chain keychain-name
```

С помощью этой команды происходит определение и именование цепочки ключей. Цепочка ключей содержит один или более ключей аутентификации, которые могут использоваться в работе. Вообще говоря, для каждого интерфейса используется по одной цепочке ключей.

г) Настройка конфигурации нумерованного ключа в цепочке ключей:

```
(keychain) key number
```

Ключи могут обозначаться номерами от 0 до 2147483647.

д) Определение текстовой строки для ключа:

```
(keychain-key) key-string text
```

В качестве ключа аутентификации используется строка аутентификации *text*. Строка может иметь длину от 1 до 80 символов (алфавитные символы в верхнем или нижнем регистре, а также цифровые символы; первый символ должен быть алфавитным).

е) Определение того, в течение какого времени полученный ключ будет считаться допустимым:

```
(keychain-key) accept-lifetime start-time {infinite | end-time |
duration seconds}
```

Параметр `start-time` с определением времени начала может быть указан в формате *hh*:*mm*:*ss month date year* (чч:мм:сс месяц число год) или *hh*:*mm*:*ss date month year* (чч:мм:сс число месяц год); должны быть заданы три первые буквы англоязычного названия месяца и все четыре цифры года. Ключевое слово `infinite` позволяет указать, что ключ остается приемлемым со времени, указанного параметром `start-time`, и далее. В ином случае может быть указано время окончания действия ключа с помощью параметра `end-time` в том же формате или задана продолжительность действия в секундах после времени начала, `start-time`.

ж) Определение того, как долго отправленный ключ может считаться допустимым:

```
(keychain-key) send-lifetime start-time {infinite | end-time | du-
ration seconds}
```

В этой команде параметры с указанием времени идентичны параметрам, определенным в п. *е*.

НА ЗАМЕТКУ

Надлежащее выполнение операций с цепочками ключей, в которых используются параметры `accept-lifetime` и (или) `send-lifetime`, возможно лишь при том условии, что синхросигналы маршрутизатора введены в действие и согласованы по отношению к другим маршрутизаторам в сети. При желании в качестве метода синхронизации может использоваться сетевой протокол времени (Network Time Protocol — NTP). Кроме того, параметры `accept-lifetime` и `send-lifetime` должны быть заданы с некоторым перекрытием на случай расхождений в синхросигналах маршрутизаторов или временны*х* несовпадений в значениях ключей.

3. Для получения дополнительной информации о средствах обработки маршрутов обратитесь к следующим разделам.
   - 8.3. Перераспределение маршрутной информации
   - 8.4. Фильтрация маршрутной информации

Пример

На рис. 6.1 показана схема сети для этого примера. Протокол RIP был введен в действие для сети 1.0.0.0, в которой применение RIP разрешено во всех показанных здесь интерфейсах. Для интерфейса Ethernet обновления в виде широковещательных сообщений не передаются вследствие применения команды `passive-interface`. Вместо этого для соседнего устройства с адресом 1.2.2.2 в этом сегменте отправляются одноадресатные обновления. В глобальной конфигурации указан протокол RIP версии 1, а это означает, что в интерфейсах Ethernet 0 и Serial 0 будут происходить передача и получение только обновлений RIP-1, а в конфигурации интерфейса Serial 1 задано, что он применяется для отправки и получения пакетов RIP-1 и RIP-2. Для интерфейса Serial 0 разделение диапазона было запрещено.

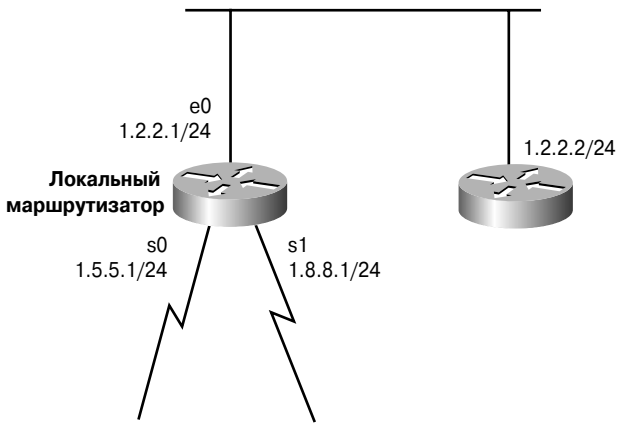

Рис. 6.1. Схема сети для примера применения протокола RIP

```
interface ethernet 0
        ip address 1.2.2.1 255.255.255.0
interface serial 0
        ip address 1.5.5.1 255.255.255.0
        encapsulation frame-relay
```

```
        no ip split-horizon
interface serial 1
        ip address 1.8.8.1 255.255.255.0
        ip rip send version 1 2
        ip rip receive version 1 2
router rip
         network 1.0.0.0
         version 1
         passive-interface ethernet 0
         neighbor 1.2.2.2
```

6.2. Протокол маршрутной информации (RIP) для IPv6

- В протоколе RIP для сети IPv6 в качестве адреса получателя для сообщений обновления RIP используется адрес группы многоадресной рассылки для маршрутизаторов с любыми версиями RIP, т.е. адрес FF02::9.
- В протоколе RIP для сети IPv6 используется порт 521 протокола UDP.

НА ЗАМЕТКУ

Способ функционирования протокола RIP для сети IPv6 не отличается от применяемого в версии RIPv2. (Дополнительные сведения о протоколе RIP для сети IPv6 см. в документе RFC 2080, “RIPng for IPv6”.)

Настройка конфигурации

1. Ввод в действие одноадресатной маршрутизации IPv6:

   ```
   (config) ipv6 unicast-routing
   ```

   Как и применительно ко всем маршрутизирующим протоколам IPv6, необходимо вначале ввести в действие одноадресатную маршрутизацию IPv6, чтобы разрешить перенаправление пакетов IPv6.

2. Ввод в действие протокола RIP для сети IPv6 во всех интерфейсах, которые должны участвовать в процессе RIP:

   ```
   (interface) ipv6 rip name enable
   ```

   В отличие от процедуры настройки конфигурации протокола RIP для сети IPv4, не нужно указывать, с применением какой версии RIP будет осуществляться процесс маршрутизации, а также задавать сети, для которых необходимо передавать анонсы. Вместо этого следует переходить от одного интерфейса к другому и активизировать средства RIP для сети IPv6. Параметр *name* служит для идентификации процесса маршрутизации IPv6.

НА ЗАМЕТКУ

Большинство параметров конфигурации, применяемых в версиях RIPv1 и RIPv2 для сети IPv4, являются применимыми и для протокола RIP в сети IPv6. Чтобы выполнить настройку конфигурации протокола RIP для сети IPv6, необходимо вначале перейти к процессу RIP, введя глобальную команду конфигурации `ipv6 router rip` *name*, где параметр *name*

указывает имя процесса RIP, введенное ранее при активизации процесса RIP в интерфейсах. Находясь в этом режиме, можно выполнить настройку RIP, как было описано выше для версии RIPv1 или RIPv2 (например, задавая в конфигурации максимальную длину путей или перераспределяя маршрутизирующие протоколы).

Пример

На рис. 6.2 показан пример настройки конфигурации маршрутизатора RouterA для использования протокола RIP в сети IPv6. Процесс RIP активизирован в обоих интерфейсах, FastEthernet0/0 и FastEthernet0/1.

Рис. 6.2. Пример применения протокола RIP в сети IPv6

```
hostname RouterA
!
ipv6 unicast-routing
!
interface fastethernet0/0
 ipv6 address 2001:429F:DA90:1::1/64
 ipv6 rip ripprocess enable
!
interface fastethernet0/1
 ipv6 address 2001:429F:DA90:2::1/64
 ipv6 rip ripprocess enable
```

6.3. Расширенный протокол маршрутизации внутреннего шлюза (Enhanced Interior Gateway Routing Protocol — EIGRP)

- Протокол EIGRP — это дистанционно-векторный протокол маршрутизации, в котором метрика вычисляется с применением комбинации параметров *delay*, *bandwidth*, *reliability*, *load* и *mtu*.
- Протокол EIGRP допускает увеличенную ширину сети: 224 транзитных перехода (количество транспортных транзитных переходов начинает увеличиваться только после достижения 15 транзитных переходов EIGRP).
- В протоколе EIGRP предусмотрено обнаружение соседних устройств с применением протокола передачи приветственных сообщений (при этом осуществляется многоадресатная рассылка по всем маршрутизаторам EIGRP; какие-либо пакеты ACK не требуются).
- В протоколе EIGRP используются частичные обновления таблицы маршрутизации (с применением надежной многоадресатной рассылки).
- Протокол EIGRP поддерживает применение масок подсетей переменной длины (Variable-Length Subnet Masking — VLSM) и суммирование маршрутов.

- В случае обнаружения изменений топологии для проверки наличия допустимых преемников применяется алгоритм DUAL. Если таковые не обнаруживаются, то повторное вычисление не выполняется.

НА ЗАМЕТКУ

В протоколе EIGRP используется протокол IP с номером 88 для обеспечения обмена данными между соседними устройствами по многоадресатному адресу 224.0.0.10. Если конкретные соседние устройства определены, то вместо этого используются их одноадресатные IP-адреса.

Настройка конфигурации

1. Ввод в действие процесса маршрутизации EIGRP:

   ```
   (global) router eigrp autonomous-system-number
   ```

   В маршрутизаторах EIGRP для определения связи с одним и тем же доменом маршрутизации применяется номер, рассматриваемый как номер автономной системы (autonomous-system — AS). Маршрутизаторы, в которых эксплуатируется протокол EIGRP с одним и тем же номером AS, могут обмениваться маршрутами.

2. Определение связи сети с номером AS протокола EIGRP:

   ```
   (router) network network-number
   ```

   Обновления передаются через эти интерфейсы, и эти же интерфейсы анонсируются. В этой конфигурации номера сетей сводятся до сетей с поддержкой классов.

НА ЗАМЕТКУ

Если происходит переход от протокола IGRP к протоколу EIGRP, то в применяемых для перехода маршрутизаторах должны эксплуатироваться оба протокола, IGRP и EIGRP. Для обеспечения автоматического перераспределения маршрутов в обоих протоколах, IGRP и EIGRP, должны применяться одинаковые номера AS или номера процессов. Как только перераспределение будет завершено, протокол IGRP можно отключить.

3. (Необязательно.) Ввод в действие процесса маршрутизации EIGRP с использованием именованной конфигурации:

   ```
   (global) router eigrp virtual-name
   ```

   В качестве альтернативы по отношению к настройке конфигурации на основе номеров AS при вводе в действие протокола EIGRP можно выполнять настройку с использованием именованной конфигурации. Если задача состоит в осуществлении настройки конфигурации EIGRP в виртуальных частных сетях IPv4 или IPv6, то создание виртуального имени становится необходимым.

4. (Необязательно.) Определение конфигурации семейства адресов и назначение ему номера AS:

   ```
   (router) address-family [ipv4 | ipv6] autonomous-system autonomous-
   system-number
   ```

   Если используется именованная конфигурация, то необходимо определять конфигурацию семейств адресов и назначать номер AS каждому семейству адресов.

5. (Необязательно.) Определение равномерного распределения нагрузки с неравной стоимостью:

```
(router) variance multiplier
```

Заданным по умолчанию значением параметра `variance` является 1 (равномерное распределение нагрузки с равной стоимостью). Параметр `multiplier` указывает предел, в котором может изменяться метрика маршрута (начиная от метрики с самой низкой стоимостью), оставаясь все еще включенной в равномерное распределение нагрузки с неравной стоимостью.

6. (Необязательно.) Корректировка весовых коэффициентов метрики:

```
(router) metric weights tos k1 k2 k3 k4 k5
```

По умолчанию применяется 32-битовая метрика — сумма задержек в сегменте и самой низкой полосы пропускания сегмента (после масштабирования и обращения). В случае однородных сетей эти операции сводятся к получению количества транзитных переходов.

(См. раздел 8.3, "Перераспределение маршрутной информации", для получения дополнительных сведений о вычислении метрики и значениях весовых коэффициентов.)

НА ЗАМЕТКУ

Для изменения метрики маршрута EIGRP может использоваться команда `bandwidth`. Но ее действие распространяется и на протокол EIGRP, и на протокол OSPF, поскольку в том и в другом для вычисления метрики используется значение полосы пропускания. Для внесения изменений, затрагивающих только EIGRP, следует корректировать метрику с использованием команды конфигурации интерфейса `delay`.

7. (Необязательно.) Корректировка процентного соотношения для полосы пропускания канала EIGRP:

```
(router) ip bandwidth-percent eigrp percentage
```

По умолчанию в протоколе EIGRP предусмотрено ограничение объема передаваемых обновлений, чтобы для них использовалось не больше 50% полосы пропускания канала. Полоса пропускания канала определяется с помощью команды конфигурации интерфейса `bandwidth`.

8. (Необязательно.) Ввод в действие тупиковой маршрутизации EIGRP:

```
(router) eigrp stub [receive-only | connected | static | summary |
receive-only leak-map map-name]
```

В топологии "центральный и периферийные" нет необходимости запрашивать периферийные маршрутизаторы в ходе изменения топологии. Чтобы ограничить диапазон рассылки запросов для предотвращения передачи запросов в тупиковые маршрутизаторы, можно ввести в действие тупиковую маршрутизацию EIGRP применительно к тупиковым маршрутизаторам. По умолчанию тупиковые маршрутизаторы анонсируют только подключенные и суммарные маршруты. При желании можно настроить конфигурацию тупикового маршрутизатора, чтобы он только получал данные о маршрутах. Можно также задать в конфигурации параметр `leak-map`, определяющий так называемую "схему утечки", ко-

торая идентифицирует маршруты, разрешенные для анонсирования в тупиковом маршрутизаторе, но при обычных обстоятельствах подавляемые. Параметр `leak-map` ссылается на схему маршрута, заданную в конфигурации маршрутизатора, в которой разрешены сети, подлежащие анонсированию. В идеальном случае следует настраивать конфигурацию центрального маршрутизатора так, чтобы он передавал в периферийные маршрутизаторы данные только о стандартных маршрутах (маршрутах, применяемых по умолчанию) или суммарных маршрутах.

9. (Необязательно.) Запрещение автоматического суммирования маршрутов:

```
(router) no auto-summary
```

Суммирование маршрутов разрешено по умолчанию. Анонсированные маршруты к подсетям суммируются в сетевые маршруты с поддержкой классов. Если для смежных подсетей назначены разные интерфейсы, то суммирование маршрутов должно быть запрещено.

10. (Необязательно.) Применение суммарных агрегированных адресов:

```
(interface) ip summary-address eigrp autonomous-system-number ad-
dress mask
```

Из интерфейса передаются анонсы с адресом и маской агрегированного маршрута. Метрика определяется как длина минимального из наиболее конкретизированных маршрутов.

11. (Необязательно.) Корректировка интервалов передачи приветственных сообщений и интервалов удержания:

```
(interface) ip hello-interval eigrp autonomous-system-number seconds
```

Приветственные сообщения по умолчанию передаются с интервалом 5 с; в передающей среде с нешироковещательным множественным доступом (nonbroadcast multiaccess — NBMA), характеризующейся низкими скоростями передачи (в канале 9T1), этот интервал составляет 60 с. Заданный по умолчанию тайм-аут задержки превышает в три раза тайм-аут передачи приветственных сообщений (и составляет 15 с в обычной среде и 180 с в среде NBMA).

12. (Необязательно.) Запрещение разделения диапазона:

```
(interface) no ip split-horizon eigrp autonomous-system-number
```

Если разрешено разделение диапазона, то обновления и запросы не передаются получателям, для которых интерфейс является следующим транзитным переходом. Разделение диапазона разрешено по умолчанию, но иногда должно быть запрещено в сети Frame Relay или SMDS.

13. (Необязательно.) Ввод в действие аутентификации EIGRP.

а) Ввод в действие аутентификации пакетов EIGRP с помощью алгоритма MD5 (Message Digest 5):

```
(interface) ip authentication mode eigrp autonomous-system-number md5
```

б) Ввод в действие цепочки ключей, применяемой для аутентификации MD5:

```
(interface) ip authentication key-chain eigrp autonomous-system-
number key-chain
```

Эта команда вводит в действие средства аутентификации в конкретном интерфейсе, в которых используется указанная цепочка ключей. С помощью данной команды можно обеспечить проверку обновлений перед их обработкой маршрутизатором.

в) Определение цепочки ключей:

```
(global) key chain name-of-chain
```

Цепочка ключей должна быть определена и ей должно быть присвоено имя. Цепочка ключей содержит один или более ключей аутентификации, которые могут использоваться в работе. Вообще говоря, для каждого интерфейса используется по одной цепочке ключей.

г) Настройка конфигурации нумерованного ключа в цепочке ключей:

```
(keychain) key number
```

Ключи могут обозначаться номерами от 0 до 2147483647.

д) Определение текстовой строки для ключа:

```
(keychain-key) key-string text
```

В качестве ключа аутентификации используется строка аутентификации *text*. Строка может иметь длину от 1 до 80 символов (алфавитные символы в верхнем или нижнем регистре, а также цифровые символы; первый символ должен быть алфавитным).

е) Определение времени, в течение которого полученный ключ будет считаться допустимым:

```
(keychain-key) accept-lifetime start-time {infinite | end-time |
duration seconds}
```

Параметр `start-time` с определением времени начала может быть указан в формате *hh*:*mm*:*ss month date year* (чч:мм:сс месяц число год) или *hh*:*mm*:*ss date month year* (чч:мм:сс число месяц год); должны быть заданы три первые буквы англоязычного названия месяца и все четыре цифры года. Ключевое слово `infinite` позволяет указать, что ключ остается приемлемым со времени, указанного параметром `start-time`, и далее. В ином случае может быть указано время окончания действия ключа с помощью параметра `end-time` в том же формате или задана продолжительность действия в секундах после времени начала, `start-time`.

ж) Определение того, как долго отправленный ключ может считаться допустимым:

```
(keychain-key) send-lifetime start-time {infinite | end-time | du-
ration seconds}
```

В этой команде параметры с указанием времени идентичны параметрам, определенным в п. *е*.

НА ЗАМЕТКУ

Надлежащее выполнение операций с цепочками ключей, в которых используются параметры `accept-lifetime` и (или) `send-lifetime`, возможно лишь при том условии, что синхросигналы маршрутизатора введены в действие и согласованы по отношению к другим

маршрутизаторам в сети. В качестве метода синхронизации может использоваться сетевой протокол времени (Network Time Protocol — NTP). Кроме того, параметры `accept-lifetime` и `send-lifetime` должны быть заданы с некоторым перекрытием на случай расхождений в синхросигналах маршрутизаторов или временны*х* несовпадений в значениях ключей.

14. Для получения дополнительной информации о средствах обработки маршрутов обратитесь к следующим разделам.
    - 8.3. Перераспределение маршрутной информации
    - 8.4. Фильтрация маршрутной информации

Пример

Схема сети показана на рис. 6.3. Настройка конфигурации маршрутизатора выполнена с учетом применения процесса маршрутизации EIGRP. По протоколу EIGRP анонсируются все непосредственно подключенные сети. В интерфейсе Fast Ethernet маршрутизатор выполняет аутентификацию EIGRP по отношению к соседним устройствам с применением алгоритма MD5. Цепочка ключей MyChain состоит из двух применимых строк, secret123 и secret987. Ключи MD5 считаются приемлемыми круглосуточно, начиная с 1 января 2001 года, кроме того, ключи MD5 передаются в течение 24 часов, начиная со времени 1:00 и даты “1 января 2001 года”.

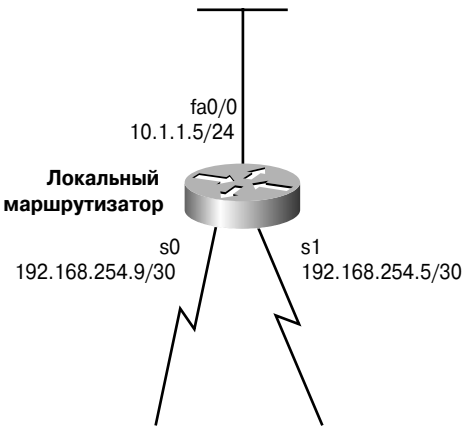

Рис. 6.3. Схема сети для примера применения протокола EIGRP

```
interface fastethernet 0/0
        ip address 10.1.1.5 255.255.255.0
        ip authentication mode eigrp 101 md5
        ip authentication key-chain eigrp 101 MyChain
key chain MyChain
        key 1
                key-string secret123
        key 2
                key-string secret987
                accept-lifetime 00:00:00 Jan 1 2001 23:59:00 Jan 1 2001
                send-lifetime 01:00:00 Jan 1 2001 01:00:00 Jan 2 2001
interface serial 0
```

```
        encapsulation frame-relay
        ip address 192.168.254.9 255.255.255.252
interface serial 1
         encapsulation frame-relay
         ip address 192.168.254.5 255.255.255.252
router eigrp 101
         network 10.1.1.0
         network 192.168.254.0
         no auto-summary
```

6.4. Расширенный протокол маршрутизации внутреннего шлюза (EIGRP) для IPv6

- Для ввода в действие протокола EIGRP в сети IPv6 необходимо задать идентификатор маршрутизатора, прежде чем он будет активизирован.
- Как и при настройке конфигурации протокола RIP в сети IPv6, конфигурация EIGRP в сети IPv6 определяется применительно к интерфейсам, которые должны участвовать в процессе EIGRP.

Настройка конфигурации

1. Ввод в действие одноадресатной маршрутизации IPv6:

   ```
   (config) ipv6 unicast-routing
   ```

   Чтобы обеспечить перенаправление пакетов IPv6, необходимо ввести в действие средства одноадресатной маршрутизации IPv6.

2. Ввод в действие процесса обеспечения функционирования сети IPv6 в интерфейсах:

   ```
   (interface) ipv6 eigrp autonomous-system-number
   ```

   Эта команда активизирует средства протокола EIGRP в интерфейсе. Если в маршрутизаторе еще не функционирует протокол EIGRP, то происходит запуск нового процесса EIGRP для указанного номера AS.

3. Переход к процессу EIGRP и определение идентификатора маршрутизатора в конфигурации:

   ```
   (config) ipv6 router eigrp autonomous-system-number
   (router) eigrp router-id ipv4-address
   ```

   Для работы EIGRP в сети IPv6 требуется 32-битовый идентификатор маршрутизатора, используемый в сообщениях EIGRP для обозначения отправителя сообщения. Введенный адрес IPv4 не должен быть действительным адресом, назначенным какому-либо из интерфейсов.

4. (Необязательно.) Задание в конфигурации суммарного агрегированного адреса для интерфейса:

   ```
   (interface) ipv6 summary-address eigrp autonomous-system-number
   ipv6-aggregate-address/prefix-length
   ```

   Из интерфейса передаются анонсы с указанием адреса агрегированного маршрута и длины префикса. Метрика определяется как длина минимального из наиболее конкретизированных маршрутов.

5. (Необязательно.) Корректировка процентного соотношения для полосы пропускания канала EIGRP:

```
(interface) ipv6 bandwidth-percent eigrp autonomous-system-number
percentage
```

По умолчанию в протоколе EIGRP предусмотрено ограничение объема передаваемых обновлений, чтобы для них использовалось не больше 50% полосы пропускания канала. Полоса пропускания канала определяется с помощью команды конфигурации интерфейса `bandwidth`.

6. (Необязательно.) Ввод в действие аутентификации EIGRP.

а) Ввод в действие аутентификации пакетов EIGRP с помощью алгоритма MD5 (Message Digest 5):

```
(interface) ipv6 authentication mode eigrp autonomous-system-
number md5
```

б) Ввод в действие цепочки ключей, применяемой для аутентификации MD5:

```
(interface) ipv6 authentication key-chain eigrp autonomous-system-
number key-chain
```

С помощью этой команды осуществляется ввод в действие средств аутентификации в указанном интерфейсе с использованием заданной цепочки ключей, что позволяет проверять обновления до их обработки маршрутизатором.

в) Определение цепочки ключей:

```
(global) key chain name-of-chain
```

Цепочка ключей должна быть определена и обозначена именем. Цепочка ключей содержит один или более ключей аутентификации, которые могут использоваться в работе. Вообще говоря, для каждого интерфейса должно быть задано по одной цепочке ключей.

г) Задании в конфигурации ключа с определенным номером, применяемого в цепочке ключей:

```
(keychain) key number
```

Ключи могут обозначаться номерами от 0 до 2147483647.

д) Определение текстовой строки для ключа:

```
(keychain-key) key-string text
```

В качестве ключа аутентификации используется строка аутентификации *`text`*. Строка может иметь длину от 1 до 80 символов (алфавитные символы в верхнем или нижнем регистре, а также цифровые символы; первый символ должен быть алфавитным).

е) Определение времени, в течение которого полученный ключ будет считаться допустимым:

```
(keychain-key) accept-lifetime start-time {infinite | end-time |
duration seconds}
```

Параметр `start-time` с определением времени начала может быть указан в формате *`hh:mm:ss month date year`* (чч:мм:сс месяц число год) или *`hh:mm:ss date month year`* (чч:мм:сс число месяц год); должны быть заданы три первые буквы англоязычного названия месяца и все четыре

цифры года. Ключевое слово `infinite` позволяет указать, что ключ остается приемлемым со времени, указанного параметром `start-time`, и далее. В ином случае может быть указано время окончания действия ключа с помощью параметра `end-time` в том же формате или задана продолжительность действия в секундах после времени начала, `start-time`.

ж) Определение того, как долго отправленный ключ может считаться допустимым:

```
(keychain-key) send-lifetime start-time {infinite | end-time | du-
ration seconds}
```

7. (Необязательно.) Корректировка интервалов передачи приветственных сообщений и интервалов удержания:

```
(interface) ipv6 hello-interval eigrp autonomous-system-number seconds
(interface) ipv6 hold-time eigrp autonomous-system-number secondAs
```

Приветственные сообщения по умолчанию передаются с интервалом 5 с; в передающей среде с нешироковещательным множественным доступом (nonbroadcast multiaccess — NBMA), характеризующейся низкими скоростями передачи (в канале 9T1), этот интервал составляет 60 с. Заданный по умолчанию тайм-аут задержки превышает в три раза тайм-аут передачи приветственных сообщений (и составляет 15 с в обычной среде и 180 с в среде NBMA).

8. (Необязательно.) Запрещение разделения диапазона:

```
(interface) no ipv6 split-horizon eigrp autonomous-system-number
```

Если разрешено разделение диапазона, то обновления и запросы не передаются получателям, для которых интерфейс является следующим транзитным переходом. Разделение диапазона разрешено по умолчанию, но иногда должно быть запрещено в сети Frame Relay или SMDS.

9. (Необязательно.) Ввод в действие тупиковой маршрутизации EIGRP:

```
(config) ipv6 router eigrp autonomous-system-number
(router) eigrp stub [receive-only | connected | static | summary |
receive-only | leak-map map-name]
```

В топологии "центральный и периферийные" нет необходимости запрашивать периферийные маршрутизаторы в ходе изменения топологии. Чтобы ограничить диапазон рассылки запросов для предотвращения передачи запросов в тупиковые маршрутизаторы, можно ввести в действие тупиковую маршрутизацию EIGRP применительно к тупиковым маршрутизаторам. По умолчанию тупиковые маршрутизаторы анонсируют только подключенные и суммарные маршруты. При желании можно настроить конфигурацию тупикового маршрутизатора, чтобы он только получал данные о маршрутах. Можно также задать в конфигурации параметр `leak-map`, определяющий так называемую "схему утечки", которая идентифицирует маршруты, разрешенные для анонсирования в тупиковом маршрутизаторе, но при обычных обстоятельствах подавляемые. Параметр `leak-map` ссылается на схему маршрута, заданную в конфигурации маршрутизатора, в которой разрешены сети, подлежащие анонсированию. В идеальном случае следует настраивать конфигурацию центрального маршрутизатора так, чтобы он передавал в периферийные маршрутизаторы данные только о стандартных маршрутах (маршрутах, применяемых по умолчанию) или суммарных маршрутах.

Пример

На рис. 6.4 показан пример настройки конфигурации маршрутизатора RouterA для использования протокола EIGRP в сети IPv6. Настройка конфигурации обоих интерфейсов FastEthernet произведена с учетом применения в них протокола EIGRP.

Рис. 6.4. Пример применения протокола EIGRP в сети IPv6

```
hostname RouterA
!
ipv6 unicast-routing
!
ipv6 router eigrp 1
 router-id 1.1.1.1
!
interface fastethernet0/0
 ipv6 address 2001:429F:DA90:1::1/64
 ipv6 eigrp 1
!
interface fasthernet0/1
 ipv6 address 2001:429F:Da90:2::1/64
 ipv6 eigrp 1
```

6.5. Открытый протокол предпочтительного выбора кратчайшего пути (Open Shortest Path First — OSPF)

- OSPF — это протокол маршрутизации с учетом состояния каналов, в котором используется метрика стоимости, вычисляемая с использованием значений полосы пропускания каналов.
- OSPF представляет собой протокол, независимый от производителя, который определен документом RFC 2328.
- В протоколе OSPF используются многоадресатные анонсы для передачи сведений об изменениях в топологии маршрутизации.
- OSPF — это протокол маршрутизации без поддержки классов, который обеспечивает работу в сетях, организованных на основе формата VLSM.

НА ЗАМЕТКУ

В протоколе OSPF используется протокол IP с номером 89 для обеспечения обмена данными и применяется многоадресатный адрес 224.0.0.5 для отправки обновлений всем маршрутизаторам OSPF. Для отправки обновлений назначенным маршрутизаторам OSPF в протоколе OSPF используется многоадресатный адрес 224.0.0.6.

- Данный иерархический протокол маршрутизации поддерживает области, что позволяет управлять распределением обновлений маршрутизации.
- Протокол OSPF поддерживает суммирование маршрутов между областями, что позволяет уменьшать до минимума количество записей в таблице маршрутизации.

Настройка конфигурации

1. (Необязательно, но рекомендовано.) Задание в конфигурации IP-адреса петлевого интерфейса для определения идентификатора маршрутизатора OSPF:

```
(global) interface loopback 0
(interface) ip address ip-address subnet mask
```

   Все маршрутизаторы OSPF идентифицируют себя и свои анонсы состояния каналов. Маршрутизаторы Cisco для выбора своего идентификатора применяют петлевой интерфейс с наиболее высоким IP-адресом, если таковой задан в конфигурации. В противном случае маршрутизатор получает свой идентификатор от физического интерфейса, имеющего самый высокий IP-адрес. Задавая петлевой адрес, можно управлять тем, каким должен быть идентификатор маршрутизатора. Эта настройка должна быть выполнена до ввода в действие процесса OSPF. Еще один вариант состоит в том, что можно указывать идентификатор маршрутизатора с помощью команды `router-id` *`ip-address`* процесса OSPF. IP-адрес, указанный в команде `router-id`, не обязательно должен быть IP-адресом, назначенным какому-либо из интерфейсов маршрутизатора.

2. Ввод в действие процесса OSPF:

```
(global) router ospf process-id
```

   Эта команда переводит устройство в режим настройки конфигурации маршрутизатора. Идентификатор процесса не зависит от маршрутизатора и используется в целях идентификации конкретного экземпляра OSPF для маршрутизатора.

3. Активизация процесса OSPF для сети и связывание этой сети с областью:

```
(router) network network-number wildcard-mask area area-id
```

   Команда `network` разрешает применение процесса OSPF в любом интерфейсе, который входит в диапазон, указанный маской с подстановочными символами. Например, параметр 172.16.0.0 с маской 0.0.255.255 разрешает применение OSPF в любом интерфейсе, которому назначен адрес с первыми двумя октетами, равными 172.16.

   Параметр `area-id` указывает, что эти сети должны быть назначены одной из областей OSPF. Параметр `area-id` может быть определен как десятичное обозначение области (от 0 до 4294967295) или в виде четырех октетов, записанных в формате IP-адреса. Формат IP-адреса может оказаться полезным, если устанавливается соответствие подсетей IP с областями OSPF. В любом случае параметр `area-id` представляет собой 32-битовое значение, которое может быть записано в любом из двух указанных форматов. Например, область 5 может также быть записана как область 0.0.0.5.

НА ЗАМЕТКУ

Сеть OSPF должна иметь *магистральную* зону, которая определена в маршрутизаторах как зона OSPF с номером 0 или 0.0.0.0.

4. (Необязательно.) Настройка конфигурации тупиковой области:

   ```
   (router) area area-id stub [no-summary]
   ```

   Эта команда отмечает область флагом как тупиковую. Если область определена как тупиковая, то для всех маршрутизаторов в этой области должен быть установлен флаг тупиковой области. Использование параметра `no-summary` для ABR приводит к созданию полностью тупиковой области, которая предотвращает введение любых внешних маршрутов или маршрутов между областями в область, заданную в конфигурации.

5. (Необязательно.) Определение стоимости стандартного маршрута, сформированного в тупиковой области:

   ```
   (router) area area-id default-cost cost
   ```

   Если установлена тупиковая область или полностью тупиковая область, то маршрутизаторам области передается стандартный маршрут вместо каких-либо внешних маршрутов или маршрутов между областями. Эта команда устанавливает заданную по умолчанию стоимость для таких стандартных маршрутов.

6. (Необязательно.) Определение конфигурации не полностью тупиковой области (not-so-stubby area — NSSA):

   ```
   (router) area area-id nssa [no-redistribution] [default-information-
   originate]
   ```

   Определение области NSSA позволяет передавать внешние маршруты через тупиковую область. Параметр `no-redistribution` используется по отношению к маршрутизатору ABR (Area Border Router — граничный маршрутизатор области), если требуется, чтобы внешние маршруты перераспределялись только в обычные области, а не в какие-либо области NSSA. Параметр `default-information-originate` используется в граничном маршрутизаторе области (ABR) для формирования стандартного маршрута в NSSA.

7. (Необязательно.) Настройка конфигурации виртуального канала для обеспечения связи в магистральной области:

   ```
   (router) area area-id virtual-link router-id [hello-interval sec-
   onds] [retransmit-interval seconds] [transmit-delay seconds] [dead-
   interval seconds] [[authentication-key key] [message-digest-key
   keyid md5 key]]
   ```

   Виртуальный канал представляет собой расширение магистральной области. Он предоставляет для магистральной области возможность связывать несмежные области. Параметр `area-id` обозначает транзитную область, т.е. область, которую необходимо пересечь для достижения магистральной области. Параметр `router-id` обозначает дополнительный маршрутизатор, который должен сформировать виртуальный канал.

НА ЗАМЕТКУ

Команда `virtual-link` должна быть задана в конфигурации каждого устройства, которое образует соединение от дальней области к магистральной области (области 0 или 0.0.0.0). Виртуальный канал является расширением магистральной области, поэтому для него также должны быть заданы все необходимые параметры аутентификации или таймеры.

8. (Необязательно.) Суммирование маршрутов между областями:

```
(router) area area-id range summary-address mask
```

Эта команда позволяет маршрутизатору ABR уменьшить количество маршрутов, передаваемых им в указанную область, путем отправки суммарного адреса вместо любого маршрута, который находится в пределах диапазона, указанного с помощью маски.

9. (Необязательно.) Определение приоритета интерфейса OSPF:

```
(interface) ip ospf priority number
```

Это значение может составлять от 0 до 255; по умолчанию применяется значение 1. Данный параметр используется для выбора назначенного маршрутизатора (Designated Router — DR) и резервного назначенного маршрутизатора (Backup Designated Router — BDR) в сетях широковещательного типа. Приоритет 0 указывает, что маршрутизатор для сети широковещательного типа не может быть маршрутизатором DR или BDR.

НА ЗАМЕТКУ

Следует избегать установления приоритета 0 протокола OSPF для всех маршрутизаторов, подключенных к широковещательному домену. Если все эти маршрутизаторы будут иметь приоритет 0, то ни один из них не сможет сформировать отношения смежности. Кроме того, не будет ни одного выбранного маршрутизатора DR.

а) (Необязательно.) Задание тайм-аута передачи приветственных сообщений:

```
(interface) ip ospf hello-interval seconds
```

Этот параметр задает количество секунд между обновлениями приветственных сообщений (значение по умолчанию — 10 с). Чтобы маршрутизаторы могли сформировать отношения смежности, значения тайм-аутов передачи приветственных сообщений в соседних устройствах должны совпадать.

б) (Необязательно.) Определение интервала ожидания отказа:

```
(interface) ip ospf dead-interval seconds
```

Этот параметр определяет интервал времени в секундах, в течение которого не должно происходить получение обновлений приветственных сообщений, чтобы соседнее устройство было объявлено как остановленное (по умолчанию это значение составляет увеличенный в четыре раза тайм-аут передачи приветственных сообщений). Чтобы маршрутизаторы могли сформировать отношения смежности, значения интервалов простоя (dead interval) в соседних устройствах должны совпадать.

в) (Необязательно.) Установка интервала повторной передачи:

```
(interface) ip ospf retransmit-interval seconds
```

Этот параметр определяет интервал времени в секундах между повторными передачами анонсов состояния каналов для соседнего устройства через интерфейс OSPF (значение по умолчанию — 5 с).

г) (Необязательно.) Установка задержки передачи:

```
(interface) ip ospf transmit-delay seconds
```

Данный параметр указывает время в секундах, которое требуется для передачи пакета обновления состояния каналов через интерфейс OSPF (значение по умолчанию — 1 с).

10. (Необязательно.) Настройка параметров интерфейса.

а) Определение стоимости интерфейса:

```
(interface) ip ospf cost
```

Этот параметр позволяет задать вручную безразмерное значение стоимости интерфейса (1–65535). Он может применяться при подключении к устройству, которое не вычисляет стоимость таким же образом, как маршрутизатор Cisco. Стоимость OSPF вычисляется как значение 10^8, деленное на величину полосы пропускания интерфейса, заданное командой `bandwidth`. Таким образом, заданная по умолчанию стоимость интерфейса может составлять 56 Кбит/с (1785), 64 Кбит/с (1562), T1 (65), E1 (48), 4 Мбит/с Token Ring (25), Ethernet (10), 16 Мбит/с Token Ring (6), FDDI (1), ATM (1), Fast Ethernet (1) или Gigabit Ethernet (1).

б) Определение эталонной пропускной способности:

```
(router) auto-cost reference-bandwidth ref-bw
```

Стоимость OSPF вычисляется путем деления полосы пропускания интерфейса на значение *ref-bw* (1–4294967 Мбит/с; значение по умолчанию — 100). По умолчанию значение *ref-bw* составляет 10^8, или 100 Мбит/с, а это означает, что каналы Fast Ethernet и Gigabit Ethernet имеют одинаковую стоимость, равную 1. Эта команда позволяет учесть различие между каналами с большой величиной полосы пропускания. Например, если значение *ref-bw* задано равным 1000, то канал Fast Ethernet (100 Мбит/с) приобретает стоимость 1000/100, или 10, а канал Gigabit Ethernet — стоимость 1000/1000, или 1.

ВНИМАНИЕ!

Эталонное значение величины полосы пропускания должно быть выбрано так, чтобы оно лишь позволяло провести различие между интерфейсами с самой высокой скоростью, но не более того. Выбор слишком высокого значения *ref-bw* приводит к получению стоимости интерфейса, которая может рассматриваться как недостижимая. Например, если эталонная полоса пропускания составляет 5000 Мбит/с (5000000000 бит/с), а полоса пропускания интерфейса — 64 Кбит/с (64000 бит/с), то итоговая стоимость может составлять 5000000000/64000, или 78125, т.е. иметь значение больше максимальной стоимости OSPF, равной 65535.

Значение эталонной полосы пропускания, равное 1000 или 2000, позволяет получить более приемлемое значение стоимости для интерфейса на 64 Кбит/с, т.е. 15625 или 31250 соответственно.

в) Настройка конфигурации интерфейса для поддержки маршрутизации OSPF по требованию:

```
(interface) ip ospf demand-circuit
```

Эта команда позволяет обеспечить подавление передачи маршрутизатором анонсов маршрутизации о состоянии каналов через заданный в конфигурации интерфейс. Необходимость в этом возникает при использовании каналов, создаваемых по требованию, таких как ISDN, или коммутируемых виртуальных каналов (switched virtual circuit — SVC).

г) Определение в конфигурации типов сетей OSPF:

```
(interface) ip ospf network { broadcast | non-broadcast | {point-
to-multipoint [non-broadcast] | point-to-point}}
```

Эта команда позволяет задавать в конфигурации тип сети OSPF независимо от типа передающей среды. Изменение типа сети позволяет изменить применяемый маршрутизатором OSPF способ формирования отношений смежности. Данная команда является особенно удобной для сетей Frame Relay, каналов ISDN, создаваемых по требованию, и сетей X.25.

НА ЗАМЕТКУ

Петлевой интерфейс автоматически отмечается как сеть OSPF типа “loop-back” (петлевой интерфейс) и анонсируется как маршрут /32.

11. (Обязательно для типов сетей, отличных от широковещательных.) Определение соседних устройств OSPF:

```
(router) neighbor ip-address [priority number] [poll-interval sec-
onds] [cost number]
```

Эта команда используется в целях формирования отношений смежности для маршрутизаторов в средах сетей, отличных от широковещательных. Параметр `priority` указывает приоритет соседнего устройства применительно к выбору назначенного маршрутизатора для типов нешироковещательных или широковещательных сетей (значение по умолчанию — 0). Параметр `poll-interval` указывает, как часто должен осуществляться опрос соседнего устройства на предмет наличия типов нешироковещательных или широковещательных сетей (значение по умолчанию — 120 с). Параметр `cost` назначает стоимость соседнего устройства. Если эта команда не применяется, то стоимость определяется на основе команды `ip ospf cost`. Если интерфейс является многоточечным, то данный вариант становится единственно применимым.

12. (Необязательно.) Определение аутентификации для области OSPF:

а) Определение аутентификации:

```
(router) area area-id authentication [message-digest]
```

С помощью этой команды настройка конфигурации области выполняется так, чтобы в ней аутентификация стала необходимой. Если аутентификация разрешена, то ее необходимо определить в конфигурации всех маршрутизаторов в области. Параметр `message-digest` устанавливает тип аутентификации для шифрования MD5.

б) Задание паролей в виде открытого текста (ключей) в интерфейсах:

```
(interface) ip ospf authentication-key key
```

Эта команда задает пароль для интерфейса в области, в которой требуется аутентификация в виде открытого текста. Параметр *key* представляет пароль как текстовую строку.

Еще один вариант состоит в следующем.

в) Задание паролей MD5 (ключей) в интерфейсах:

```
(interface) ip ospf message-digest-key keyid md5 key
```

Эта команда определяет пароль (ключ) для интерфейса, участвующего в обмене данными в области с конфигурацией, настроенной для аутентификации MD5. Ключ вводится как текстовая строка из алфавитно-цифровых символов длиной не больше 16. Параметр *keyid*, который может иметь значения от 1 до 255, представляет один возможный ключ аутентификации, который может совместно использоваться соседними маршрутизаторами. Если для соседних устройств задан один и тот же параметр *keyid*, то для них строка *key* также должна быть одинаковой. Чтобы можно было сменять ключ MD5 с переходом на новое значение, необходимо задать в конфигурации дополнительную пару *keyid/key*. Маршрутизаторы будут пытаться перейти на новый ключ, продолжая передавать анонсы, и принимать старый ключ до тех пор, пока не произойдет обновление во всех соседних устройствах.

13. (Необязательно.) Задание в конфигурации административного расстояния для маршрутов OSPF:

```
(router) distance ospf {[intra-area dist] [inter-area dist2]
[external dist3]}
```

Эта команда позволяет задавать административные расстояния для OSPF применительно к каждому типу маршрута (каждое из этих значений по умолчанию равно 110). Если используется эта команда, то маршрутизатор получает возможность различить внешний маршрут и маршрут между областями, чтобы выбрать один из них, не сравнивая метрики.

14. (Необязательно.) Изменение таймеров вычисления маршрута:

```
(router) timers spf spf-delay spf-holdtime
```

Этот параметр устанавливает задержку (значение по умолчанию — 5 с) и тайм-аут задержки (значение по умолчанию — 10 с) для вычисления SPF. Значение задержки указывает время в секундах, по истечении которого маршрутизатор запускает вычисление SPF после изменения топологии. Тайм-аут задержки определяет продолжительность времени ожидания между последовательными обновлениями SPF. Эта команда позволяет уменьшить издержки, связанные с вычислением SPF, которые обусловлены частым появлением через короткое время изменений в топологии, вызванных наличием маршрутизаторов OSPF, не имеющих достаточных обрабатывающих мощностей.

15. (Необязательно.) Настройка конфигурации процесса OSPF для преобразования имен с использованием системы DNS:

```
(global) ip ospf name-lookup
```

Данная команда выполняет настройку конфигурации маршрутизатора так, чтобы он предпринимал попытки поиска в системе DNS для преобразования адресов в имена узлов при выполнении любой команды `show`, связанной с поддержкой OSPF.

ВНИМАНИЕ!

Эта команда запускается аналогично любой другой команде интерфейса OSPF, поэтому ее ввод в действие часто происходит непреднамеренно во время настройки конфигурации OSPF. Если оказалось, что эта команда непреднамеренно введена в действие, то формирование данных о работе OSPF для вывода на дисплей может происходить очень медленно.

16. (Необязательно.) Ввод в действие перераспределения OSPF для обработки маршрутов, относящихся к подсетям:

```
(router) redistribute protocol [as-number | process-id] subnets
```

Одна из конкретных рекомендаций, о которой следует помнить, занимаясь перераспределением маршрутов к подсетям в сети OSPF, состоит в применении команды `redistribute subnets`. Если эта информация не задана, то в процессе OSPF происходит выбор для перераспределения только маршрутов с поддержкой классов. Дополнительные сведения о перераспределении приведены в разделе 8.4.

17. (Необязательно.) Суммирование маршрутов в ходе их перераспределения в процессе OSPF:

```
(router) summary-address address mask
```

Эта команда позволяет передавать единственный анонс применительно ко всем маршрутам, перераспределяемым в OSPF, которые находятся в пределах адресного пространства, определенного параметрами с указанием адреса и маски. Дополнительные сведения о перераспределении приведены в разделе 8.3.

18. (Необязательно.) Настройка конфигурации граничного маршрутизатора автономной системы (Autonomous System Boundary Router — ASBR) для принудительного формирования стандартного маршрута в домене OSPF:

```
(router) default-information originate [always] [metric value]
[metric-type 1 | 2] [route-map map-name]
```

Ввод в действие этой команды равносилен передаче маршрутизатору ASBR указания сформировать стандартный маршрут в домен OSPF. По существу, это служит для всех прочих участвующих маршрутизаторов OSPF указанием, что ASBR является маршрутизатором, предназначенным для передачи такого трафика, для которого не существует маршрута в таблице маршрутизации. Параметр `always` означает, что ASBR должен всегда отправлять сведения об этом маршруте. Значение `metric` задает метрику для стандартного маршрута (значение по умолчанию — 10). Параметр `metric-type` указывает тип внешнего канала, анонсируемого в домен OSPF. Это поле может быть задано как `1` (внешний маршрут типа 1) или `2` (внешний маршрут типа 2; это — значение по умолчанию). Параметр `route-map` указывает схему маршрута, в которой должно быть разрешено анонсирование стандартных маршрутов.

19. (Необязательно.) Предотвращение лавинной рассылки анонсов о состоянии каналов (LSA) OSPF через интерфейсы в широковещательных, нешироковещательных и двухточечных сетях:

    ```
    (interface) ip ospf database-filter all out
    ```

    В протоколе OSPF предусмотрена лавинная рассылка новых анонсов LSA через все интерфейсы в одной и той же области за исключением интерфейса, в который поступает анонс LSA. Если к конкретной области подключены избыточные интерфейсы, это может вызвать возникновение излишней лавинной рассылки и, таким образом, бесполезное расходование полосы пропускания. Для предотвращения чрезмерной лавинной рассылки в области можно заблокировать лавинную рассылку анонсов LSA из избыточных интерфейсов.

20. (Необязательно.) Предотвращение лавинной рассылки анонсов LSA по протоколу OSPF через интерфейсы в многоточечных сетях.

    ```
    (router) neighbor ip-address database-filter all out
    ```

    Можно также заблокировать лавинную рассылку анонсов LSA через интерфейсы в многоточечных сетях, но для этого необходимо указать IP-адрес соседнего устройства.

21. Для получения дополнительной информации о средствах обработки маршрутов обратитесь к следующим разделам.

    - 8.3. Перераспределение маршрутной информации
    - 8.4. Фильтрация маршрутной информации

Пример

Схема сети показана на рис. 6.5. Идентификатор маршрутизатора OSPF был задан равным 99.99.99.99 с помощью IP-адреса петлевого интерфейса. Процесс OSPF введен в действие, а интерфейс Ethernet 0 помещен в область Area 0. Интерфейс Serial 0 помещен в область Area 1, а интерфейс Serial 1 — в область Area 2. Область Area 1 задана в конфигурации как полностью тупиковая. Настройка конфигурации области Area 0 выполнена в целях применения аутентификации с помощью открытого текста. Область Area 2 является также транзитной областью для одной из несмежных областей, поэтому был установлен виртуальный канал. Поскольку виртуальный канал подключен к магистральной области, для него также должна быть выполнена настройка конфигурации в целях применения аутентификации. Интерфейс Ethernet 0 определен так, чтобы маршрутизатор, к которому он относится, не мог стать назначенным. Для интерфейса Serial 1 изменены значения тайм-аутов передачи приветственных сообщений и тайм-аутов простоя.

```
interface loopback 0
        ip address 99.99.99.99 255.255.255.255
interface ethernet 0
        ip address 1.2.2.1 255.255.255.0
        ip ospf priority 0
        ip ospf authentication-key KaTiE
interface serial 0
        ip address 1.5.5.1 255.255.255.0
        encapsulation frame-relay
        ip ospf network-type point-to-multipoint
```

```
        frame-relay map ip 1.5.5.2 110 broadcast
        frame-relay map ip 1.5.5.3 111 broadcast
interface serial 1
       ip address 1.8.8.1 255.255.255.0
       ip ospf hello-interval 20
       ip ospf dead-interval 95
router ospf 101
       network 1.2.2.1 0.0.0.0 area 0
       network 1.5.5.1 0.0.0.0 area 1
       network 1.8.8.1 0.0.0.0 area 2
       area 1 stub no-summary
       area 0 authentication
       area 2 virtual-link 100.100.100.100 authentication-key KaTiE
```

Рис. 6.5. Схема сети для примера применения протокола OSPF

6.6. Открытый протокол предпочтительного выбора кратчайшего пути (OSPF) версии 3 (для IPv6)

- В конфигурации интерфейсов указано, что должен применяться протокол IPv6 для OSPF (OSPFv3) вместо инструкций `network`.
- В одном и том же канале могут эксплуатироваться несколько экземпляров OSPF.
- С помощью адресов, локальных в канале, может осуществляться поиск смежных соседних устройств.
- Процедуры аутентификации основаны на использовании протокола IPsec (обязательное средство IPv6), а не протокола OSPF.
- Адресом IPv6, эквивалентным адресу IPv4 224.0.0.5, является FF02::5, а адресом, эквивалентным 224.0.0.6, — FF02::6.

- В версии OSPFv3 введены два новых типа анонсов LSA. Анонсы LSA типа 8 используются для лавинной рассылки, локальной в канале. Анонсы LSA типа 9, т.е. LSA с префиксом, внутренним по отношению к области, формируются граничным маршрутизатором области (Area Border Router — ABR) и передаются в магистральную область.

Настройка конфигурации

1. Ввод в действие одноадресатной маршрутизации IPv6:

   ```
   (config) ipv6 unicast-routing
   ```

   Как и применительно ко всем маршрутизирующим протоколам IPv6, необходимо вначале ввести в действие одноадресатную маршрутизацию IPv6, чтобы разрешить перенаправление пакетов IPv6.

2. Ввод в действие протокола OSPFv3:

   ```
   (config) ipv6 router ospf process-id
   ```

3. Назначение 32-битового идентификатора маршрутизатора:

   ```
   (router) router-id ipv4-address
   ```

   Версия OSPFv3 предназначена для использования в сети IPv6, но для нее все еще требуется 32-битовый идентификатор маршрутизатора. Этот идентификатор представляет собой адрес IPv4, который не обязательно должен быть адресом, назначенным какому-либо интерфейсу.

4. Ввод в действие процесса OSPF в интерфейсах:

   ```
   (interface) ipv6 ospf process-id area area-number
   ```

   В отличие от OSPFv2, в конфигурации не требуется указывать инструкции `network`, относящиеся к процессу, которые функционируют в маршрутизаторе. При использовании версии OSPFv3 осуществляется ввод в действие процесса OSPF в отдельных интерфейсах, которые должны участвовать в процессе маршрутизации.

5. (Необязательно.) Определение в конфигурации приоритета интерфейса OSPF:

   ```
   (interface) ipv6 ospf priority number
   ```

   Это значение может составлять от 0 до 255; по умолчанию применяется значение 1. Данный параметр используется для выбора назначенного маршрутизатора (Designated Router — DR) и резервного назначенного маршрутизатора (Backup Designated Router — BDR) в сетях широковещательного типа. Приоритет 0 указывает, что маршрутизатор для сети широковещательного типа не может быть маршрутизатором DR или BDR.

6. (Необязательно.) Определение стоимости интерфейса:

   ```
   (interface) ipv6 ospf cost cost
   ```

   Эта команда действует так же, как и команда, относящаяся к версии OSPFv2.

7. (Необязательно.) Суммирование маршрутов между областями:

   ```
   (router) area area-number range summary-address/prefix-length
   ```

   С помощью данной команды можно разрешить маршрутизатору ABR уменьшить количество маршрутов, передаваемых им в указанную область, путем

передачи суммарного адреса вместо любого маршрута, который находится в пределах диапазона, заданного параметром *prefix-length*.

Пример

На рис. 6.6 показан пример настройки конфигурации маршрутизатора RouterA для использования протокола OSPFv3. Активизация процесса OSPF осуществляется в обоих интерфейсах FastEthernet. Маршрутизатор RouterA выполняет роль маршрутизатора ABR, один из каналов которого подключен к области Area 1, а другой — к области Area 0. Кроме того, интерфейс FastEthernet0/1 задан в конфигурации с приоритетом интерфейса 0, что позволяет предотвратить участие маршрутизатора, к которому он относится, в каком-либо процессе выбора DR/BDR.

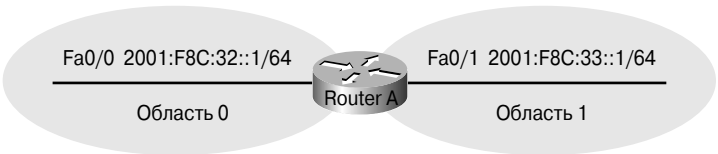

Рис. 6.6. Пример применения протокола OSPFv3

```
hostname RouterA
!
ipv6 unicast-routing
!
ipv6 router ospf 1
 router-id 1.1.1.1
!
interface fastethernet0/0
 ipv6 address 2001:F8C:32::1/64
 ipv6 ospf 1 area 0
!
interface fastethernet0/1
 ipv6 address 2001:F8C:33::1/64
 ipv6 ospf 1 area 1
 ipv6 ospf 1 priority 0
```

6.7. Интегрированный протокол IS-IS

- IS-IS — это протокол маршрутизации с учетом состояния каналов, который опубликован организацией по стандартизации ISO в 1992 году на основе фазы V стандарта DECnet.
- IS-IS — это протокол маршрутизации без поддержки классов, который обеспечивает работу в сетях, организованных на основе формата VLSM.
- Данный иерархический протокол маршрутизации поддерживает области, что позволяет управлять распределением обновлений маршрутизации.
- Протокол IS-IS поддерживает суммирование маршрутов между областями, что позволяет уменьшать до минимума количество записей в таблице маршрутизации.
- Протокол IS-IS поддерживает аутентификацию в домене и области.

Настройка конфигурации

1. (Обязательно.) Ввод в действие процесса IS-IS:

   ```
   (global)router isis [area tag]
   ```

   Эта команда вводит в действие протокол маршрутизации IS-IS. Если какой-то конкретный маршрутизатор подключен к нескольким областям IS-IS, то должен использоваться параметр `tag` для указания области, связанной с маршрутизатором. В различных маршрутизаторах осуществляется сравнение областей для установления уровней доменов и определения того, как должен происходить обмен данными.

2. (Обязательно.) Задание в конфигурации идентификатора маршрутизатора:

   ```
   (router) net network-entity-title
   ```

   Эта команда позволяет указать область и системный идентификатор маршрутизатора. Идентификатор сети не должен разрешать маршрутизацию. Это — идентификатор маршрутизатора в областях, определенных командой `router isis`. Параметр `net` указывает точку доступа к сетевой службе (network service access point — NSAP) с использованием формата наподобие 47.0004.004d.0001.0000.0cn.1m.00, где последний байт всегда равен 0 (.00). Шесть байтов, находящихся непосредственно перед n-селектором, представляют собой системный идентификатор (0000.0c11.1111). Системный идентификатор имеет постоянную длину и не может быть изменен. Системный идентификатор должен быть уникальным для каждого устройства в пределах каждой области (уровень 1), а также по всей магистральной области (уровень 2). Все байты, расположенные перед системным идентификатором, представляют собой идентификатор области (47.0004.004d.0001). Если протокол IS-IS используется только для осуществления маршрутизации в сети IP, то в конфигурации так или иначе должна быть задана сеть в целях определения системного идентификатора и идентификатора области маршрутизатора.

3. (Необязательно.) Указание типа маршрутизатора IS-IS:

   ```
   (interface) is-type {level-1 | level-1-2 | level-2-only}
   ```

   Маршрутизатор может представлять собой маршрутизатор только уровня 1 (внутриобластной), маршрутизатор уровня 2 (межобластной) или маршрутизатор обоих уровней, 1 и 2.

4. (Обязательно.) Активизация маршрутизации IS-IS в интерфейсе:

   ```
   (interface) ip router isis [area tag]
   ```

   Если маршрутизатор имеет несколько областей, то следует использовать параметр *`area tag`* для указания области, в которой работает интерфейс.

5. (Необязательно.) Указание типа цепи IS-IS для интерфейса:

   ```
   (interface) isis circuit-type {level-1 | level-1-2 | level-2-only}
   ```

   Эта команда применяется для задания в конфигурации типа отношений смежности, для которых желательна поддержка соседних устройств в указанном интерфейсе. Могут быть установлены отношения смежности уровня 1, если настройка конфигурации соседнего устройства выполнена с учетом применения общей области. Что касается параметра `level-1-2`, то отношения смежности

уровней 1 и 2 могут быть установлены, если маршрутизаторы имеют общую область; в противном случае устанавливаются только отношения смежности уровня 2 (это — значение по умолчанию). Если применяется параметр `level-2-only`, то формируются отношения смежности только уровня 2, если настройка соседних устройств выполнена с указанием типов каналов L2 или L1L2.

6. (Необязательно.) Определение метрики в интерфейсе IS-IS:

   ```
   (interface) isis metric default-metric {level-1 | level-2}
   ```

   Эта команда указывает стоимость IS-IS для данного интерфейса. Значение стоимости используется для определения оптимального маршрута. Диапазон значений стоимости составляет от 0 до 63; по умолчанию применяется значение 10.

7. (Необязательно.) Определение тайм-аута передачи приветственных сообщений:

   ```
   (interface) isis hello-interval seconds {level-1 | level-2}
   ```

   Эта команда задает интервал времени в секундах между передаваемыми маршрутизатором пакетами приветственных сообщений в указанном интерфейсе. Параметры `level-1` и `level-2` позволяют задавать значения таймеров отдельно для каждого типа интерфейса, за исключением последовательного интерфейса.

8. (Необязательно.) Установка интервала повторной передачи:

   ```
   (interface) isis retransmit-interval seconds
   ```

   Данная команда указывает в секундах, как долго маршрутизатор должен находиться в ожидании между повторными передачами пакетов состояния каналов (Link State Packet — LSP) по протоколу IS-IS для двухточечных каналов.

9. (Необязательно.) Управление частотой передачи пакетов LSP:

   ```
   (interface) isis lsp-interval seconds
   ```

   Эта команда позволяет управлять частотой передачи из интерфейса обновлений LSP. Задавая параметр *`seconds`*, можно определять или контролировать частоту передачи обновлений LSP из интерфейса в двухточечном канале. Это позволяет уменьшить объем издержек в канале, через который происходит отправка пакетов. С другой стороны, если значение этого параметра будет изменено должным образом, то уменьшится количество пакетов LSP, получаемых другой стороной.

10. (Необязательно.) Ограничение частоты повторной передачи LSP:

    ```
    (interface) isis retransmit-throttle-interval milliseconds
    ```

    Эта команда позволяет управлять частотой повторной передачи из интерфейса одних и тех же обновлений LSP. Устанавливая параметр *`milliseconds`*, можно задавать или контролировать частоту последовательной передачи обновлений, касающихся одного и того же пакета LSP.

11. (Необязательно.) Управление параметрами обновления отношений смежности:

    ```
    (interface) isis hello-multiplier multiplier {level-1 | level-2}
    ```

    Эта команда позволяет управлять тем, сколько пакетов может быть пропущено, прежде чем отношения смежности будут рассматриваться как прекращенные. Параметр *`multiplier`* указывает количество пропущенных пакетов; значение

по умолчанию равно 3. Параметр *multiplier* может быть задан для маршрутизаторов уровня 1 или 2.

12. (Необязательно.) Определение приоритета для управления тем, какое устройство должно стать назначенным маршрутизатором:

```
(interface) isis priority value {level-1 | level-2}
```

Эта команда устанавливает значение приоритета, передаваемое из интерфейса. Устройство с наивысшим приоритетом, заданным в интерфейсе, который подключен к многоточечной широковещательной сети, становится назначенным маршрутизатором для этой сети. Заданное по умолчанию значение равно 64.

13. (Необязательно.) Назначение интерфейсу пароля.

```
(interface) isis password password {level-1 | level-2}
```

Задавая пароль, можно управлять тем, с какими устройствами должен взаимодействовать маршрутизатор IS-IS. Пароли уровней 1 и 2 устанавливаются независимо и имеют формат открытого текста.

14. (Необязательно.) Назначение пароля области:

```
(router) area password password
```

Чтобы все маршрутизаторы в области могли обмениваться пакетами LSP, в их конфигурациях должен быть задан один и тот же пароль. Маршрутизаторы уровня 1 в области обмениваются друг с другом паролем области.

15. (Необязательно.) Назначение пароля домену:

```
(router) domain-password password
```

Чтобы все маршрутизаторы в домене могли обмениваться пакетами LSP, в их конфигурациях должен быть задан один и тот же пароль. Маршрутизаторы уровня 2 в сети обмениваются друг с другом паролем домена.

16. (Необязательно.) Применение суммирования с охватом нескольких областей:

```
(router) summary-address address mask {level-1 | level-1-2 | level-2}
```

Эта команда позволяет указывать в конфигурации маршрутизаторов IS-IS, что должно применяться суммирование при перераспределении данных, полученных от другого протокола маршрутизации. Суммирование может быть задано для каждого уровня. Оно позволяет уменьшить количество записей в таблице маршрутизации.

17. (Необязательно.) Формирование стандартного маршрута:

```
(router) default-information originate [route-map map-name]
```

Эта команда позволяет ввести стандартный маршрут в область IS-IS. После каждого перераспределения маршрутизатор не вставляет в таблицу маршрутизации стандартный маршрут автоматически. Данная команда дает возможность сформировать стандартный маршрут. С помощью параметра `route-map` можно обеспечить создание маршрута по условию.

18. Для получения дополнительной информации о средствах обработки маршрутов обратитесь к следующим разделам.

- 8.3. Перераспределение маршрутной информации
- 8.4. Фильтрация маршрутной информации

Пример

В данном примере показана настройка конфигурации протокола IS-IS, выполняемая так, чтобы маршрутизатор Kiddie находился в области Area 1 и имел идентификатор устройства 1. Конфигурация каждого интерфейса настраивается на выполнение маршрутизации по интегрированному протоколу IS-IS, а в конфигурации интерфейса Ethernet 0 задается пароль для предотвращения передачи неавторизованных обновлений LSP. Кроме того, приоритет интерфейса Ethernet 0 для маршрутизаторов уровня 1 устанавливается равным 90, чтобы маршрутизатор, к которому относится этот интерфейс, стал предпочтительным назначенным маршрутизатором в сегменте. Маршруты RIP перераспределяются из подсети 172.16.254.254 от маршрутизатора, в котором эксплуатируется протокол OSPF, перераспределяются в IS-IS для уровня 1 и суммируются в адрес сети класса B. На рис. 6.7 показана основная схема сети для данного примера применения маршрутизатора.

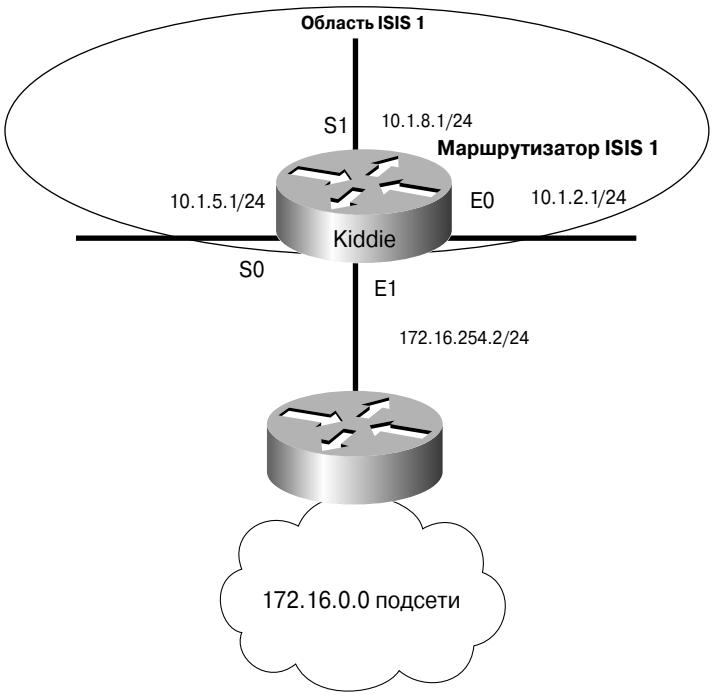

Рис. 6.7. Пример применения средств IS-IS

```
interface ethernet 0
       ip address 10.1.2.1 255.255.255.0
       ip router isis
       isis password KaTiE
       isis priority 90 level-1
interface ethernet 1
       ip address 172.16.254.2 255.255.255.0
interface serial 0
       ip address 10.1.5.1 255.255.255.0
       encapsulation ppp
```

```
       ip router isis
interface serial 1
       ip address 10.1.8.1 255.255.255.0
       ip router isis
router isis
       net 01.0000.0000.0001.00
       redistribute ospf 101 level-1 metric 40
         summary-address 172.16.0.0 255.255.0.0 level-1
router ospf 1
         network 172.16.254.2 0.0.0.0 area 0
```

6.8. Интегрированный протокол IS-IS для IPv6

Протокол IS-IS для IPv6 действует так же, как протокол IS-IS для IPv4. До выхода программного обеспечения Cisco IOS выпуска 12.2(15)T в протоколе IS-IS для IPv6 поддерживались только единственные топологии. Это означает, что если требовалось эксплуатировать оба варианта, IS-IS для IPv4 и IS-IS для IPv6, то эти два протокола должны были совместно использовать общую топологию, а настройка конфигурации всех интерфейсов должна была выполняться для обоих протоколов. Начиная с программного обеспечения Cisco IOS выпуска 12.2(15)T корпорацией Cisco была дополнительно предусмотрена возможность применения сразу нескольких топологий. Больше нет необходимости придерживаться ограничения, согласно которому для разных протоколов должна применяться одна и та же топология сети, а также больше не требуется настраивать конфигурацию всех интерфейсов, чтобы они поддерживали оба протокола.

Протокол IS-IS для IPv6 функционирует почти идентично протоколу IS-IS для IPv4 (включая команды CLI), поэтому в данном разделе приведен минимальный объем сведений о настройке конфигурации. (Для ознакомления с остальными командами см. предыдущий раздел, посвященный интегрированному протоколу IS-IS.)

Настройка конфигурации

1. Ввод в действие одноадресатной маршрутизации IPv6:

   ```
   (config) ipv6 unicast-routing
   ```

   Как и применительно ко всем маршрутизирующим протоколам IPv6, необходимо вначале ввести в действие одноадресатную маршрутизацию IPv6, чтобы разрешить перенаправление пакетов IPv6.

2. Переход в режим настройки конфигурации IS-IS и задание в конфигурации адреса NET (Network Entity Title — заголовок сетевой сущности):

   ```
   (config) router isis area-tag
   (router) net network-entity-title
   ```

   Эти команды аналогичны командам IS-IS для IPv4.

3. Активизация средств IS-IS сети IPv6 в интерфейсе:

   ```
   (interface) ipv6 router isis area-tag
   ```

   Эта команда разрешает применение процесса маршрутизации в интерфейсе.

6.9. Протокол граничного шлюза (Border Gateway Protocol — BGP)

- BGP — это маршрутно-векторный протокол маршрутизации. Обновления маршрутизации содержат полный список транзитных сетей (*маршрутов автономных систем*), необходимых для достижения дальней сети.
- Циклы маршрутизации обнаруживаются и предотвращаются путем поиска номера локальной автономной системы (autonomous system — AS) в пути AS.
- Одноранговые узлы BGP определяются относительно номера их локальной автономной системы. Одноранговые узлы в пределах одной и той же автономной системы формируют отношения с применением протокола IBGP (Interior BGP), тогда как одноранговые узлы в разных автономных системах используют протокол EBGP (Exterior BGP).
- Одноранговые узлы IBGP обмениваются друг с другом информацией о достижимости, а также перераспределяют информацию BGP в протоколы внутреннего шлюза (Interior Gateway Protocol — IGP), функционирующие в пределах общей автономной системы. (В качестве протоколов IGP могут применяться другие протоколы маршрутизации, такие как RIP, IGRP, EIGRP, OSPF и IS-IS.)
- Одноранговые узлы IBGP должны синхронизировать информацию BGP с информацией IGP для обеспечения распространения маршрутов IGP по локальной автономной системе.
- Многовыходной дискриминатор (Multi-Exit Discriminator — MED) — это безразмерная метрика, которая может быть изменена с помощью схемы маршрутов.
- Для управления процессом выбора пути назначается локальный приоритет. Локальные приоритеты анонсируются вместе с префиксами сети по всей автономной системе. Поэтому они являются значимыми только в пределах данной автономной системы.
- Кроме того, назначается атрибут `weight` с указанием весового коэффициента для управления процессом выбора пути. Весовые коэффициенты являются значимыми только для локального маршрутизатора.
- Протокол BGP предусматривает выбор наилучшего пути к получателю в следующем порядке.
  1. Если следующий транзитный переход недоступен, он не должен рассматриваться.
  2. Предпочтение отдается самому высокому значению весового коэффициента.
  3. Предпочтение отдается самому высокому значению локального приоритета.
  4. Предпочтительным является маршрут, начинающийся от локального маршрутизатора.
  5. Предпочтительным является самый короткий путь в автономной системе, если от локального маршрутизатора не начинается ни один маршрут.
  6. Предпочтение отдается началу с самым низким значением (`igp < egp < incomplete`).

7. Предпочтительным является самый низкий дескриминатор MED (недостающий MED считается равным 0).
8. Предпочтительным по отношению к внутреннему пути является внешний путь.
9. Если синхронизация запрещена и остаются только внутренние пути, то предпочтительным является путь через ближайшее соседнее устройство IGP.
10. Предпочтительным является установленный раньше, более устойчивый путь.
11. Предпочтение отдается самому низкому IP-адресу, определяющему идентификатор маршрутизатора BGP.

НА ЗАМЕТКУ

В протоколе BGP для формирования надежных транспортных соединений между одноранговыми или соседними маршрутизаторами используются и порт 179 протокола UDP, и порт 179 протокола TCP.

Настройка конфигурации

1. Ввод в действие процесса маршрутизации BGP и связывание локального маршрутизатора с автономной системой:

   ```
   (global) router bgp as-number
   ```

2. Определение всех соседних устройств BGP:

   ```
   (router) neighbor {ip-address | peer-group} remote-as as-number
   ```

   Соседние устройства могут быть указаны с помощью IP-адреса или имени группы одноранговых узлов. Группа одноранговых узлов представляет собой результат группирования нескольких соседних устройств, которые характеризуются наличием общего набора атрибутов или одинаковых политик обновления. С помощью этой команды определяется каждое соседнее устройство BGP. Для соседних устройств IBGP номер AS является таким же, который используется в команде `router bgp`. Соседние устройства IBGP должны быть достижимыми с помощью средств маршрутизации IGP, причем они не обязательно должны находиться в одной и той же подсети. Что касается соседних устройств EBGP, то для них номер автономной системы будет другим. В конфигурацию соседнего устройства может быть добавлено необязательное текстовое описание:

   ```
   (router) neighbor {ip-address | peer-group} description text-string
   ```

НА ЗАМЕТКУ

Соседние устройства IBGP не перераспределяют и не перенаправляют полученные маршруты во все другие соседние устройства IBGP в пределах автономной системы. Вместо этого они перенаправляют указанную информацию своим соседним устройствам EBGP. Важно, чтобы в конфигурации отношения IBGP со всеми прочими соседними устройствами в пределах автономной системы задавались в виде полной сети соединений. Если эта задача является слишком сложной, то должны использоваться либо конфедерации BGP, либо рефлекторы маршрутов.

Соседние устройства EBGP должны быть непосредственно подключены друг к другу и иметь общую подсеть. В некоторых случаях это невозможно. В таком случае необходимо выполнить настройку конфигурации для использования протокола IGP или статического маршрута, чтобы два соседних устройства стали досягаемыми друг для друга. После этого можно задать в конфигурации множественный транзитный переход EBGP:

```
(router) neighbor ip-address ebgp-multihop ttl
```

Значение *ttl* указывает время существования в форме количества транзитных переходов (от 1 до 255; значение по умолчанию — 255 транзитных переходов).

3. (Необязательно.) Задание в конфигурации интерфейса, что должны использоваться соединения BGP по протоколу TCP:

   ```
   (router) neighbor {ip-address | peer-group} update-source interface
   ```

   Как правило, в протоколе BGP используется адрес отправителя из "наилучшего локального интерфейса" при обмене данными с соседним одноранговым устройством IBGP. Этот адрес не всегда может быть оптимальным, особенно если требуется применение петлевого интерфейса. Чтобы переопределить этот стандартный адрес отправителя, можно задать значение параметра *interface*. Как правило, для одноранговых узлов IBGP используется петлевой интерфейс, поскольку он всегда является рабочим и доступным. Если применяется петлевой интерфейс, то он должен быть доступным для дальних соседних устройств IBGP.

4. Определение сетей для анонсирования с помощью протокола BGP как исходных для маршрутов из локальной автономной системы. Определение списка, включающего до 200 сетей:

   ```
   (router) network network-number [mask mask]
   ```

   Указанные сети должны быть представлены в таблице маршрутизации как непосредственно подключенные сети, статические маршруты или маршруты, полученные с помощью динамических процессов маршрутизации. Необязательный параметр *mask* позволяет определять суперсети, в которые входят данные сети.

   Еще один вариант состоит в следующем.

   Перераспределение маршрутов из домена маршрутизации IGP:

   ```
   (router) redistribute protocol [process-id] ... [route-map map]
   ```

   Как правило, локальные сети (находящиеся в пределах локальной автономной системы) должны быть указаны с помощью команды `network`. Однако в случае необходимости маршруты IGP могут быть перераспределены в протоколе BGP. Для фильтрации перераспределяемых маршрутов IGP должна использоваться схема маршрутов.

5. (Необязательно.) Распространение агрегированных адресов или адресов суперсетей для уменьшения размера таблицы маршрутизации:

   ```
   (router) aggregate-address address mask [as-set] [summary-only]
   [suppress-map map] [advertise-map map] [attribute-map map]
   ```

   Указанный агрегированный адрес формируется, если есть по крайней мере еще одна более конкретная запись в таблице BGP. И агрегированный адрес, и более конкретные адреса анонсируются, если не указано ключевое слово

summary-only. Если агрегированный адрес составлен более конкретными маршрутами из нескольких автономных систем, то применение ключевого слова as-set приводит к тому, что анонсируется также совокупность номеров исходных автономных систем.

Для подавления более конкретных маршрутов (suppress-map) или формирования некоторых агрегированных адресов, подлежащих анонсированию (advertise-map), могут использоваться схемы маршрутов. В случае необходимости можно откорректировать атрибуты BGP агрегированного адреса (attribute-map). Для каждого адреса можно использовать схему маршрутов, указывая ключевое слово match ip address или match as-path для выбора маршрутов. Изменение атрибутов осуществляется путем применения команды set в схеме маршрутов.

6. (Необязательно.) Запрещение синхронизации между BGP и IGP:

```
(router) no synchronization
```

По умолчанию протокол BGP предусматривает переход в состояние ожидания на то время, пока локальные средства IGP распространяют маршрутную информацию по автономной системе. Синхронизация с BGP разрешена, и маршруты, подлежащие анонсированию с помощью протокола BGP, проверяются перед включением в таблицы IGP. Если синхронизация не требуется, то она может быть запрещена.

7. (Необязательно.) Задание в конфигурации атрибутов и метрик для выбора лучшего пути.

а) Весовой коэффициент сети является значимым в локальном масштабе; он не анонсируется и не распространяется.

Задание атрибута weight в условиях согласования с соседним устройством BGP:

```
(router) neighbor {ip-address | peer-group} weight weight
```

Значение параметра weight составляет от 0 до 65535. Если источником пути является данный маршрутизатор, то значение weight по умолчанию устанавливается равным 32768, а для путей, для которых он не является источником, значение weight становится равным 0. Предпочтительным является путь с более высоким значением параметра weight.

Еще один вариант состоит в следующем.

Задание атрибута weight с использованием схемы маршрута:

```
(route-map) set weight weight
```

(Дополнительные сведения об использовании схемы маршрута приведены в п. 12.)

б) Распространение локального значения приоритета в пределах локальной автономной системы.

Определение заданного по умолчанию локального значения приоритета для обновлений в пределах автономной системы:

```
(router) bgp default local-preference value
```

Локальное значение приоритета может находиться в пределах от 0 до 4294967295 и по умолчанию равно 100. Предпочтительным является путь с более высоким локальным значением приоритета.

Еще один вариант состоит в следующем.

Задание локального значения приоритета с использованием схемы маршрута:

```
(route-map) set local-preference value
```

(Дополнительные сведения об использовании схемы маршрута приведены в п. 12.)

в) Обмен между автономными системами значениями метрики или MED. Предусмотрено получение этого значения, но оно переустанавливается в 0, если происходит его передача в другую автономную систему.

Определение заданного по умолчанию значения MED для маршрутов, перераспределяемых в протоколе BGP:

```
(router) default-metric med
```

Значения MED могут находиться в пределах от 1 до 4294967295. Предпочтительным является путь с *меньшим* значением MED.

Еще один вариант состоит в следующем.

Задание значения MED с использованием схемы маршрута:

```
(route-map) set metric metric
```

(Дополнительные сведения об использовании схемы маршрута приведены в п. 12.)

8. (Необязательно.) Определение в конфигурации атрибута `community` для анонсируемых маршрутов.

НА ЗАМЕТКУ

Как правило, маршрутизатор сравнивает метрики, полученные только от соседних устройств в общей автономной системе. Чтобы сравнить метрики для путей, анонсируемых всеми соседними устройствами независимо от автономной системы, можно воспользоваться следующей командой:

```
(router) bgp always-compare-med
```

а) Использование схемы маршрута для задания значения параметра `community`:

```
(route-map) set community community [additive]
```

(Дополнительные сведения об использовании схемы маршрута приведены в п. 12.) Схема маршрута используется для сопоставления маршрутов и задания атрибута `community` с тем, чтобы маршруты группировались в единые сообщества. Значение параметра с номером сообщества представляет собой произвольно выбранное число от 0 до 4294967200, а атрибут `community` задается как коллекция этих значений. Маршрут может быть элементом более чем одного сообщества. Ключевое слово `additive` применяется для добавления нового значения к списку существующих значений. Предусмотрена возможность использовать предварительно определенные значения: `internet`

(анонсировать маршрут для сообщества Интернета или для всех одноранговых узлов), `no-export` (не анонсировать маршрут для одноранговых узлов EBGP) и `no-advertise` (не анонсировать маршрут ни для одного одноранговых узла).

б) Передача атрибута `community` соседним устройствам BGP:

```
(router) neighbor {ip-address | peer-group} send-community
```

По умолчанию атрибут `community` не передается соседним устройствам в обновлениях BGP. Эта команда разрешает передавать значение атрибута одноранговым узлам BGP.

9. (Необязательно.) Использование фильтрации номеров сообществ для согласования входящих анонсов путей.

а) Задание в конфигурации списка сообществ для выполнения согласования:

```
(global) ip community-list community-list-number {permit | deny}
community-value
```

Для согласования значения сообщества используется одна или более инструкций `community list` с общим номером списка (от 1 до 99), расположенных в последовательном порядке. Параметр `value` может представлять собой единственное значение или строку значений, разделенных пробелами. Значения находятся в пределах от 0 до 4294967200 и могут включать предварительно определенные значения `internet`, `no-export` и `no-advertise`. В конце списка сообществ неявно формируются инструкция `deny all`.

б) Задание в конфигурации схемы маршрута в целях применения списка сообществ:

```
(route-map) match community-list community-list-number [exact]
```

В схеме маршрута используется параметр *`community-list-number`*, представляющий собой значение от 1 до 99, которое сопоставляется со значением номера сообщества. Ключевое слово `exact` предназначено для точного сопоставления списка значений номеров сообществ.

10. (Необязательно.) Использование фильтрации маршрутов с номерами сетей для ограничения распространения маршрутной информации, предназначенной для усвоения или анонсирования.

а) Применение списка префиксов для выполнения фильтрации:

```
(router) neighbor {ip-address | peer-group} prefix-list prefix-
list-name {in out}
```

Список префиксов с именем, указанным параметром *`prefix-list-name`*, используется в целях разрешения или запрещения доступа к сетям с учетом значений определенного количества ведущих битов (префиксов) в номерах сетей. (См. раздел 14.1 для получения дополнительной информации о списках префиксов.)

б) Создание нумерованного стандартного списка доступа для выполнения фильтрации:

```
(global) access-list list-number {deny permit} network wildcard
```

Список доступа, обозначенный номером от 1 до 99, может применяться для разрешения или запрещения доступа к сети с указанным номером (допускается применение подстановочного символа). 0 указывает, что согласование должно быть точным, а 1 допускает согласование с любым значением.

НА ЗАМЕТКУ

В случае фильтрации номеров сетей, относящихся к суперсетям, должен использоваться расширенный список доступа для согласования номера сети и маски подсети:

```
(global) access-list list-number {deny permit} ip network net-wildcard
subnet-mask mask-wildcard
```

в) Создание именованного стандартного списка доступа для выполнения фильтрации:

```
(global) ip access-list standard name
(access-list) {permit deny} network [wildcard]
```

г) Использование списка распределения в целях применения стандартного или расширенного списка доступа IP для фильтрации:

```
(router) neighbor {ip-address peer-group} distribute-list access-
list {in out}
```

Список доступа (нумерованный или именованный) служит для фильтрации номеров сетей в обновлениях маршрутизации, передаваемых в прямом или обратном направлении между определенными соседними устройствами. Ключевые слова `in` и `out` указывают направление фильтрации.

11. (Необязательно.) Использование фильтрации путей автономной системы для управления входящими и исходящими обновлениями BGP.

а) Создание списка доступа к путям автономной системы для выполнения фильтрации путей автономной системы:

```
(global) ip as-path access-list as-path-list-number {permit |
deny} as-regular-expression
```

Параметр `as-path-list-number` (со значениями в пределах от 1 до 199) позволяет разрешать или запрещать передачу обновлений BGP, основанных на согласовании значения параметра `as-regular-expression` с содержанием пути автономной системы. (Исчерпывающие инструкции по созданию регулярных выражений с определением автономной системы см. в разделе 14.4, “Регулярные выражения”.) Если задача состоит в согласовании пути автономной системы для протокола BGP, то можно воспользоваться табл. 6.1, в которой перечислены обычно применяемые регулярные выражения.

б) Использование списка фильтров в целях применения списка доступа путей автономной системы для фильтрации:

```
(router) neighbor {ip-address | peer-group} filter-list as-path-
list-num {in out}
```

Список доступа путей автономной системы применяется для фильтрации путей автономной системы в обновлениях маршрутизации, передаваемых в прямом или обратном направлении между определенными соседними

устройствами. Можно использовать ключевые слова `in` и `out` для указания направления фильтрации. В конфигурации могут быть заданы только один фильтр пути AS типа `in` и один фильтр пути AS типа `out`.

Таблица 6.1. Широко применяемые регулярные выражения

Регулярное выражение	Пример	Результат
.*	.*	Выполняет согласование с любой информацией о пути
^n$	^400$	Служит для согласования с путями, которые начинаются со значения `AS n` и заканчиваются значением `AS n`. (Таким образом, `AS n` представляет собой единственный путь.)
^$	^$	Обеспечивает согласование с путями, которые исходят из локальной автономной системы
^n_ ^n_.*	^400_ ^400_.*	Выполняет согласование с путями, которые начинаются со значения `AS n`. Обновления исходят из `AS n`. Применение альтернативного выражения приводит к получению таких же результатов
_n$.*_n$	_400$.*_400$	Обеспечивает согласование с путями, которые заканчиваются значением `AS n`. Обновления исходят из `AS n`. Применение альтернативного выражения приводит к получению таких же результатов
_n_	_400_	Предусматривает согласование с путями, которые проходят через автономную систему `AS n`
_n m_	_400 300_	Предусматривает согласование с путями, которые проходят точно через `AS n`, а затем — через `AS m`

НА ЗАМЕТКУ

Напомним, что при передаче обновления каждым одноранговым узлом BGP происходит *добавление в качестве префикса* его собственного номера автономной системы к пути автономной системы. Это означает, что путь автономной системы формируется справа налево так, что обозначение исходной автономной системы находится в крайнем справа конце строки пути автономной системы. Одноранговый узел, который должен передавать обновление в последнюю очередь, включает обозначение своей автономной системы в крайней слева части строки пути. Для проверки результатов применения регулярного выражения до его включения в список доступа пути автономной системы можно воспользоваться командой `show ip bgp regexp` *`regular-expression`*.

12. (Необязательно.) Использование схемы маршрута для управления входящими и исходящими обновлениями BGP или для их изменения.

a) Создание схемы маршрута для сопоставления и изменения атрибутов BGP:

```
(global) route-map map-name [permit | deny] [sequence-num]
```

Схема маршрута может быть составлена из одной или более инструкций, вычисляемых в последовательном порядке, согласно необязательному порядковому номеру. Ключевое слово `permit` (применяемое по умолчанию) вынуждает вычислять инструкцию `route-map` и предпринимать действие.

Предусмотрена возможность использовать одну или более необязательных инструкций `match` наряду с необязательными командами `set`. Если в кон-

фигурации задано больше одной инструкции `match`, все условия должны быть выполненными, прежде чем будет предпринято действие `set`. Если после вычисления всех инструкций схемы маршрута не обнаруживается соответствие, передача или прием обновления не происходит.

1. Настройка конфигурации условия согласования. Согласование с путем автономной системы в обновлении:
   `(route-map) match as-path` *`as-path-list`*

   Параметр *`as-path-list`* (обозначенный номером от 1 до 199) используется для согласования регулярного выражения автономной системы, как в п. 11, *а*.

   Согласование номера сети в обновлении:
   `(route-map) match ip address access-list [...access-list]`

   Номера сетей в обновлении согласуются с нумерованным или именованным списком доступа IP (стандартным или расширенным). (См. п. 10, *а* или 10, *б*.)

   Согласование со значением сообщества в обновлении:
   `(route-map) match community-list community-list [exact]`

   Для согласования со значением сообщества используется список сообществ (от 1 до 99). Ключевое слово `exact` предназначено для указания точного согласования со списком значений сообществ. (См. п. 9, *а*.)
2. Задание в конфигурации команды `set` для изменения атрибута. Изменение пути автономной системы:
   `(route-map) set as-path prepend` *`as-path-string`*

   Строка *`as-path-string`* присоединяется к атрибуту пути AS в качестве префикса. Указав в качестве префикса обозначение локальной автономной системы несколько раз, можно изменить длину пути, чтобы повлиять на процесс выбора пути в дальнем одноранговом узле. Изменение параметра `origin` в протоколе BGP:
   `(route-map) set origin {igp egp` *`as`* `incomplete}`

   Параметр `origin` может принимать значение `igp` (источник обновления находится внутри локальной автономной системы; обычно это можно наблюдать, если используется команда `network` протокола BGP или если маршруты IGP перераспределяются в BGP), `egp` (маршрут получен от протокола EGP из автономной системы *`as`*) или `incomplete` (источник обновления неизвестен или в BGP перераспределяется статический маршрут).

   Изменение атрибута `community`:
   `(route-map) set community {community [additive] | none}`

   Атрибут `community` может принимать одно из следующих значений *`community`*: 32-битовое число (от 1 до 4294967200), номер автономной системы и 2-байтовый номер сообщества в формате *`as`*`:`*`nn`*, `local-AS` (маршрут не анонсируется вне локальной автономной системы), `no-export` (маршрут не анонсируется в следующую автономную систему) или `no-advertise` (маршрут не анонсируется ни для одного однорангового узла).

Если используется ключевое слово additive, то указанное значение *community* добавляется к существующему атрибуту community. Применение ключевого слова none приводит к удалению всех значений *community*.

Изменение разгрузки BGP:

```
(route-map) set dampening halflife reuse suppress max-suppress-
time
```

С помощью этой команды устанавливаются параметры разгрузки маршрута BGP. (Дополнительные сведения приведены в п. 15.) Параметр *halflife* изменяется в пределах от 1 до 45 мин (значение по умолчанию — 15 мин), порог штрафа *reuse* изменяется в пределах от 1 до 20000 (значение по умолчанию — 750), порог штрафа *suppress* изменяется в пределах от 1 до 20000 (значение по умолчанию — 2000) и параметр *max-suppress-time* изменяется в пределах от 1 до 20000 мин (значение по умолчанию — 60 мин). Разгрузка может быть установлена только по отношению к схемам маршрута, на которые имеется ссылка в команде bgp dampening.

Изменение локального значения приоритета:

```
(route-map) set local-preference value
```

Локальный приоритет изменяется в пределах от 0 до 4294967295 (значение по умолчанию — 100). Предпочтительными являются более высокие локальные значения приоритета.

Изменение значения весового коэффициента (только для входящей схемы маршрута):

```
(route-map) set weight weight
```

Значение весового коэффициента BGP изменяется в пределах от 0 до 65535 (значение по умолчанию не изменяется). Весовые коэффициенты, установленные с помощью схемы маршрута, переопределяют весовые коэффициенты, заданные в командах neighbor протокола BGP. Предпочтительными являются маршруты с более высокими весовыми коэффициентами.

Изменение значения MED:

```
(route-map) set metric [+ | -] metric
```

Параметр metric изменяется в пределах от 0 до 4294967295. Если вместе со значением указан знак “плюс” или “минус”, корректировка значения метрики осуществляется с учетом знака. Предпочтительными являются более низкие значения метрики.

б) Применение схемы маршрута к входящим или исходящим обновлениям с учетом конкретного соседнего устройства:

```
(router) neighbor {ip-address | peer-group} route-map map-name {in
| out}
```

Для изменения обновлений, входящих или исходящих по отношению к указанному соседнему устройству BGP, используется схема маршрута с именем *map-name*.

13. (Необязательно.) Уменьшение объема внутренних одноранговых отношений с использованием конфедераций BGP.

    а) Создание идентификатора конфедерации:

    ```
    (router) bgp confederation identifier autonomous-system
    ```

    Конфедерация получает идентификатор, *autonomous-system*, что позволяет представлять ее во внешнем мире как единственную автономную систему.

    б) Указание автономных систем, которые принадлежат к конфедерации:

    ```
    (router) bgp confederation peers autonomous-system [autonomous
    system]
    ```

    Соседние устройства EBGP в пределах конфедерации обмениваются обновлениями так, как если бы они были одноранговыми узлами IBGP.

НА ЗАМЕТКУ

Для каждой автономной системы в конфедерации должна быть определена полносвязная сеть одноранговых узлов IBGP с помощью команд `neighbor` протокола BGP. Безусловно, определение конфедерации приводит к сокращению общего размера полносвязной сети IBGP внутри общей конфедерации автономных систем, но даже в меньших внутрених автономных системах должно соблюдаться требование по созданию полносвязной сети.

14. (Необязательно.) Уменьшение объема одноранговых отношений с использованием рефлекторов маршрута.

    а) Задание в конфигурации рефлектора маршрута и его клиентов:

    ```
    (router) neighbor ip-address route-reflector-client
    ```

    Локальный маршрутизатор определяется в конфигурации как рефлектор маршрута BGP и ретранслирует обновления BGP, передавая их всем клиентам IBGP. Одноранговый узел *ip-address* определяется в конфигурации как клиент. Рефлектор маршрута и его клиенты образуют *кластер*. Сеть, соединяющая клиентов, не обязательно должна быть полносвязной. Рефлекторы маршрутов должны составлять совместно друг с другом полносвязную сеть между кластерами.

    б) Для избыточных рефлекторов маршрута в пределах кластера назначается конкретный идентификатор кластера:

    ```
    (router) bgp cluster-id {cluster-id | ip-address}
    ```

    Эта команда используется в каждом рефлекторе маршрута для присваивания общего 4-байтового идентификационного номера кластера (значение от 1 до 4294967295, или 4 байт в формате IP-адреса). Идентификатор кластера передается наряду с обновлениями другим рефлекторам маршрута. Это позволяет обнаруживать циклы.

15. (Необязательно.) Сведение к минимуму самопроизвольного изменения маршрута с помощью разгрузки маршрута.

    а) Ввод в действие разгрузки маршрута BGP:

    ```
    (global) bgp dampening
    ```

Эффект самопроизвольного изменения маршрута можно свести к минимуму следующим образом.

Если происходит самопроизвольное изменение маршрута к автономной системе, разгружающий маршрутизатор назначает совокупное значение штрафа. Маршрут обозначается как проблемный в поле состояния буфера истории команд, но все еще анонсируется.

Дальнейшее самопроизвольное изменение влечет за собой применение дополнительных штрафов. После того как совокупное значение штрафа становится больше параметра *suppress limit*, маршрут переводится в состояние "разгруженный" и больше не анонсируется.

После прохождения периода *half-life* без самопроизвольного изменения штраф уменьшается наполовину. Результаты уменьшения штрафа проверяются через каждые 5 с.

После того как значение штрафа падает ниже предела *reuse limit*, подавление маршрута отменяется и он снова анонсируется. Маршруты, подвергшиеся подавлению, проверяются через каждые 10 с с учетом этого условия.

Подавление маршрутов происходит только до истечения предельного значения времени *max-suppress*.

б) Настройка параметров разгрузки маршрута:

```
(global) bgp dampening half-life reuse suppress max-suppress
[route-map map]
```

Параметр *half-life* изменяется в пределах от 1 до 45 мин (значение по умолчанию — 15 мин), порог штрафа *reuse* изменяется в пределах от 1 до 20000 (значение по умолчанию — 750), порог штрафа *suppress* изменяется в пределах от 1 до 20000 (значение по умолчанию — 2000) и параметр *max-suppress-time* изменяется в пределах от 1 до 20000 мин (значение по умолчанию — 60 мин).

16. (Необязательно.) Задание в конфигурации сетевых таймеров BGP:

```
(router) timers bgp keepalive holdtime
```

Параметр *keepalive* указывает частоту в секундах, с которой маршрутизатор отправляет сообщения с пакетами поддержки соединения BGP одноранговому узлу BGP. (Значение по умолчанию — 60 с.) Параметр *holdtime* указывает в секундах, как долго маршрутизатор должен ожидать получения сообщения с пакетом поддержки соединения, прежде чем объявить одноранговый узел BGP не функционирующим. (Значение по умолчанию — 180 с.)

17. (Необязательно.) Ввод в действие мягкой перенастройки:

```
(router) neighbor [ip-address | peer-group-name] soft-
reconfiguration [inbound]
```

Мягкая перенастройка (soft-reconfiguration) позволяет учитывать возможность более быстрого восстановления при переустановке одноранговой узла BGP. Если применяется мягкая перенастройка, то все обновления, полученные от соседнего устройства, сохраняются в неизменном виде.

Пример

На рис. 6.8 показан маршрутизатор, настройка конфигурации которого выполнена для работы по протоколу BGP в автономной системе 10000. Два одноранговых узла IBGP (в автономной системе 10000) имеют IP-адреса 190.67.17.254 и 190.67.41.3. Локальный маршрутизатор выполняет функции рефлектора маршрута BGP, а каждый из одноранговых узлов IBGP является клиентом рефлектора маршрута BGP. Еще один маршрутизатор, одноранговый узел EBGP (не находящийся в автономной системе 10000), имеет IP-адрес 217.6.15.1.

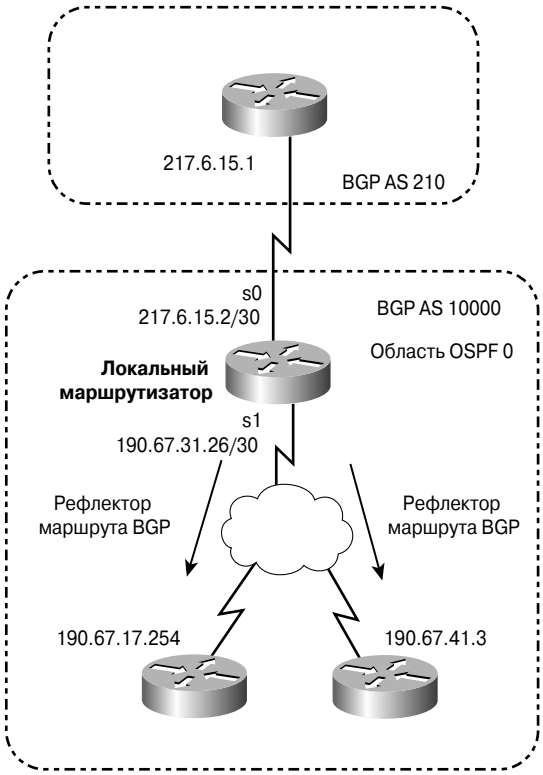

Рис. 6.8. Схема сети для примера применения протокола BGP

Одноранговый узел EBGP получает информацию о сообществе BGP. Схема маршрута `ispcommunity` вынуждает применять подавление анонсов маршрута по отношению к маршрутам к адресу 190.67.18.0. Но что касается маршрутов к адресу 190.67.0.0, то к строке сообщества добавляется дополнительное значение сообщества, равное 10000:1 (автономная система 10000 и сообщество 1).

Применительно к входящим обновлениям BGP, поступающим от однорангового узла EBGP, задана схема маршрута `ispfilter`, которая ссылается на список доступа 1 пути автономной системы. Для обновлений, которые содержат путь, включающий только автономную систему 1001, или путь, проходящий через автономную систему 1002, устанавливается значение локального приоритета, равное 40.

Маршруты BGP (включая подсети) из автономной системы 10000 перераспределяются в OSPF с метрикой 500.

```
interface serial 0
        ip address 217.6.15.2 255.255.255.252
interface serial 1
        ip address 190.67.31.26 255.255.255.252
router bgp 10000
        network 217.6.15.0
        neighbor 217.6.15.1 description ISP peer
        neighbor 217.6.15.1 remote-as 210
        neighbor 217.6.15.1 route-map ispfilter in
        neighbor 217.6.15.1 send-community
        neighbor 217.6.15.1 route-map ispcommunity out
        neighbor 190.67.17.254 remote-as 10000
        neighbor 190.67.17.254 route-reflector-client
        neighbor 190.67.41.3 remote-as 10000
        neighbor 190.67.41.3 route-reflector-client
router ospf 101
        redistribute bgp 10000 metric 500 subnets
        passive-interface serial 0
        network 217.6.15.0 0.0.0.255 area 0
        network 190.67.31.0 0.0.0.255 area 0
route-map ispfilter permit 10
        match as-path 1
        set local-preference 40
route-map ispfilter permit 20
        ip as-path access-list 1 permit ^1001$
        ip as-path access-list 1 permit _1002_
route-map ispcommunity permit 10
        match ip address 2
        set community no-advertise
route-map ispcommunity permit 20
        match ip address 1
        set community 10000:1 additive
route-map ispcommunity permit 30
access-list 1 permit 190.67.0.0 0.0.255.255
access-list 2 permit 190.67.18.0 0.0.0.255
```

6.10. Протокол граничного мультипротокольного шлюза (BGP) для IPv6

- Протокол MBGP представляет собой расширение протокола BGP версии 4, которое поддерживает маршрутизацию для нескольких семейств протокольных адресов (например, многоадресатных адресов IPv4, одноадресатных адресов IPv6, многоадресатных адресов IPv6, адресов VPNv4 и т.д.).
- Протокол MBGP определен в документе RFC 2283. Средства протокола MBGP функционируют в сеансе BGP и используют отдельные семейства адресов и отдельные базы данных для каждого семейства адресов.
- В протоколе MBGP одновременно применяются порты 179 протоколов UDP и TCP.

Настройка конфигурации

1. Настройка конфигурации процесса маршрутизации BGP:

   ```
   (config) router bgp autonomous-system-number
   ```

2. Задание в конфигурации идентификатора маршрутизатора:

   ```
   (router) bgp router-id ipv4-address
   ```

   В протоколе BGP используется 32-битовый идентификатор маршрутизатора для обозначения пакетов. Если настройка конфигурации маршрутизатора выполнена для работы только по протоколу IPv6, то необходимо задавать в конфигурации идентификатор маршрутизатора вручную.

3. (Необязательно.) Запрещение использования семейства одноадресатных адресов IPv4:

   ```
   (router) no bgp default ipv4-unicast
   ```

   Если маршрутизатор предназначен для работы только по протоколу IPv6, то с помощью этой команды можно без опасений удалить всю маршрутную информацию, относящуюся к IPv4.

4. Задание в конфигурации соседнего устройства BGP:

   ```
   (router) neighbor ipv6-address remote-as as-number
   ```

   Определение в конфигурации соседних устройств BGP для IPv6 осуществляется так же, как в случае применения BGP для IPv4.

5. Определение поддержки семейства одноадресатных адресов IPv6:

   ```
   (router) address-family ipv6 unicast
   ```

   Протокол MBGP поддерживает понятие “семейства адресов”, позволяющего сгруппировать общие характеристики с учетом версии IP, одноадресатной или многоадресатной адресации, а также экземпляра виртуальной маршрутизации и перенаправления (Virtual Routing and Forwarding — VRF). Эту команду можно задавать несколько раз для определения характеристик нескольких семейств адресов. По умолчанию, если не задано ни одно семейство адресов, предполагается использование одноадресатных адресов IPv4 и осуществление поддержки соседних устройств. Поддержка одноадресатных адресов IPv6 должна быть явно определена в конфигурации.

6. Активизация обмена префиксами маршрутов с соседним устройством IPv6:

   ```
   (router-af) neighbor ipv6-address activate
   ```

   Активизация средств протокола MBGP осуществляется с учетом семейств адресов.

НА ЗАМЕТКУ

Большинство команд, приведенных выше для BGP, могут применяться для работы с протоколом MBGP. Хотя команды внешне одинаковы, между ними имеется различие, связанное с применением режима настройки конфигурации семейства адресов.

7. Определение маршрутов к сетям, анонсируемых с помощью протокола MBGP как исходящих из локальной автономной системы:

а) Определение списка, который включает до 200 сетей:

```
(router-af) network network-number/prefix-length
```

Данные об указанных сетях должны присутствовать в таблице одноадресатной маршрутизации с определением того, являются ли они непосредственно подключенными, имеется ли к ним статический маршрут или сведения о них получены от динамических процессов маршрутизации.

Еще один вариант состоит в следующем.

б) Перераспределение маршрутов из IGP:

```
(router-af) redistribute protocol [process-id] ... [route-map map]
```

Как правило, локальные сети (находящиеся в пределах локальной автономной системы) должны быть указаны с помощью команды `network`; но в случае необходимости маршруты IGP могут быть перераспределены в BGP. Для фильтрации перераспределяемых маршрутов IGP должна использоваться схема маршрутов.

8. Описание настройки других атрибутов и операций BGP, используемых в командах, приведено в разделе 6.9. Чтобы можно было применить эти команды к средствам протокола MBGP для IPv6, необходимо вначале убедиться в том, что указано семейство адресов IPv6 и соседнее устройство MBGP активизировано.

Пример

На рис. 6.9 показан пример настройки конфигурации маршрутизатора RouterB для использования протокола MBGP. Для маршрутизатора RouterB задана связь одноранговых узлов iBGP с маршрутизатором RouterA и связь одноранговых узлов eBGP с маршрутизатором RouterC.

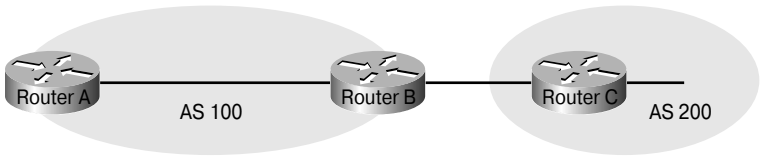

Рис. 6.9. Пример применения протокола MBGP в сети IPv6

```
hostname RouterB
!
ipv6 unicast-routing
!
interface fastethernet 0/0
   description ***Link to RouterA***
   ipv6 address 2001:1:1:1::1/64
!
interface fastethernet0/1
 description ***Link to RouterC***
 ipv6 address 2001:2:2:2::1/64
!
router bgp 100
 bgp router-id 1.1.1.1
 no bgp default ipv4-unicast
 neighbor 2001:2:2:2::2 remote-as 200
```

```
neighbor 2001:1:!:1::2 remote-as 100
address-family ipv6 unicast
   neighbor 2001:2:2:2::2 activate
   neighbor 2001:1:1:1::2 activate
   network 2001:1:1:!::/64
   network 2001:2:2:2::/64
```

Источники дополнительной информации

Ниже приведены рекомендуемые источники дополнительных сведений по адресованию и службам IP, представленным в настоящей главе.

Все протоколы маршрутизации IP

- Allan Leinwand and Bruce Pinsky, *Cisco Router Configuration*, Second Edition, Cisco Press, ISBN 1578702410 (пер. с англ. *Конфигурирование маршрутизаторов Cisco, 2-е изд.*, ISBN 5-8459-0568-0, ИД "Вильямс", 2001 г).
- Stephen McQuerry, *Interconnecting Cisco Network Devices*, Cisco Press, ISBN 1578701112.
- Mark A. Sportack, *IP Routing Fundamentals*, Cisco Press, ISBN 157870071X.
- Robert Wright, *IP Routing Primer*, Cisco Press, ISBN 1578701082.
- Jeff Doyle, *Routing TCP/IP*, Volume 1, Cisco Press, ISBN 1578700418.
- Khalid Raza and Mark Turner, *Large-Scale IP Network Solutions*, Cisco Press, ISBN 1578700841.
- Faraz Shamim, Zaheer Aziz, Johnson Lui, and Abe Martey, *Troubleshooting IP Routing Protocols*, Cisco Press, ISBN 1587050196.

EIGRP

- Ivan Pepelnjak, *EIGRP Network Design Solutions*, Cisco Press, ISBN 1578701651.
- Catherine Paquet and Diane Teare, *Building Scalable Cisco Networks*, Cisco Press, ISBN 1578702283 (пер. с англ. *Создание масштабируемых сетей Cisco*, ISBN 5-8459-0307-6, ИД "Вильямс", 2002 г).
- Alvaro Retana, Don Slice, and Russ White, *Advanced IP Network Design*, Cisco Press, ISBN 1578700973.
- "IGRP Metric", технические заметки Cisco TAC, www.cisco.com/warp/public/103/3.html.

OSPF

- Thomas M. Thomas II, *OSPF Network Design Solutions*, Cisco Press, ISBN 1578700469 (пер. с англ. *Структура и реализация сетей на основе протокола OSPF, 2-е изд.*, ISBN 5-8459-0594-X, ИД "Вильямс", 2004 г).
- Catherine Paquet and Diane Teare, *Building Scalable Cisco Networks*, Cisco Press, ISBN 1578702283.

- Alvaro Retana, Don Slice, and Russ White, *Advanced IP Network Design, Cisco Press*, ISBN 1578700973.
- *Initial Configurations for OSPF Over Frame Relay Subinterfaces*, пример конфигурации Cisco, `www.cisco.com/warp/public/104/22.html`.

BGP и MBGP

- *BGP Case Studies*, технические заметки Cisco TAC, `www.cisco.com/warp/public/459/bgp-toc.html`.
- *Using the Border Gateway Protocol for Interdomain Routing*", практический пример Cisco TAC, `www.cisco.com/univercd/cc/td/doc/cisintwk/ics/icsbgp4.htm`.
- *BGP Best Path Selection Algorithm*, технические заметки Cisco TAC, `www.cisco.com/warp/public/459/25.shtml`.
- Sam Halabi and Danny McPherson, *Internet Routing Architectures*, Second Edition, Cisco Press, ISBN 157870233X (пер. с англ. *Принципы маршрутизации в Internet, 2-е изд.*, ISBN 5-8459-0188-X, ИД "Вильямс", 2001 г).
- Jeff Doyle, *Routing TCP/IP*, Volume 2, Cisco Press, ISBN 1578700892.
- William Parkhurst, *BGP4 Command and Configuration Reference*, Cisco Press, ISBN 158705017X (пер. с англ. *Справочник по командам и настройке протокола BGP-4 маршрутизаторов Cisco*, ISBN 5-8459-0374-2, ИД "Вильямс", 2002 г).
- Catherine Paquet and Diane Teare, *Building Scalable Cisco Networks*, Cisco Press, ISBN 1578702283 (пер. с англ. *Создание масштабируемых сетей Cisco*, ISBN 5-8459-0307-6, ИД "Вильямс", 2002 г).
- Alvaro Retana, Don Slice, and Russ White, *Advanced IP Network Design*, Cisco Press, ISBN 1578700973.