

Протокол RIP



Успешно сдайте бесплатный сертификационный экзамен в Академии "Инфинет" и получите статус сертифицированного инженера Инфинет.

[Пройти сертификационный экзамен](#)

Содержание

- [Описание](#)
- [Алгоритм работы RIP](#)
 - [Запуск протокола RIP](#)
 - [Рассылка маршрутной информации](#)
 - [Добавление маршрутов в RIB](#)
 - [Добавление маршрутов в FIB](#)
 - [Контроль за таймерами](#)
 - [Контроль за изменениями в сети](#)
 - [Появление нового канала связи](#)
 - [Выход из строя канала связи](#)
 - [Выход из строя маршрутизатора](#)
- [Возникновение ложных маршрутов](#)
- [Особенности протокола RIP](#)
- [Дополнительные материалы](#)
 - [Прочее](#)

Описание

RIP (Routing Information Protocol - протокол маршрутной информации) - протокол динамической маршрутизации, в основе которого лежит алгоритм Беллмана-Форда. Протокол обладает следующими характеристиками:

- первая версия протокола RIP разработана в 1969 году, описана в [RFC 1058](#);
- вторая версия протокола RIP разработана в 1994 году, описана в [RFC 2454](#). Эта версия является основной для использования в IPv4-сетях. Между первой и второй версиями отсутствует обратная совместимость;
- существует версия протокола RIP, разработанная для сетей IPv6. Эта версия называется RIPng и описана в [RFC 2080](#);
- протокол RIP является внутренним протоколом маршрутизации дистанционно-векторного типа;
- в качестве метрики используется число хопов, т.е. число маршрутизаторов, через которое проходит путь к сети назначения. Максимальное значение метрики - 16, что ограничивает размер сети, в которой может быть использован протокол RIP;
- за протоколом RIP версии 2 зарезервирован адрес групповой рассылки 224.0.0.9. В первой версии протокола используется широковещательный адрес 255.255.255.255;
- для передачи служебной информации используются UDP-датаграммы, за протоколом закреплён порт 520;
- первая версия протокола RIP поддерживает только передачу маршрутов о классовых сетях, вторая - бесклассовых;
- для протокола RIP используется значение distance 120;
- протокол RIP поддерживает аутентификацию: маршрутная информация будет принята только от маршрутизатора, для которого совпало значение ключа.

Алгоритм работы RIP

Рассмотрим пример распространения маршрутной информации в сети с использованием протокола RIP. Для этого рассмотрим следующую схему (рис. 1):

- сеть состоит из четырёх маршрутизаторов R1, R2, R3 и R4, соединённых по кольцевой схеме, образующих домен RIP. Под доменом RIP понимается совокупность маршрутизаторов, обменивающихся маршрутной информацией с помощью протокола RIP;
- маршрутизатор R1 имеет внешний канал связи с сетью WAN-1;
- для каждого из каналов связи выделена самостоятельная сеть IP.

На маршрутизаторах необходимо настроить протокол RIP. Сеть WAN-1 является внешней, т.е. маршрут к этой сети должен быть добавлен в домен RIP как внешний.

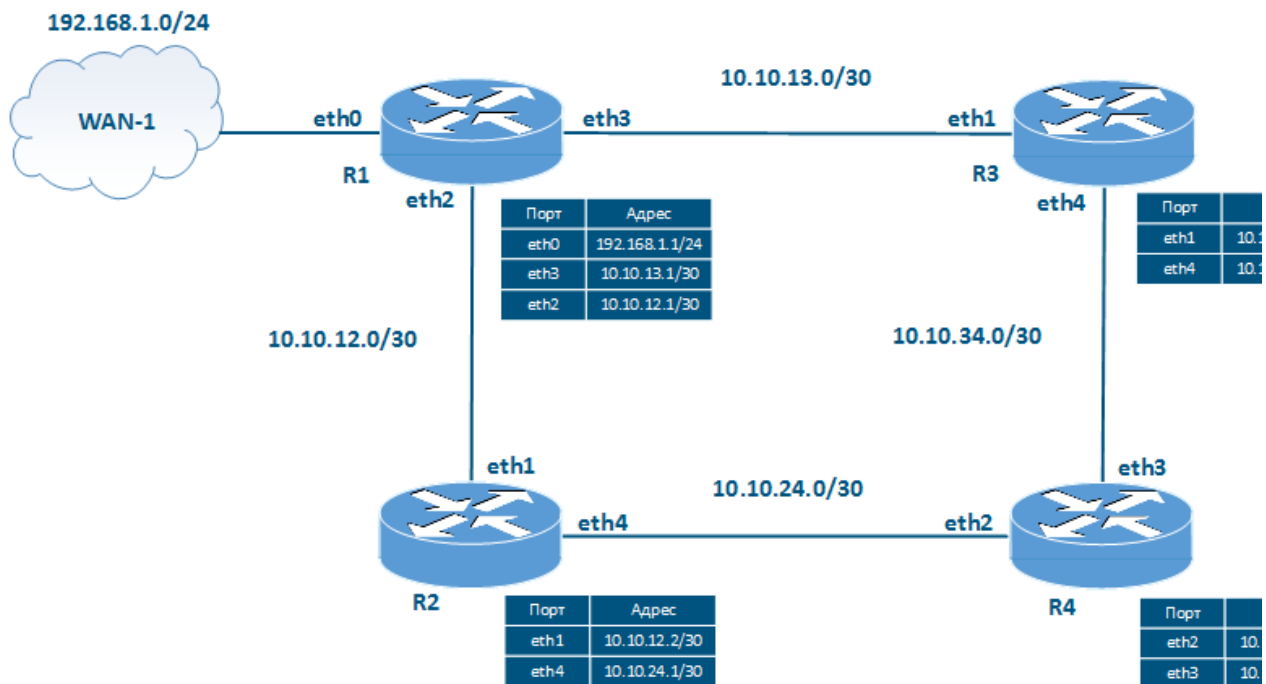


Рисунок 1 - Схема сети для пояснения принципов работы RIP

В рассматриваемом примере сосредоточимся на распространении маршрутной информации от маршрутизатора R1, маршруты от других устройств будут распространяться аналогично.

Алгоритм работы протокола RIP в рассматриваемой схеме выглядит следующим образом:

1. Запуск протокола RIP.
2. Рассылка маршрутной информации.
3. Добавление маршрутов в RIB.
4. Добавление маршрутов в FIB.
5. Контроль за таймерами.
6. Контроль за изменениями в сети.

Запуск протокола RIP

На данном этапе на маршрутизаторах должен быть активирован протокол RIP и определён список интерфейсов, которые будут участвовать в работе RIP.

Определение списка выполняется с использованием команды "network A.B.C.D/M". Все сетевые интерфейсы, IP-адреса которых принадлежат указанному диапазону, участвуют в работе протокола RIP. Это значит, что с этих интерфейсов будет выполняться рассылка маршрутной информации, и информация о сетях, связанных с этими интерфейсами, будет передана другим маршрутизаторам.

Если интерфейс должен быть включен в работу протокола RIP, но рассылка маршрутной информации через этот интерфейс не должна выполняться, то этот интерфейс может быть настроен как пассивный.

Будем считать, что на маршрутизаторе R1 выполнены команды "network 10.10.13.0/30" и "network 10.10.12.0/30". В этом случае, маршрутизатор будет считать, что протокол RIP запущен на интерфейсах eth2 и eth3.

Рассылка маршрутной информации

Рассылка маршрутной информации о сетях, подключенных к маршрутизатору R1, выполняется в следующей последовательности:

- **Этап 1:** маршрутизатор R1 формирует служебные сообщения с маршрутной информацией. Служебные сообщения содержат информацию о сетях 10.10.13.0/30 и 10.10.12.0/30, т.к. интерфейсы, связанные с этими сетями включены в протокол RIP на этапе [запуска протокола](#). Также в служебные сообщения включается информация о сети 192.168.1.0/24, т.к. по условиям задачи маршрутизатор R1 должен выполнять редистрибуцию внешних маршрутов. Значение метрики для каждой из сетей устанавливается равным 1.
- **Этап 2:** маршрутизатор рассылает служебные сообщения, сформированные на этапе 1 (рис. 2а). Рассылка выполняется через интерфейсы eth2 и eth3, включённые в RIP на этапе [запуска протокола](#).

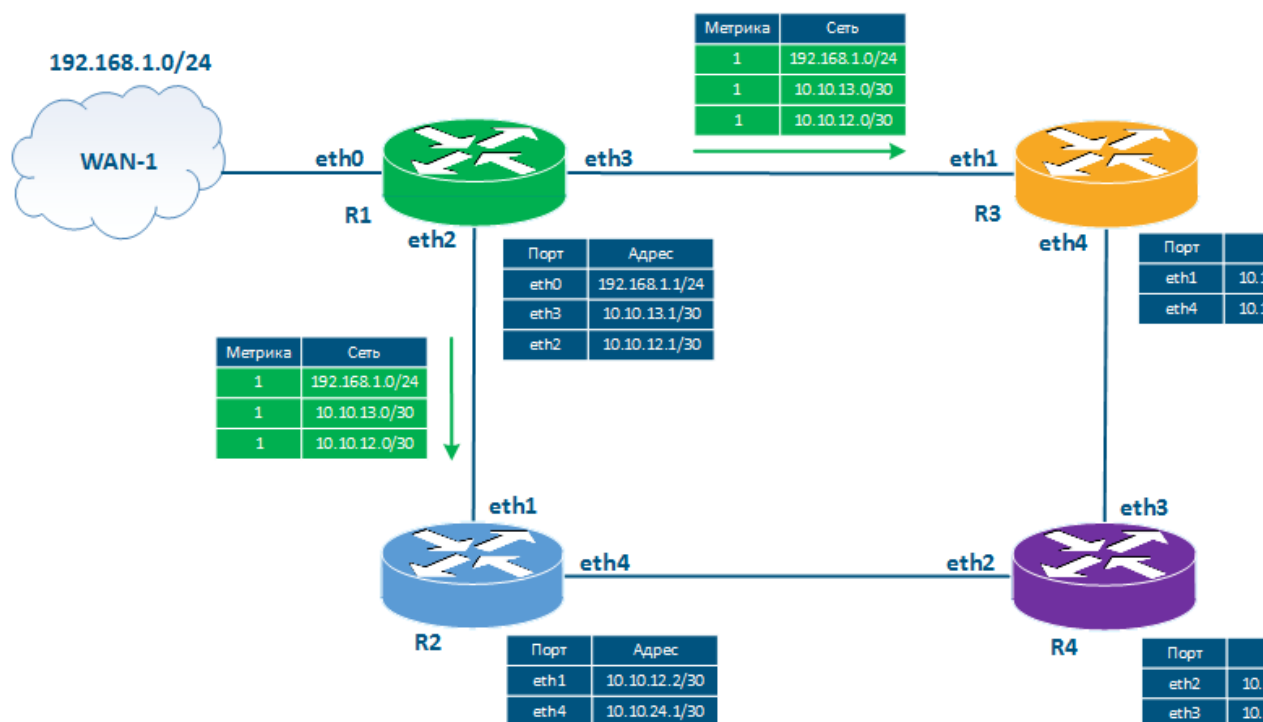


Рисунок 2а - Рассылка маршрутной информации маршрутизатором R1

- Этап 3:** маршрутизаторы R2 и R3 формируют служебные сообщения для передачи маршрутной информации маршрутизатору R4:
 - R2:** маршрутизатор включает в служебное сообщение сети 192.168.1.0/24 и 10.10.13.0/30, полученные от маршрутизатора R1, инкрементируя значение метрики. Информация о сети 10.10.12.0/30, полученная от маршрутизатора R1, игнорируется, т.к. маршрутизатор R2 непосредственно подключен к этой сети. Вместо этого маршрутизатор R2 включает в служебное сообщение сеть 10.10.12.0/30 с метрикой 1, анонсируя сеть самостоятельно. Кроме того, в служебное сообщение включается информация о сети 10.10.24.0/30.
 - R3:** маршрутизатор включает в служебное сообщение сети 192.168.1.0/24 и 10.10.12.0/30, полученные от маршрутизатора R1, инкрементируя значение метрики. Информация о сети 10.10.13.0/30, полученная от маршрутизатора R1, игнорируется, т.к. маршрутизатор R3 непосредственно подключен к этой сети. Вместо этого маршрутизатор R3 включает в служебное сообщение сеть 10.10.13.0/30 с метрикой 1, анонсируя сеть самостоятельно. Кроме того, в служебное сообщение включается информация о сети 10.10.34.0/30.
- Этап 4:** маршрутизаторы R2 и R3 отправляют служебные сообщения, сформированные на предыдущем этапе, маршрутизатору R4 (рис. 2б). Следует иметь в виду, что маршрутизаторы R2 и R3 отправляют маршрутную информацию маршрутизатору R1, но этот процесс не будет рассматриваться в данном примере.

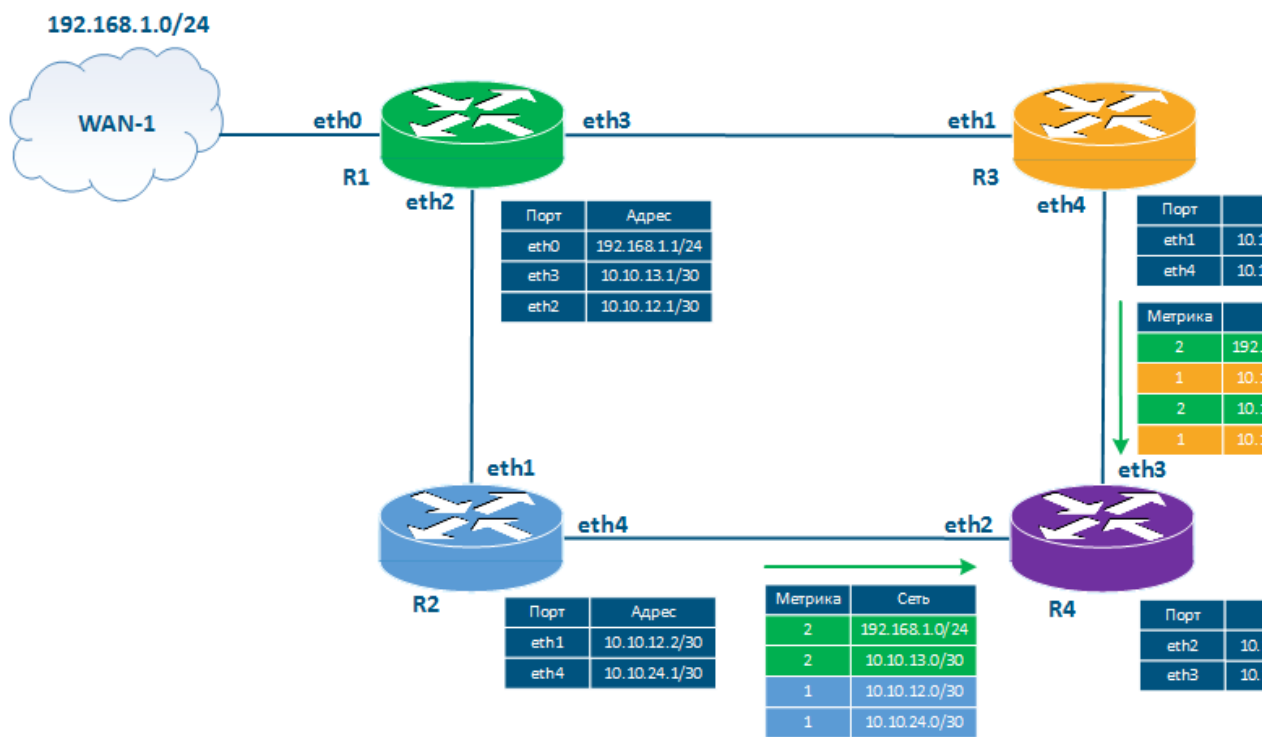


Рисунок 26 - Рассылка маршрутной информации маршрутизаторами R2 и R3

Добавление маршрутов в RIB

После обмена служебными сообщениями, маршрутизаторы добавляют полученные маршруты в RIB. При этом часть маршрутов отфильтровывается. При фильтрации маршрутной информации устройства руководствуются следующими принципами:

- в RIB может быть добавлен только один маршрут к сети назначения;
- при наличии двух маршрутов к одной и той же сети, в RIB добавляется маршрут с меньшим значением метрики;
- в RIB может быть добавлен маршрут с большим значением метрики, если он получен от того же источника;
- если существует два маршрута в одну сеть назначения с одинаковыми значениями метрики, то в RIB будет добавлен маршрут, полученный первым.

Будем считать, что маршрутизатор R4 получил служебное сообщение от маршрутизатора R2 раньше, чем от R3. Тогда, в соответствии с представленными принципами, маршрутизаторы добавляют в RIB следующую маршрутную информацию:

Маршрутизатор R2		
Сеть назначения	Метрика	Шлюз
10.10.12.0/30	1	-
10.10.24.0/30	1	-
10.10.13.0/30	2	10.10.12.1
192.168.1.0/24	2	10.10.12.1
Маршрутизатор R3		
Сеть назначения	Метрика	Шлюз
10.10.13.0/30	1	-

10.10.34.0/30	1	-
10.10.12.0/30	2	10.10.1 3.1
192.168.1.0 /24	2	10.10.1 3.1
Маршрутизатор R4		
Сеть назначения	Метрика	Шлюз
10.10.24.0/30	1	-
10.10.34.0/30	1	-
10.10.12.0/30	2	10.10.2 4.1
10.10.13.0/30	2	10.10.3 4.1
192.168.1.0 /24	3	10.10.2 4.1

Добавление маршрутов в FIB

Экспорт маршрутов из RIB в FIB сопровождается анализом значений distance, закреплёнными за источником маршрутов. За протоколом RIP закреплено значение distance = 120, поэтому часть из маршрутов, добавленных в RIB на предыдущем этапе будет отфильтрована. В частности, все маршруты с метрикой 1 будут отброшены, т.к. это маршруты к непосредственно присоединённым сетям, для которых используется значение distance = 0.

Контроль за таймерами

Рассылка маршрутной информации, рассмотренная [выше](#), циклически повторяется. Период повторения равен величине update timer. По умолчанию update timer равен 30 секундам. Таким образом, каждые 30 секунд выполняется рассылка всей маршрутной информации в сети.

Следует понимать, что маршрутизаторы не устанавливают отношений соседства и не синхронизируют время обмена маршрутной информацией, поэтому время отправки служебных сообщений маршрутизаторами распределяется в интервале 30 секунд, что позволяет избежать всплесков передачи служебного трафика в сети.

После того, как маршрут, полученный с помощью протокола RIP, помещён в RIB, запускается timeout timer, равный по умолчанию 180 секундам. Если в течении 180 секунд маршрутизатор не получает обновление маршрута, то маршрут будет помечен как недоступный, т.е. значение метрики такого маршрута устанавливается равным 16. Маршрутизатор не может использовать такой маршрут для передачи данных.

Обмен служебными данными RIP не является гарантированным, поэтому значение timeout timer должно быть больше, чем update timer. В противном случае, возможны ложные срабатывания и определение маршрутов как недоступных.

После добавления маршрута в RIB, помимо timeout timer, запускается garbage timer, значение которого по умолчанию равно 240 секунд. Если в течение 240 секунд маршрутизатор не получает обновление маршрутной информации, то такой маршрут будет удалён из таблицы маршрутизации.

Обновление маршрутной информации сбрасывает timeout timer и garbage timer в исходные значения.

Контроль за изменениями в сети

RIP является протоколом динамической маршрутизации, поэтому должен адаптироваться к изменениям в сети. Среди изменений можно выделить три сценария:

- появление нового канала связи;
- выход из строя канала связи;
- выход из строя маршрутизатора.

Появление нового канала связи

Добавим в рассматриваемую схему новый канал связи между маршрутизатором R1 и WAN-2 (рис. 3а). В этом случае, сеть WAN-2 будет внешней по отношению к протоколу RIP, а значит маршрут к этой сети будет распространяться аналогично маршруту к сети WAN-1: маршрутизатор R1 будет анонсировать эту сеть с метрикой 1, R2 и R3 инкрементируют значение метрики и передадут маршрут R4. Алгоритм действий при появлении новых маршрутизаторов, включённых в домен RIP, будет аналогичным.

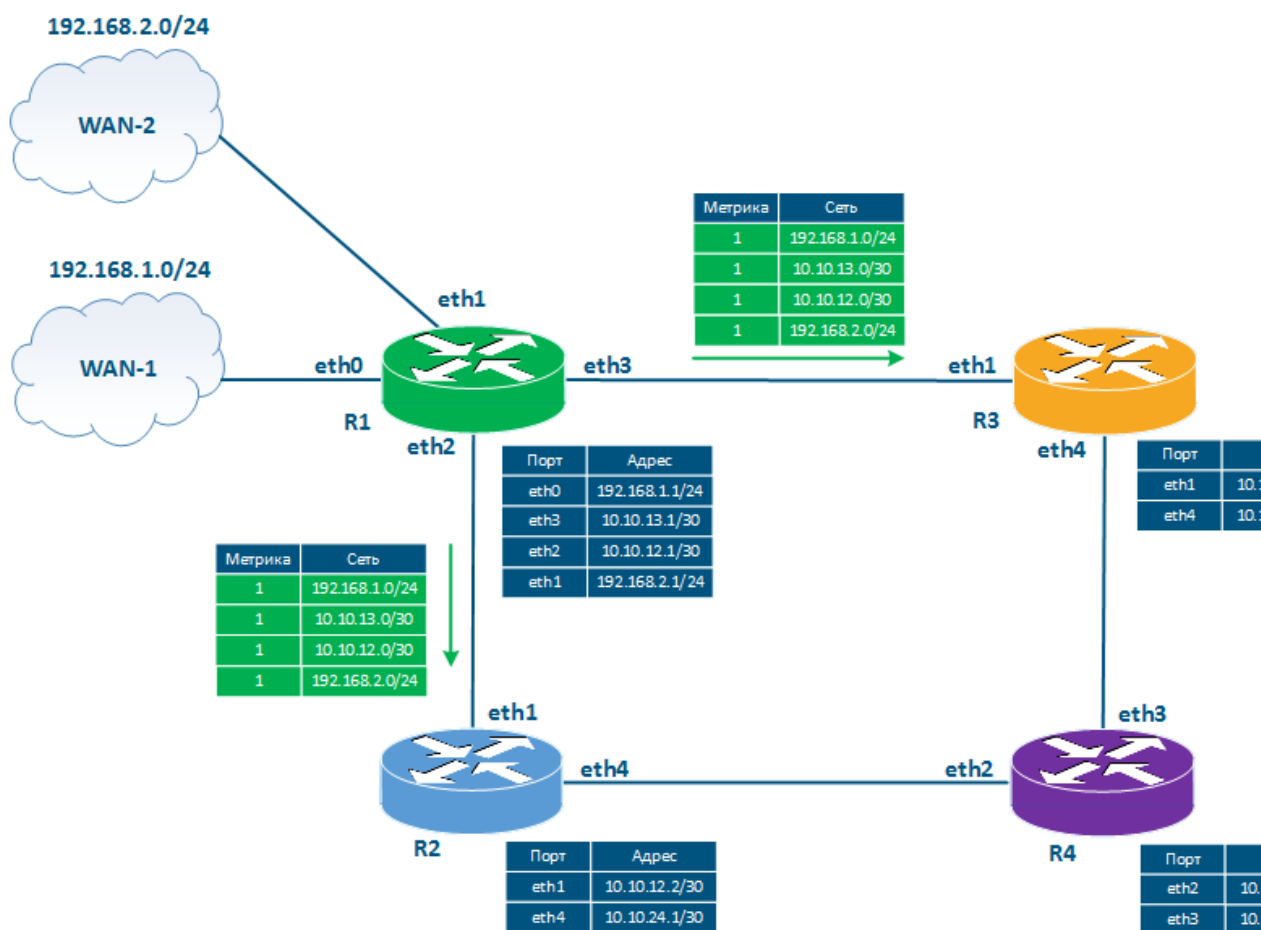


Рисунок 3а - Пример рассылки служебных сообщений при появлении нового канала связи

Выход из строя канала связи

Рассмотрим сценарий, в котором вышел из строя канал связи между маршрутизаторами R1 и R3 (рис. 3б):

- **Этап 1:** интерфейсы eth3 маршрутизатора R1 и eth1 маршрутизатора R3 перейдут в статус down.
- **Этап 2:** маршрутизаторы R1 и R3 установят в RIB маршрут к сети 10.10.13.0/30 значение метрики 16.
- **Этап 3:** в соответствии с истечением update timer, маршрутизаторы R1 и R3 сформируют служебное сообщение, включающее известную маршрутную информацию. В это сообщение включается путь к недоступной сети, причём метрика этого маршрута устанавливается равной 15.
- **Этап 4:** маршрутизаторы R2 и R4 получают служебные сообщения от R1 и R3, инкрементируют значение метрики и помещают маршрут в RIB. В RIB маршрутизаторов R2 и R4 уже есть маршрут к сети 10.10.13.0/30 с метрикой 2, но т.к. источниками новых маршрутов с худшей метрикой являются те же маршрутизаторы, то маршрут в RIB будет заменён на маршрут с метрикой 16. Таким образом все маршрутизаторы сети получают информацию о недоступности канала связи.

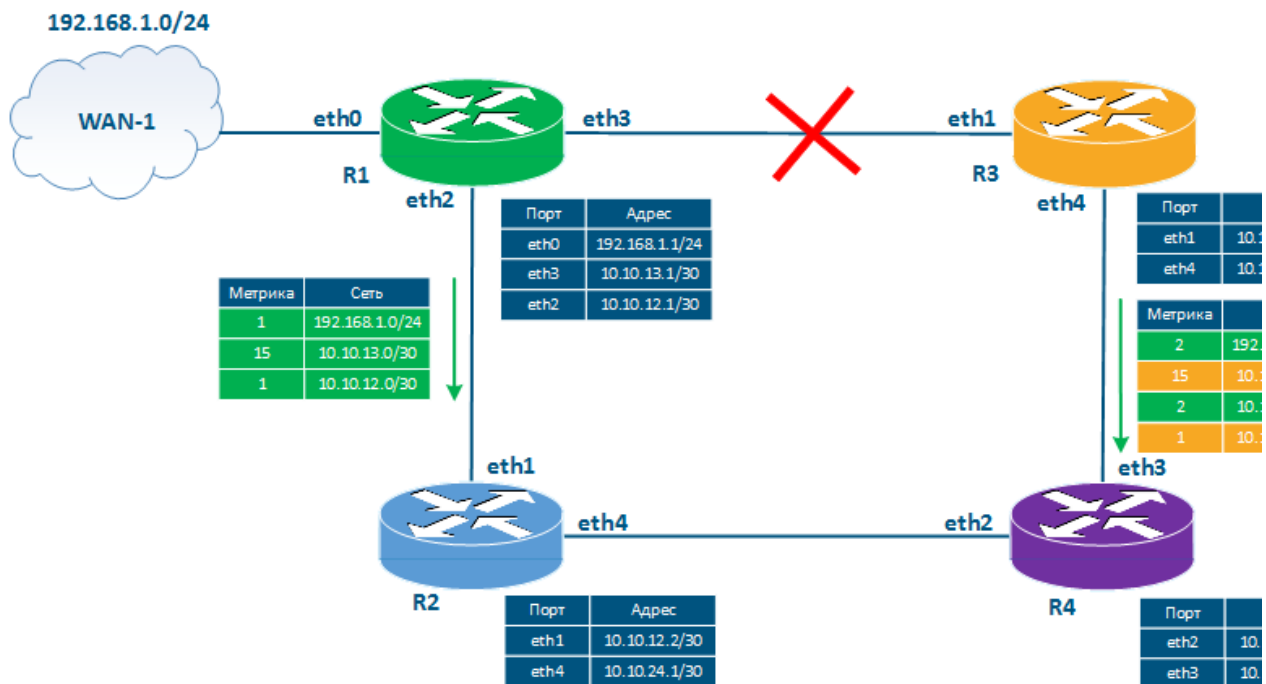


Рисунок 36 - Пример рассылки служебных сообщений при выходе из строя канала связи

Время, в течение которого распространяется обновлённая информация зависит от размеров сети и зависит от значения update timer. Учитывая, что максимальный размер сети - 16 хопов, а update timer по умолчанию равен 30 секундам, то в худшем сценарии время распространения информации о недоступности канала связи будет равно $15 \times 30 = 450$ секунд.

Выход из строя маршрутизатора

Дополним схему двумя коммутаторами SW1 и SW2 (рис. 3в) и рассмотрим сценарий выхода из строя маршрутизатора R1.

При выходе из строя маршрутизатора R1, он не успевает отправить обновление маршрутной информации о своей недоступности маршрутизаторам R2 и R3. Кроме того, R2 и R3 не узнают о недоступности R1, поскольку они непосредственно подключены к коммутаторам SW1 и SW2, которые не поддерживают работу протокола RIP. В этом случае, маршрутизаторы сети будут считать R1 доступным на протяжении timeout timer и будут использовать маршруты, связанные с R1. В частности, в таблице маршрутизации всех маршрутизаторов будут активны маршруты к сетям 10.10.12.0/30, 10.10.13.0/30 и 192.168.1.0/24.

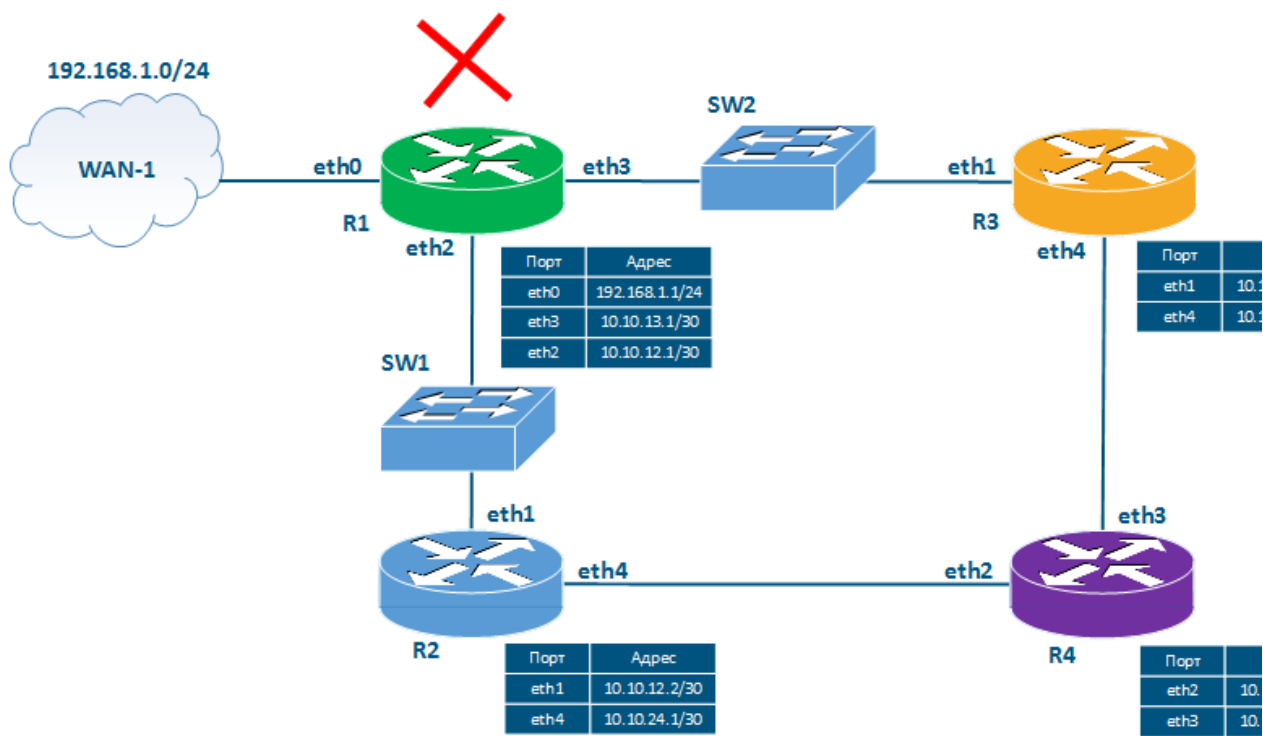


Рисунок 3в - Пример рассылки сообщений при выходе из строя маршрутизатора R1

Возникновение ложных маршрутов

Упростим рассматриваемую схему, оставив два маршрутизатора R1 и R3 (рис. 4а). Будем считать, что маршрутизаторы обменялись маршрутной информацией и таблицы маршрутизации устройств находятся в актуальном состоянии.

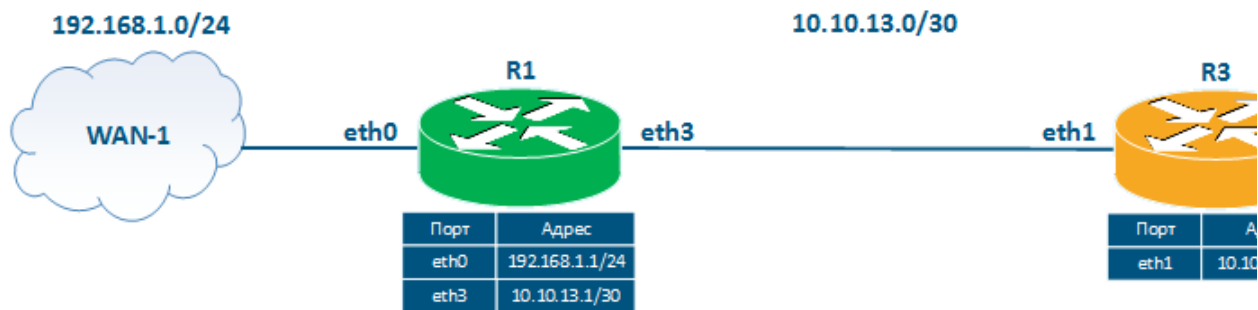


Рисунок 4а - Схема сети для сценария возникновения ложных маршрутов

Маршрутизатор R1		
Сеть назначения	Метрика	Шлюз
10.10.13.0/30	1	-
192.168.1.0/24	1	-
Маршрутизатор R3		
Сеть назначения	Метрика	Шлюз
10.10.13.0/30	1	-
192.168.1.0/24	2	10.10.13.1

Пусть канал связи между маршрутизатором R1 и внешней сетью WAN-1 вышел из строя (рис. 4б). Маршрутизатор R1 устанавливает для такого маршрута метрику равную 16, однако не формирует служебное сообщение с обновлённой маршрутной информацией, т.к. значение update timer равно 25 секунд. В то же время update timer на маршрутизаторе R3 равен 3 секундам.

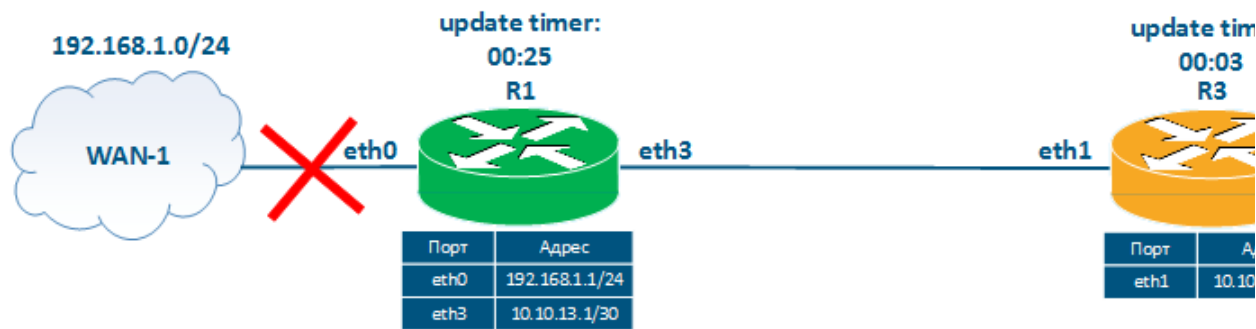


Рисунок 4б - Возникновение неисправности с каналом связи R1 - WAN-1

Маршрутизатор R1		
Сеть назначения	Метрика	Шлюз
10.10.13.0/30	1	-
192.168.1.0/24	16	-

Маршрутизатор R3		
Сеть назначения	Метрика	Шлюз
10.10.13.0/30	1	-
192.168.1.0/24	2	10.10.13.1

Через 3 секунды после выхода из строя канала связи R1 - WAN-1 истекает время update timer маршрутизатора R3, поэтому R3 отправляет обновление маршрутной информации маршрутизатору R1 (рис. 4в). Это обновление содержит информацию о сетях 10.10.13.0/30 и 192.168.1.0/24. Маршрутизатор R1 добавляет в RIB маршрут к сети 192.168.1.0/24, т.к. его метрика лучше чем у маршрута, который уже добавлен в RIB.

Образовалась петля маршрутизации, каждый из маршрутизаторов, передавая трафик в сеть 192.168.1.0/24, ссылается на другой маршрутизатор. Таким образом трафик будет передаваться маршрутизаторами друг другу до истечения значения TTL. Помимо образования петли маршрутизации стоит обратить внимание на то, что оба маршрута являются ложными, т.к. связь с сетью 192.168.1.0/24 потеряна.

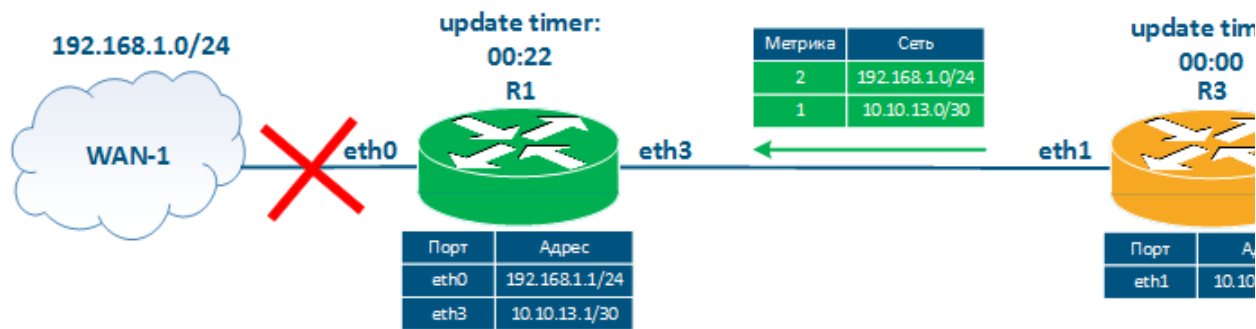


Рисунок 4в - Отправка служебного сообщения с маршрутной информацией маршрутизатором R3

Маршрутизатор R1		
Сеть назначения	Метрика	Шлюз
10.10.13.0/30	1	-

192.168.1.0/24	3	10.10.13.2
Маршрутизатор R3		
Сеть назначения	Метрика	Шлюз
10.10.13.0/30	1	-
192.168.1.0/24	2	10.10.13.1

Использование ложного маршрута будет продолжаться до истечения timeout timer на маршрутизаторе R3, после чего R3 установит для этого маршрута значение метрики равной 16. В следующей рассылке маршрутной информации маршрутизатор R1 передаст маршрутизатору R3 сведения о маршрутах к сетям 10.10.13.0/30 и 192.168.1.0/24 (рис. 4г). Поскольку метрика маршрута к сети 192.168.1.0/24 будет равна 3, что меньше 16, то маршрутизатор R3 добавит ложный маршрут в RIB, инкрементируя значение метрики.

Обмен ложным маршрутом будет продолжаться до того момента, пока значение метрики не достигнет недопустимого значения 16. При настройках по умолчанию это произойдёт через 36 минут после неисправности канала связи между R1 и WAN-1.

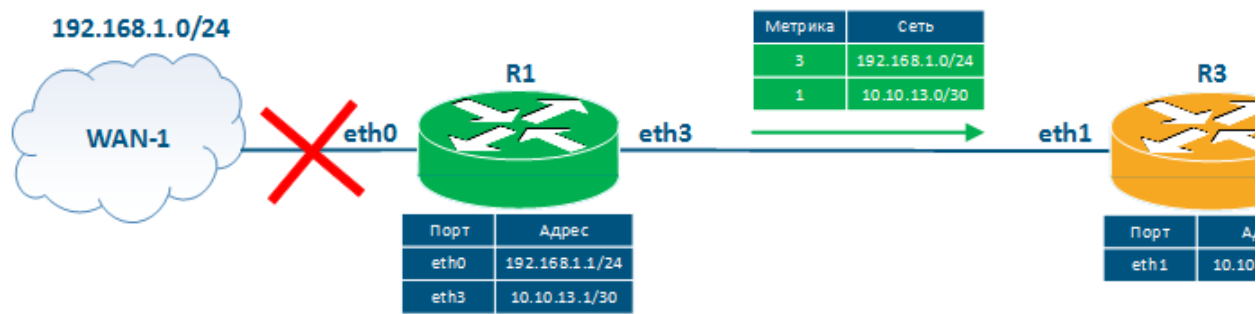


Рисунок 4г - Отправка служебного сообщения с маршрутной информацией маршрутизатором R1

Маршрутизатор R1		
Сеть назначения	Метрика	Шлюз
10.10.13.0/30	1	-
192.168.1.0/24	3	10.10.13.2
Маршрутизатор R3		
Сеть назначения	Метрика	Шлюз
10.10.13.0/30	1	-
192.168.1.0/24	4	10.10.13.1

Для того, чтобы избежать возникновения ложных маршрутов в протоколе RIP используются следующие механизмы:

- split-horizont:** маршрутизаторы не рассылают обновление маршрутной информации тем маршрутизаторам, которые являются источниками этой информации. В рассматриваемом примере (рис. 4г) маршрутизатор R3 не будет включать в рассылку для маршрутизатора R1 информацию о маршруте к сети 192.168.1.0/24, т.к. источником этой информации является R1. Это позволит избежать описанной ситуации, но не будет эффективно работать в схеме с большим числом маршрутизаторов. Если предположить, что в схеме участвуют четыре маршрутизатора (рис. 1) и вышел из строя канал связи с WAN-1, то маршрутизаторы R2 и R3 не будут передавать для R1 информацию о маршруте к сети 192.168.1.0/24. Однако в RIB маршрутизатора R4 присутствует этот маршрут и он будет включён в периодическую рассылку маршрутной информации, что приведёт к возникновению ложного маршрута.
- poison-reverse:** данный механизм подразумевает немедленную рассылку обновлений о недоступных маршрутах без ожидания окончания таймера update timer. Недоступный маршрут рассылается с метрикой 15, инкрементация которого каждым из маршрутизаторов-получателей приведёт к недоступности маршрута в RIB. Механизм имеет недостаток, т.к. распространение маршрутной информации о недоступном маршруте требует определённого времени, в течение которого может быть отправлено сообщение со старой маршрутной информацией, где недоступный маршрут будет отмечен как доступный.
- garbage-timer:** устройство не принимает обновления для маршрутов, отмеченных как недоступные до истечения garbage-timer.

Перечисленные механизмы позволяют адаптировать протокол RIP для современных сетей, т.к. существование ложных маршрутов на протяжении 36 минут или время схождения протокола, равное 450 секундам, является недопустимым для многих сервисов.

Особенности протокола RIP

К особенностям протокола RIP можно отнести следующие пункты:

- алгоритм работы, используемый в протоколе RIP, прост для понимания и настройки;
- протокол RIP является стандартным, поэтому может быть реализован в устройствах различных производителей сетевых устройств;
- в протоколе возможно возникновение ложных маршрутов: этот недостаток был устранён добавлением в протокол дополнительных функций, которые усложнили логику работы и реализации протокола в сетевых устройствах;
- ограничение на размер сети, в котором может быть использован алгоритм RIP;
- долгое время адаптации сети к изменениям.

Дополнительные материалы

Прочее

1. [RFC 1058](#)
2. [RFC 2454](#)
3. [RFC 2080](#)
4. [Команда ARDA](#)
5. [Команда ARIP](#)
6. [Команда RIP](#)