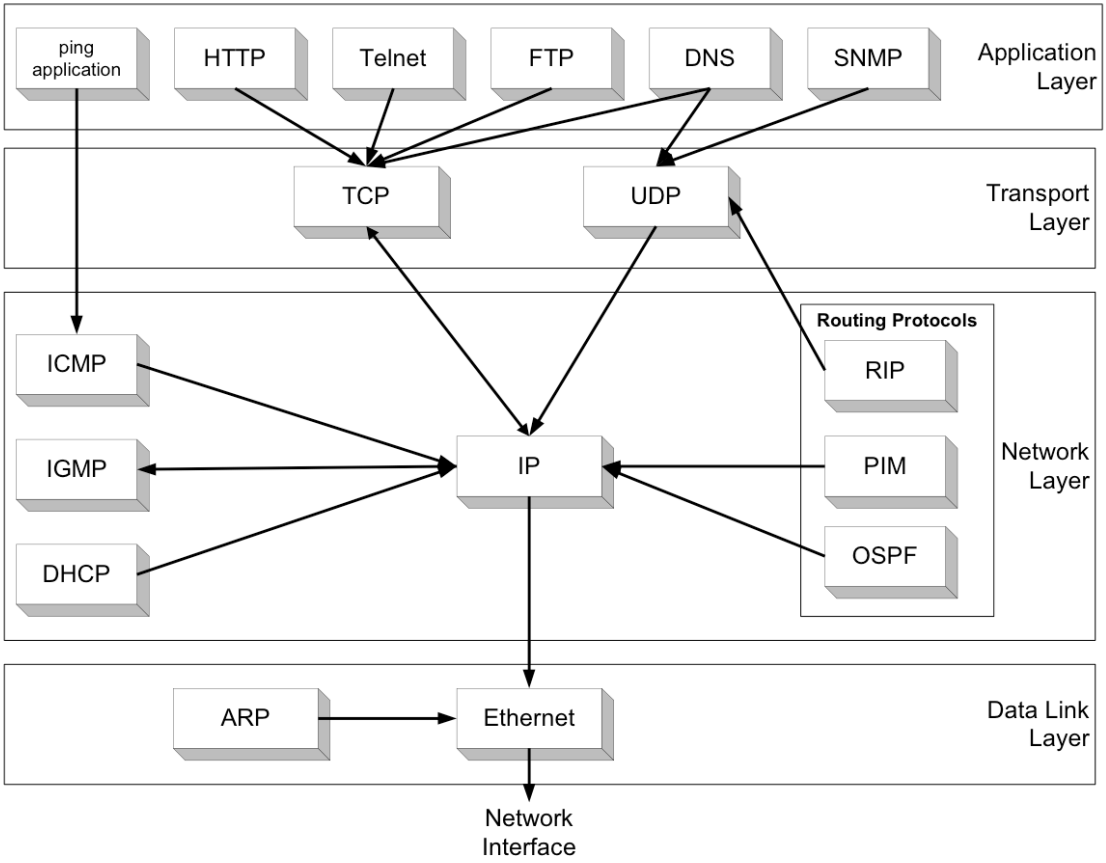
Протоколы RIP и BGP.



Протокол RIP (Routing Information Protocol — протокол маршрутной информации) является внутренним протоколом маршрутизации (IGP) дистанционно-векторного типа (DVA).

Будучи простым в реализации, этот протокол чаще всего используется в небольших сетях. Для IP имеются две версии RIP — RIPv1 и RIPv2.

Протокол RIPv1 не поддерживает масок. Протокол RIPv2 передает информацию о масках сетей, поэтому он в большей степени соответствует требованиям сегодняшнего дня. Так как построение таблиц маршрутизации в обеих версиях протокола принципиально не отличается, в дальнейшем для упрощения записей будет описываться работа версии 1.

Для измерения расстояния до сети стандарты протокола RIP допускают различные виды метрик: хопы, значения пропускной способности, вносимые задержки, надежность сетей (то есть соответствующие признакам D, T и R в поле качества сервиса IP-пакета), а также любые комбинации этих метрик. В большинстве реализаций RIP используется простейшая метрика — количество хопов, то есть количество промежуточных маршрутизаторов, которые нужно преодолеть пакету до сети назначения.

Протокол BGP (Border Gateway Protocol) – относится к классу протоколов маршрутизации внешнего шлюза (EGP — External Gateway Protocol). Основные реализации Cisco IOS, Juniper JunOS, Bird, OpenBGPD, Quagga, Huawei VRP, Mikrotik RouterOS

На текущий момент BGP является основным протоколом динамической маршрутизации в сети Internet между AS.

1. Построение таблицы маршрутизации RIP.

Рассмотрим процесс построения таблицы маршрутизации с помощью протокола RIP на примере составной сети, изображенной на рис. 1. Мы разделим этот процесс на 5 этапов.

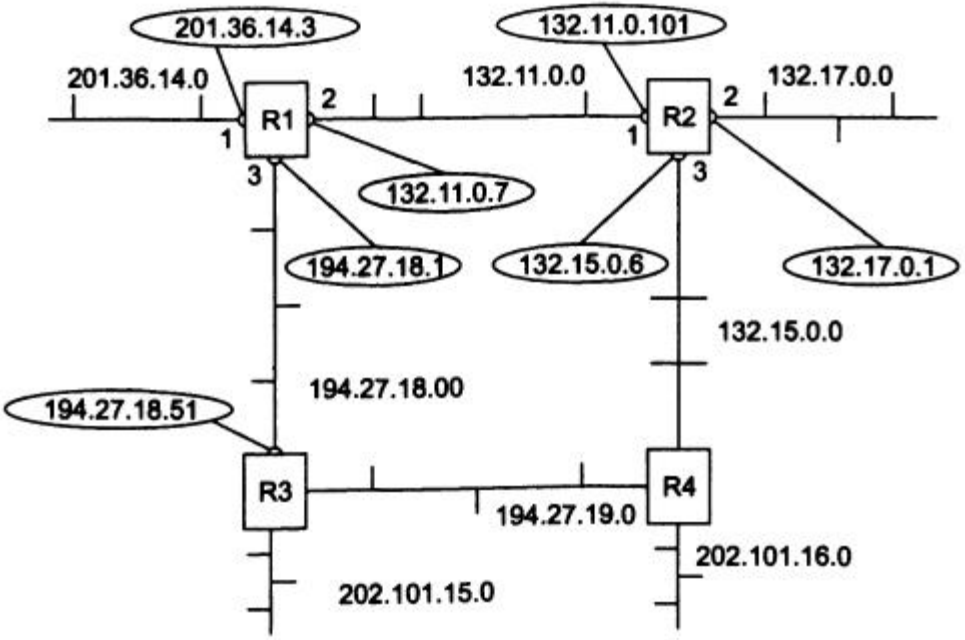


Рис. 1. Сеть, построенная на маршрутизаторах RIP.

1.1. Создание минимальной таблицы (инициализация).

Данная составная сеть включает 8 IP-сетей, связанных 4 маршрутизаторами с идентификаторами: Rl, R2, R3 и R4. На рисунке адреса портов маршрутизаторов в отличие от адресов сетей помещены в овалы.

В исходном состоянии на каждом маршрутизаторе программным обеспечением стека TCP/IP автоматически создается минимальная таблица маршрутизации, в которой учитываются только непосредственно подсоединенные сети. Например,

Таблица 1. Минимальная таблица маршрутизации маршрутизатора R1.

Номер сети	Адрес следующего маршрутизатора	Порт	Расстояние
201.36.14.0	201.36.14.3	1	1
132.11.0.0	132.11.0.7	2	1
194.27.18.0	194.27.18.1	3	1

Таблица 2. Минимальная таблица маршрутизации маршрутизатора R2.

Номер сети	Адрес следующего маршрутизатора	Порт	Расстояние
132.11.0.0	132.11.0.101	1	1
132.17.0.0	132.17.0.1	2	1
132.15.0.0	132.15.0.6	3	1

1.2. Рассылка минимальной таблицы соседям.

После инициализации каждый маршрутизатор начинает посылать своим соседям сообщения протокола RIP, в которых содержится его минимальная таблица. RIP-сообщения передаются в дейтаграммах протокола UDP и включают два параметра для каждой сети: ее IP-адрес и расстояние до нее от маршрутизатора передающего сообщение.

По отношению к любому маршрутизатору соседями являются те маршрутизаторы, которым данный маршрутизатор может передать IP-пакет по какой-либо своей сети, не пользуясь услугами промежуточных маршрутизаторов. Например, для маршрутизатора R1 соседями являются маршрутизаторы R2 и R3, а для маршрутизатора R4 — маршрутизаторы R2 и R3.

Таким образом, маршрутизатор R1 передает маршрутизаторам R2 и R3 следующие сообщения:

- сеть 201.36.14.0, расстояние 1;
- сеть 132.11.0.0, расстояние 1;
- сеть 194.27.18.0, расстояние 1.

1.3. Получение RIP-сообщений от соседей и их обработка.

После получения аналогичных сообщений от маршрутизаторов R2 и R3 маршрутизатор R1 наращивает каждое полученное поле метрики на единицу и запоминает, через какой порт и от какого маршрутизатора получена новая информация. Затем маршрутизатор начинает сравнивать новую информацию с той, которая хранится в его ТМ (см. табл. 3).

Номер сети	Адрес следующего маршрутизатора	Порт	Расстояние
201.36.14.0	201.36.14.3	1	1
132.11.0.0	132.11.0.7	2	1
194.27.18.0	194.27.18.1	3	1
132.17.0.0	132.11.0.101	2	2
132.15.0.0	132.11.0.101	2	2
194.27.19.0	194.27.18.51	3	2
202.101.15.0	194.27.18.51	3	2
~~132.11.0.0~~	~~132.11.0.101~~	~~2~~	~~2~~
~~194.27.18.0~~	~~194.27.18.51~~	~~3~~	~~2~~

Записи с 4 по 9 получены от соседних маршрутизаторов, и они претендуют на помещение в ТМ. Однако только записи с 4 по 7 попадают в таблицу, а записи 8 и 9 — нет. Это происходит потому, что они содержат данные об уже имеющихся в ТМ R1 сетях, а расстояние до них больше (или равно), чем в существующих записях.

Протокол RIP замещает запись о сети только в том случае, если новая информация имеет лучшую метрику (меньше), чем имеющаяся или остается та запись, которая пришла в маршрутизатор **первая по времени**. (Существует исключение — если худшая информация о сети пришла от того же маршрутизатора, на основании сообщения которого была создана данная запись, то худшая информация замещает лучшую. Аналогичные операции с новой информацией выполняют и остальные маршрутизаторы сети.

1.4. Рассылка новой таблицы соседям.

Каждый маршрутизатор отсылает новую ТМ в виде RIP-сообщения всем своим соседям. В этом сообщении он помещает данные обо всех известных ему сетях: как о непосредственно подключенных, так и о которых маршрутизатор узнал из RIP-сообщений.

1.5. Получение RIP-сообщений от соседей и их обработка.

Этап 5 повторяет этап 3 — маршрутизаторы принимают RIP-сообщения, обрабатывают содержащуюся в них информацию и на ее основании корректируют свои таблицы маршрутизации.

Посмотрим, как это делает маршрутизатор R1 (табл. 4).

На этом этапе маршрутизатор R1 получает от маршрутизатора R3 информацию о сети 132.15.0.0, которую тот, в свою очередь, на предыдущем цикле работы получил от

маршрутизатора R4. Маршрутизатор уже знает о сети 132.15.0.0, причем старая информация имеет лучшую метрику, чем новая, поэтому новая информация об этой сети отбрасывается.

О сети 202.101.16.0 маршрутизатор R1 узнает на этом этапе впервые, причем данные о ней приходят от двух соседей — от R3 и R4. Поскольку метрики в этих сообщениях указаны одинаковые, то в таблицу попадают данные, пришедшие первыми. В нашем примере считается, что маршрутизатор R2 опередил маршрутизатор R3 и первым переслал свое RIP-сообщение маршрутизатору R1.

Таблица 4. Таблица маршрутизации маршрутизатора R1.

Номер сети	Адрес следующего маршрутизатора	Порт	Расстояние
201.36.14.0	201.36.14.3	1	1
132.11.0.0	132.11.0.7	2	1
194.27.18.0	194.27.18.1	3	1
132.17.0.0	132.11.0.101	2	2
132.15.0.0	132.11.0.101	2	2
~~132.15.0.0~~	~~194.27.18.51~~	~~3~~	~~3~~
194.27.19.0	194.27.18.51	3	2
104.27.10.0	132.11.0.101	2	3
202.101.15.0	194.27.18.51	3	2
202.101.16.0	132.11.0.101	2	3
~~202.101.16.0~~	~~104.27.18.51~~	~~3~~	~~3~~

Если маршрутизаторы периодически повторяют этапы рассылки и обработки RIP-сообщений, то за конечное время в сети установится корректный режим маршрутизации.

Под корректным режимом маршрутизации здесь понимается такое состояние таблиц маршрутизации, когда все сети достижимы из любой сети с помощью некоторого рационального маршрута. Пакеты будут доходить до адресатов и не зацикливаться в петлях, подобных той, которая образуется на рис. 1, маршрутизаторами R1, R2, R3 и R4.

2. Адаптация маршрутизаторов RIP к изменениям состояния сети.

Очевидно, если в сети все маршрутизаторы, их интерфейсы и соединяющие их линии связи остаются работоспособными, то объявления по протоколу RIP можно делать достаточно редко, например один раз в день. Однако в сетях постоянно происходят изменения — меняется работоспособность маршрутизаторов и линий связи, кроме того, маршрутизаторы и линии связи могут добавляться в существующую сеть или же выводиться из ее состава.

Одна из проблем RIP — медленная сходимость, то есть изменения, произошедшие на одном из участков Интернета, распространяются очень медленно через остальной Интернет. Для адаптации к изменениям в сети протокол RIP использует ряд механизмов.

К новым маршрутам маршрутизаторы RIP адаптируются просто — они передают новую информацию в очередном сообщении своим соседям и постепенно эта информация становится известна всем маршрутизаторам сети.

А вот к изменениям, связанным с **потерей какого-либо маршрута**, маршрутизаторы RIP адаптируются сложнее. Это связано с тем, что в формате сообщений протокола RIP нет поля, которое бы указывало на то, что путь к данной сети больше не существует.

Для уведомления о том, что некоторый маршрут недействителен, используются:

- истечение времени жизни маршрута TTL;
- указание специального (бесконечного) расстояния до сети, ставшей недоступной.

2.1. Механизм истечения времени жизни маршрута.

- Основан на том, что каждая запись ТМ, полученная по протоколу RIP или из сканирования собственных интерфейсов, имеет время жизни (**TTL маршрута**).
- Из TTL каждую секунду вычитается единица. Если за время тайм-аута не придет новое сообщение об этом маршруте, он помечается как недействительный (удаляется из ТМ).
- При завершении TTL записей о собственных интерфейсах производится их инициализация.
- При поступлении очередного RIP-сообщения, которое подтверждает справедливость данной записи, TTL устанавливается в исходное состояние.
- В качестве тайм-аута выбрано значение 180 секунд, а период рассылки примерно равен 30 секунд (в действительности используется случайное число между 25 и 35, что сделано, для предотвращения синхронизации маршрутизаторов при рассылке обновлений).
- Шестикратный запас времени таймаута нужен для уверенности в том, что сеть действительно стала недоступной, а не просто произошли потери RIP-сообщений (а это возможно, так как протокол RIP использует ненадёжный транспортный протокол UDP:520).
- Если какой-либо маршрутизатор отказывает, то перестаёт слать своим соседям сообщения о сетях, которые можно достичь через него, и через 180 секунд все записи, порожденные этим маршрутизатором, у его ближайших соседей станут недействительными.
- После этого процесс повторится уже для ближайших соседей — они вычеркнут подобные записи через 360 секунд. Для третьего соседа – через 540 секунд (почти 10 минут) и т.д.

Как видно, сведения о сетях, пути к которым не могут теперь проходить через отказавший маршрутизатор, распространяются по сети не очень быстро. В этом заключается одна из причин выбора в качестве периода рассылки небольшой величины в 30 секунд.

2.2. Механизм рассылки бесконечного расстояния до сети.

Механизм TTL работает в тех случаях, когда маршрутизатор не может послать соседям сообщение об отказавшем маршруте, так как либо он сам неработоспособен, либо неработоспособна линия связи, по которой можно было бы передать сообщение.

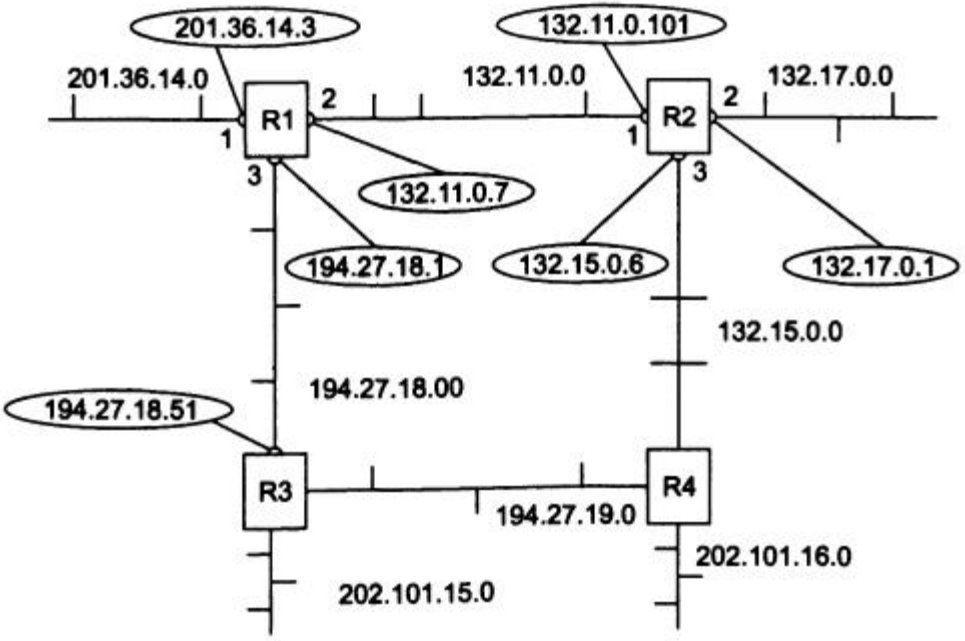
Когда же сообщение послать можно, маршрутизаторы RIP используют прием, заключающийся в указании бесконечного расстояния до сети ставшей недоступной.

- В протоколе RIP бесконечным условно считается расстояние в 16 хопов. Причиной выбора в качестве «бесконечного» расстояния столь небольшого числа является то, что в некоторых случаях отказы связей в сети вызывают длительные периоды некорректной работы маршрутизаторов RIP, выражающейся в зацикливании пакетов в петлях сети. И чем меньше расстояние, используемое в качестве «бесконечного», тем такие периоды короче.
- Получив сообщение, в котором расстояние до некоторой сети равно 16 (или 15, что приводит к тому же результату, так как маршрутизатор наращивает полученное значение на 1), маршрутизатор должен проверить, исходит ли эта «плохая» информация о сети от того же маршрутизатора, сообщение которого послужило в свое время основанием для записи о данной сети в таблице маршрутизации. Если это тот же маршрутизатор, то информация считается достоверной и маршрут помечается как недоступный.

3. Маршрутные петли в RIP.

3.1. Пример маршрутной петли в RIP.

Рассмотрим случай зацикливания пакетов на примере сети, изображенной на рис.



3.1.1. Пусть маршрутизатор R1 обнаружил, что его связь с непосредственно подключенной сетью 201.36.14.0 потеряна (например, по причине отказа интерфейса 201.36.14.3).

3.1.2. Маршрутизатор R1 отмечает в своей таблице маршрутизации, что **сеть 201.36.14.0 недоступна.** В лучшем случае он обнаружит это перед самой отправкой RIP-сообщений, а в худшем случае сразу же после отправки очередных RIP-сообщений, так что до начала нового цикла его объявлений, в котором он должен сообщить соседям, что расстояние до сети 201.36.14.0 стало равным 16, остается в среднем 15 секунд.

3.1.3. Каждый маршрутизатор работает на основании своего собственного таймера, не синхронизируя работу по рассылке объявлений с другими маршрутизаторами. Поэтому с вероятностью **50%, маршрутизатор R2 опередит маршрутизатор R1** и передаст ему свое сообщение (см. табл. 5). раньше, чем R1 успеет передать новость о недостижимости сети 201.36.14.0.

Таблица 5. Таблица маршрутизации маршрутизатора R2.

Номер сети	Адрес следующего маршрутизатора	Порт	Расстояние
201.36.14.0	132.11.0.7	1	2

Эта запись, полученная от маршрутизатора R1, была корректна до отказа интерфейса 201.36.14.3; теперь **она устарела**, но маршрутизатор R2 об этом не знает.

3.1.4. Маршрутизатор R1 получает новую информацию о сети **201.36.14.0 — эта сеть якобы достижима через маршрутизатор R2 с метрикой 2**.

Раньше R1 игнорировал эту информацию, так как его собственная метрика была лучше. Теперь R1 должен принять данные о сети 201.36.14.0, полученные от R2, и заменить запись в таблице маршрутизации о недостижимости этой сети (табл. 6).

Таблица 6. Таблица маршрутизации маршрутизатора R1.

Номер сети	Адрес следующего маршрутизатора	Порт	Расстояние
201.36.14.0	132.11.0.101	2	3

3.1.5. В результате в сети образуется маршрутная петля: пакеты, направляемые узлам сети 201.36.14.0, станут передаваться маршрутизатором R2 маршрутизатору R1, а маршрутизатор R1 будет возвращать их маршрутизатору R2.

IP-пакеты продолжат циркулировать по этой петле до тех пор, пока не истечет время жизни каждого IP-пакета (255 хопов).

3.2. Время жизни маршрутной петли.

Рассмотрим периоды времени, кратные времени жизни записей в таблицах маршрутизаторов.

- Время 0-180 с. После отказа интерфейса в маршрутизаторах R1 и R2 будут сохраняться некорректные записи. Маршрутизатор R2 по-прежнему снабжает маршрутизатор R1 своей записью о сети 201.36.14.0 с метрикой 2, так как ее время жизни не истекло. Пакеты зацикливаются.
- Время 180-360 с. В начале этого периода у маршрутизатора R2 истекает время жизни записи о сети 201.36.14.0 с метрикой 2, так как маршрутизатор R1 в предыдущий период посылал ему сообщения о сети 201.36.14.0 с худшей метрикой, чем у R2, и они не могли подтверждать эту запись. Теперь маршрутизатор R2 принимает от маршрутизатора R1 запись о сети 201.36.14.0 с метрикой 3 и трансформирует ее в запись с метрикой 4. Маршрутизатор R1 не получает новых сообщений от маршрутизатора R2 о сети 201.36.14.0 с метрикой 2, поэтому время жизни его записи начинает уменьшаться. Пакеты продолжают зацикливаться.
- Время 360-540 с. У маршрутизатора R1 истекает время жизни записи о сети 201.36.14.0 с метрикой 3. Маршрутизаторы R1 и R2 опять меняются ролями — R2 снабжает R1 устаревшей информацией о пути к сети 201.36.14.0, уже с метрикой 4, которую R1 преобразует в метрику 5. Пакеты продолжают зацикливаться.

Если бы в протоколе RIP не было выбрано **расстояние 16 в качестве недостижимого**, то описанный процесс длился бы очень долго (пока не была бы исчерпана разрядная сетка поля

расстояния, и при очередном наращивании расстояния было бы зафиксировано переполнение).

В результате маршрутизатор R2 на очередном этапе описанного процесса получает от маршрутизатора R1 метрику 15, которая после наращивания, превращаясь в метрику 16, фиксирует недостижимость сети. Таким образом, в нашем примере период нестабильной работы сети длился 36 минут!

Ограничение в 15 хопов сужает область применения протокола RIP до сетей, в которых число промежуточных маршрутизаторов не может быть больше 15. Для более масштабных сетей нужно применять другие протоколы маршрутизации, например OSPF, или разбивать сеть на автономные области.

Приведенный пример хорошо иллюстрирует главную причину нестабильности маршрутизаторов, работающих по протоколу RIP. Эта причина коренится в самом принципе работы дистанционно-векторных протоколов — использовании информации, полученной из «вторых рук». Действительно, маршрутизатор R2 передает маршрутизатору R1 информацию о достижимости сети 201.36.14.0, за достоверность которой он сам не отвечает.

ПРИМЕЧАНИЕ.

Не следует думать, что при любых отказах интерфейсов и маршрутизаторов в сетях возникают маршрутные петли. Маршрутные петли даже без дополнительных методов борьбы с ними возникают в среднем не более чем в половине потенциально возможных случаев.

4. Методы борьбы с ложными маршрутами в протоколе RIP.

Протокол RIP даже при борьбе с ложными маршрутами не в состоянии полностью исключить в сети переходные состояния, а лишь снижает подобные проблемы.

4.1. Расщепление горизонта (spilt horizon).

При этом методе данные о достижимых узлах сети передаются всем маршрутизаторам, кроме того, от которого эта информация исходила.

Если бы маршрутизатор R2 поддерживал технику расщепления горизонта, то он бы не передал маршрутизатору R1 устаревшую информацию о сети 201.36.14.0, так как получил он ее именно от маршрутизатора R1.

Расщепление горизонта не помогает когда петли образуются не 2, а большим числом маршрутизаторов.

Например, в случае потери связи маршрутизатора R1 с сетью 201.36.14.0. Маршрутизаторы R2 и R3 не будут возвращать R1 данные о сети 201.36.14.0 с метрикой 2, так как они получили эту информацию от R1. Однако они будут передавать R1 информацию о достижимости сети 201.36.14.0 с метрикой 4, так как получили эту информацию от R4.

Для предотвращения зацикливания пакетов **по составным петлям** при отказах связей применяются приемы, называемые тригтерными обновлениями и замораживанием изменений.

4.2. Триггерные обновления.

Прием триггерных обновлений состоит в том, что маршрутизатор, получив данные об изменении метрики до какой-либо сети, не ждет истечения периода передачи таблицы маршрутизации, а **передает данные об изменившемся маршруте немедленно.**

Этот прием может во многих случаях предотвратить передачу устаревших сведений об отказавшем маршруте, но он **перегружает сеть служебными сообщениями, поэтому триггерные объявления также делаются с некоторой задержкой.** По этой причине возможна ситуация, когда регулярное обновление в каком-либо маршрутизаторе чуть опережает по времени приход триггерного обновления от предыдущего в цепочке маршрутизатора, и данный маршрутизатор успевает передать по сети устаревшую информацию о несуществующем маршруте.

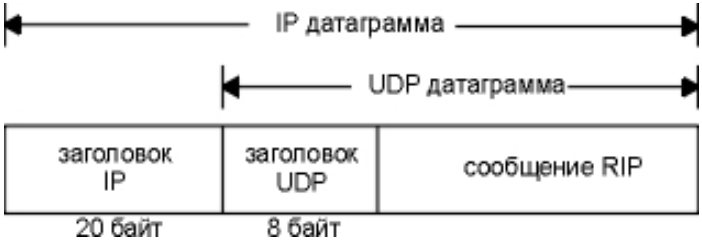
4.3. Замораживание изменений.

Прием замораживания изменений связан с **введением тайм-аута на принятие новых данных о сети, которая только что стала недоступной.**

Этот тайм-аут защищает R1 от принятия устаревших сведений от маршрутизаторов находящихся на некотором расстоянии. Предполагается, что в течение тайм-аута «замораживания изменений» эти маршрутизаторы вычеркнут данный маршрут из своих таблиц, так как не получают о нем новых подтверждений и не будут распространять устаревшие сведения по сети.

5. Формат RIP-пакетов.

Официальная спецификация протокола RIPv1 находится в RFC 1058 [Hedrick 1988]. RIP сообщения передаются в UDP:520 дейтаграммах, как показано на рисунке.



5.1. Формат RIPv1 сообщения запроса-ответа.

Octet	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
00	**Команда (1-6)**								**Версия (1)**								**(Должен быть 0)**															
04	**Семейство адресов (0 или 2)**																**(Должен быть 0)**														
08	**32-бит адрес сети (узла)**																															
12	**(Должен быть 0)**																															
16	**(Должен быть 0)**																															
20	**Показатель (1-16)**																															
24-n	**До 24 маршрутизаторов с тем же форматом, что и предыдущие 20 байт (с 04 по 24)**																															

Поле команда равно 1 - это запрос, если 2 - отклик. Существуют еще два значения поля команды (3 и 4), а также два недокументированных значения: опрос (5) и пункт опроса (6). В запросе находится требование к другой системе послать всю или часть ее таблицы маршрутизации. В отклике содержится вся или часть таблицы маршрутизации отправителя.

Поле версия обычно установлено в 1, однако для RIP Version 2 (раздел "RIP Version 2") это значение устанавливается в 2.

Семейство адресов - всегда равно 2 для TCP/IP адресов.

IP адрес сети/узла - определяет адрес пункта назначения. RIP отводит 14 байт для этого поля в применении к любым протоколам. Однако IP в настоящее время использует только 4 байта. Остаток адреса заполняется нулями.

Показатель - в роли показателя RIP выступает счетчик пересылок.

В одном RIP сообщении может быть объявлено до 25 маршрутов. Ограничение в 25 определяется полным размером RIP сообщения, 20x25+4=504, меньше чем 512 байт. Из-за ограничения в 25 маршрутов, на один запрос, как правило, требуется послать несколько откликов, чтобы передать всю таблицу маршрутизации.

5.2. Функционирование процесса-демона routed.

Давайте посмотрим, как обычно работает routed (демон маршрутизации в Linux) с использованием RIP.

- **Инициализация**. Когда демон стартует, он определяет все активизированные интерфейсы и посылает пакет с запросом в каждый интерфейс. Запрос рассылается широковещательными сообщениями, если сеть их поддерживает. Порт назначения UDP:520 (демон маршрутизации на другом маршрутизаторе). Характеристики подобного запроса следующие: поле команды = 1, поле семейство адресов =0 и показатель = 16. Этот формат соответствует **специальному запросу**, в ответ на который требуется послать полную ТМ.
- **Запрос принят**. В случае специального запроса, который мы только что описали, запрашивающему отправляется полная таблица маршрутизации. Возвращается ответ.
- **Ответ принят**. Если ответ признан корректным, таблица маршрутизации может быть обновлена. Могут быть добавлены новые записи, существующие записи могут быть модифицированы или удалены.
- **Регулярное обновление** маршрутизации. Каждые 30 секунд вся или часть таблицы маршрутизации отправляется каждому соседнему маршрутизатору. Таблица маршрутизации распространяется широковещательными сообщениями (в случае Ethernet) или отправляется на другой конец канала точка-точка.
- **Незапланированное обновление**. Происходит в том случае, если изменяется показатель маршрута. В этом случае нет необходимости посылать таблицу маршрутизации целиком, передается только та запись, которая была изменена.

5.3. RIP Version 2.

RFC 1388 [Malkin 1993] определяет расширения функциональности RIP, которые в целом обычно называются RIPv2.

Эти расширения не изменяют протокол, однако добавляют дополнительную информацию в поля, помеченные как "должны быть равны нулю" (must be zero) на рисунке выше.

RIP и RIPv2 могут взаимодействовать в том случае, если RIP игнорирует поля, которые должны быть установлены в ноль.

Формат сообщения RIPv2.

Octet	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
00	**Команда (1-6)**								**Версия (2)**								**Домен маршрутизации**															
04	**Семейство адресов (0 или 2 или 0xFFFF)**																**Признак маршрута**															
08	**32-бит IP адрес сети (узла)**																															
12	**32-бит маска подсети**																															
16	**32-бит IP адрес следующей пересылки**																															
20	**Показатель (1-16)**																															
24-n	**До 24 маршрутизаторов с тем же форматом, что и предыдущие 20 байт (с 04 по 24)**																															

Поле версии для RIPv2 устанавливается в 2.

Домен маршрутизации - это идентификатор маршрутизирующего демона, которому принадлежит этот пакет. В реализациях Unix это должен быть идентификатор процесса демона. Это поле позволяет администратору запустить RIP на одном и том же маршрутизаторе несколько раз, причем каждый будет функционировать с одним доменом маршрутизации.

RIPv2 поддерживать протоколы внешних маршрутизаторов. **Поле признак маршрута** предназначено для того, чтобы хранить номер автономной системы для EGP и BGP.

RIPv2 поддерживает **Маску подсети** для каждого пункта соответствует своему IP адресу.

RIPv2 поддерживает **IP адрес следующей пересылки** - это IP адрес пункта назначения, куда должны посылаться пакеты. Значение 0 в этом поле означает, что пакеты должны отправляться в систему, которая послала RIP сообщение.

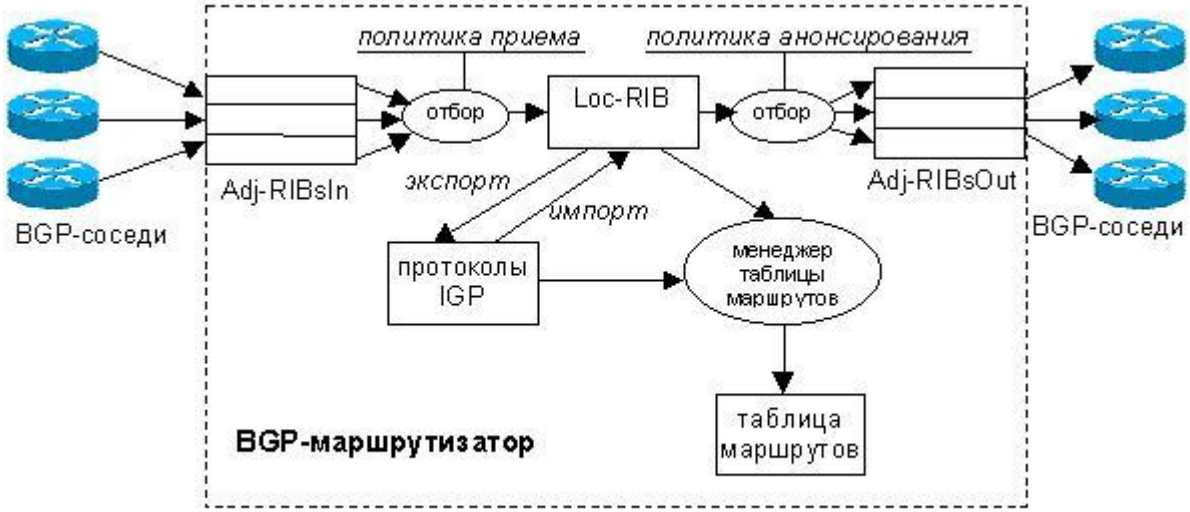
RIPv2 поддерживает **аутентификацию,** чем защищает сообщения против неполномочного объявления. Для этого в RIPv2 используются первые 20 байт запись в RIP сообщении: Семейство адресов =0xffff, Признак маршрута =2 определяет метод, используемый для аутентификации. Оставшиеся 16 байт содержат реальные данные аутентификации (пароль в открытом виде).

RIPv2 поддерживает **групповые запросы** в дополнение к широковещательным. При этом уменьшается загрузка хостов, которые не принимают RIP-2 сообщения.

6. Протокол BGP.

6.1. Общая схема работы.

Маршрутизаторы соседних АС, решившие обмениваться маршрутной инфой, устанавливают между собой соединения по протоколу BGP и становятся соседями (BGP-peers).



BGP использует алгоритм path vector, являющийся развитием DVA. BGP-соседи рассылают (анонсируют, advertise) друг другу векторы путей (path vectors). Вектор путей, в отличие от

вектора расстояний, содержит не просто адрес сети и расстояние до нее, а адрес сети и список атрибутов (path attributes), описывающих различные характеристики маршрута от маршрутизатора-отправителя в указанную сеть.

Данных, содержащихся в атрибутах пути, должно быть достаточно, чтобы маршрутизатор-получатель, проанализировав их с точки зрения **политики** своей АС, мог принять решение о приемлемости или неприемлемости полученного маршрута.

6.2. Реализация BGP.

Пара BGP-соседей устанавливает между собой соединение по протоколу TCP, порт 179.

Поток информации, которым обмениваются BGP-соседи по протоколу TCP, состоит из последовательности BGP-сообщений. Максимальная длина сообщения 4096 октетов, минимальная - 19.

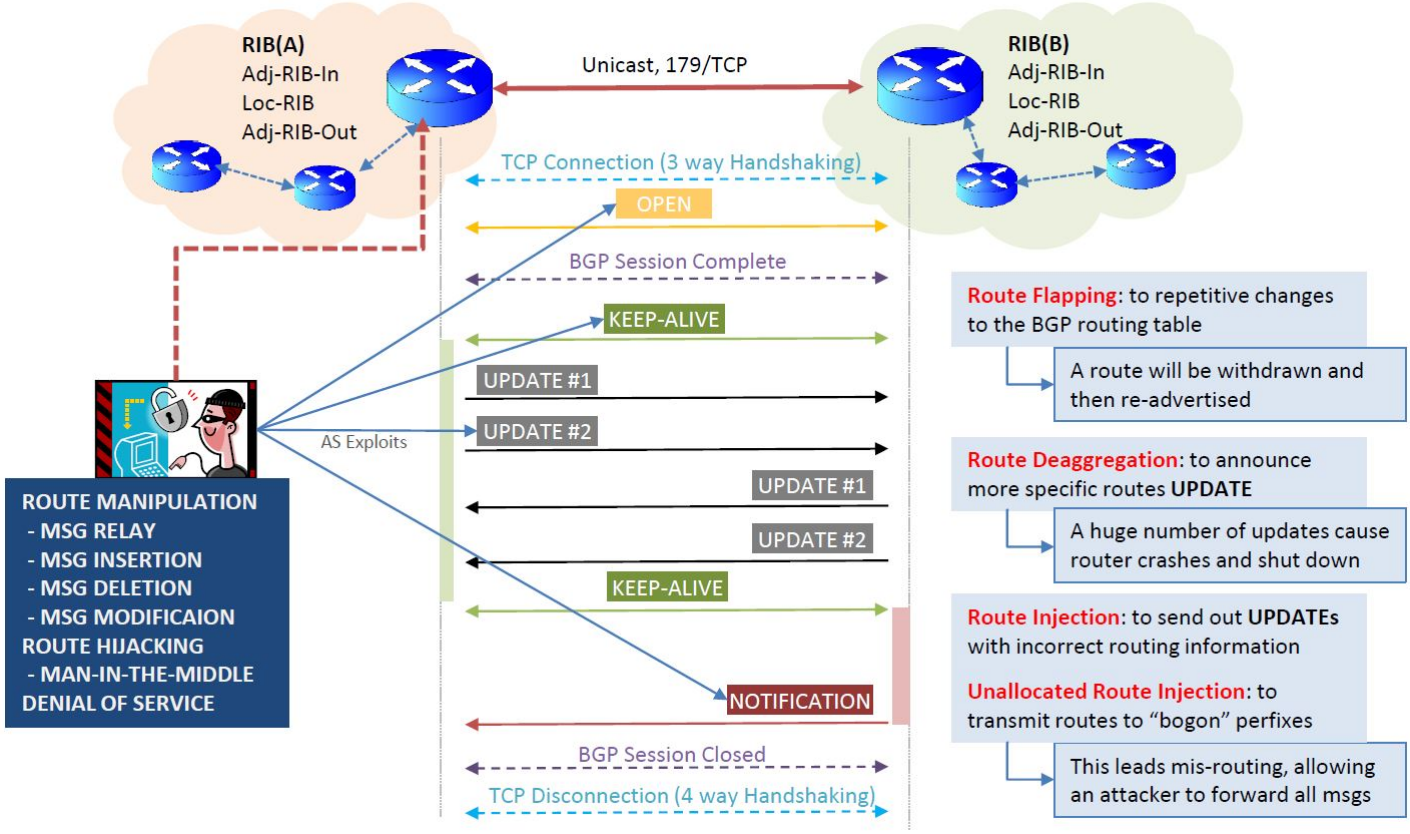


Схема работы BGP.

6.3. Типы BGP-сообщений.

Имеется 4 типа сообщений.

OPEN - посылается после установления TCP-соединения. Ответом на OPEN является сообщение KEEPALIVE, если вторая сторона согласна стать BGP-соседом; иначе посылается сообщение NOTIFICATION с кодом, поясняющим причину отказа, и соединение разрывается.

KEEPALIVE - сообщение предназначено для подтверждения согласия установить соседские отношения, а также для мониторинга активности открытого соединения: для этого BGP-соседи обмениваются KEEPALIVE-сообщениями через определенные интервалы времени.

UPDATE - сообщение предназначено для анонсирования и отзыва маршрутов. После установления соединения с помощью сообщений UPDATE пересылаются все маршруты, которые маршрутизатор хочет объявить соседу (full update), после чего пересылаются только данные о добавленных или удаленных маршрутах по мере их появления (partial update).

NOTIFICATION - сообщение этого типа используется для информирования соседа о причине закрытия соединения. После отправления этого сообщения BGP-соединение закрывается.

6.4. Формат BGP-сообщения.

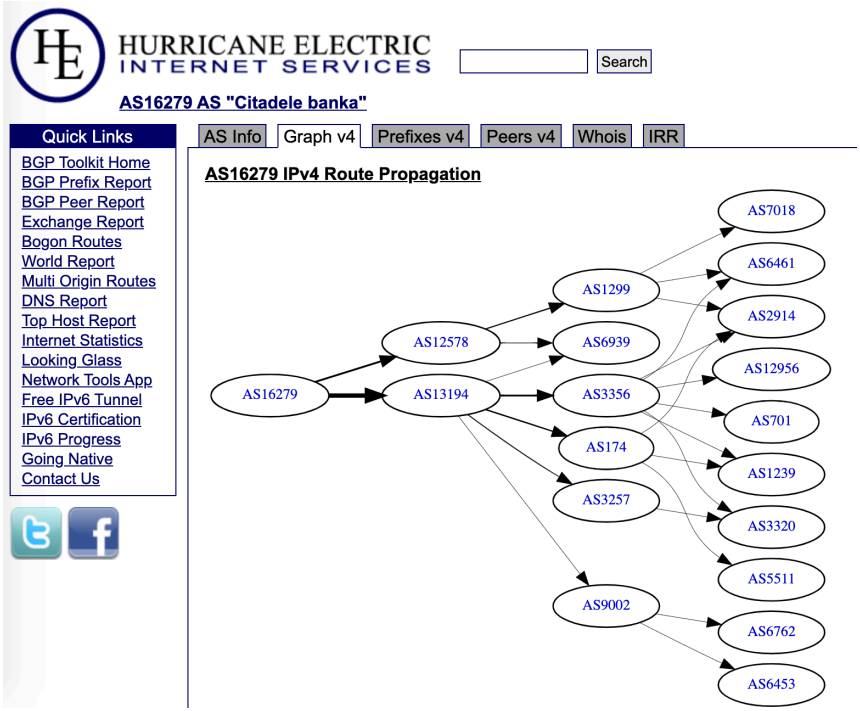
Сообщение протокола BGP состоит из заголовка и тела. Заголовок имеет длину 19 октетов и состоит из следующих полей:

Формат BGP-сообщения

- маркер: в сообщении OPEN всегда, и при работе без аутентификации - в других собщениях, заполнен единицами. Иначе содержит аутентификационную информацию. Сопутствующая функция маркера - повышение надежности выделения границы сообщения в потоке данных.
- длина сообщения в октетах, включая заголовок.
- тип сообщения:
    - 1 - OPEN
    - 2 - KEEPALIVE
    - 3 - UPDATE
    - 4 - NOTIFICATION

6.5. AS BGP propagation graph example

1. Find Latvian ASNs Report https://bgp.he.net/report/world
2. Find AS Citadele Banka AS16279 https://bgp.he.net/AS16279
3. Look BGP Peers on Graph v4 (“Path to Internet”):
   - AS16279->AS12578->AS6939 (Hurricane Electric)
   - AS16279->AS13194->AS174 (Cogent Communication)
4. Read AS Info about all Ass
   - Company Name & Origin Country
   - Company Website & Network Map
   - Internet Exchanges Nrs
   - Prefixes Originated Nrs
   - Prefixes Announced Nrs
   - AS Paths Observed Nrs
5. Find CAIDA AS Rank on site https://asrank.caida.org/



7. Упражнения.

1. Каков размер RIP-сообщения, которое извещает только одну сеть? Какой размер RIP-сообщения извещает N сетей? Выведите формулу, которая показывает зависимость между числом извещенных сетей и размером RIP-сообщения.
2. Маршрутизатор имеет следующую таблицу RIP-маршрутизации:

Сеть1	4	B
Сеть2	2	C
Сеть3	1	F
Сеть4	5	G

Каким будет содержание таблицы, если маршрутизатор получит следующее RIP-сообщение от маршрутизатора C:

Сеть1	2
Сеть2	1
Сеть3	3
Сеть4	7

3. Используя рис.1, покажите извещение связи маршрутизатора для маршрутизатора R3.
4. Используя рис.1, покажите извещение связи маршрутизатора для маршрутизатора R4.