

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«СИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ»

КАФЕДРА ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ

ЛАБОРАТОРНАЯ РАБОТА № 6
«Динамическая маршрутизация
трафика в компьютерных сетях»

Автор: С.Н. Мамоиленко

Новосибирск - 2016

Оглавление

Цель работы.....	3
Теоретическое введение	3
1 Понятия «кратчайший маршрут», «метрика», «конвергенция алгоритма»	3
2 Классификация протоколов динамической маршрутизации.	3
3 Протокол RIP	4
3.1 Версии протокола и форматы пакетов.....	5
3.2 Построение топологии сети	6
3.3 Обработка изменений в топологии сети	6
3.4 Защита от петель в сетях. Технология «расщепления горизонта». Триггерные обновления. Замораживание изменений.....	7
4 Протокол OSPF.....	8
4.1 Состояние канала. Связи маршрутизаторов. Зоны.	9
4.3 Метрики каналов связей в OSPF	10
4.4 Формирование связей между маршрутизаторами. Состояние соседей.....	10
4.5 Объявления о состоянии каналов связей.	10
4.1 Команды протокола OSPF. Форматы пакетов	11
5 Понятие автономной системы. Взаимодействие протоколов маршрутизации.....	12
6 Конфигурирование протоколов динамической маршрутизации на оборудование CISCO	13
6.1 Конфигурирование протокола RIP.....	14
6.2 Конфигурирование протокола OSPF.....	15
Задание на лабораторную работу	16
Контрольные вопросы	16

Цель работы

Получить навыки по конфигурированию протоколов динамической маршрутизации в локальных компьютерных сетях (RIP, OSPF).

Теоретическое введение

В основу функционирования маршрутизаторов локальных компьютерных сетей положена технология выбора маршрута следования пакетов на основе таблиц маршрутизации. В таких таблицах указывается направление передачи пакета для конкретной сети, группы сетей (CIDR) или для всех неизвестных сетей (маршрут «по умолчанию»). В качестве направления передачи может использоваться другой маршрутизатор локальной сети (одной из сетей, к которой подключен маршрутизатор) или непосредственная передача данных с применением средств канального уровня. Принимая решение о передаче каждого пакета сетевое устройство просматривает свою локальную таблицу маршрутизации и выбирает подходящее направление.

Для полноценного функционирования компьютерной сети необходимо обеспечить корректное конфигурирование таблиц маршрутизации всех сетевых устройств. Если в конфигурации сети происходят какие-либо изменения, то они должны быть внесены во все таблицы, которые эти изменения затрагивают. Очевидно, что в сетях, в которых изменения конфигурации происходят относительно часто, необходимо обеспечить автоматическую реконфигурацию таблиц маршрутизации.

Для самостоятельной настройки своих таблиц маршрутизаторы должны регулярно обмениваться ими. Для этого разработаны специальные протоколы. Не смотря на то, что маршрутизация включает в себя два этапа: формирование таблиц и выбор маршрутов, протоколы обмена таблицами часто называют протоколами динамической маршрутизации (здесь далее будет тоже применяться такой термин).

1 Понятия «кратчайший маршрут», «метрика», «конвергенция алгоритма»

Обмениваясь таблицами маршрутизации и формируя свою собственную маршрутизатор выбирает до каждой из известных ему сетей наилучший маршрут. Очевидно, что наилучшим маршрутом между двумя точками является *кратчайший маршрут* – маршрут, имеющий наименьшее расстояние. Расстояние между сетями в разных протоколах измеряется по-разному. В любом случае расстояние между сетями складывается из характеристик всех каналов передачи информации, которые необходимо преодолеть, чтобы достичь необходимую сеть. Характеристику канала, используемую для определения расстояния, называют *метрикой*.

В качестве метрик может использоваться единичное значение или показатель пропускной способности и/или надежность канала. В некоторых протоколах вводится дополнительная метрика, характеризующая недостижимость сети. Также может использоваться нулевая метрика, характеризующая непосредственное подключение маршрутизатора к сети. Обычно, чем меньше метрика, тем меньше расстояние.

Главная задача протоколов маршрутизации- формирование согласованных таблиц маршрутизации. Согласованная таблица – это такая таблица, которая обеспечивает передачу данных между сетями за конечное число шагов. При изменениях в сети таблицы становятся несогласованными, т.е. передача данных между некоторыми сетями оказывается невозможной. Время, в течение которого таблицы приводятся в согласованное состояние называется *временем конвергенции* (или сходимости алгоритма).

2 Классификация протоколов динамической маршрутизации.

Маршрутизаторы, используя протоколы динамической маршрутизации, собирают информацию от своих соседей (маршрутизаторов, имеющих непосредственное подключение) о топологии сети связей, обрабатывают её и формируют свое «видение» конфигурации сети.

В сформированной таким образом таблице маршрутизации каждому маршруту выставляется период времени, в течение которого он будет существовать на данном маршрутизаторе. Это делается, в первую очередь для того, чтобы гарантировать, что если маршрутизатор, который сообщил о существовании этой сети по каким-либо причинам больше не будет подтверждать этот факт, то маршрут будет признан несуществующим (и удален из таблицы).

Протоколы динамической маршрутизации можно разделить на два больших класса: *централизованные и распределённые*. В первом случае в сети выбирается один из маршрутизаторов, который формирует у себя таблицу маршрутов и распространяет её между другими маршрутизаторами сети. Другие маршрутизаторы, при этом, не выполняют никаких построений таблиц маршрутизаторов, а лишь используют полученную таблицу. В распределённых алгоритмах все маршрутизаторы находятся в равных условиях и каждый из них самостоятельно строит таблицу маршрутизации. Очевидно, что надежность распределённых алгоритмов маршрутизации выше, чем у централизованных (в них при выходе из строя центрального маршрутизатора вся сеть оказывается неработоспособной).

Далее в лабораторной работе будет рассматриваться распределённые протоколы динамической маршрутизации. Такие протоколы можно разделить на два класса: дистанционно-векторные алгоритмы (от англ. Distance Vector Algorithm, DVA) и алгоритмы состояний связей (от англ. Link State Algorithm, LSA).

В *дистанционно-векторных алгоритмах* каждый маршрутизатор регулярно рассылает вектор, в котором указывает расстояние до всех (или некоторых) известных ему сетей всем своим соседям. Формирование таблиц маршрутизации основано на алгоритме Беллмана-Форда-Мура¹. Получив вектор каждый маршрутизатор увеличивает значения расстояний с учетом расстояния «до себя» и формирует свою таблицу маршрутизации, выбирая наилучший маршрут до каждой сети. В конце концов, каждый маршрутизатор узнает через соседние маршрутизаторы информацию обо всех имеющихся сетях и о расстояниях до них.

Дистанционно-векторные алгоритмы применимы для небольших сетей. Ограничение связано с тем, что с увеличением количества сетей, о которых необходимо передавать информацию объем трафика и время конвергенции алгоритма резко увеличиваются.

К дистанционно-векторным относятся протоколы: RIP, IGRP, BGP, AODV и др.

В *алгоритмах, основанных на состоянии связей*, каждый маршрутизатор рассылает информацию только о сетях, к которым он имеет непосредственную связь. В результате каждый маршрутизатор самостоятельно строит топологию сети и выбирает наименьшие расстояния до каждой сети. Для расчета расстояний используется алгоритм Дейкстры.

К протоколам, основанным на состояниях каналов связей, относятся IS-IS, OSPF, NLSP, OLSR и др.

Некоторые протоколы маршрутизации реализуют как элементы дистанционно-векторных алгоритмов, так и алгоритмов на основе состояний каналов. Примером таких алгоритмов можно назвать – EIGRP.

3 Протокол RIP

Протокол RIP (от англ. Routing Information Protocol) относится к дистанционно-векторным протоколам динамической маршрутизации. Считается, что он самый распространённый протокол в небольших компьютерных сетях. Впервые протокол был предложен в 1969 году как основной для сети ARPANET.

В качестве метрики протокол использует целое число из диапазона от 0 до 15. Число 16 задает бесконечную длину маршрута. Обычно для каналов используются единичные метрики, в результате считается, что максимальная длина маршрута, т.е. количество переходов (маршрутизаторов) между двумя любыми сетями, не может быть больше 15.

¹ <http://kvodo.ru/bellman-ford-algorithm.html>

По умолчанию каждый маршрутизатор широковещательно рассылает свой вектор в сеть каждый 30 секунд. Протокол работает на прикладном уровне модели OSI, использует в качестве транспорта протокол UDP и за службой, реализующей протокол RIP, закреплен порт номер 520.

3.1 Версии протокола и форматы пакетов

Существует три версии этого протокола:

- RIP версии 1. Обеспечивает передачу информации о сетях, описываемых классовым способом. Формат пакета представлен на рисунке 1. Протокол описан в RFC 1058²;
- RIP версии 2. Поддерживает маски сетей переменной длины и авторизацию маршрутизаторов. Формат пакета представлен на рисунке 2. Протокол описан в RFC 2453³;
- RIPvng. Поддерживает IP версии 6. Эта версия протокола далее в лабораторной работе не рассматривается.

Команда (8 бит)	Версия (8 бит)	Должно быть ноль (16 бит)
Идентификатор адресной схемы (16 бит)		Должно быть ноль (16 бит)
IP-адрес (32 бита)		
Должно быть ноль (32 бита)		
Должно быть ноль (32 бита)		
Количество переходов (32 бита)		
Идентификатор адресной схемы (16 бит)		Должно быть ноль (16 бит)
IP-адрес (32 бита)		
Должно быть ноль (32 бита)		
Должно быть ноль (32 бита)		
Количество переходов (32 бита)		
...		
Идентификатор адресной схемы (16 бит)		Должно быть ноль (16 бит)
IP-адрес (32 бита)		
Должно быть ноль (32 бита)		
Должно быть ноль (32 бита)		
Количество переходов (32 бита)		

Рисунок 1 – Формат пакета RIP версии 1

Команда(8 бит)	Версия(8 бит)	Домен маршрутизации(16 бит)
Идентификатор адресной схемы(16 бит)		Метка маршрута(16 бит)
IP-адрес(32 бита)		
Маска подсети(32 бита)		
Следующий переход(32 бита)		
Метрика(32 бита)		

Рисунок 2 – Формат пакета RIP версии 2

Протоколом предусматривается две команды (поле «команда» пакета RIP): запрос вектора и ответ вектора. Следующими полями указываются: используемая версия протокола, идентификатор системы адресации узлов (для TCP/IP задан код 2) и значение вектора. Одним пакетом может передаваться вся таблица или её часть (если она содержит информацию более чем о 25 сетях).

Команда запроса используется маршрутизатором для получения таблиц маршрутизации от своих соседей по собственной инициативе. Потребность использования этой команды может возникнуть в момент включения маршрутизатора (или начала работы на нем демона RIP) или в случае повреждения текущей таблицы.

² <http://tools.ietf.org/html/rfc1058>

³ <http://tools.ietf.org/html/rfc2453>

Команда ответа используется для формирования ответа на запрос или для регулярного распространения своего вектора.

Формат элемента вектора зависит от версии протокола. Все версии первым полем указывают тип используемой адресации узлов в сети. Для стандарта TCP/IP задан тип с номером 2. В версии 1 каждый элемент содержит идентификатор сети (соответствует одному из классов сети) и метрика (расстояние до сети). В версии 2 указываются поля «маска подсети», «адрес маршрутизатора» (next hop), а также указывается тип маршрута (домен маршрутизации): «внешний» или «внутренний». Внешний маршрут заимствован граничным маршрутизатором из информации другого протокола маршрутизации (об этом будет подробнее сказано ниже).

Маршрутизатор, работающий по протоколу версии 2, способен обрабатывать информацию, отправленную в формате протокола версии 1.

3.2 Построение топологии сети

Работа маршрутизатор, поддерживающего протокол RIP, выполняется в несколько этапов.

Этап 1. Создание минимальной таблицы. На этом этапе маршрутизатор формирует начальный вектор, в который включает информацию о всех сетях, к которым он имеет непосредственное подключение. Каждый коммутатор такую таблицу формирует самостоятельно.

Этап 2. Рассылка собственной таблицы своим соседям. После того, как сформирован локальный вектор он регулярно рассылается через все интерфейсы маршрутизатора (которые участвуют в формировании топологии сети).

Этап 3. Получение и обработка векторов от своих соседей. Получив вектор от своего соседа, маршрутизатор увеличивает значение метрик с учетом метрики канала, через который поступило RIP-сообщений.

В результате обработки вектора маршрутизатор может обнаружить несколько путей до какой-либо сети. В итоговую таблицу маршрутизатор включает только один наилучший маршрут до каждой сети. Наилучшим считается маршрут, имеющий наименьшее значение метрики и идущий через маршрутизатор, с наибольшим значением сетевого адреса (идентификатора маршрутизатора).

Далее этапы 2 и 3 выполняются циклически. В результате периодической рассылки, получению и обработке векторов за конечное время маршрутизатор получает рабочую таблицу маршрутизации.

3.3 Обработка изменений в топологии сети

Важной способностью протоколов динамической маршрутизации является возможность автоматического реагирования на изменения, произошедшие в топологии сети.

Если какой-либо маршрутизатор обнаруживает, что какие-то из его интерфейсов переходят в неработоспособное состояние, то он изменяет собственную таблицу маршрутизации и рассылает изменённый вектор по всем своим рабочим интерфейсам.

В случае, если произошли какие-либо изменения с существующими маршрутами, то они указываются в новом векторе и доводятся до сведения всех маршрутизаторов.

Ситуация исчезновения каких-либо маршрутов сложнее. Формат пакета позволяет передать информацию только о существующих маршрутах и никак не позволяет сообщить об их исчезновении.

Для исключения информации о каком-либо маршруте используется два механизма:

- таймер жизни (TTL) маршрута в динамической таблице маршрутизации;
- передача маршрута с метрикой, соответствующей бесконечному расстоянию до сети.

Механизм TTL маршрута предполагает наличие в таблице маршрутизации дополнительного поля, указывающего сколько времени указанный маршрут будет считаться действующим. Если в течение этого времени не получено ни от одного из соседей информации о существовании этого маршрута, то маршрут помечается как недействительный. Если получено сообщение с таким маршрутом, то таймер TTL начинает отсчитываться заново.

Время жизни маршрута выбирается кратным времени рассылки RIP сообщений по сети. По умолчанию TTL равен 180 секундам (6-ти кратный период рассылки сообщений).

Использование TTL для маршрутов работает хорошо, но требует большого интервала времени для реагирования на изменения в сети. Предположим, что один из маршрутизаторов сети по какой-либо причине перестал рассылать информацию о маршрутах, которые проходили через него. Его соседние маршрутизаторы переведут все эти маршруты в недействительное состояние через 180 секунд. Их соседи переведут маршруты в недействительное состояние уже через 360 секунд и так далее.

Чтобы ускорить процесс схождения маршрутизаторы, которые продолжают рассылать свои векторы и обнаруживают, что какой-либо маршрут становится недействительным продолжают рассылать информацию о нем, но ставят ему метрику 16 (т.е. указывают, что маршрут недостижим). В результате время реакции маршрутизаторов сокращается.

Получив сообщение о недостижимости некоторой сети маршрутизатор изменяет свой вектор только в том случае, если изначально он узнал об этом маршруте от того же маршрутизатора. Если информацию о недостижимости маршрута пришла от другого соседа, то она игнорируется (т.е. в собственной таблице есть маршрут с лучшим значением вектора).

3.4 Защита от петель в сетях. Технология «расщепления горизонта». Триггерные обновления. Замораживание изменений

Рассмотрим пример работы протокола RIP в сети, конфигурация которой представлена на рисунке 3. Имеется три сети и два соединяющих их коммутатора. Используя протокол RIP коммутатор R1 сообщает коммутатору R2 о том, что он имеет прямое подключение к сетям 192.168.1.0/24 или 10.0.0.0/24 (указывая метрику 0). Получив сообщение от R1 маршрутизатор увеличивает значение метрики и понимает, что через R1 ему доступны маршруты до указанных сетей с расстоянием 1 (было 0, прибавили метрику 1 канала между R1 и R2). Поскольку R2 уже в своей таблице имеет запись с маршрутом до сети 10.0.0.0/24 и его метрика меньше (она равна 0), то полученная запись об этой сети игнорируется, а запись о сети 192.168.1.0 заносится в таблицу. Аналогичная ситуация происходит с таблицей маршрутизатора R1 и он узнает о маршруте до сети 172.16.0.0/24 с метрикой 1.

Предположим, что по какой-то причине маршрутизатор R1 теряет связь с сетью 192.168.1.0/24. Обнаружив это, R1 указывает в своей таблице в соответствующей строке метрику 16. Поскольку таймеры маршрутизаторов не синхронизированы, то может возникнуть ситуация, что после того, как R1 изменил свою таблицу, но до того, как он её будет рассылать, маршрутизатор R2 пришлет свою таблицу, в которой по-прежнему укажет, что у него есть маршрут до сети 192.168.1.0 с метрикой 1. Маршрутизатор R1 исправит свою таблицу (поскольку в его таблице метрика 16 явно больше метрики 1), указав в ней, что пакеты, предназначенные сети 192.168.1.0 необходимо передавать маршрутизатору R2 и расстояние этого маршрута будет равным 2. В результате в сети появится петля. Если какой-либо узел из сети 172.16.0.0/24 попытается передать пакет в сеть 192.168.1.0/24, то этот пакет будет циркулировать между R1 и R2 до тех пор, пока не превысит свое время жизни TTL.

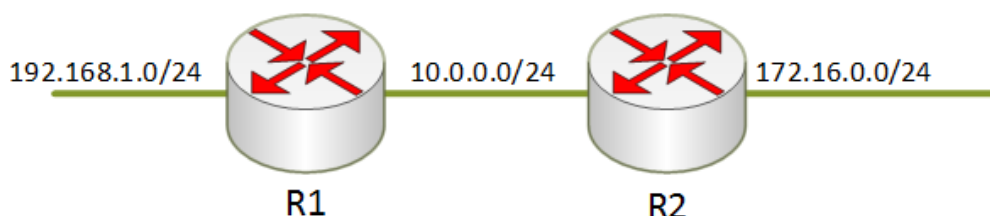


Рисунок 3 – Пример сети с возможностью образования петель в таблице маршрутизации

Защиту от образования таких петель обеспечивает технология, называемая – *расщеплением горизонта* (split-horizon). Суть этой технологии заключается в том, что информация о маршруте не передается в интерфейс, через который маршрутизатор «узнал» о существовании этого маршрута.

Технология расщепления горизонта работает только в случае образования петель между двумя соседними коммутаторами. В случае, если петля образована тремя и более коммутаторами, то эта технология оказывается неработоспособной.

Рассмотрим пример сети, представленной на рисунке 4. Пусть сеть уже находится в рабочем состоянии и маршрутизатор R1 принимает решение о недоступности сети 192.168.1.0/24. Предположим, что R1 отправил свою таблицу R2 и R3. Пусть на 1 секунду позже R2, не успев ещё получить сообщение от R1, отправляет R3 свою таблицу, в которой по-прежнему указывает, что знает маршрут до сети 192.168.1.0/24 с расстоянием 1. Маршрутизатор R3, получив сообщение от R1 изменяет свою таблицу, указывая до сети 192.168.1.0/24 расстояние 16, но получив сообщение от R2 изменяет это расстояние до 2. Поскольку лучший маршрут до сети 192.168.1.0/24 маршрутизатор R3 получает от R2, то он отправляет R1 сообщение с метрикой 2. R1, в свою очередь отправляет этот маршрут R2. В результате формируется петля.

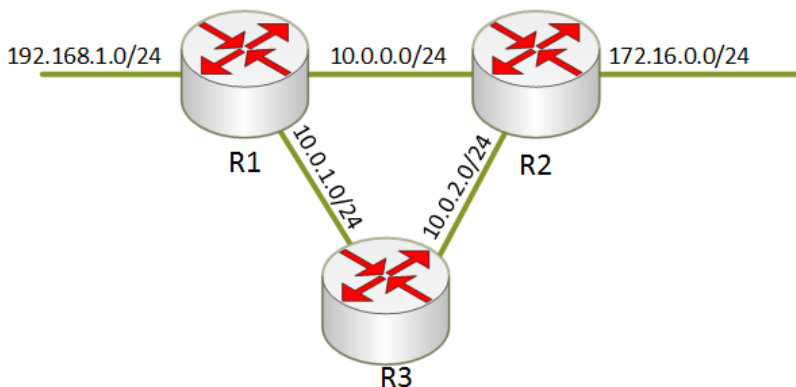


Рисунок 4 - Пример сети из трех маршрутизаторов с возможностью образования петель в таблице маршрутизации

В двух рассмотренных случаях петля возникает в первую очередь из-за того, что присутствует разрыв во времени между установлением факта недоступности сети и отправкой этой информации соседним маршрутизаторам. Для исключения этого недостатка стали применять технологию *триггерных обновлений*, согласно которой маршрутизатор получив информацию об изменении метрики какой-либо сети не ждет следующего интервала для рассылки своей таблицы, а делает это немедленно (рассылая только изменения). Такой подход увеличивает объем трафика в сети, но позволяет сократить время распространения изменений.

Даже в условии применения триггерных изменений может случиться так, что обновления не успеют вовремя поступить на соседний маршрутизатор. Чтобы усилить защиту от таких ситуаций применяют её одну технологию – *замораживание изменений*. Суть этой технологии заключается в том, что для сети, которая стала недоступной вводится некоторый период времени, в течение которого другие изменения метрики не принимаются. Размер этого периода выбирается таким, чтобы гарантировать, что самая дальняя сеть успеет получить информацию о недоступности сети.

4 Протокол OSPF

Популярным протоколом динамической маршрутизации в локальных сетях ЭВМ является протокол Open Shortest Path First (OSPF). Протокол был разработан IETF в 1988 году. Последняя версия протокола представлена в RFC 2328⁴.

Протокол OSPF имеет меньшее время сходимости, чем протокол RIP. Кроме того, OSPF изначально учитывает описание сетей с помощью масок переменной длины (VLSM).

Протокол OSPF относится к протоколам состояния каналов. Основная идея протоколов этого класса состоит в том, что маршрутизаторы рассылают информацию о состоянии своих каналов и ретранслируют сообщения о состоянии каналов других маршрутизаторов. В результате каждый

⁴ <http://tools.ietf.org/html/rfc2328>

маршрутизатор отвечает только за собственные каналы, но имеет информацию о состоянии каналов всех своих соседей.

Собрав информацию от своих соседей маршрутизатор самостоятельно строит свое видение топологии сети и выбирает кратчайшие маршруты до всех известных ему сетей. Поиск маршрутов в OSPF производится с помощью алгоритма Дейкстра.

Следует отметить, что протокол OSPF поддерживает три типа сетей: широковещательные (Ethernet, Token Ring), точка-точка (T1, E1) и сети с множественным доступом (Frame Relay). Далее в этой лабораторной работе рассматривается работа протокола OSPF только в широковещательных сетях.

4.1 Состояние канала. Связи маршрутизаторов. Зоны.

Для функционирования протокола OSPF каждый маршрутизатор собирает информацию о состоянии своих каналов связей, соседних маршрутизаторов и каналов связей, имеющих у соседних маршрутизаторов. *Состояние канала* — это описание сетевого интерфейса и его отношений с соседними маршрутизаторами. Описание интерфейса включает, например, его IP-адрес, маску, тип сети, к которой он подключен, маршрутизаторы, подключенные к этой сети и т.п. В результате каждый маршрутизатор собирает у себя информацию обо всех сетях.

Коллекция всех состояний каналов представляет собой *базу данных состояний каналов*. Цель работы OSPF – обеспечить полную синхронизацию баз данных состояний каналов на всех маршрутизаторах сети. В результате каждый маршрутизатор рассчитывает свою таблицу маршрутизации.

Каждый маршрутизатор несет ответственность только за собственные каналы. Если он обнаруживает какие-либо изменения в них, то он сообщает об этом всем своим соседям. Сообщения, с помощью которых распространяется информация о состоянии каналов, называются объявлениями о состоянии связей (англ. Link State Advertisement, LSA). LSA распространяются всем соседям с помощью специального группового адреса – 224.0.0.5.

Для сокращения объемов передаваемой служебной информации и времени сходимости алгоритма поиска кратчайших путей протокол OSPF предусматривает разделение сети ЭВМ на непересекающиеся области – *зоны* (англ. area). Маршрутизаторы, интерфейсы которых принадлежат к разным областям OSPF называются *пограничными* (англ. area border router, ABR). Маршрутизатор, все интерфейсы которого находятся в одной зоне называется *внутренним* (англ. Internal router, IR).

Чтобы сократить объемы передаваемой по сети служебной информации и времени её распространения до всех маршрутизаторов зоны внутри каждой зоны строится топология связей маршрутизаторов. Все маршрутизаторы устанавливают связь друг с другом. Один из маршрутизаторов сети выбирается главным (назначенным, англ. *Designated Router, DR*). Основной задачей этого маршрутизатора является ведение эталонной базы данных состояний каналов. Все маршрутизаторы регулярно сообщают друг другу о своем существовании. Обо всех изменениях в своих каналах связей и о том, что какой-либо коммутатор прекратил присылать информацию о своем существовании маршрутизаторы зоны сообщают своему DR, а он уже сообщает об этом остальным маршрутизаторам зоны.

Главный маршрутизатор зоны определяется путем выборов в начальной стадии функционирования протокола OSPF. Критерием выбора служит приоритет маршрутизатора и его идентификатор. Идентификатором маршрутизатора, по умолчанию, является его наибольший (в числовом выражении) IP адрес. Главным выбирается маршрутизатор, имеющий наибольшее значение приоритета и идентификатора. Выборы главного маршрутизатора не вытесняющие, т.е. при появлении в сети маршрутизатора с большим значением приоритета перевыборы не производятся (они инициируются либо в случае отказа DR, либо по его инициативе).

Очевидно, что централизация управления сети негативно сказывается на её надежности. Поэтому в сети дополнительно выбирают резервный главный маршрутизатор (Backup Designated Router, BDR), которые хранят копию эталонной базы связей каналов и начинают работать в случае выхода из строя DR. Маршрутизаторы DR и BDR обмениваются эталонной базой используя специальный групповой адрес – 224.0.0.6. Запасной DR выбирается аналогично DR.

4.3 Метрики каналов связей в OSPF

В алгоритме OFPS метрика канала связи обратно пропорциональна его пропускной способности. Формула для расчета метрики: метрика = 100 000 000/пропускная способность в бит/с. Например, стоимость передачи данных через 10-ти мегабитный канал Ethernet — $10^8/10^7 = 10$, стоимость передачи данных через канал T1 — $10^8/1544000 = 64$.

Метрика канала может задаваться администратором вручную.

4.4 Формирование связей между маршрутизаторами. Состояние соседей.

Основная работа маршрутизатора при реализации алгоритма OSPF заключается в мониторинге состояний каналов связей и информировании соседних маршрутизаторов о изменениях в них.

Для контроля состояний каналов связей все маршрутизаторы регулярно обмениваются небольшими служебными сообщениями. Получив такое сообщение от своего соседа маршрутизатор считает, что его сосед является работоспособным и никаких изменений с его каналами связей не произошло. Перестав получать такие сообщения или обнаружив изменения в своих каналах связей маршрутизатор «бьет тревогу» и сообщает об этом всем своим соседям (через DR). Эти же служебные сообщения используются для «знакомства» маршрутизаторов.

Получив сообщение от неизвестного соседа, относящегося к той же зоне, маршрутизатор устанавливает с ним двухстороннюю связь (т.е. они запоминают информацию друг о друге, определяют свои роли в отношении друг друга и синхронизируют LSADB). Считается, что сосед относится к той же зоне, если сообщение было получено через допустимый интерфейс и в сообщении указаны правильные значения служебных полей (подробнее ниже).

В процессе знакомства маршрутизаторы могут находиться в следующих состояниях: инициализации (init), двухстороннее знакомство (Two-way), подготовки к синхронизации LSADB (exstart), синхронизации LSADB (exchange), завершении установления связи (loading), готовом (full).

Канал связи с маршрутизатором находится в состоянии «инициализация» (англ. Init) если было получено сообщение от неизвестного соседа. Получив такое сообщение маршрутизатор запоминает соседа, формирует ему ответное служебное сообщение со списком своих соседей, указав уже в нем нового соседа.

Переход в состояние *двухстороннего знакомства* осуществляется тогда, когда от нового соседа будет получено очередное служебное сообщение, в котором текущий маршрутизатор будет указан как соседний. В конце этого этапа маршрутизаторы решают, нужно ли продолжать установление соседства. Решение основывается на списках соседей маршрутизаторов. Если в списках обоих маршрутизаторов нет незнакомых соседей, то этап завершается выбором для зоны маршрутизаторов, выполняющих роли DR и BDR. Если при установлении связи с каким-либо маршрутизатором был установлен факт наличия DR или BDR в сети, то выборы не проводятся.

Обмен базой состояний каналов связей (LSADB) инициирует ведущий маршрутизатор. На этапе подготовки к обмену (англ. Exchange start) маршрутизаторы устанавливают начальный порядковый номер, который будет использоваться в пакетах обмена данными. Порядковый номер обеспечивает получение маршрутизатором последней информации из LSADB и перезапрос у мастера потерянных сообщений.

На следующем этапе производится непосредственный обмен базой состояний каналов (англ. Exchange). При этом может быть произведена лавинная рассылка базы другим соседним маршрутизаторам (расположенным в других сетях, чем DR и BDR).

Заключительным этапом синхронизации LSADB маршрутизатор удаляет весь мусор, возникший в процессе обмена, а также все устаревшие записи из своей LSADB.

После завершения обновления LSADB маршрутизатор переходит в работоспособное состояние (англ. Full).

4.5 Объявления о состоянии каналов связей.

Существует пять типов объявления о состоянии каналов.

Все маршрутизаторы генерируют каналы маршрутизации (RL). Эти каналы описывают состояние интерфейсов маршрутизатора внутри определенной области. Лавинная рассылка этих каналов выполняется только внутри области маршрутизатора.

Сетевые каналы (NL) генерируются выделенным маршрутизатором (DR) сегмента. Они обозначают маршрутизаторы, подключенные к сегменту.

Суммарные каналы (SL) — это межобластные каналы (тип 3), они перечисляют сети, которые находятся в других областях, но при этом принадлежат автономной системе. Суммарные каналы внедряются пограничным маршрутизатором области (ABR) от магистрали к другим областям (и обратно). Эти каналы используются для агрегирования между областями.

Другой тип суммарных каналов — суммарные каналы ASBR. Они представляют собой каналы типа 4, указывающие на ASBR. Эти каналы гарантируют, что все маршрутизаторы будут знать путь выхода из автономной системы.

Последний тип — это тип 5, внешние каналы (EL), которые вводятся в домен пограничным маршрутизатором автономной системы (ASBR).

4.1 Команды протокола OSPF. Форматы пакетов

Протокол работает на сетевом уровне (имеет свой код – 89). Информация передается либо в режиме юникаста (конкретному маршрутизатору) или многоадресной рассылкой в группах: 224.0.0.5 (все OSPF маршрутизаторы сети) и 224.0.0.6 (все маршрутизаторы, имеющие роль DR или BDR). Формат пакета представлен на рисунке 5.

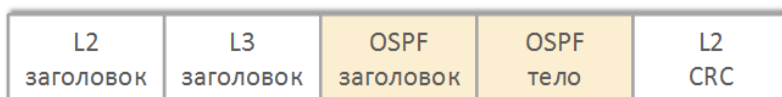


Рисунок 5 – Формат пакета протокола OSPF

Содержательная часть пакетов OSPF начинается с 24-х байтового заголовка (см. рисунок 6). В первом поле указывается версия протокола OSPF. Существует три версии протокола, первые две из которых поддерживают IP версии 4, а третья – IP версии 6.

Версия (8 бит)	Тип (8 бит)	Длина пакета (16 бит)
Идентификатор маршрутизатора отправителя (32 бита)		
Идентификатор области сети (32 бита)		
Контрольная сумма (16 бита)	Тип аутентификации (16 бита)	
Аутентификационная информация (64 бита)		

Рисунок 6 – Формат OSPF заголовка

В поле «тип» указывается команда протокола, которая передается в пакете. Протоколом предусматривается 5 команд: hello, Database Description, Link State Request, Link State Update, Link State Acknowledgment. О формате пакета команды hello будет сказано ниже. Подробнее о форматах пакетов других команд следует прочитать в RFC 2328.

Следующими полями заголовка OSPF указываются идентификатор маршрутизатора, сгенерировавшего пакет и группы маршрутизаторов (зоны), которой предназначен этот пакет.

Далее в заголовке OSPF пакета указывается контрольная сумма и информация для аутентификации. Контрольная сумма рассчитывается для всего OSPF пакета (включая заголовок)

с использованием алгоритма Флетчера⁵. Аутентификационная информация используется для защиты от маршрутизаторов, установка в сеть которых была не санкционирована. Предусмотрено три типа аутентификации: 0 – без проверки, 1 – с использованием пароля в виде открыто передаваемой в поле «аутентификационные данные» текстовой строки; 2 – с применением MD5 кода для передачи пароля.

Команда № 1 называется hello и предназначена для обмена небольшими служебными сообщениями между маршрутизаторами. Форма пакета, содержащего такую команду, представлен на рисунке 7.

Маска сети (32 бита)		
Hello-интервал (16 бит)	Опции (8 бит)	Приоритет (8 бит)
Время жизни маршрутизатора (32 бита)		
Назначенный маршрутизатор сети (32 бита)		
Запасной назначенный маршрутизатор сети (32 бита)		
Список соседей маршрутизатора (от 0 бит, группами по 32 бита)		

Рисунок 7 – формат OSPF пакета для команды hello

Первым полем команды hello указывается маска подсети, в которой передается информация. Если значение этой маски отличается от значений, установленного для интерфейса, получившего сообщение hello, то сообщение игнорируется. Далее в пакете указывается значение служебных интервалов времени:

- hello интервал – время, через которое маршрутизатор должен отправлять hello-пакеты своим соседям.
- Время жизни маршрутизатора – период времени, в течении которого маршрутизатор обязан хотя бы один раз отправить hello-пакет. Если по истечении этого времени от соседа не было получено ни одного hello-пакета, что считается, что обнаружен факт изменения его состояния (скорее всего сосед не работает).

Также в hello-пакета указывается значение приоритета соседнего маршрутизатора, идентификаторы главного и запасного маршрутизаторов зоны и список соседей маршрутизатора. В поле «Опции» указываются возможности маршрутизатора (например, является ли он пограничным).

5 Понятие автономной системы. Взаимодействие протоколов маршрутизации

С развитием телекоммуникационных технологий и протоколов динамической маршрутизации стало очевидно, что применение везде одинаковых правил поведения маршрутизаторов невозможно. Сети формируются из подсистем, которые управляются разными людьми и даже реализованные с использованием различных телекоммуникационных технологий.

В результате появился термин *автономная система* (англ. autonomous system, AS), который описывает сеть или её часть, находящуюся под управлением одних администраторов и реализующую единую политику динамической маршрутизации трафика. Примером автономной сети можно назвать сеть одного предприятия, в которой реализуется, например, протокол RIP. Если

⁵ http://en.wikipedia.org/wiki/Fletcher's_checksum

на предприятии в части сети функционирует RIP, а в другой части OSPF, то это означает, что на предприятии существует две автономные системы.

Взаимодействие автономных систем осуществляется через пограничные маршрутизаторы, на которых одновременно реализуется несколько протоколов динамической маршрутизации.

Пограничные маршрутизаторы могут интегрировать информацию о топологии сети, получаемую по разным протоколам и транслировать её во все автономные системы. В этом случае важным является правильное конфигурирование метрик каналов (т.е. значения метрик в разных протоколах различны).

6 Конфигурирование протоколов динамической маршрутизации на оборудование CISCO

Настройка протоколов динамической маршрутизации осуществляется в режиме конфигурирования маршрутизатора командой `router` протокол [параметры] (см. рисунок 8). Для протокола RIP параметры не указывается. Для OSPF – указывается номер процесса, реализующего протокол. Для пограничных маршрутизаторов зон на одном маршрутизаторе может быть запущено несколько процессов (по одному для каждой зоны). Отключить протокол маршрутизации можно с помощью команды `no router`.

```
Router(config)#router ?
  bgp      Border Gateway Protocol (BGP)
  eigrp    Enhanced Interior Gateway Routing Protocol (EIGRP)
  ospf     Open Shortest Path First (OSPF)
  rip      Routing Information Protocol (RIP)
```

Рисунок 8 – Команда конфигурирования протоколов динамической маршрутизации.

Просмотреть информацию протоколов динамической маршрутизации можно в привилегированном режиме с помощью команды `show ip protocols`.

```
Router#
Router#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 15 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface          Send Recv Triggered RIP Key-chain
  Loopback0          2      2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  1.0.0.0
Passive Interface(s):
Routing Information Sources:
  Gateway           Distance       Last Update
Distance: (default is 120)

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 0. 0 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
  Routing Information Sources:
    Gateway           Distance       Last Update
  Distance: (default is 110)
```

Рисунок 9 – Пример вывода информации о протоколах динамической маршрутизации

Удалить из таблицы маршрутизации информацию, сгенерированную динамически, можно в привилегированном режиме с помощью команды `clear ip route`.

6.1 Конфигурирование протокола RIP

В режиме конфигурирования протокола RIP динамической маршрутизации можно задать:

- Интерфейс(ы), через которые анонсируются сети в процессе реализации протокола (команда `network`);
- интерфейс(ы), через которые запрещены прием и передача информации по протоколу динамической маршрутизации (пассивные интерфейсы, команда `passive-interface`);
- правила интеграции информации из разных протоколов динамической маршрутизации (команда `redistribute`);
- версию используемого протокола (команда `version`);

Процесс настройки протокола включает как минимум одно действие - указание какой(ие) интерфейс(ы) должны распространять информацию по протоколу RIP (см. рисунок 10). Интерфейсы определяются их IP адресом. Допускается указать команду `network` несколько раз. Следует отметить, что протокол группирует интерфейсы используя классовый метод сетевой адресации и использует все интерфейсы для приема и отправки сообщений RIP!

```
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#network 1.1.1.1
Router(config-router)#version 2
Router(config-router)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 7 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface          Send Recv Triggered RIP Key-chain
  Loopback0          2     2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  1.0.0.0
Passive Interface(s):
Routing Information Sources:
  Gateway         Distance      Last Update
Distance: (default is 120)
```

Рисунок 10 – Пример простейшего конфигурирования протокола RIP

Чтобы в сообщения, генерируемые по RIP протоколу на граничном маршрутизаторе включить информацию, полученную по протоколу OSPF следует использовать команду `redistribute ospf` и в качестве параметра указать метрику, которая будет присвоена всем сетям из протокола OSPF, а также указать информацию о каких каналах связей использовать (внутренние, внешние класса 1, внешние класса 2). Тип канала определяется источником информации: внутренние – получены по протоколу OSPF самостоятельно, внешние класса 1 – получены путем однократной интеграции протоколов, внешние класса 2 – все остальные.

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#redistribute ospf 1 metric 4
Router(config-router)#redistribute ospf 1 match internal
Router(config-router)#redistribute ospf 1 match external 1
Router(config-router)#redistribute ospf 1 match external 2
Router(config-router)#end
Router#
```

Рисунок 11 – Пример конфигурирование интеграции с протоколом OSPF

Указать интервал времени, через который будут рассылаться таблицы маршрутизации можно с помощью команды `timers basic`.

Включить в рассылаемую таблицу маршрут по умолчанию до текущего маршрутизатора можно с помощью команды `default-information originate`.

6.2 Конфигурирование протокола OSPF

В режиме конфигурирования протокола OSPF динамической маршрутизации можно задать:

- параметры зон, к которым относятся интерфейсы коммутатора (команда `area`);
- Интерфейс(ы), через которые анонсируются сети в процессе реализации протокола (команда `network`);
- интерфейс(ы), через которые запрещены прием и передача информации по протоколу динамической маршрутизации (пассивные интерфейсы, команда `passive-interface`);
- правила интеграции информации из разных протоколов динамической маршрутизации (команда `redistribute`);
- идентификатор маршрутизатора (команда `router-id`). По умолчанию, в качестве идентификатора используется максимальный (по значению) IP адрес маршрутизатора.

Процесс настройки протокола включает как минимум одно действие - указание какой(ие) интерфейс(ы) должны распространять информацию по протоколу OSPF (см. рисунок 12) и к какой зоне относятся эти интерфейсы. Интерфейсы задаются указанием их сетевых параметров – IP адреса и маски (маска инвертируется!!!).

```
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 1.1.1.0 0.0.0.255 area 0
Router(config-router)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    1.1.1.0 0.0.0.255 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1         110          00:00:44
  Distance: (default is 110)
```

Рисунок 12 Пример конфигурирования протокола OSPF

Определить следует ли включать информацию, полученную по протоколу RIP можно с помощью команды `redistribute rip subnets`. Параметр `subnets` указывает, что следует использовать маски подсетей. Также можно задать метрику присеваемую маршрутам из RIP протокола.

Посмотреть информацию о функционировании протокола OSPF можно в привилегированном режиме с помощью команды `show ip ospf`. Команде можно задать дополнительные параметры для вывода информации о: соседях и их состояниях, интерфейсах и их состояниях в рамках реализации OSPF, содержанием LSADB и др.

Задание на лабораторную работу

1. В существующей сети Ваше предприятия удалите все статические маршруты и маршруты «по умолчанию» на маршрутизаторах главного и дополнительного офисов.
2. Сконфигурируйте маршрутизаторы Ваших офисов так, чтобы они по последовательному интерфейсу обменивались информацией о маршрутах с использованием протокола RIP. Таблицы RIP должны приниматься только по последовательным интерфейсам. Убедитесь в правильности сформированных таблиц маршрутизации.
3. Используя многопользовательское окружение подключите маршрутизатор дополнительного офиса к маршрутизаторам дополнительных офисов двух других предприятий (те, в свою очередь, тоже должны быть соединены между собой, образуя кольцо из трех сетей 172.16.N.0/24).
4. Сконфигурируйте в сетях 172.16.N.0/24 функционирование протокола OSPF (объединив все маршрутизаторы в зону и сделав их пограничными). Обеспечьте интеграцию информации, полученной по протоколу RIP в данные протокола OSPF и наоборот. Продемонстрируйте связь между сетевыми узлами разных предприятий.
5. Продемонстрируйте отказоустойчивость связи между маршрутизаторами дополнительных офисов предприятий. Запустите бесконечный пинг от узла сети своего главного офиса до узла сети главного офиса соседнего предприятия. Отключите на маршрутизаторе дополнительного офиса канал, идущий в сеть соседнего предприятия. Как быстро сеть перейдет в связанное состояние?

Контрольные вопросы

1. Что такое динамическая маршрутизация? Какие этапы в ней присутствуют?
2. Чем отличаются векторные алгоритмы маршрутизации от алгоритмов на основе состояний каналов связей? Приведите положительные и отрицательные стороны каждого типа алгоритмов.
3. Что такое метрика маршрута? Зачем она используется? Как она рассчитывается при формировании таблиц маршрутизации статическим способом и протоколами динамической маршрутизации?
4. Может ли в таблице маршрутизации быть несколько строк, описывающих путь до одной и той же сети?
5. Что такое технология «расщепления горизонта»? Приведите положительный и отрицательный пример применения этой технологии.
6. Зачем в протоколе RIP используются триггерные обновления?
7. В каких состояниях может находиться связь между соседями по OSPF протоколу?
8. За счет чего сокращается объем передаваемой по сети служебной информации при использовании протокола OSPF?
9. Как происходит интеграция RIP и OSPF на пограничных коммутаторах?