ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ
ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
КАФЕДРА ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

ПРЕЗЕНТАЦИЯ НА ТЕМУ: «ПРОТОКОЛЫ МАРШРУТИЗАЦИИ»

ПО ПРЕДМЕТУ: ТЕОРИЯ ПОСТРОЕНИЯ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ И СИСТЕМ

студента группы 07001736
Дульцева Андрея Юрьевича

Для преподавателя доцента кафедры ИТСИТ БелГУ
Девициной Светланы Николаевны

БЕЛГОРОД 2017

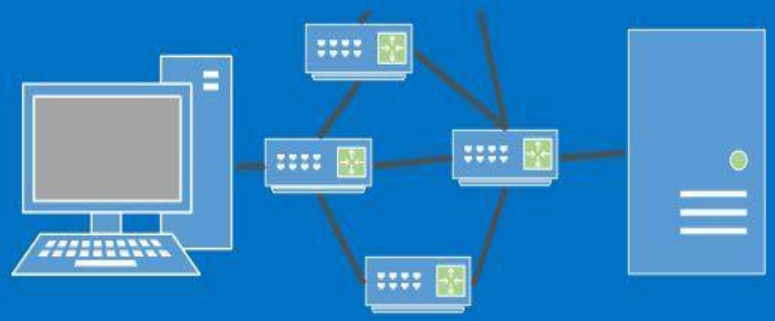
ИНТЕРМЕДИЯ

Одиссее среди сетей связи.

Статическая и динамическая маршрутизация

- Статическая маршрутизация — это настраиваемый вручную путь, который остается постоянным во время работы маршрутизатора.
- Динамическая маршрутизация — это путь, создаваемый динамически с использованием специальных протоколов маршрутизации.

Статическая



Динамическая

Протокол маршрутизации. Или капитан корабля потока данных.

Маршрутизация — это процесс направления пакета по лабиринту сетей, находящихся между отправителем и получателем.

Следует отличать выбор маршрута от перенаправления данных.

В связи с тем, что сети существуют как с фиксированной топологией так и с аморфной между модемами структурами, приходиться анализировать топологию сетей для оптимальной, по какому либо признаку, передачи сообщения, дабы данные в сетях связи приходили по назначению в конечный пункт и своевременно, независимо.

ИСПОЛНИТЕЛЬ ЖЕЛАНИЙ ПРОТОКОЛА - ДЕМОН

НА СЛУЖБЕ КАПИТАНА – ДЕМОНЫ. 6-7

МЕТРИКА. 8

Программы и службы исполняющие протоколы. На службе капитана – демоны.

Протокол маршрутизации — сетевой протокол, используемый маршрутизаторами, для определения возможных маршрутов следования данных в составной компьютерной сети.

Обработкой хранением и сбором данных по правилам протокола маршрутизации занимаются **демоны** (программы, в исключительных случаях аппаратные средства ЭВМ), появились в цифровых сетях.

Когда пропадает канал связи, демоны быстро находят альтернативные маршруты, если они существуют, и сообщают о них в сети, связанные с этим каналом. Обеспечивают демоны и межпротокольное взаимодействие и формирование протокольных единиц данных в том числе для маршрутизации).

Демоны маршрутизации собирают информацию из трех источников: конфигурационных файлов, существующих таблиц маршрутизации и “родственных” демонов других систем. Собранные данные объединяются, и вычисляется оптимальный набор маршрутов, после чего новые маршруты записываются в системную таблицу (и при необходимости посылаются другим системам посредством протоколов маршрутизации). Состояние сети время от времени меняется, поэтому демоны должны периодически опрашивать друг друга, чтобы убедиться в актуальности имеющейся у них информации.

Конкретный алгоритм вычисления маршрутов зависит от протоколов. Последние бывают двух типов: Дистанционно-векторные и топологические.

Метрика

Экономичным, быстрым могут считать маршрут с наименьшим числом переходов, с наименьшей задержкой, с наименьшими финансовыми затратами.

Для целей маршрутизации качество канала связи определяется числом, называемым метрикой стоимости. Путем сложения метрик отдельных отрезков пути вычисляется общая стоимость маршрута. В простейших системах каждому каналу назначается стоимость 1, и в результате метрикой маршрута становится число переходов. Но любой из перечисленных выше критериев может являться метрикой стоимости.

КЛАССИФИКАЦИЯ ПРОТОКОЛОВ

ДИСТАНЦИОННО-ВЕКТОРНЫЕ ПРОТОКОЛЫ 10-12

ТОПОЛОГИЧЕСКИЕ ПРОТОКОЛЫ 13-14

ВНУТРЕННИЕ И ВНЕШНИЕ ПРОТОКОЛЫ 15

ДОПОЛНИТЕЛЬНАЯ КЛАССИФИКАЦИЯ ПРОТОКОЛОВ 16 -17

Дистанционно-векторные протоколы

В основе дистанционно-векторных протоколов лежит следующая идея: если маршру тизатор X находится в пяти переходах от сети Y и является моим соседом, то я нахожусь в шести переходах от данной сети. Демон, работающий по такому протоколу, объявля ет о том, как далеко, по его расчетам, расположены известные ему сети. Если сосед ние демоны не “знают” более коротких маршрутов к этим сетям, они помечают данный компьютер как оптимальный шлюз. В противном случае они просто игнорируют этот анонс. Предполагается, что со временем таблицы маршрутизации придут в стабильное состояние.

Это довольно красивая идея, и если бы все работало так, как задумано, маршрути зация существенно упростилась бы. К сожалению, описанный алгоритм не лучшим об разом справляется с изменениями топологии.

2 Иногда стабилизация таблиц вообще не
наступает вследствие возникновения бесконечных циклов (например, маршрутизатор X получает информацию от маршрутизатора Y и посылает ее маршрутизатору Z, кото рый возвращает ее маршрутизатору Y). На практике приходится вводить сложные эв ристические правила или задавать ограничения. К примеру, в протоколе RIP (Routing Information Protocol — протокол маршрутной информации) считается, что любая сеть, находящаяся на расстоянии более пятнадцати переходов, недоступна.

Дистанционно-векторные протоколы оказываются
слишком “словоохотливыми”. Например, протокол RIP требует, чтобы маршрутизаторы
осуществляли широковещательную рассылку всей имеющейся у них информации каждые 30 секунд. В протоколе EIGRP обновления анонсируются каждые 90 секунд.
В противоположность этому в протоколе BGP (Border Gateway Protocol — протокол
пограничного шлюза) вся таблица посылается один раз, после чего изменения распро
страняются по мере возникновения. Такая оптимизация позволяет существенно снизить
“переговорный” трафик (большей частью, ненужный).

Дистанционно-векторные протоколы

Аббре-виатура	Полное название	Область применения
RIP	Routing Information Protocol (протокол маршрутной информации)	Локальные сети
RIPng	Routing Information Protocol (протокол маршрутной информации), следующее поколение	Локальные сети с протоколом IPv6
EIGRP[a]	Enhanced Interior Gateway Routing Protocol (улучшенный протокол маршрутизации внутреннего шлюза)	Глобальные сети, корпоративные локальные сети
BGP	Border Gateway Protocol (протокол пограничного шлюза)	Магистральные сети Интернета

Топологические протоколы

В топологических протоколах, или протоколах состояния канала, информация рассылается в относительно необработанном виде. Записи выглядят примерно так: “Маршрутизатор X является смежным по отношению к маршрутизатору Y, и канал функционирует”. Полный набор таких записей образует карту сетевых связей, на основании которой каждый маршрутизатор может сформировать собственную таблицу. Основное преимущество топологических протоколов, по сравнению с дистанционно-векторными, заключается в способности быстро стабилизировать таблицы маршрутизации в случае непредвиденного сбоя. К издержкам относится необходимость хранения полной карты соединений на каждом узле, для чего требуются дополнительные процессорные мощности и память.

Топологические протоколы сложнее дистанционно-векторных, зато они позволяют реализовать такие технологии, как маршрутизация на основании запрашиваемого типа обслуживания (поле TOS IP-пакета) и поддержка нескольких маршрутов к одному адресату.
Распространение получили только два топологических протокола: OSPF и IS-IS.

Внутренние и внешние протоколы

Маршрутизация внутри автономной системы отличается от маршрутизации между такими системами. Протоколы второго типа (внешние, или протоколы внешних шлюзов) должны управлять множеством маршрутов к различным сетям и учитывать тот факт, что соседние маршрутизаторы находятся под контролем других людей. Внешние протоколы не раскрывают топологию автономной системы, поэтому в определенном смысле их можно рассматривать как второй уровень маршрутизации, на котором соединяются группы сетей, а не отдельные компьютеры или кабели.

Дополнительная классификация протоколов

- В беспроводных сетях используются протоколы маршрутизации,
- которые по принципу работы можно разделить на:
- 1. Проактивные или табличные (англ. proactive, table-driven).
- Периодически рассылают по сети служебные сообщения с информацией обо
- всех изменениях в ее топологии. Каждый узел строит таблицу маршрутизации, откуда при необходимости передачи сообщения какому-либо узлу считывается
- маршрут к этому адресату.
- 2. Реактивные или работающие по запросу (англ. reactive, on-demand).
- Составляют маршруты до конкретных узлов лишь при возникновении
- необходимости в передаче им информации. Для этого узел-отправитель
- широковещательно рассылает по сети сообщение-запрос, которое должно дойти
- до узла-адресата.

- 3. Гибридные (англ. hybrid). Данные протоколы комбинируют
- механизмы проактивных и реактивных протоколов. Как правило, они разбивают
- сеть на множество подсетей, внутри которых функционирует проактивный протокол, а взаимодействие между ними осуществляется реактивными методами.
- 4. Проактивные протоколы.
- 5 .Реактивные протоколы
- 6. Протоколы геомаршрутизации.

ПРОТОКОЛЫ - ПОДРОБНОСТИ

ПРОТОКОЛ OLSR (OPTIMIZED LINK-STATE ROUTING) 19

ПРОТОКОЛЫ RIP И RIPNG

ПРОТОКОЛ OSPF

ПРОТОКОЛ EIGRP

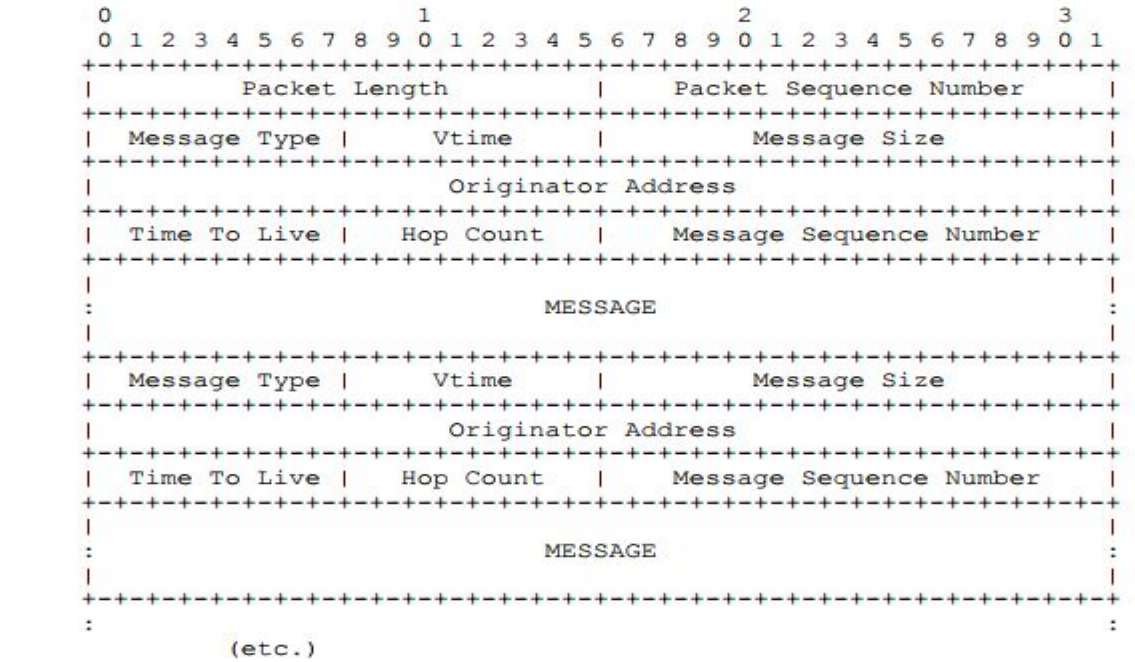
протокол OLSR (Optimized Link-State Routing)

- Проактивные протоколы. Один из наиболее применяемых проактивных
- протоколов OLSR (Optimized Link-State Routing) основан на сборе и
- распространении служебной информации о состоянии сети. В результате
- обработки этой информации каждый узел может построить модель текущего состояния сети в виде формального описания графа, вершины которого ставятся в соответствие узлам сети, рёбра (или дуги) – линиям связи (линкам). Имея такой граф, любой узел может вычислить «длины» кратчайших путей до всех адресатов в сети и выбрать «оптимальный» маршрут, ведущий к любому конкретному узлу сети. Данный алгоритм хорошо реагирует на множество непредвиденных событий, к которым, прежде всего, следует отнести:
- 1. Спонтанные отказы/восстановления узлов и линий.
- 2. Повреждения и ремонт узлов сети.
- 3. Агрессивные воздействия «внешней среды», приводящие к
- блокировке отдельных элементов системы.

- 4. Подключения и отключения узлов и линий при оперативной
- передислокации абонентов.
- Применение ресурса пропускной способности для служебного тра-
- фика протокола OLSR наиболее эффективно в сетях с высокой плотностью
- узлов. OLSR постоянно использует некоторый ресурс пропускной способности
- для служебного трафика.

3.3. Packet Format

The basic layout of any packet in OLSR is as follows (omitting IP and UDP headers):



3.3.1. Packet Header

Packet Length

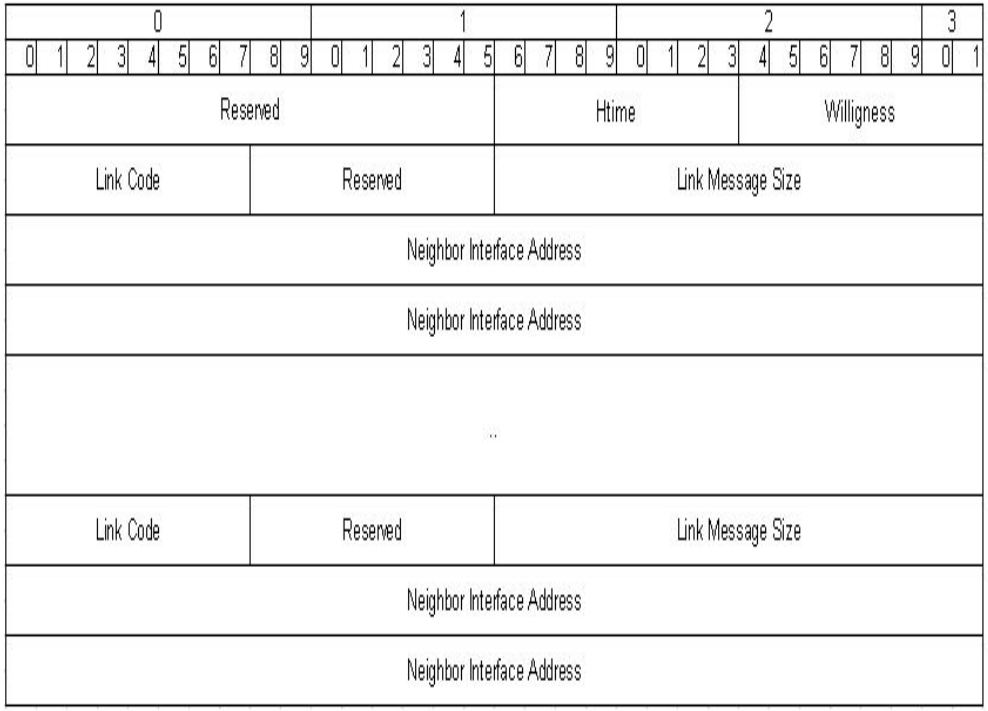
The length (in bytes) of the packet

Packet Sequence Number

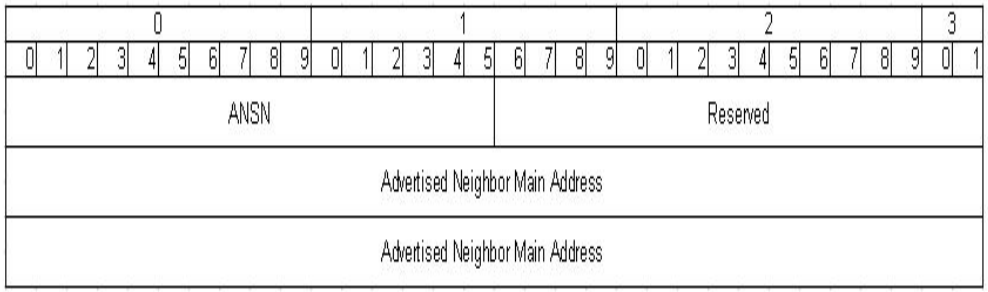
The Packet Sequence Number (PSN) MUST be incremented by one each time a new OLSR packet is transmitted. "Wrap-around" is handled as described in section 19. A separate Packet Sequence Number is maintained for each interface such that packets transmitted over an interface are sequentially enumerated.

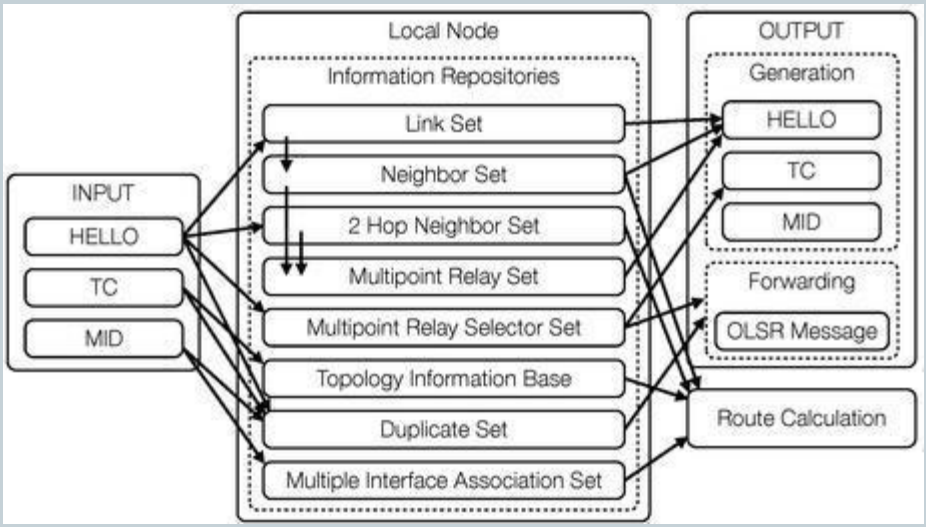
OLSR использует "Привет" сообщения, чтобы найти его одним прыжком соседей и два прыжка соседей через их ответы. Затем Отправитель может выбрать многоточечного реле (MHP) в расчете на один узел хоп, который предлагает лучшие маршруты для двух узлов. Каждый узел имеет также MHP набор селектор, в котором перечислены узлы, которые выбрали его в качестве узла MHP. OLSR использует контроль топологии (TC) сообщения вместе с экспедиторских MHP распространять соседом информацию по всей сети. *Узла и сети связи* (ВНД) сообщения используются OLSR для распространения рекламы маршрутную сеть таким же образом TC-Сообщений рекламируют принимающей стороны.

Привет [редактировать]



Топология управления (TC) [редактировать]




Local Node
Information Repositories
Link Set
Neighbor Set
2 Hop Neighbor Set
Multipoint Relay Set
Multipoint Relay Selector Set
Topology Information Base
Duplicate Set
Multiple Interface Association Set
INPUT
HELLO
TC
MID
OUTPUT
Generation
HELLO
TC
MID
Forwarding
OLSR Message
Route Calculation

Протоколы RIP и RIPng

RIP (Routing Information Protocol — протокол маршрутной информации) — это старый протокол компании Xerox, адаптированный для IP-сетей. Его IP-версия была описана примерно в 1988 году в документе RFC1058. Существует три версии этого протокола: RIPv1, RIPv2 и RIPng только для протокола IPv6 (ng (next generation) означает “следующее поколение”). Все версии этого протокола представляют собой простые Дистанционно-векторные протоколы, метрикой стоимости в которых является количество переходов. Поскольку протокол RIP разрабатывался в те времена, когда отдельные компьютеры были дорогими, а сети маленькими, в версии RIPv1 предполагается, что все узлы, находящиеся
на расстоянии пятнадцати и более переходов, недоступны. В более поздних версиях это
ограничение не было снято, чтобы стимулировать администраторов сложных сетей пе
реходить на более сложные протоколы маршрутизации

Протокол RIPng

представляет собой переформулирование протокола RIP в терминах протокола IPv6. Он может использоваться только в рамках протокола IPv6, в то время как протокол RIPv2 — только в рамках протокола IPv4. Если вы хотите использовать как протокол IPv4, так и протокол IPv6 вместе с протоколом RIP, то RIP и RIPng необходи мо выполнять как отдельные протоколы.

2. Protocol Specification

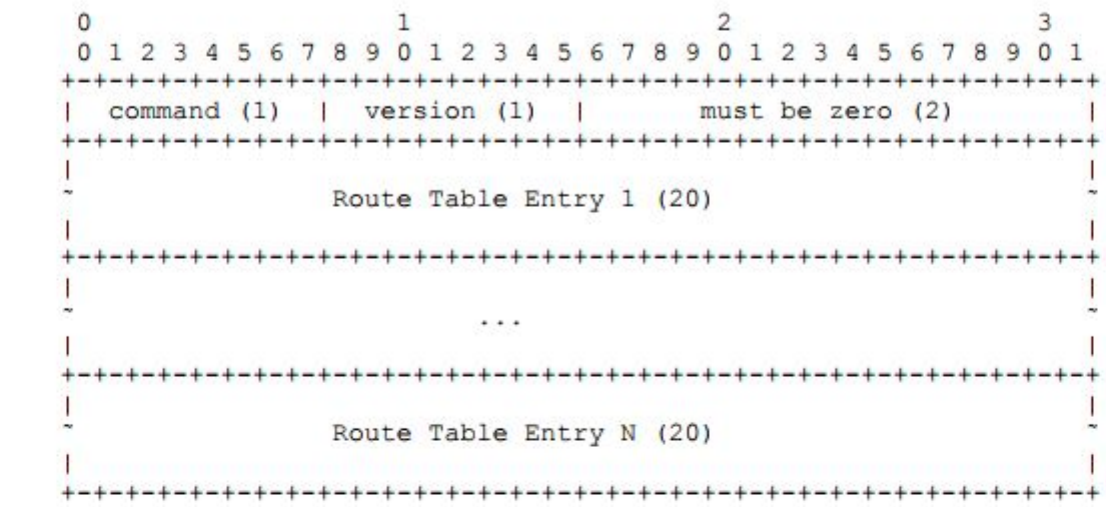
RIPng is intended to allow routers to exchange information for computing routes through an IPv6-based network. RIPng is a distance vector protocol, as described in [1]. RIPng should be implemented only in routers; IPv6 provides other mechanisms for router discovery [10]. Any router that uses RIPng is assumed to have interfaces to one or more networks, otherwise it isn't really a router. These are referred to as its directly-connected networks. The protocol relies on access to certain information about each of these networks, the most important of which is its metric. The RIPng metric of a network is an integer between 1 and 15, inclusive. It is set in some manner not specified in this protocol; however, given the maximum path limit of 15, a value of 1 is usually used. Implementations should allow the system administrator to set the metric of each network. In addition to the metric, each network will have an IPv6 destination address prefix and prefix length associated with it. These are to be set by the system administrator in a manner not specified in this protocol.

Each router that implements RIPng is assumed to have a routing table. This table has one entry for every destination that is reachable throughout the system operating RIPng. Each entry contains at least the following information:

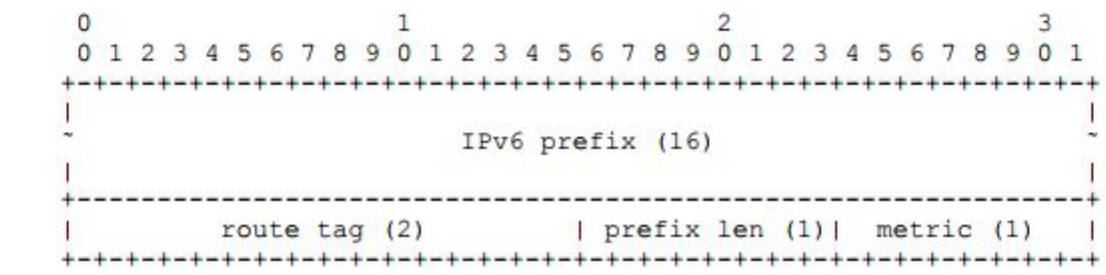
- The IPv6 prefix of the destination.
- A metric, which represents the total cost of getting a datagram from the router to that destination. This metric is the sum of the costs associated with the networks that would be traversed to get to the destination.
- The IPv6 address of the next router along the path to the destination (i.e., the next hop). If the destination is on one of the directly-connected networks, this item is not needed.
- A flag to indicate that information about the route has changed recently. This will be referred to as the "route change flag."
- Various timers associated with the route. See section 2.3 for more details on timers.

The entries for the directly-connected networks are set up by the router using information gathered by means not specified in this protocol. The metric for a directly-connected network is set to the cost of that network. As mentioned, 1 is the usual cost. In that case, the RIPng metric reduces to a simple hop-count. More complex metrics may be used when it is desirable to show preference for some

The RIPng packet format is:



where each Route Table Entry (RTE) has the following format:



The maximum number of RTEs is defined below.

Протокол OSPF

OSPF (Shortest Path First Open — открытый протокол первоочередного обнаружения кратчайших маршрутов) является самым популярным топологическим протоколом. Термин “первоочередное обнаружение кратчайших маршрутов” (shortest path first) означает специальный математический алгоритм, по которому вычисляются маршруты;
термин “открытый” (open) — синоним слова “непатентованный”. Основная версия протокола OSPF (версия 2) определена в документе RFC2328, а расширенная версия протокола OSPF, поддерживающая протокол IPv6 (версия 3), — в документе RFC5340. Первая версия протокола OSPF устарела и сейчас не используется.

- OSPF — протокол промышленного уровня, который эффективно функционирует
- в крупных сетях со сложной топологией. По сравнению с протоколом RIP, он имеет ряд преимуществ, включая возможность управления несколькими маршрутами, ведущими к одному адресату, и возможность разделения сети на сегменты (“области”), которые будут делиться друг с другом только высокоуровневыми данными маршрутизации. Сам протокол очень сложный, поэтому имеет смысл использовать его только в крупных системах, где важна эффективность маршрутизации. Для эффективного использования протокола OSPF необходимо, чтобы ваша схема адресации имела иерархический характер.
- В спецификации протокола OSPF не навязывается конкретная метрика стоимости.
- По умолчанию в реализации этого протокола компанией Cisco в качестве метрики используется пропускная способность сети.

Протокол EIGRP

EIGRP (Enhanced Interior Gateway Routing Protocol — протокол маршрутизации внутренних шлюзов) — это патентованный протокол маршрутизации, используемый только маршрутизаторами компании Cisco. Протокол IGRP был разработан для устранения некоторых недостатков протокола RIP еще в те времена, когда не было такого надежного стандарта, как протокол OSPF. Протокол IGRP был отклонен в пользу протокола EIGRP, который допускает произвольные сетевые маски CIDR. Протоколы IGRP и EIGPR конфигурируются одинаково, несмотря на различия в их организации.

Протокол EIGRP поддерживает протокол IPv6, но в нем, как и во всех других про токолах маршрутизации, адресные пространства IPv6 и IPv4 конфигурируются отдельно и существуют как параллельные домены маршрутизации.

Протокол EIGRP является дистанционно-векторным, но он спроектирован так, чтобы избежать проблем зацикливания и медленной стабилизации, свойственных другим протоколам данного класса. В этом смысле протокол EIGRP считается образцом. Для большинства применений протоколы EIGRP и OSPF обеспечивают равные функциональные возможности.

IS-IS: протокол маршрутизации между промежуточными системами. Протокол IS-IS (Intra-domain Intermediate System to Intermediate System Routing Protocol) является ответом на протокол OSPF со стороны организации ISO. Первоначально он предназначался для маршрутизации в рамках сетевых протоколов OSI, но впоследствии был расширен для поддержки IP-маршрутизации.

Оба протокола — IS-IS и OSPF — создавались в начале 90-х годов, когда протоколы организации ISO преднамеренно хранились в тайне. Благо

Протоколы RDP и NDP

Протокол RDP (Router Discovery Protocol — протокол обнаружения маршрутизаторов) использует ICMP-сообщения, посылаемые по групповому IP-адресу 224.0.0.1, для распространения информации о других маршрутизаторах в сети. К сожалению, не все маршрутизаторы в настоящее время рассылают такие сообщения, и не все компьютеры могут их принимать. Остается надеяться, что когда-нибудь этот протокол станет более популярным.

Протокол NDP (Neighbor Discovery Protocol — протокол обнаружения соседнего узла), основанный на протоколе IPv6, объединяет функциональные возможности протоколов RDP и ARP (Address Resolution Protocol — протокол разрешения адреса), используемых для отображения адресов IPv4 в адреса аппаратных устройств в локальных сетях. Поскольку этот протокол является основным компонентом протокола IPv6, он используется там, где используется протокол IPv6, и протоколы маршрутизации в рамках протокола IPv6 основаны именно на нем.

Документы с описанием протоколов

RFC	Название	Авторы
1075	Distance Vector Multicast Routing Protocol	Waitzman et al.
1256	ICMP Router Discovery Messages	Deering
1724	RIP Version 2 MIB Extension	Malkin, Baker
2080	Ring for IPv6	Malkin, Minnear

RFC	Название	Авторы
2328	OSPF Version 2	Moy
2453	RIP Version 2	Malkin
4271	A Border Gateway Protocol 4 (BGP-4)	Rekhter, Li, et al.
4552	Authentication/Confidentiality for OSPFv3	Gupta, Melam
4822	RIPv2 Cryprographic Authentication	Arkinson, Fanto
4861	Neighbor Discovery for IPv6	Narten et al.
5175	IPv6 Router Advertisement Flags Option	Haberman, Hinden
5308	Routing IPv6 with IS-IS	Hopps
5340	OSPF for IPv6	Coltun et al.
5643	Management Information Base for OSFv3	Joyal, NManral, et al.