Обзор стратегий маршрутизации и маршрутизаторов

Операционные системы

Перегудов Александр Вадимович

Содержание

# 1 Введение

Маршрутизация играет ключевую роль в современных компьютерных сетях, обеспечивая передачу данных от отправителя к получателю через множество сетевых устройств. В контексте быстроразвивающихся технологий информационной сети, понимание стратегий маршрутизации и роли маршрутизаторов становится все более важным для инженеров сетей и администраторов.

Целью данного реферата является обзор основных принципов и стратегий маршрутизации, а также роли маршрутизаторов в современных сетях. Будут рассмотренны ключевые концепции, включая структуру протоколов TCP/IP, организацию сетей с использованием подсетей, маршрутизацию и основные протоколы маршрутизации.

В рамках данного доклажа также будут рассмотрены различные стратегии маршрутизации, включая статическую и динамическую маршрутизацию, а также основные протоколы, такие как RIP, OSPF, EIGRP и BGP. Понимание этих концепций и стратегий поможет лучше осознать функционирование современных сетей.

# 2 Обзор стратегий маршрутизации и маршрутизаторов

## 2.1 Общие сведения о работе сети

Компютерная сеть представляет собой множество устройств связанных между собой посредством сетевых интерфейсов. Эти устройства включают в себя компьютеры, серверы, принтеры, маршрутизаторы, коммутаторы и другие устройства которые имеют сетевой интерфейс. Компютерная сеть позволяет обмениваться данными между всеми устройствами в такой сети.

Сетевой интерфейс может быть аппаратным и программным компонентом.

### 2.1.1 Сетевой интерфейс как аппаратный компонент

Сетевой интерфейс (аппаратный компонент) - Устройство, позволяющее компьютеру взаимодействовать с другими устройствами в сети.

Существует несколько популярных вариантов таких сетевых интерфейсов.

1. Ethernet-адаптер - устройство, позволяющее подключить компьютер посредством провода.
2. Wi-Fi-адаптер - устройство, позволяющее подключить компьютер по бесроводной связи посредством протокола Wi-Fi.
3. Bluetooth-адаптер - устройство, позволяющее подключить компьютер по бесроводной связи посредством протокола Bluetooth.

Существуют также аппаратные сетевые адаптеры которые способны подключаться к сети разными способами а не только одним. Например, чаще всего плата беспроводного адаптера способна работать так с Wi-Fi так и с Bluetooth протоколами.

### 2.1.2 Сетевой интерфейс как программный компонент

Сетевой интерфейс (программный компонент) - Абстракция, через которую операционная система управляет сетевым аппартатным компонентом.

Посредством такой абстракции опреационная система способна считывать данные которые принял сетевой адаптер а также отправлять данные в сеть.

В UNIX-системах сетевые интерфейсы обычно идентифицируются с помощью уникальных имен, таких как “eth0”, “wlan0” и т. д.

Сетевые интерфейсы в UNIX-системах могут быть настроены и управляемы с помощью различных инструментов и командной строки. Например, для настройки сетевого интерфейса в Linux можно использовать утилиты, такие как ifconfig, ip, или непосредственно изменять конфигурационные файлы, такие как /etc/network/interfaces.

### 2.1.3 Топология сети

Компьютерная сеть может иметь разную сетевую топологию.

Топология сети - физическая или логическая структура сети, определяющая способ, которым компьютеры и другие устройства подключаются друг к другу и обмениваются данными.

Основные физические топологии:

Звезда (Star Topology): В этой топологии каждый компьютер подключен к центральному устройству, такому как коммутатор или маршрутизатор. Все данные передаются через центральное устройство, что обеспечивает простоту управления и возможность быстрого обнаружения и изоляции проблем. Однако отказ центрального устройства может привести к отказу всей сети.

Кольцо (Ring Topology): В этой топологии каждый компьютер подключен к двум соседним компьютерам, создавая замкнутую цепь. Данные передаются по кольцу от одного компьютера к другому до тех пор, пока не достигнут адресата. Кольцевая топология обеспечивает хорошую пропускную способность и надежность, но отказ одного компьютера может повлиять на работу всего кольца.

Шина (Bus Topology): В этой топологии все компьютеры подключены к одному общему кабелю, который действует как шина. Компьютеры могут передавать данные непосредственно через этот кабель. Отказ одного компьютера не приводит к остановке всей сети, но добавление новых устройств может быть сложным и может привести к ухудшению производительности.

Дерево (Tree Topology): Эта топология является комбинацией звезды и шины. Группы компьютеров подключены к центральному устройству, которое в свою очередь подключено к другим центральным устройствам и т. д., образуя иерархическую структуру. Это позволяет создавать крупные сети с высокой пропускной способностью и управляемостью.

Сетка (Mesh Topology): В этой топологии каждый компьютер подключен к каждому другому компьютеру в сети. Это обеспечивает высокую надежность и отказоустойчивость, так как данные могут передаваться по разным маршрутам. Однако с ростом числа компьютеров сеть может стать сложной и дорогостоящей в управлении.

В подавляюшем большинстве случаев используется топология звезда.

## 2.2 Стек tcp/ip

Сетевая модель OSI (The Open Systems Interconnection model) — сетевая модель стека сетевых протоколов OSI/ISO. Посредством данной модели различные сетевые устройства могут взаимодействовать друг с другом. Модель определяет различные уровни взаимодействия систем. Каждый уровень выполняет определённые функции при таком взаимодействии.

Модель не смогла дать полное описание сети и не получила поддержку архитекторов на заре Интернета, который впоследствии нашел отражение в менее предписывающем TCP/IP, в основном под руководством Инженерного совета Интернета (IETF). В данный момент сетевая модель OSI не используется на практике, но используется в сфере обучения для того чтобы показать концепцию разделения на уровни. Поэтому будет рассмотрен стек TCP/IP.

### 2.2.1 Общие сведения

Набор интернет-протоколов обеспечивает сквозную передачу данных, определяющую, как данные должны пакетироваться, обрабатываться, передаваться, маршрутизироваться и приниматься. Эта функциональность организована в четыре слоя абстракции (если не считать физический уровень), которые классифицируют все связанные протоколы в соответствии с объёмом задействованных сетей. От самого низкого до самого высокого уровня — это уровень связи, содержащий методы связи для данных, которые остаются в пределах одного сегмента сети; интернет-уровень, обеспечивающий межсетевое взаимодействие между независимыми сетями; транспортный уровень, обрабатывающий связь между хостами; и прикладной уровень, который обеспечивает обмен данными между процессами для приложений.

### 2.2.2 Физический уровень

Физический уровень занимается реальной передачей необработанных битов по каналу связи. Принципиальными вопросами здесь являются следующие: какое напряжение должно использоваться для отображения единицы, а какое для нуля; сколько микросекунд длится бит; может ли передача производиться одновременно в двух направлениях; как устанавливается начальная связь и как она прекращается, когда обе стороны закончили свои задачи; из какого количества проводов должен состоять кабель и какова функция каждого провода. Вопросы разработки в основном связаны с механическими, электрическими и процедурными интерфейсами, а также с физическим носителем, лежащим ниже физического уровня.

### 2.2.3 Канальный уровень

Основная задача уровня передачи данных — быть способным передавать «сырые» данные физического уровня по надежной линии связи, свободной от необнаруженных ошибок, и маскировать реальные ошибки, так что сетевой уровень их не видит. Эта задача выполняется при помощи разбиения входных данных на кадры, обычный размер которых колеблется от нескольких сот до нескольких тысяч байт. Кадры данных передаются последовательно с обработкой кадров подтверждения, отсылаемых обратно получателем. Еще одна проблема, возникающая на уровне передачи данных (а также и на большей части более высоких уровней), — как не допустить ситуации, когда быстрый передатчик заваливает приемник данными. Может быть предусмотрен некий механизм регуляции, который информировал бы передатчик о наличии свободного места в буфере приемника на текущий момент.

### 2.2.4 Сетевой уровень

Сетевой уровень занимается управлением операциями подсети. Важнейшим моментом здесь является определение маршрутов пересылки пакетов от источника к пункту назначения. Маршруты могут быть жестко заданы в виде таблиц и редко меняться либо, что бывает чаще, автоматически изменяться, чтобы избегать отказавших компонентов. Кроме того, они могут задаваться в начале каждого соединения, например, терминальной сессии, такого как подключения к удаленной машине. Наконец, они могут быть в высокой степени динамическими, то есть вычисляемыми заново для каждого пакета с учетом текущей загруженности сети. Если в подсети одновременно присутствует слишком большое количество пакетов, то они могут закрыть дорогу друг другу, образуя заторы в узких местах. Недопущение подобной закупорки также является задачей сетевого уровня в соединении с более высокими уровнями, которые адаптируют загрузку. В более общем смысле, сетевой уровень занимается предоставлением определенного уровня сервиса (это касается задержек, времени передачи, вопросов синхронизации).

### 2.2.5 Транспортный уровень

Транспортный уровень обеспечивает надежную передачу данных между процессами(экземплярами программ)

Он создан для того, чтобы объекты одного ранга на приемных и передающих хостах могли поддерживать связь. На этом уровне должны быть описаны два сквозных протокола. Первый, TCP (Transmission Control Protocol — протокол управления передачей), является надежным протоколом с установлением соединений, позволяющим без ошибок доставлять байтовый поток с одной машины на любую другую машину объединенной сети. Он разбивает входной поток байтов на отдельные сообщения и передает их межсетевому уровню. На пункте назначения получающий TCP-процесс собирает из полученных сообщений выходной поток. Кроме того, TCP осуществляет управление потоком, чтобы быстрый отправитель не завалил информацией медленного получателя. Второй протокол этого уровня, UDP (User Dataram Protocol — протокол пользовательских дейтограмм), является ненадежным протоколом без установления соединения, не использующим последовательное управление потоком протокола TCP, а предоставляющим свое собственное. Он также широко используется в одноразовых клиент-серверных запросах и приложениях, в которых оперативность важнее аккуратности, например при передаче речи и видео.

### 2.2.6 Прикладной уровень

Прикладной уровень содержит набор популярных протоколов, необходимых пользователям. Одним из наиболее распространенных является протокол передачи гипертекста HTTP (HyperText Transfer Protocol), который составляет основу технологии Всемирной паутины. Когда браузер запрашивает веб-страницу, он передает ее имя (адрес) и рассчитывает на то, что сервер, на котором расположена страница, будет использовать HTTP. Сервер в ответ отсылает страницу. Другие прикладные протоколы используются для передачи файлов, электронной почты, сетевых рассылок.

### 2.2.7 Зачем нужно это разделение на уровни

Такое разделение на уровни нужно чтобы делегировать ответственность за выполнение разного рода задач. Дробление задач на множество подзадач действительно рабочий метод который позволяет решить большинство (если вообще не все) задач, какими бы сложными они ни казались. Так как каждый уровень выполняет свою подзадачу, то можно легко менять методы выполнения этих подзадач не затрагивая при этом всю остальную систему. Например, при написании протокола на прикладном уровне, программисту не обязательно знать как происходит процесс маршрутизации, как шифруются данные при передаче, каким образом определяются и доставляются недошедшие пакеты и т.д. Каждый уровень выполняет только свою часть общей задачи, а потому такая архитектура системы расширяема и имеет возможность на замену определённых частей системы.

## 2.3 Сетевой уровень. Подсети

Сетевой уровень TCP/IP отвечает за маршрутизацию данных между различными сетями, включая разделение сетей на подсети.

Каждое сетевое устройство имеет MAC-адрес и IP-адрес.

### 2.3.1 MAC-адрес

MAC-адрес (MAC - Media Access Control) - уникальный идентификатор, присваиваемый каждой единице сетевого оборудования или некоторым их интерфейсам в компьютерных сетях Ethernet. MAC-адрес имеет длину 48 бит (6 байт), обычно записывается в виде шестнадцатеричного числа, разделенного двоеточием или тире. Например: 00:1A:2B:3C:4D:5E

Этот адрес “вшит” производителем в сетевой адаптер. Он не меняется. Такой адрес позволяет определять устройства в сети. При отправке данных устройство добавляет в эти самые данные информацию о MAC-адресе получателя и отправителя(то есть себя). Таким образом центральное устройство, к которому подключены все остальные устройства, может решить кому именно данные передать. Центральное устройство имеет таблицу соответствия сетевого интерфейса и MAC-адреса подключенного к этому интерфейсу устройства. После того как в таблице было найденно соответствие, центральное устройстро отправляет данные дальше по конкретному интерфейсу. Такое устройство называется коммутатором.

Множество сетевых устройств соединённых непосредственно между собой или через коммутатор образуют подсеть.

### 2.3.2 IP-адрес

IP-адрес (Internet Protocol Address) - Уникальный числовой идентификатор, присваиваемый каждому устройству в компьютерной сети, подключенному к сети, использующей протокол IPv4 (Internet Protocol). IP-адрес позволяет идентифицировать устройство в сети. IP-адрес использует 32-битные адреса и записывается в виде четырех десятичных чисел, разделенных точками. Например: 192.168.0.1

Также существует IPv6 разработанный для замены IPv4. Такой адрес использует 128-битные адреса. По некоторым причинам он не может ввестись в эксплуатацию уже многие годы хотя такое новшество исправит сразу несколько проблем присущих IPv4 Например: 2001:0db8:85a3:0000:0000:8a2e:0370:7334

MAC-адрес используются устройствами в одной сети. По этой причине используя только MAC-адрес не получиться отправить данные устройству в другой сети. Даже если соединить коммутаторы рахных сетей то они всё равно не смогут понять куда отправлять данные, ведь в таблице нет MAC-адресов устройств другой сети(подключенных к другому коммутатору). Для передачи данных между разными сетями используется IP-адрес. Устройства в разных сетях имеют разную маску подсети. Так устройства одной подсети имеют одинаковую часть IP-адреса. Чаще всего это 24 бита (3 числа).

Например: 192.168.0.1, 192.168.0.2, 192.168.0.3, 192.168.0.4 - IP-адреса устройств в одной сети а 192.168.0.1, 192.100.0.2, 192.68.0.3, 192.99.0.4 - IP-адреса устройств в разных сетях.

Сети соединяются посредством специальных устройств - маршрутизаторов.

В отличии от коммутатора маршрутизатор работает не только с MAC-адресами но и IP-адресами. Когда устройство пытается отправить данные устройству в другой сети, то это устройство подставляет MAC-адрес маршрутизатора (шлюза сети) в информацию о получателе. При этом указывая IP-адрес устройства в другой сети. После, маршрутизатор уже с помощью своей таблицы и IP-адреса определяет куда дальше передавать данные. С помощью некоторых протоколов маршрутизации и таблицы маршрутизации маршрутизатор отправит данные в нужную сеть.

## 2.4 Маршрутизация

Между сетями скорее всего будет не один маршрутизатор. Скорее всего сети будут разделять десятки маршрутизаторов. При этом сетей может быть бесчётное множество. Для того чтобы найти оптимальный путь доставки данных используется маршрутизация.

Маршрутизация - Процесс пересылки данных от отправителя к получателю через компьютерные сети, используя оптимальные пути. Она осуществляется маршрутизаторами, которые принимают решения о том, какие пути использовать для доставки пакетов данных на основе информации о сети.

Таблица маршрутизации (Routing Table) - это набор данных, который содержит информацию о доступных маршрутах в сети и инструкции для маршрутизатора о том, куда направить пакеты данных, чтобы доставить их к назначению.

## 2.5 Основные протоколы и стратегии маршрутизации

Существует множество протоколов маршрутизации. Каждый протокол реализует маршрутизацию по разному. Ниже будут приведены самые популярные протоколы маршрутизации

### 2.5.1 RIP (Routing Information Protocol)

RIP — так называемый протокол дистанционно-векторной маршрутизации, который оперирует транзитными участками (хоп, hop) в качестве метрики маршрутизации.

Максимальное количество транзитных участков, разрешенное в RIP — 15 (метрика 16 означает «бесконечно большую метрику»). Каждый RIP-маршрутизатор по умолчанию вещает в сеть свою полную таблицу маршрутизации раз в 30 секунд, довольно сильно нагружая низкоскоростные линии связи.

В современных сетевых средах RIP — не самое лучшее решение для выбора в качестве протокола маршрутизации, так как его возможности уступают более современным протоколам, таким как EIGRP, OSPF. Ограничение на 15 транзитных участков не дает применять его в больших сетях. Преимущество этого протокола — простота конфигурирования. Сети работающие с этим протоколом почти невозможно встретить в наше время.

### 2.5.2 OSPF (Open Shortest Path First)

Протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (link-state technology) и использующий для нахождения кратчайшего пути алгоритм Дейкстры.

Протокол OSPF был разработан IETF в 1988 году. Последняя версия протокола представлена в RFC 2328 (1998 год). Протокол OSPF представляет собой протокол внутреннего шлюза (Interior Gateway Protocol — IGP). Протокол OSPF распространяет информацию о доступных маршрутах между маршрутизаторами одной автономной системы. OSPF имеет следующие преимущества:

1. Высокая скорость сходимости по сравнению с дистанционно-векторными протоколами маршрутизации
2. Поддержка сетевых масок переменной длины (VLSM)
3. Оптимальное использование пропускной способности с построением дерева кратчайших путей.

OSPF является протоколом маршрутизации с открытым исходным кодом и использует алгоритм Дейкстры для определения кратчайшего пути. Он поддерживает переменную длину префиксов и автоматическое обнаружение соседей. OSPF часто используется в крупных сетях и Интернете из-за своей масштабируемости и быстродействия.

Принцип работы заключается в следующем:

1. После включения маршрутизаторов протокол ищет непосредственно подключенных соседей и устанавливает с ними «дружеские» отношения.
2. Затем они обмениваются друг с другом информацией о подключенных и доступных им сетях. То есть они строят карту сети (топологию сети). Данная карта одинакова на всех маршрутизаторах.
3. На основе полученной информации запускается алгоритм SPF (Shortest Path First, «выбор наилучшего пути»), который рассчитывает оптимальный маршрут к каждой сети. Данный процесс похож на построение дерева, корнем которого является сам маршрутизатор, а ветвями — пути к доступным сетям. Данный процесс, то есть конвергенция, происходит очень быстро.

### 2.5.3 EIGRP (Enhanced Interior Gateway Routing Protocol)

EIGRP (Enhanced Interior Gateway Routing Protocol) — протокол маршрутизации, разработанный фирмой Cisco на основе протокола IGRP той же фирмы. Релиз протокола состоялся в 1994 году. EIGRP использует механизм DUAL для выбора наиболее короткого маршрута.

Более ранний и практически не используемый ныне протокол IGRP был создан как альтернатива протоколу RIP (до того, как был разработан OSPF). После появления OSPF Cisco представила EIGRP — переработанный и улучшенный вариант IGRP, свободный от основного недостатка дистанционно-векторных протоколов — особых ситуаций с зацикливанием маршрутов — благодаря специальному алгоритму распространения информации об изменениях в топологии сети. EIGRP более прост в реализации и менее требователен к вычислительным ресурсам маршрутизатора, чем OSPF. Также EIGRP имеет более продвинутый алгоритм вычисления метрики DUAL (Diffusing Update ALgorithm), который может использовать 5 различных компонентов для расчета:

1. Bandwidth (Пропускная способность). Минимальная пропускная способность для данного маршрута (а не сумма цен (cost) в отличие от OSPF).
2. Delay (Задержка). Суммарная задержка на всём пути маршрута.
3. Reliability (Надежность). Наихудший показатель надёжности на всём пути маршрута, основанный на keepalive.
4. Loading (Загруженность). Наихудший показатель загруженности интерфейса на всём пути маршрута, основанный на количестве трафика проходящего через интерфейс и настроенном на нём параметре bandwidth.
5. MTU. Минимальный размер MTU на всём пути маршрута. По умолчанию, EIGRP использует только первые два компонента, так как надежность и загруженность — динамические величины, которые могут изменяться до нескольких раз в секунду. Соответственно, каждое изменение вызывает перерасчет метрики для маршрутов и использование процессорной мощности маршрутизатора до 100 %. MTU не является динамической величиной, но не используется по причине слабого влияния на метрику маршрута.

### 2.5.4 BGP (Border Gateway Protocol)

BGP (Border Gateway Protocol, протокол граничного шлюза) — протокол динамической маршрутизации.

Относится к классу протоколов маршрутизации внешнего шлюза (англ. EGP — Exterior Gateway Protocol).

На текущий момент является основным протоколом динамической маршрутизации в сети Интернет.

Протокол BGP предназначен для обмена информацией о достижимости подсетей между AS (АС, AS — autonomous system, автономные системамы), то есть группами маршрутизаторов под единым техническим и административным управлением, использующими протокол внутридоменной маршрутизации для определения маршрутов внутри себя и протокол междоменной маршрутизации для определения маршрутов доставки пакетов в другие АС. Передаваемая информация включает в себя список АС, к которым имеется доступ через данную систему. Выбор наилучших маршрутов осуществляется исходя из правил, принятых в сети.

BGP поддерживает бесклассовую адресацию и использует суммирование маршрутов для уменьшения таблиц маршрутизации. С 1994 года действует четвёртая версия протокола, все предыдущие версии являются устаревшими.

BGP, наряду с DNS, является одним из главных механизмов, обеспечивающих функционирование Интернета.

BGP является протоколом прикладного уровня и функционирует поверх протокола транспортного уровня TCP (порт 179). После установки соединения передаётся информация обо всех маршрутах, предназначенных для экспорта. В дальнейшем передаётся только информация об изменениях в таблицах маршрутизации. При закрытии соединения удаляются все маршруты, информация о которых передана противоположной стороной.

# 3 Заключение

В данном докладе были рассмотрели основные принципы работы сети, стек протоколов TCP/IP, концепцию подсетей, маршрутизацию и основные протоколы и стратегии маршрутизации. Понимание этих концепций является важным для проектирования, настройки и поддержки современных сетей.

# Список литературы

Э. Таненбаум, Д. Уэзеролл "Компьютерные сети" 5-е изд. 2016 г.

Э. Таненбаум, Х. Бос "Современные операционные системы" 4-е изд. 2015 г.

Д. Куроуз, К. Росс "Компьютерные сети. Нисходящий подход" 2016 г.

У. Брайан "Внутреннее устройство Linux" 2016 г.

А. Робачевский "Интернет изнутри. Экосистема глобальной сети" 2017 г.