

Сетевая пересылка и маршрутизация.

1. IP-forwarding и IP-routing.

- **IP-forwarding** — это процесс пересылки IP-пакетов от узла-отправителя к узлу-получателю в IP-сети с произвольной топологией на основе решения задачи о маршрутизации.
- **IP-routing** — это процесс решающий задачу выбора наилучшего маршрута.
- **Node** (сетевой узел) — любое устройство имеющее сетевой интерфейс с настроенным протоколом TCP/IP;
- **Host** (хост) — узел, не обладающий возможностями маршрутизации пакетов;
- **Router** (маршрутизатор) — узел, обладающий возможностями маршрутизации (перенаправление дейтаграмм из одной сети в другую), обычно такой узел имеет несколько сетевых-интерфейсов (со своими MAC- и IP-адресами), подключенными к разным IP-сетям.



Фундаментальная разница между хостом и маршрутизатором заключается в том, что хост никогда не перенаправляет дейтаграммы с одного своего интерфейса на другой, но, IP-уровень на узле может быть сконфигурирован таким образом, чтобы выполнять функции маршрутизации (ip-forwarding), в дополнение к тому, что он работает в качестве сетевого интерфейса, иначе дейтаграммы, не предназначенные хосту, будут молча удалены.

На рисунке показана упрощенная модель процессов forwarding и routing на IP уровне.

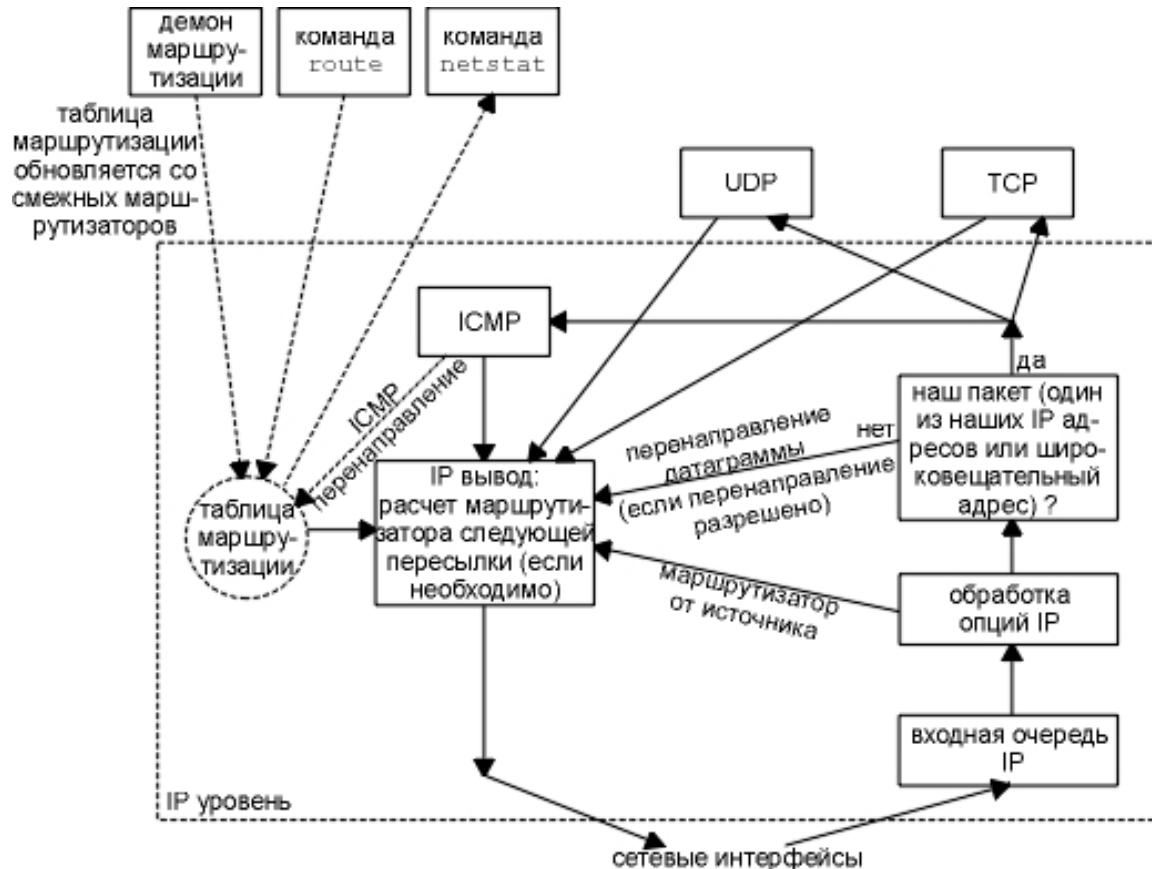


Рис. Действия, выполняемые IP уровнем интерфейса.

Для пересылки пакета IP-уровень должен владеть следующей информацией:

- Адрес назначения.
- Адрес соседнего маршрутизатора, от которого он может узнать об удаленных сетях.
- Доступные пути ко всем удаленным сетям.
- Наилучший путь к каждой удаленной сети.
- Методы обслуживания и проверки информации о маршрутизации.

В целом процесс IP-пересылки одинаков в сетях любого размера и представляет собой серию отдельных операций прямой или косвенной маршрутизации пакетов.

Если целевая сеть непосредственно подключена к маршрутизатору, то для отправки пакетов используется **прямая пересылка**, иначе - **косвенная пересылка** через посредника.

Пути доступа к удаленной сети маршрутизатор узнаёт с помощью маршрутизации **статической** (информацию вручную вводит администратор) или **динамической** (местоположение сетей определяется из информации от соседних маршрутизаторов).

Если в сети **произойдет изменение**, то протокол динамической маршрутизации информирует об изменении все маршрутизаторы **автоматически**. Если же используется статическая маршрутизация, обновить таблицы маршрутизации на всех устройствах придется системному **администратору вручную**.

2. Процесс прямой IP-пересылки.

Когда один узел IP-сети отправляет пакет другому узлу, то в заголовке IP указываются IP-адрес отправителя и IP-адрес получателя. Отправка пакета происходит следующим образом:

1) Отправитель определяет, находится ли получатель в той же самой IP-сети, что и отправитель (локальной), или в другой IP-сети (удаленной). Для этого отправитель производит поразрядное умножение IP-отправителя и IP-получателя на маску подсети-отправителя. Если результаты совпадают, значит, оба узла находятся в одной подсети.

2) Если узлы в одной IP-сети, то отправитель проверяет ARP-кэш на наличие MAC-адреса получателя. Если нужная запись имеется, то дальше отправка пакетов производится напрямую узлу-получателю на канальном уровне. Если нужной записи нет, то отправитель посылает ARP-запрос с IP-адресом получателя, ответ помещает в ARP-кэш и передача пакета также производится на канальном уровне (между сетевыми адаптерами компьютеров).

3) Если отправитель и получатель расположены в разных IP-сетях, то отправитель посылает данный пакет сетевому узлу, который указан в таблице маршрутизации как наилучший или который в конфигурации отправителя указан как DefaultGateway. Основной шлюз всегда находится в той же IP-сети, что и узел-отправитель, поэтому взаимодействие происходит на канальном уровне (после выполнения ARP-запроса).

В целом процесс IP-пересылки представляет собой серию отдельных операций прямой или косвенной пересылки пакетов.

3. Косвенная пересылка и таблицы маршрутизации.

Каждый сетевой узел принимает решение о пересылки пакета на основе таблицы маршрутизации, которая хранится в оперативной памяти данного узла. Определяется интерфейс, куда будет послан пакет в следующей последовательности:

- Поиск совпадающего адреса хоста.
- Поиск совпадающего адреса сети.
- Поиск пункта по умолчанию (обычно указывается как сеть с идентификатором 0.0.0.0).

С другой стороны, политика маршрутизации устанавливает правила, по которым решается, какой маршрут будет внесен в таблицу маршрутизации.

IP-модуль осуществляет **механизм пересылки**, тогда как маршрутизирующий демон обычно определяет **политику маршрутизации**.

Таблицы маршрутизации существуют не только у маршрутизаторов с несколькими интерфейсами, но и у рабочих станций, подключаемых к сети через сетевой адаптер.

Таблицу маршрутизации в системе Windows можно посмотреть командой `route print`, а в Linux командой `netstat -r`.

Каждая таблица маршрутизации содержит набор записей, которые могут формироваться различными способами:

- **автоматические записи**, созданные автоматически системой на основе конфигурации протокола TCP/IP на каждом из сетевых адаптеров, см. `ifconfig/ipconfig`;
- **автоматические записи**, созданные автоматически системой для специальных маршрутов, например, `loopback 127.0.0.0/8`.
- **статические записи**, созданные администратором, например, командой `route add` (Linux, Windows) или в консоли службы Routing and Remote Access Service (Windows);
- **динамические записи**, созданные ICMP сообщением о перенаправлении (ICMP redirect), см. лекцию об ICMP;
- **динамические записи**, созданные ICMP сообщениями поиска маршрутизатора (ICMP Router Discovery) и объявления маршрутизатора (ICMP Router Advertisement), см. лекцию об ICMP;
- **динамические записи**, созданные различными протоколами маршрутизации (RIP v1/v2, RIPng (IPv6) OSPF, BGP v1/v2, BGP v3/v4 (IPv6) и др.). Эти протоколы будут рассмотрены ниже.

Рассмотрим примеры типичных таблиц маршрутизации: для рабочих станций в локальной сети и для сервера, имеющего несколько сетевых интерфейсов.

3.1. Таблица маршрутизации (ТМ) рабочей станции Windows.

Пример ТМ, которую строит хост Windows XP на основе конфигурации своих интерфейсов.

```
C:\>route print
IPv4 таблица маршрута
=====
Список интерфейсов (Interface List)
0x1 ..... MS TCP Loopback interface
0x10002 ...00 c0 26 a1 6e 05 ..... Realtek RTL8139 Family PCI Fast Ethernet NIC
=====
Активные маршруты (Active Routes):
    Сетевой адрес          Маска сети          Адрес шлюза          Интерфейс          Метрика
(Network Destination)    (Netmask)          (Gateway)            (Interface)        (Metric)
    0.0.0.0                0.0.0.0            192.168.1.1         192.168.1.10       1
    127.0.0.0              255.0.0.0          127.0.0.1           127.0.0.1          1
    192.168.1.0            255.255.255.0      192.168.1.10        192.168.1.10       20
    192.168.1.10          255.255.255.255    127.0.0.1           127.0.0.1          20
    192.168.1.255         255.255.255.255    192.168.1.10        192.168.1.10       20
    224.0.0.0              240.0.0.0          192.168.1.10        192.168.1.10       20
    255.255.255.255       255.255.255.255    192.168.1.10        192.168.1.10       1
Основной шлюз (Default Gateway): 192.168.1.1
=====
Постоянные маршруты (Persistent Routes):
Отсутствует (None)
```

Пример, для Windows XP, с настройками: IP/маска — 192.168.1.10/24, шлюз — 192.168.1.1.

Interface List (Список интерфейсов) — список сетевых адаптеров, установленных в компьютере. Интерфейс Loopback присутствует всегда. Ethernet NIC — сетевая карта.

Active Routes. Далее идёт сама таблица маршрутов. Каждая строка таблицы — это маршрут для какой-либо IP-сети.

Default Gateway (Основной шлюз) — соответствует значению IP-адреса основного шлюза в конфигурации TCP/IP данной станции. это адрес маршрутизатора, на который отправляется трафик, для которого невозможно определить маршрут исходя из таблиц маршрутизации.

Что произойдет, если не найдено совпадение с указанным пунктом назначения и маршрут по умолчанию отсутствует?

Если дейтаграмма была сгенерирована непосредственно этим хостом, то приложению, которое отправило дейтаграмму, возвращается ошибка (host unreachable) или (network unreachable). Если дейтаграмма должна быть перенаправлена, посылающему хосту возвращается ICMP сообщение о недоступности хоста.

Persistent Routes (Постоянные маршруты) — список статических маршрутов рабочей станции, которые созданы администратором командой route. В данном примере нет ни одного такого.

Читать любую запись в таблице маршрутизации нужно следующим образом:
«Чтобы доставить пакет в сеть с адресом из поля **Сетевой адрес**
и маской из поля **Маска сети**,
нужно через интерфейс с IP-адресом из поля **Интерфейс**
послать пакет по IP-адресу из поля **Адрес шлюза**,
а «стоимость» такой доставки будет равна числу из поля **Метрика**.»

В таблице определено множество записей (маршрутов) с разными параметрами.

- 0.0.0.0/0 — маршрут «неопределённый» (сравнивается последним) для отправки пакетов на основной шлюз.
- 127.0.0.1/8 — маршрут для отправки unicast пакетов во внутренней сети узла (себе).
- 192.168.1.0/24 — маршрут для отправки unicast пакетов в локальной IP-сети (своей сети).
- 192.168.1.10/32 — маршрут для отправки unicast пакетов для IP данного узла (себе).
- 192.168.1.255/32 — маршрут для отправки пакетов на broadcast-адрес для всех узлов сети.
- 224.0.0.0/6 — маршрут для отправки multicast пакетов во внутренней сети узла (себе).
- 255.255.255.255/32 — маршрут для отправки unicast пакетов данному узла данной сети.

В Windows используется стоимости метрики, которая основана на скорости соединения.

Скорость связи	Метрика
Больше или равен 2 ГБ	5
Больше, чем 200 МБ	10
Больше 80 МБ и меньше или равно 200 МБ	20
Больше 20 МБ и меньше или равно 80 МБ	25
Больше, чем 4 Мбайт и меньше или равно 20 МБ	30
Более 500 КБ и меньше или равен 4 МБ	40
Меньше или равно 500 КБ	50

3.2. Таблица маршрутизации Linux.

Команды `route -n`, `netstat -nr`. Без опции `-n` команда `netstat` просматривает файл `/etc/networks`, и берет оттуда имена сетей, при этом может получиться некоторая путаница с именами хостов.

```
$ netstat -nr
Kernel IP routing table
Destination      Gateway          Genmask         Flags           Metric Ref    Use   Iface
0.0.0.0          192.168.111.1   0.0.0.0         UG              0       0      0    eth0
192.168.111.0    0.0.0.0         255.255.255.0   U              0       0      0    eth0
127.0.0.1        127.0.0.1       0.0.0.0         UH              0       0      0    lo0
224.0.0.0        140.252.1.32    0.0.0.0         U              1       0      0    eth0
140.252.13.35    140.252.1.183   0.0.0.0         UGHD           1       0      0    eth0
```

В Linux/UNIX для конкретного маршрута может быть показано несколько флагов, например:

- U - маршрут активен.
- G - маршрут подключен к шлюзу (маршрутизатору). Если этот флаг не установлен, считается, что пункт назначения подключен непосредственно.
- H - маршрут ведет к хосту, что означает, что в качестве пункта назначения используется полный адрес хоста. Если этот флаг не установлен, то маршрут указывает на сеть.
- D - маршрут был создан посредством перенаправления ICMP redirect.
- M - маршрут был модифицирован посредством перенаправления ICMP-redirect.

Ref – счётчик соединений, Use – счётчик количества переданных пакетов.

3.3. Таблица маршрутизации (ТМ) маршрутизатора.

Рассмотрим типичную сеть с несколькими маршрутизаторами.

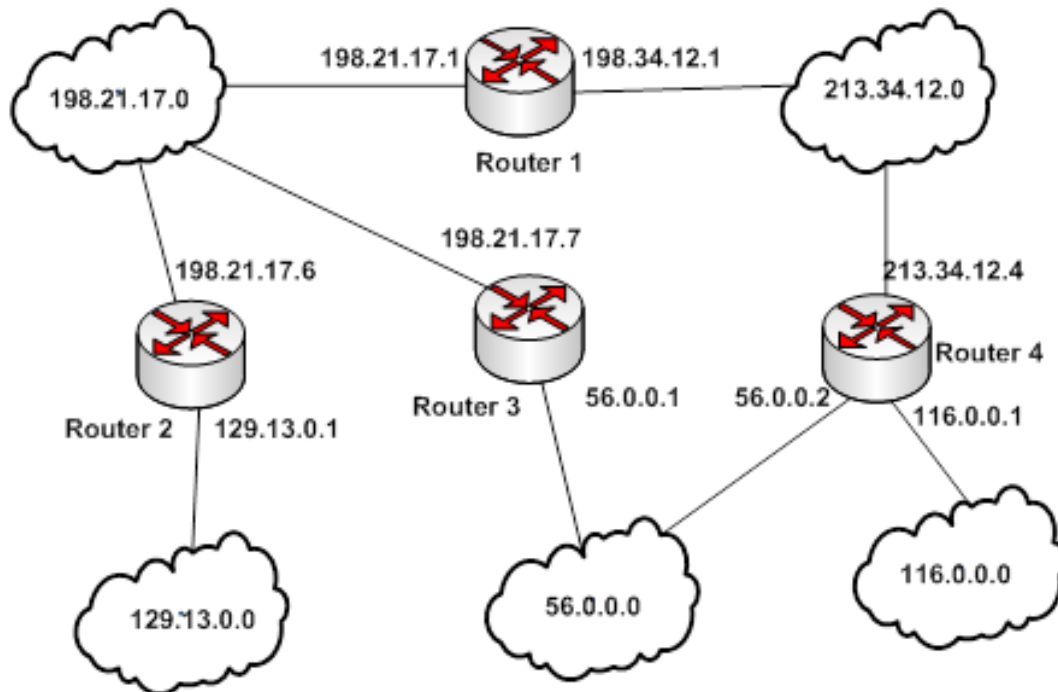


Таблица маршрутизации для Router 2 представляет собой типичный пример таблицы маршрутов, использующей IP-адреса сетей, для сети, представленной на рисунке выше.

Сетевой адрес	Маска сети	Адрес шлюза	Интерфейс	Метрика
129.13.0.0	255.255.0.0	-	129.13.0.1	подключен
198.21.17.0	255.255.255.0	-	198.21.17.6	подключен
213.34.12.0	255.255.255.0	198.21.17.1	198.21.17.6	1
56.0.0.0	255.0.0.0	198.21.17.7	198.21.17.6	1
116.0.0.0	255.0.0.0	198.21.17.7	198.21.17.6	2
116.0.0.0	255.0.0.0	198.21.17.1	198.21.17.6	2
0.0.0.0	0.0.0.0	198.21.17.7	198.21.17.6	-

Многомаршрутные таблицы. Здесь представлена многомаршрутная таблица маршрутизации, так как содержится два маршрута до сети 116.0.0.0. В случае построения одномаршрутной таблицы маршрутизации, указывается лишь один путь к сети 116.0.0.0 по наименьшему значению метрики или из других соображений. Многомаршрутные таблицы позволяют гибче и быстрее реагировать на изменения в сетях.

Next hop routing. В этой таблице в столбце "Сетевой адрес" указываются адреса всех сетей, которым данный маршрутизатор может передавать пакеты. В стеке TCP/IP принят так называемый одношаговый подход к оптимизации маршрута продвижения пакета (**next-hop routing**) – каждый маршрутизатор и конечный узел принимает участие в выборе только одного шага передачи пакета. Поэтому в каждой строке таблицы маршрутизации указывается не весь маршрут в виде последовательности IP-адресов маршрутизаторов, через которые должен пройти пакет, а только один IP-адрес - **адрес следующего маршрутизатора**, которому нужно

передать пакет. Вместе с пакетом следующему маршрутизатору передается ответственность за выбор следующего шага маршрутизации. Одношаговый подход к маршрутизации означает **распределенное решение задачи выбора маршрута**. Это снимает ограничение на максимальное количество транзитных маршрутизаторов на пути пакета.

Default gateway. Одношаговая маршрутизация обладает еще одним преимуществом - она позволяет сократить объем таблиц маршрутизации в конечных узлах и маршрутизаторах за счет использования в качестве номера сети назначения так называемого маршрута по умолчанию – default (0.0.0.0), который обычно занимает (обрабатывается) в таблице маршрутизации последнюю строку. Если в таблице маршрутизации есть такая запись, то все пакеты с номерами сетей, которые отсутствуют в таблице маршрутизации, передаются маршрутизатору, указанному в строке default. Поэтому маршрутизаторы часто хранят в своих таблицах ограниченную информацию о сетях интерсети, пересылая пакеты для остальных сетей в порт и маршрутизатор, используемые по умолчанию. Подразумевается, что маршрутизатор, используемый по умолчанию, передаст пакет на магистральную сеть, а маршрутизаторы, подключенные к магистрали, имеют полную информацию о составе интерсети.

Специфичные записи о маршруте к узлу. Специфичный для узла маршрут содержит вместо номера сети полный IP-адрес, то есть адрес, имеющий ненулевую информацию не только в поле номера сети, но и в поле номера узла. Предполагается, что для такого конечного узла маршрут должен выбираться не так, как для всех остальных узлов сети, к которой он относится. В случае, когда в таблице есть разные записи о продвижении пакетов для всей сети N и ее отдельного узла D, имеющего адрес N-D, при поступлении пакета, адресованного узлу N-D, маршрутизатор отдаст предпочтение записи для N-D.

3.4. Поддержка таблиц маршрутизации.

Есть два способа поддержки актуального состояния таблиц маршрутизации: ручной и автоматический.

Ручной способ подходит для небольших сетей. В этом случае в таблицы маршрутизации вручную заносятся статические записи для маршрутов. Записи создаются либо командой `route add` (Linux), либо в консоли Службы маршрутизации и удаленного доступа (Windows).

В больших сетях ручной способ становится слишком трудоёмким, чреват ошибками и недостаточно оперативен. **Автоматическое построение** и модификация таблиц маршрутизации производится так называемыми «динамическими маршрутизаторами».

Динамические алгоритмы маршрутизации отслеживают изменения в топологии сети, вносят необходимые изменения в таблицы маршрутов и обмениваются данной информацией с другими маршрутизаторами.

4. Алгоритмы маршрутизации.

Основные требования к алгоритмам маршрутизации:

- точность;
- простота;
- надёжность;
- стабильность;
- справедливость;
- оптимальность.

Существуют различные алгоритмы построения таблиц для одношаговой (**Next hop routing**) маршрутизации. Их можно разделить на три класса:

- алгоритмы фиксированной маршрутизации;
- алгоритмы простой маршрутизации;
- алгоритмы адаптивной маршрутизации.

Независимо от алгоритма, используемого для построения таблицы маршрутизации, результат их работы имеет единый формат. За счет этого в одной и той же сети различные узлы могут строить таблицы маршрутизации по своим алгоритмам, а затем обмениваться между собой недостающими данными. Поэтому маршрутизатор, работающий по алгоритму адаптивной маршрутизации, может снабдить конечный узел, применяющий алгоритм фиксированной маршрутизации, сведениями о пути к сети, о которой конечный узел ничего не знает.

4.1. Фиксированная маршрутизация.

Этот способ применяется в сетях с простой топологией связей и основан на ручном составлении таблицы маршрутизации администратором сети.

Часто используется для магистралей крупных сетей, так как сама магистраль может иметь простую структуру с очевидными наилучшими путями следования пакетов в подсети, присоединенные к магистрали.

Выделяют следующие алгоритмы:

- **Однопутевая фиксированная маршрутизация** – это когда между двумя абонентами устанавливается единственный путь. Сеть с такой маршрутизацией неустойчива к отказам и перегрузкам.
- **Многопутевая фиксированная маршрутизация** – может быть установлено несколько возможных путей и вводится правило выбора пути. Эффективность такой маршрутизации падает при увеличении нагрузки. При отказе какой-либо линии связи необходимо менять таблицу маршрутизации, для оперативности в каждом узле связи обычно хранится несколько таблиц.

4.2. Простая маршрутизация.

Это способы маршрутизации не требующие изменения таблиц маршрутизации при изменении топологии и состояния сети передачи данных, обеспечиваются различными алгоритмами:

- **Случайная маршрутизация** – это передача сообщения из узла в любом случайно выбранном направлении, за исключением направлений по которым сообщение поступило узел.
- **Циклическое обслуживание (RR - Round-Robin)** – это передача сообщения из узла в одном последовательно по кругу выбранном направлении, за исключением направлений по которым сообщение поступило узел.
- **Лавинная маршрутизация** – это передача сообщения из узла во всех направлениях, кроме направления по которому сообщение поступило в узел. Такая маршрутизация гарантирует малое время доставки пакета, за счет ухудшения пропускной способности.
- **Маршрутизация по предыдущему опыту** – каждый пакет имеет счетчик числа пройденных узлов, в каждом узле связи анализируется счетчик и запоминается тот маршрут, который соответствует минимальному значению счетчика. Такой алгоритм позволяет приспосабливаться к изменению топологии сети, но процесс адаптации протекает медленно и неэффективно.

В целом, простая маршрутизация не обеспечивает направленную передачу пакета и имеет низкую эффективности. Основными достоинствами являются простота и обеспечение устойчивой работы сети при выходе из строя различных частей сети, может быть использована маршрутизатором при сильной перегрузке.

4.3. Адаптивная маршрутизация.

Это основной вид алгоритмов маршрутизации, применяющихся маршрутизаторами в современных сетях со сложной топологией. Адаптивная маршрутизация основана на том, что маршрутизаторы периодически обмениваются специальной топологической информацией об имеющихся в интерсети сетях, а также о связях между маршрутизаторами. Обычно учитывается не только топология связей, но и их пропускная способность и состояние.

Адаптивные протоколы имеют распределенный характер, работа распределена между всеми маршрутизаторами, выделяют следующие алгоритмы:

- **Локальная адаптивная маршрутизация** – каждый узел независимо формирует и поддерживает информацию о состоянии линий связи, длины очереди и маршрутах.
- **Глобальная адаптивная маршрутизация** – основана на использовании информации получаемой от соседних узлов. Для этого каждый узел содержит таблицу маршрутизации, в которой указано метрика прохождения сообщений. На основе информации, получаемой из соседних узлов, значение таблицы пересчитывается с учетом длины очереди в самом узле.
- **Централизованная адаптивная маршрутизация** – существует некоторый центральный узел, который занимается сбором информации о состоянии сети. Этот центр формирует управляющие пакеты, содержащие таблицы маршрутизации и рассылает их в узлы связи.
- **Гибридная адаптивная маршрутизация** – основана на использовании таблицы периодически рассылаемой центром и на анализе длины очереди на самом узле.

4.4. Показатели алгоритмов маршрутизации (метрики).

Каким образом определяется предпочтительность маршрута по сравнению с другими? Для этого в алгоритмах маршрутизации используются различные показатели (метрики). Сложные алгоритмы маршрутизации могут базироваться на множестве метрик, комбинируя их в виде одного гибридного показателя. Ниже перечислены часто используемые метрики:

4.4.1. Длина маршрута.

Длина маршрута является наиболее общим показателем маршрутизации. Протоколы маршрутизации определяют "количество пересылок" (количество хопов), т. е. показатель, характеризующий число проходов, которые пакет должен совершить на пути от источника до пункта назначения через элементы объединения сетей (такие как маршрутизаторы).

4.4.2. Стоимость.

Некоторые протоколы маршрутизации позволяют администраторам сети назначать произвольные цены на каждый канал сети. В этом случае метрикой тракта является сумма расходов, связанных с каждым каналом, который был traversирован.

4.4.3. Надежность.

Надежность, в контексте алгоритмов маршрутизации, относится к надежности каждого канала сети (обычно описываемой в терминах соотношения бит/ошибка). Некоторые каналы сети могут отказывать чаще, чем другие. Отказы одних каналов сети могут быть устранены легче

или быстрее, чем отказы других каналов. При назначении оценок надежности могут быть приняты в расчет любые факторы надежности. Оценки надежности обычно назначаются каналам сети администраторами. Как правило, это произвольные цифровые величины.

4.4.4. Задержка.

Под задержкой маршрутизации обычно понимают отрезок времени, необходимый для передвижения пакета от источника до пункта назначения через объединенную сеть. Задержка зависит от многих факторов, включая полосу пропускания промежуточных каналов сети, очереди в порт каждого маршрутизатора на пути передвижения пакета, перегруженность сети на всех промежуточных каналах сети и физическое расстояние, на которое необходимо переместить пакет. Т. к. здесь имеет место конгломерация нескольких важных переменных, задержка является наиболее общим и полезным показателем.

4.4.5. Полоса пропускания.

Полоса пропускания относится к имеющейся мощности трафика какого-либо канала. При прочих равных показателях, канал Ethernet 10 Mbps предпочтителен любой арендованной линии с полосой пропускания 64 Кбайт/с. Хотя полоса пропускания является оценкой максимально достижимой пропускной способности канала, маршруты, проходящие через каналы с большей полосой пропускания, не обязательно будут лучше маршрутов, проходящих через менее быстродействующие каналы. Использована как метрика в Windows-хостах.

5. Протоколы маршрутизации.

Протокол маршрутизации — это сетевой протокол, который используется маршрутизаторами (роутерами) с целью определения маршрутов пересылки данных в составной вычислительной сети (интрасеть).

Протоколы маршрутизации классифицируются в соответствии с алгоритмами маршрутизации описанными выше в предыдущем разделе.

Протоколы маршрутизации делятся на два вида в зависимости от сферы применения:

- **Interior Gateway Protocol (IGP)** - внутридоменной маршрутизации (**RIP, OSPF**);
- **Exterior Gateway Protocol (EGP)** - междоменной маршрутизации (**EGP, BGP**).

А также протоколы маршрутизации делятся на три типа в зависимости от типов алгоритмов, построения маршрутов в сети:

- **Source or Policy Based Algorithm** – алгоритмы маршрутизации от источника (**IP и ACL**).
- **Distance Vector Algorithm (DVA)** - дистанционно-векторные протоколы (**RIP, GGP, EGP, IGRP, BGP**);
- **Link State Algorithm (LSA)** - протоколы состояния каналов связи (**IS-IS, OSPF**).

Перечень наиболее часто используемых протоколов маршрутизации составляют протоколы: RIP v1/v2, RIPng (IPv6), OSPF, BGP v4 (IPv6).

5.1. Внутренние и внешние протоколы маршрутизации.

5.1.1. Автономные системы (Autonomous systems).

Internet изначально строилась как сеть, объединяющая большое количество уже существующих систем. С самого начала в ее структуре выделяли магистральную сеть (core backbone network), а сети, присоединяющиеся к магистрали, рассматривались как автономные системы (autonomous systems, AS).

Магистральная сеть и каждая из автономных систем имели свое собственное административное управление и собственные протоколы маршрутизации.

Необходимо подчеркнуть, что автономная система и домен имен Internet - это разные понятия, которые служат разным целям.

AS объединяет сети, в которых под общим административным руководством одной организации осуществляется маршрутизация, а домен объединяет компьютеры (возможно, принадлежащие разным сетям), в которых под общим административным руководством одной организации осуществляется назначение уникальных символьных имен. Естественно, области действия автономной системы и домена имен могут в частном случае совпадать, если одна организация выполняет обе указанные функции.

Все **AS имеют уникальный 16-разрядный номер**. InterNIC выделяет номер для организации, учредившей новую автономную систему.

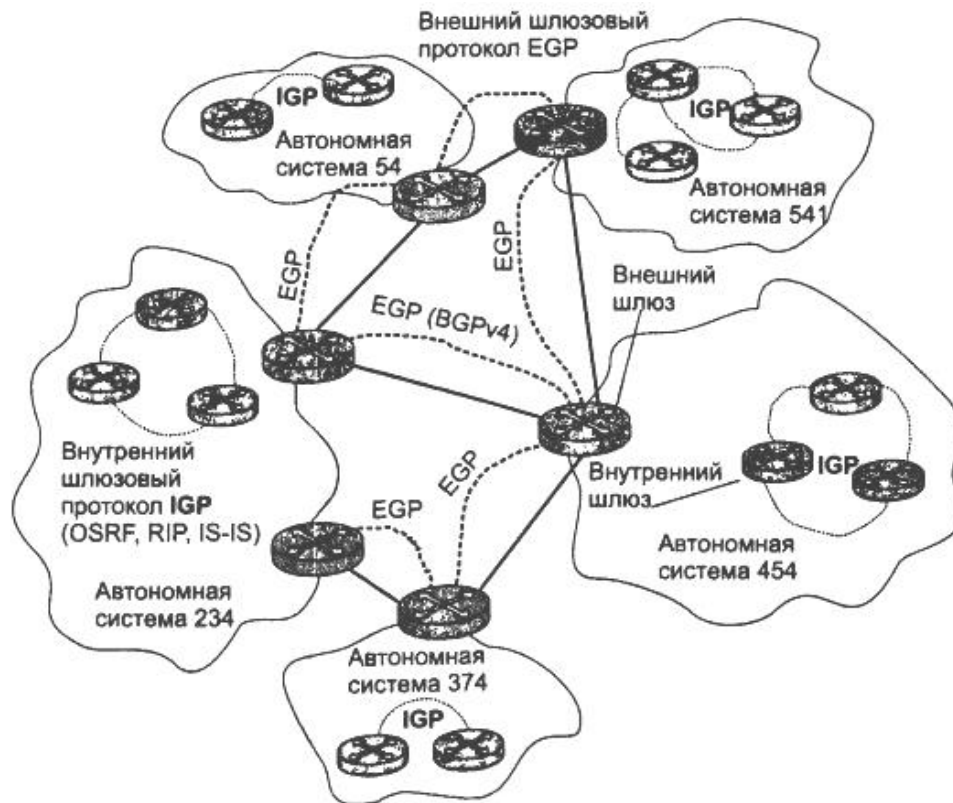


Рис. 1 Автономные системы (AS) Internet.

Протоколы маршрутизации внутри автономных систем называются протоколами внутренних шлюзов (**interior gateway protocol, IGP**), а протоколы, определяющие обмен маршрутной информацией между внешними шлюзами и шлюзами магистральной сети - протоколами внешних шлюзов (**exterior gateway protocol, EGP**).

Магистраль сети также является автономной системой. Внутри магистральной сети также допустим любой собственный внутренний протокол IGP.

Цель разделения всей сети Internet на AS - в ее многоуровневом **модульном представлении**, что необходимо для любой крупной системы, способной к расширению в больших масштабах. Изменение протоколов маршрутизации внутри какой-либо AS никак не должно влиять на работу остальных AS. Кроме того, деление Internet на AS должно способствовать **агрегированию** информации в магистральных и внешних шлюзах.

До введения автономных систем использовался двухуровневый подход, то есть сначала маршрут определяется как последовательность сетей, а затем ведёт непосредственно к заданному узлу в конечной сети (именно этот подход мы использовали до сих пор).

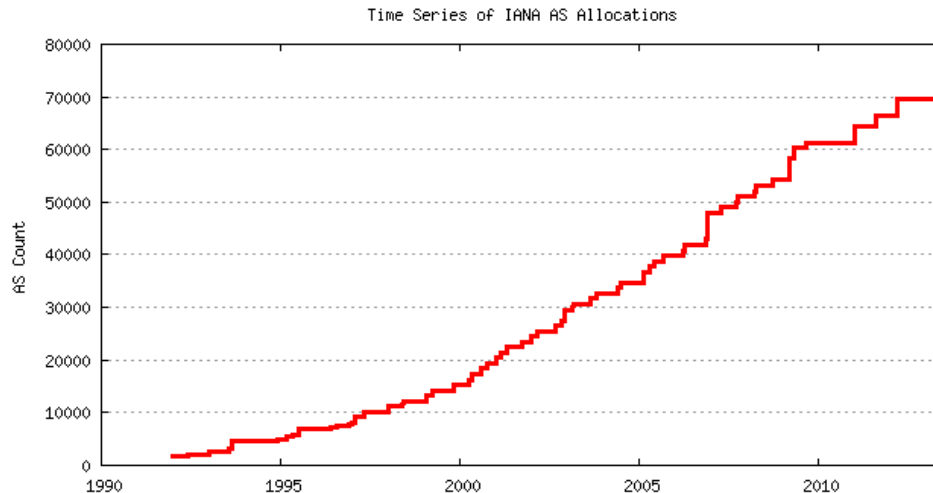
С появлением автономных систем появляется третий, верхний, уровень маршрутизации — сначала маршрут определяется как последовательность автономных систем, затем — как последовательность сетей и только потом ведёт к конечному узлу.

Выбор маршрута между автономными системами осуществляют внешние шлюзы, использующие особый тип протокола маршрутизации, так называемый внешний шлюзовой протокол (**Exterior Gateway Protocol, EGP**). В настоящее время для работы в такой роли

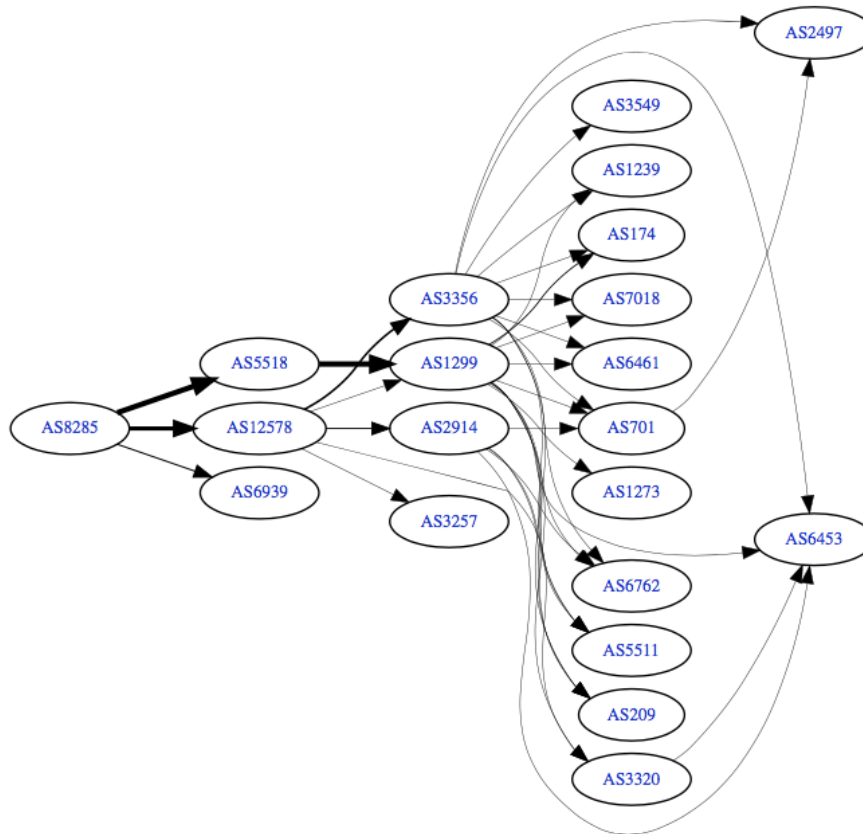
сообщество Интернета утвердило стандартный пограничный шлюзовой протокол версии 4 (**Border Gateway Protocol, BGPv4**). В качестве адреса следующего маршрутизатора в протоколе BGPv4 указывается адрес **точки входа в соседнюю AS**.

За маршрут внутри автономной системы отвечают внутренние шлюзовые протоколы (**Interior Gateway Protocol, IGP**). К числу IGP относятся знакомые нам протоколы RIP, OSPF и IS-IS. В случае транзитной автономной системы эти протоколы указывают точную последовательность маршрутизаторов от точки входа в автономную систему до точки выхода из нее.

На конец 2016 г. выделено 64 495 ASN, см. <http://thyme.rand.apnic.net/current/data-used-autnums>



Демонстрация взаимодействия ASN, см. http://bgp.he.net/AS8285#_graph4



5.2. Дистанционно-векторный алгоритм DVA.

В **DVA** (Distance Vector Algorithm) маршрутизаторы рассылают друг другу вектор содержащий «расстояние» от передающего маршрутизатора до всех известных ему сетей. Под «расстоянием» подразумевается любая из метрик, в частности, может быть количество пройденных маршрутизаторов (по хопам) или время, затраченное на передачу пакетов.

Маршрутизатор модифицирует вектора полученные от соседних маршрутизаторов (увеличивает значение метрик), дополняет своими данными (о своих непосредственно подключенных сетях), выбирает из нескольких альтернативных путей лучший по выбранной метрике, строит собственный вектор и транслирует вектор дальше по сети от своего имени.

В результате чего, все маршрутизаторы получают информацию обо всех сетях подключенных к interior-сети и о расстоянии (метрики) до них через соседние маршрутизаторы.

Недостатки DVA. DVA хорошо работают только в относительно небольших сетях, так как:

- маршрутизаторы постоянно обмениваются векторами расстояний, что приводит к забиванию линий связи широковещательным трафиком в больших сетях;
- алгоритм не всегда корректно реагирует на изменения в конфигурации сети, поскольку маршрутизаторы передают обобщенную информацию полученную косвенно от других маршрутизаторы и не содержит конкретного представления о топологии связей.

Самыми распространенными представителями DVA является протоколы **RIP** и **BGP**.

5.3. Алгоритм состояния связей - LSA.

LSA (Line State Algorithm) снабжает все маршрутизаторы информацией, необходимой для построения графа связей составной вычислительной сети. Все маршрутизаторы основываются на одинаковых графах, в следствии чего:

- маршрутизаторы быстрее реагирует на изменение конфигурации сети;
- быстрее вычисляется оптимальный маршрут следования, по выбранным метрикам.

Дополнительную информацию о других сетях маршрутизаторы получают путём обмена короткими пакетами **HELLO**, со своими соседями. В отличии от DVA, который постоянно обменивается большими ширококестательными пакетами, алгоритм LSA использует небольшие пакеты с информацией только о состояниях линий связи. Более развернутую информацию о сетях, алгоритм LSA передает в том случае, когда, на основе пакетов HELLO, было зафиксировано изменение состояния линий связи (например, маршрутизатор вышел из строя или добавили новый маршрутизатор). На основе графа сети LSA строят SP Tree для определения маршрута.

Как результат, LSA более приспособлен к большим составным вычислительным сетям, поскольку содержит меньшее количество ширококестательных пакетов, что увеличивает пропускную способность и устойчивость составной сети.

Протоколы, основанные на алгоритме состояния связей (LSA), являются **OSPF**(Open Shortest Path First, алгоритм кратчайшего пути) стека TCP/IP и **IS-IS** (Intermediate System to Intermediate System) стека OSI.

6. Дополнительные возможности маршрутизаторов.

Наряду с функцией маршрутизации многие устройства обладают следующими важными дополнительными функциональными возможностями, которые значительно расширяют сферу применения этих устройств.

6.1. Поддержка одновременно нескольких протоколов маршрутизации.

В протоколах маршрутизации обычно предполагается, что маршрутизатор строит свою таблицу на основе работы только этого одного протокола. Деление Internet на автономные системы также направлено на исключение использования в одной автономной системе нескольких протоколов маршрутизации. Тем не менее иногда в большой корпоративной сети приходится поддерживать одновременно несколько таких протоколов, чаще всего это складывается исторически. При этом таблица маршрутизации может получаться противоречивой - разные протоколы маршрутизации могут выбрать разные следующие маршрутизаторы для какой-либо сети назначения. Большинство маршрутизаторов решает эту проблему за счет придания приоритетов решениям разных протоколов маршрутизации. Высший приоритет отдается статическим маршрутам (администратор всегда прав), следующий приоритет имеют маршруты, выбранные протоколами состояния связей, такими как OSPF, а низшим приоритетов обладают маршруты дистанционно-векторных протоколов, как самых несовершенных.

6.2. Приоритеты сетевых протоколов.

Можно установить приоритет одного протокола сетевого уровня над другими. На выбор маршрутов эти приоритеты не оказывают никакого влияния, они влияют только на порядок, в котором многопротокольный маршрутизатор обслуживает пакеты разных сетевых протоколов. Это свойство бывает полезно в случае недостаточной полосы пропускания кабельной системы и существования трафика, чувствительного к временным задержкам, например голосового трафика, передаваемого одним из сетевых протоколов.

6.3. Защита от широковещательных штормов (broadcast storm).

Одна из характерных неисправностей сетевого программного обеспечения - самопроизвольная генерация с высокой интенсивностью широковещательных пакетов. Широковещательным штормом считается ситуация, в которой процент широковещательных пакетов превышает 20 % от общего количества пакетов в сети. Обычный коммутатор или мост слепо передает такие пакеты на все свои порты, как того требует его логика работы, засоряя, таким образом, сеть. Борьба с широковещательным штормом в сети, соединенной коммутаторами, требует от администратора отключения портов, генерирующих широковещательные пакеты. Маршрутизатор не распространяет такие пакеты во все объединяемые им сети.

6.4. Поддержка политики маршрутных объявлений.

В большинстве протоколов обмена маршрутной информацией (например, RIP, OSPF) предполагается, что маршрутизатор объявляет в своих сообщениях обо всех сетях, которые ему известны. Аналогично предполагается, что маршрутизатор при построении своей таблицы учитывает все адреса сетей, которые поступают ему от других маршрутизаторов сети. Однако существуют ситуации, когда администратор хотел бы скрыть существование некоторых сетей в определенной части своей сети от других администраторов, например, по соображениям безопасности. Или же администратор хотел бы запретить некоторые маршруты, которые могли бы существовать в сети. При статическом построении таблиц маршрутизации решение таких проблем не составляет труда. Динамические же протоколы маршрутизации не позволяют стандартным способом реализовывать подобные ограничения.

Существует только один широко используемый протокол динамической маршрутизации, в котором описана возможность существования правил, ограничивающих распространение некоторых адресов в объявлениях, - это протокол BGP. Необходимость поддержки таких правил в протоколе BGP понятна, так как это протокол обмена маршрутной информацией между автономными системами, где велика потребность в административном регулировании маршрутов (например, некоторый поставщик услуг Internet может не захотеть, чтобы через него транзитом проходил трафик другого поставщика услуг). Разработчики маршрутизаторов исправляют этот недостаток стандартов протоколов, вводя в маршрутизаторы поддержку правил передачи и использования маршрутной информации, подобных тем, которые рекомендует BGP.

6.5. Поддержка не маршрутизируемых протоколов.

Таких как NetBIOS, NetBEUI или DEC LAT, которые не оперируют с таким понятием, как сеть. Маршрутизаторы могут обрабатывать пакеты таких протоколов двумя способами.

Brouter. В первом случае они могут работать с пакетами этих протоколов как мосты, то есть передавать их на основании изучения MAC-адресов.

Маршрутизатор необходимо сконфигурировать особым способом, чтобы по отношению к некоторым не маршрутизируемым протоколам на некоторых портах он выполнял функции моста, а по отношению к маршрутизируемым протоколам - функции маршрутизатора.

Такой мост/маршрутизатор иногда называют brouter (bridge плюс router).

Инкапсуляция в протокол. Другим способом передачи пакетов не маршрутизируемых протоколов является инкапсуляция этих пакетов в пакеты какого-либо сетевого протокола.

Некоторые производители маршрутизаторов разработали собственные протоколы, специально предназначенные для инкапсуляции не маршрутизируемых пакетов. Кроме того, существуют стандарты для инкапсуляции некоторых протоколов в другие, в основном в IP.

Примером такого стандарта является протокол DLSw, определяющий методы инкапсуляции пакетов SDLC и NetBIOS в IP- пакеты, а также протоколы PPTP и L2TP, инкапсулирующие кадры протокола PPP в IP-пакеты.

6.6. Разделение функций построения и использования ТМ.

Основная вычислительная работа проводится маршрутизатором при составлении таблицы маршрутизации с маршрутами ко всем известным ему сетям. Эта работа состоит в обмене пакетами протоколов маршрутизации, такими как RIP или OSPF, и вычислении оптимального пути к каждой целевой сети по некоторому критерию.

Для вычисления оптимального пути на графе, как того требуют протоколы состояния связей, необходимы значительные вычислительные мощности.

После того как таблица маршрутизации составлена, функция продвижения пакетов происходит весьма просто - осуществляется просмотр таблицы и поиск совпадения полученного адреса с адресом целевой сети. Если совпадение есть, то пакет передается на соответствующий порт маршрутизатора.

Некоторые маршрутизаторы поддерживают только функции продвижения пакетов по готовой таблице маршрутизации. Такие маршрутизаторы являются усеченными маршрутизаторами, так как для их полноценной работы требуется наличие полнофункционального маршрутизатора, у которого можно взять готовую таблицу маршрутизации. Этот маршрутизатор часто называется сервером маршрутов.

Отказ от самостоятельного выполнения функций построения таблицы маршрутизации резко удешевляет маршрутизатор и повышает его производительность.

7. Упражнения.

1. Должен ли быть адрес интерфейса loopback всегда 127.0.0.1?
2. Может ли путь IP пакета различаться для разных портов UDP?
3. Может ли путь IP пакета различаться для разных протоколов (TCP, UDP, ICMP)?
4. Просмотрите таблицу маршрутизации Вашей системы и опишите каждую запись.
5. Найдите и просмотрите информацию об AS для известных латвийских банков: Swedbank, DNB Nord, Citadele.

Используйте

- <http://www.bgplookingglass.com/list-of-autonomous-system-numbers> для поиска номера ASN организации;
- <http://viewdns.info/asnlookup/> для анализа информации о том откуда и кто управляет AS;
- <https://mxtoolbox.com> для получения прочей информации.