4. Инфраструктура сети

- Маршрутизаторы и их настройка

- Протоколы маршрутизации (OSPF, EIGRP, RIP)

- IP-адресация, подсети, NAT

Тема 4. Инфраструктура сети

# Маршрутизаторы



Маршрутизатор — специализированное устройство, которое пересылает пакеты между различными сегментами сети на основе правил и таблиц маршрутизации. Маршрутизатор может связывать разнородные сети различных архитектур. Для принятия решений о пересылке пакетов используется информация о топологии сети и определённые правила, заданные администратором.

Маршрутизатор имеет следующие функции в сети:

1. **Передача данных между сетями** — маршрутизатор направляет пакеты данных от источника к месту назначения через правильные маршруты.
2. **Выбор оптимального пути** — определяет лучший маршрут для каждого пакета на основе текущих условий сети.
3. **Обмен маршрутной информацией** — использует протоколы маршрутизации для обмена данными о доступных путях с другими маршрутизаторами.
4. **Фильтрация и безопасность** — обеспечивает контроль доступа и фильтрацию трафика с помощью правил и списков контроля доступа.
5. **Поддержка функций NAT** — преобразует приватные IP-адреса в публичные для выхода в интернет и обратно.
6. **Обеспечение качества обслуживания (QoS**) — приоритизация важного трафика для повышения эффективности работы сети.
7. **Обеспечение восстановления соединений** — реагирует на сбои и выбирает альтернативные маршруты для поддержания связи.

**Таблица маршрутизации:**

Таблица маршрутизации содержит информацию, на основе которой маршрутизатор принимает решение о дальнейшей пересылке пакетов. Таблица состоит из записей — маршрутов, в каждой из которых указаны:

* Сетевой адрес и маска — идентифицируют сеть или узел назначения;
* Адрес шлюза — следующий маршрутизатор, которому следует передавать пакеты (если пакет отправляется локально, используется адрес интерфейса или 127.0.0.1);
* Интерфейс — сетевой адаптер, через который осуществляется отправка;
* Метрика — числовой приоритет маршрута (чем меньше значение, тем выше приоритет), используемый для выбора оптимального пути.

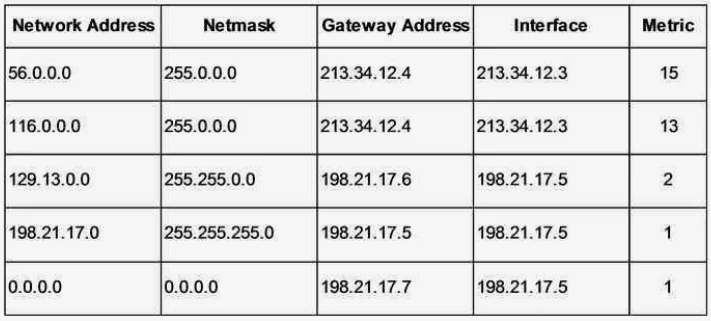


Таблица маршрутизации создается двумя способами:

Статическая маршрутизация — записи этой таблицы вводят и меняют вручную администраторы, что требует его постоянного участия, но остается очень стабильной и не нагружает устройство;

Динамическая маршрутизация — таблицу обновляют автоматически с помощью специальных протоколов (например, RIP, OSPF). Динамическая маршрутизация помогает сети оставаться актуальной и искать лучшие пути, но требует больше ресурсов и может возникать путаница при высокой нестабильности сети.

**Принцип работы маршрутизатора:**

Маршрутизатор получает данные в виде пакетов, смотрит на адрес назначения и с помощью встроенных таблиц маршрутизации выбирает лучший путь, чтобы передать эти данные дальше — например, в другую сеть или интернет. Он постоянно обменивается информацией с другими маршрутизаторами, чтобы знать, какие маршруты доступны и какие из них работают лучше всего, благодаря чему обеспечивает быструю и надежную доставку данных.

# Настройка маршрутизатора

**Конфигурация интерфейсов и назначение IP-адресов:**

Интерфейсы — это сетевые порты маршрутизатора, через которые он подключается к различным сетям. Чтобы маршрутизатор мог обмениваться данными, каждый интерфейс необходимо настроить: назначить IP-адрес и включить его.

Рассмотрим основные шаги для настройки интерфейсов и правильного назначения IP-адресов.

|  |  |
| --- | --- |
| Войти в режим администрирования | enable |
| Перейти в режим глобальной конфигурации | configure terminal |
| Выбрать интерфейс для настройки (например, Ethernet 0/0) | interface Ethernet0/0 |
| Назначить IP-адрес и маску подсети | ip address 192.168.1.1 255.255.255.0 |
| Включить интерфейс | no shutdown |
| Выйти из режима настройки интерфейса и сохраниться | exit  exit  write memory |
| Просмотр статуса интерфейсов и их IP-адресов | show ip interface brief |
| Подробная информация об интерфейсе | show interface Ethernet0/0 |

**Настройка доступа к маршрутизатору и безопасность:**

|  |  |
| --- | --- |
| Конфигурация пароля для доступа к режиму администрирования | |
| Установить пароль для перехода в привилегированный режим | enable secret your\_password |
| Установить пароль для режима конфигурации (консольный доступ) | line console 0  password console\_password  login  exit |
| Установить пароль для удалённого доступа по Telnet | line vty 0 4  password telnet\_password  login  exit |
| Настройка SSH для безопасного удалённого доступа | |
| Задать доменное имя | ip domain-name example.com |
| Сгенерировать RSA-ключи | crypto key generate rsa |
| Включить SSH только для удаленного доступа | line vty 0 4  transport input ssh  login local  exit |
| Создать локальных пользователей с паролями | username admin privilege 15 secret admin\_password |
| Включить аутентификацию пользователей по локальной базе | aaa new-model |

Протоколы маршрутизации

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

Применение протокола маршрутизации позволяет избежать ручного ввода всех допустимых маршрутов, что, в свою очередь, снижает количество ошибок, обеспечивает согласованность действий всех маршрутизаторов в сети и облегчает труд администраторов.

В зависимости от алгоритма маршрутизации протоколы делятся на два вида:

* дистанционно-векторные протоколы (принимают решения на основе информации о расстоянии до сети (DVA));
* протоколы состояния каналов связи (учитывают полную топологию сети (LSA)).

По области применения выделяют протоколы:

* для междоменной маршрутизации (используются для обмена маршрутами между разными автономными системами);
* для внутридоменной маршрутизации (используются внутри одной сети или организации).

- Принцип работы — дистанционно-векторный протокол с максимальным числом хопов 15.

- Применимость — простые и небольшие сети.

- Ограничения — медленное конвергирование, ограниченная масштабируемость.

**Протокол RIP:**

RIP (англ. Routing Information Protocol) — один из самых простых и старых протоколов динамической маршрутизации, основанный на дистанционно-векторном алгоритме. Он использует количество промежуточных маршрутизаторов (хопов) в качестве метрики для выбора пути, при этом максимальное количество хопов ограничено 15, что ограничивает размер сети. RIP широко применяется в небольших и простых сетевых средах с ограниченной топологией.

Преимущества RIP:

* Простота настройки и администрирования;
* Низкие требования к ресурсам маршрутизатора;
* Хорошо подходит для небольших сетей с простой структурой.

Недостатки RIP:

* Медленная конвергенция, что может приводить к временным петлям и несовместимым таблицам маршрутизации;
* Ограничение максимального количества хопов (15), что не даёт работать в больших сетях;
* Отсутствие поддержки VLSM и более сложных метрик, что снижает гибкость маршрутизации.

Принцип работы:

* После включения маршрутизаторы отправляют периодические обновления о своих известных сетях всем соседям каждые 30 секунд;
* Каждый маршрутизатор обновляет таблицу маршрутизации на основе полученных данных, выбирая путь с минимальным числом хопов;
* Это простой и периодический обмен информацией, без построения полной карты сети;
* Конвергенция происходит медленно, особенно при изменениях в топологии.

**Протокол OSPF:**

OSPF (англ. Open Shortest Path First) — протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала и использующий для нахождения кратчайшего пути алгоритм Дейкстры.

OSPF широко используется во внутриорганизационных сетях (внутридоменная маршрутизация), подходит для сетей любого размера — от небольших офисных до больших корпоративных инфраструктур. Он хорошо масштабируется и легко адаптируется к изменяющейся топологии.

OSPF имеет следующие преимущества:

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

Но помимо преимуществ протокол имеет и свои недостатки:

* Сложность настройки и администрирования по сравнению с простыми дистанционно-векторными протоколами;
* Повышенные требования к ресурсам маршрутизатора (память, процессор), особенно в крупных сетях;
* Требует тщательной организации и планирования иерархии областей для эффективной работы.

Принцип работы заключается в следующем:

* После включения маршрутизаторов протокол ищет непосредственно подключенных соседей и устанавливает с ними «дружеские» отношения.
* 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.
* 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.

**Протокол EIGRP:**

EIGRP (англ. Enhanced Interior Gateway Routing Protocol) — протокол динамической маршрутизации, разработанный Cisco, являющийся гибридом между дистанционно-векторными и протоколами состояния каналов. Использует расширенную метрику, учитывающую пропускную способность, задержку, надёжность и загрузку канала. EIGRP подходит для больших и сложных корпоративных сетей, обеспечивая высокую скорость конвергенции и надёжность.

Преимущества EIGRP:

* Быстрая конвергенция благодаря использованию механизмов DUAL (Diffusing Update Algorithm);
* Гибкая и сложная метрика для выбора оптимального маршрута;
* Поддержка VLSM и CIDR;
* Эффективное использование пропускной способности за счёт передачи только изменений (неполные обновления).

Недостатки EIGRP:

* Протокол проприетарный, ограниченный оборудованием Cisco и совместимыми устройствами;
* Сложность настройки по сравнению с RIP;
* Высокие требования к аппаратным ресурсам при крупных сетях.

Принцип работы:

* При запуске маршрутизаторы EIGRP устанавливают соседство с напрямую подключёнными роутерами;
* Обмениваются полными и частичными обновлениями информации о маршрутах;
* Используют алгоритм DUAL для быстрого вычисления оптимальных путей и предотвращения маршрутизаторных петель;
* За счёт поддержки частичных обновлений и отслеживания состояния соседей обеспечивают высокую стабильность и скорость реакции на изменения.

# IP-адресация и трансляция адресов

**IP-адреса:**

IP-адрес (Internet Protocol Address) — уникальный числовой идентификатор устройства в сети, позволяющий ему взаимодействовать с другими устройствами по протоколу IP. IP-адреса бывают двух типов: IPv4 и IPv6.

IPv4 — это 32-битное число, обычно записываемое в виде четырёх чисел от 0 до 255, разделённых точками, например: 192.168.1.1. В IPv4 доступно около 4,3 миллиардов уникальных адресов, но из-за их нехватки был введён IPv6.

IPv6 — это 128-битное число, записываемое в виде восьми групп по четыре шестнадцатеричных символа, например: 2001:0db8:85a3:0000:0000:8a2e:0370:7334. Он решает проблему ограничения IPv4 и обеспечивает значительно больше адресов.

Обмен данными по IP-адресам работает следующим образом. Представим, что человек открывает сайт. Его устройство, например, компьютер, отправляет запрос на IP-адрес сайта через роутеры и серверы. Содержимое страницы сайта возвращается на IP-адрес пользователя. Эти данные поступают не целиком, а по частям — пакетами. Сервер их получает, обрабатывает и отправляет ответные пакеты на IP-адрес пользователя. Его устройство собирает эти пакеты, чтобы отобразить страницу сайта целиком.



**Маска подсети:**

Маска подсети (subnet mask) — это специальный числовой код, который способен определить, к какой сети относится конкретный IP-адрес и какие устройства к ней подключены. Это позволяет эффективно передавать данные: если компьютеры в одной сети, информация идёт напрямую, если в разных — через маршрутизатор. Кроме того, маски позволяют делить большие сети на более мелкие. Это помогает управлять трафиком и повышать безопасность его передачи.  
  
Маска подсети похожа на IP-адрес и разделяет его на составляющие:

* Сетевой адрес — определяет, в какой сети расположен компьютер;
* Адрес узла — индивидуальный номер устройства в сети.



**NAT (Network Address Translation):**

NAT (Network Address Translation) — преобразование частных IP-адресов в публичные для выхода устройств локальной сети в интернет, а также обеспечение безопасности путем скрытия внутренней сетевой структуры.

Существует несколько типов NAT, рассмотрим основные из них:

* Статический NAT — сопоставление одного частного IP-адреса с одним публичным адресом постоянно;
* Динамический NAT — сопоставление частных адресов с одним из пула публичных адресов по мере необходимости;
* PAT (Port Address Translation) — множественные частные адреса используют один публичный IP-адрес, различаясь по номерам портов (также известен как NAT overload).

Когда устройство внутри локальной сети инициирует соединение с интернетом, NAT заменяет его частный IP-адрес на публичный IP-адрес маршрутизатора. Это позволяет дефицитным публичным IP-адресам использоваться более эффективно.

Роутер ведет таблицу соответствий между внутренними приватными IP-адресами и внешними публичными IP-адресами, тем самым обеспечивая правильное направление ответных пакетов обратно к нужному устройству внутри сети. Это защищает локальные устройства от прямого доступа из внешней сети, так как внешний компьютер не видит их непосредственные адреса.

Использование перенаправления портов и NAT позволяет балансировать между защитой локальной сети от внешних угроз и возможностью предоставления доступных Интернет-сервисов.

Существуют также преимущества и недостатки преобразования NAT. К преимуществам можно отнести:

* экономию публичных IP-адресов за счёт использования одного адреса для множества внутренних устройств;
* повышение безопасности благодаря скрытию внутренних IP-адресов от внешней сети;
* возможность подключения большого числа устройств при ограниченном пуле публичных адресов.

К недостаткам преобразования NAT относятся:

* осложнение работы некоторых протоколов и приложений, которые зависят от исходных IP-адресов или используют динамические порты (например, VoIP, онлайн-игры);
* дополнительная нагрузка на маршрутизатор;
* нарушение принципа прозрачной адресации, что может затруднять организацию некоторых сетевых сервисов, таких как VPN или peer-to-peer соединения.