Основы маршрутизации

Определение оптимального пути между сетями и пересылка IP-пакетов через цепочку промежуточных узлов.

L3 OSI (Сетевой уровень)

IP отправителя и получателя неизменны на всём пути (без NAT)

L2 кадры (Канальный уровень)

MAC-адреса перезаписываются роутером на каждом участке пути

СХЕМА ПУТИ IP-ПАКЕТА МЕЖДУ СЕТЯМИ



Основные устройства маршрутизации

Кто участвует в пересылке пакетов между сетями и чем роутер отличается от обычного коммутатора.

R — Маршрутизатор (Router)

Главное устройство на границе разных сетей. Анализирует IP-адрес получателя и выбирает маршрут по таблице.

L3 — L3-коммутатор

Внешне похож на обычный свитч, но маршрутизирует аппаратно на огромной скорости. Основа корпоративных сетей.

PC — Конечный хост

Сравнивает IP цели со своей маской подсети. Если адрес «чужой» — шлёт пакет на шлюз по умолчанию (Default Gateway).

КЛЮЧЕВОЕ ОТЛИЧИЕ: L2-КОММУТАТОР VS РОУТЕР (L3)

L2-коммутатор (Switch)

- Работает строго внутри одной локальной сети (LAN).
- Строит таблицу MAC-адресов портов.
- Не заглядывает внутрь IP-пакета и не меняет кадр.

VS

Роутер (L3-устройство)

- Связывает разные сети между собой.
- Снимает старый заголовок Ethernet, смотрит IP назначения.
- Выбирает выходной порт и пакует пакет в новый L2-кадр.

Таблица маршрутизации: разбор полей

Хранится в оперативной памяти (RAM) для поиска маршрута за микросекунды.

Код	Префикс сети	[AD / Метрика]	Next Hop (via)	Выходной порт
C	192.168.1.0/24	[0 / 0]	Directly connected	GigabitEthernet0/0
S	10.50.0.0/16	[1 / 0]	via 192.168.1.2	GigabitEthernet0/0
R	172.16.0.0/16	[120 / 2]	via 192.168.1.5	GigabitEthernet0/1

Коды источника

C — прямая сеть
S — статика (вручную)
R / O / B — RIP, OSPF, BGP

AD (1-е число)

Степень доверия к источнику.
Меньше = лучше:
Static 1, OSPF 110, RIP 120

Метрика (2-е число)

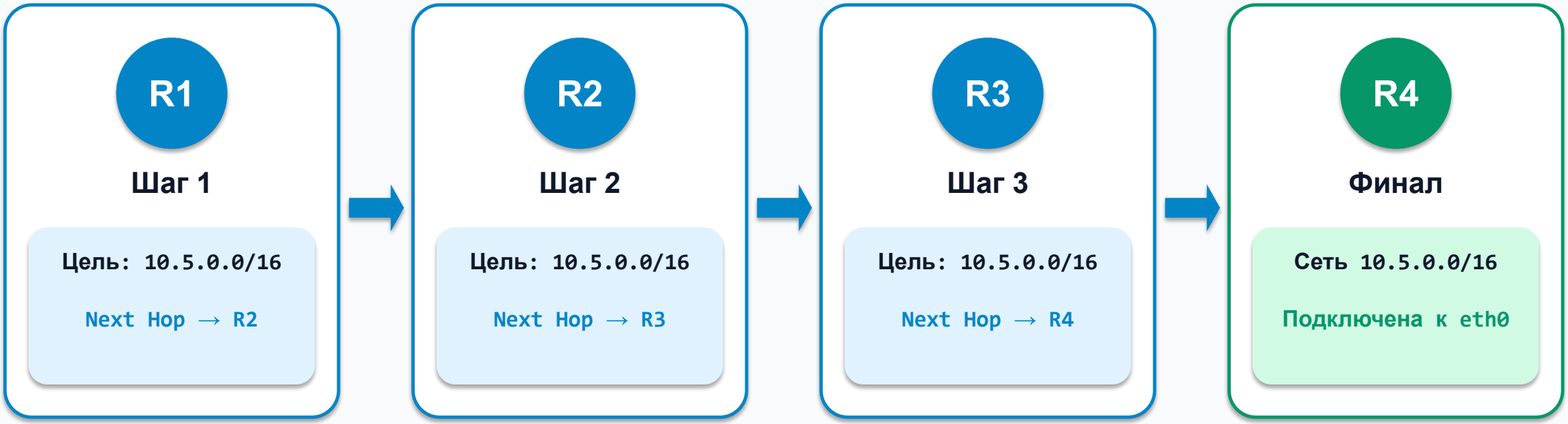
«Цена» пути внутри одного протокола: число прыжков, задержка или скорость.

Если нет совпадений

Роутер удаляет пакет и шлёт отправителю ICMP «Destination Unreachable».

Принцип пересылки Hop by Hop

Ни один роутер не хранит весь путь целиком — каждый знает только свой следующий шаг (Next Hop).



Преимущество «прыжок за прыжком»: компактные таблицы маршрутизации и полная независимость узлов — при аварии на другом конце интернета вашему роутеру не нужно перестраиваться.

Longest Prefix Match и маршрут 0.0.0.0/0

Если пакет подходит под несколько записей, всегда побеждает запись с самой длинной маской.

Записи в таблице роутера

1. `10.0.0.0/8` — 8 бит
2. `10.1.0.0/16` — 16 бит
3. `10.1.2.0/24` — 24 бита
4. `0.0.0.0/0` — 0 бит (Default)

Золотое правило: длина маски важнее метрики и административной дистанции (AD).

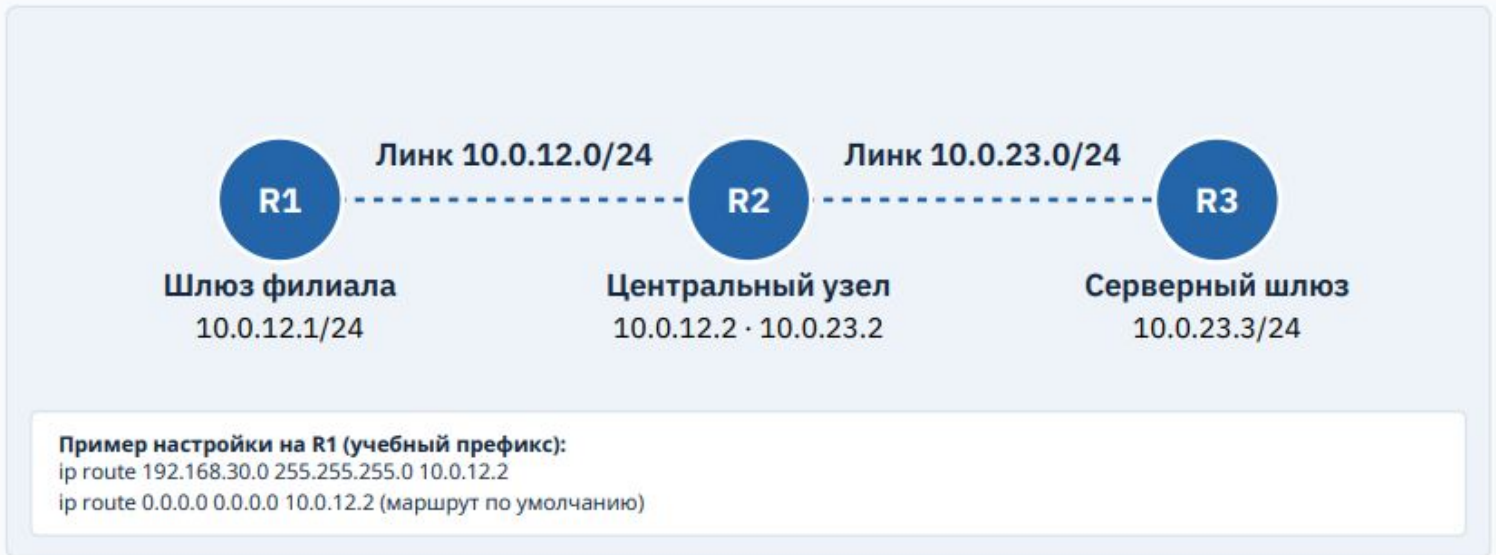
IP-адрес пакета	Подходят	Выбор (Победитель)
10.1.2.5	/8, /16, /24	**10.1.2.0/24 (24 бита)**
10.1.3.7	/8, /16	**10.1.0.0/16 (16 бит)**
10.9.9.9	только /8	**10.0.0.0/8 (8 бит)**
8.8.8.8 (DNS)	нет точных	**0.0.0.0/0 (Шлюз провайдера)**

Статическая маршрутизация: суть и применение

РУЧНОЕ УПРАВЛЕНИЕ ТРАФИКОМ

Администратор вручную вносит в таблицу маршрутизации каждого узла целевые префиксы и адреса следующего перехода (next-hop).

Оптимален для тупиковых (stub) сегментов, небольших офисных сетей, маршрута по умолчанию (0.0.0.0/0) и плавающего резервирования (floating static route).



Пример настройки на R1 (учебный префикс):
ip route 192.168.30.0 255.255.255.0 10.0.12.2
ip route 0.0.0.0 0.0.0.0 10.0.12.2 (маршрут по умолчанию)



Плюсы и минусы статической маршрутизации

ПРЕИМУЩЕСТВА · КОНТРОЛЬ

Сильные стороны

Полный контроль и предсказуемость: трафик строго следует назначенному администратором интерфейсу или шлюзу.
Отсутствие служебного обмена: маршрутизаторы не отправляют периодические анонсы и обновления в канал связи.
Экономия ресурсов: процессор и оперативная память узла освобождены от вычислений метрик и построения топологических графов.
Информационная безопасность: топология внутренней сети не раскрывается соседним устройствам через сетевые протоколы.

ОГРАНИЧЕНИЯ · ЭКСПЛУАТАЦИЯ

Слабые стороны и риски

Сложность масштабирования: добавление новой подсети требует ручной переконфигурации каждого маршрутизатора в тракте.
Высокий риск человеческой ошибки: опечатка в маске или адресе next-hop может вызвать блэкхол или постоянную петлю передачи.
Отсутствие автоадаптации: при физическом отказе промежуточного транзита маршрут не перестраивается без IP SLA или BFD.
Высокие эксплуатационные затраты: регулярное сопровождение распределённых схем требует непрерывного ручного аудита таблиц.

Динамическая маршрутизация

Роутеры сами строят и проверяют таблицы маршрутизации, рассылая соседям Hello-пакеты и анонсы сетей.

Корпоративные сети

Десятки филиалов и сотни узлов — ручная настройка невозможна.

Провайдеры и ЦОД

Постоянно меняющаяся топология и сотни новых подсетей.

Резервирование каналов

Автоматическое переключение трафика при обрыве основного кабеля.

Глобальный Интернет

Вся связность мирового масштаба держится на динамике.



Плюсы и минусы динамической маршрутизации

Мы платим ресурсами процессора и сложностью настройки за отказоустойчивость и автоматизацию.

✓ Преимущества

Автоматизация

Не нужно вручную прописывать маршруты на сотнях роутеров.

Быстрая сходимость

Автоматический пересчёт обходного пути за секунды при аварии.

Масштабируемость

Лёгкий рост сети до тысяч узлов и десятков филиалов.

Балансировка (ECMP)

Деление трафика поровну между равнозначными каналами.

✕ Недостатки (Плата)

Нагрузка на железо

Расчёт топологии требует мощного CPU и оперативной памяти.

Служебный трафик

Hello-пакеты и обновления постоянно занимают часть канала.

Сложность диагностики

Ошибка в фильтрах маршрутов может «положить» всю сеть.

Риски безопасности

Фейковые анонсы перехватывают трафик — нужна криптоаутентификация.

IGP, EGP и метрики маршрутизации

ИЕРАРХИЯ ПРОТОКОЛОВ И ВЫБОР ПУТИ

IGP (Interior Gateway Protocol): работа внутри одной автономной системы (AS) для достижения максимальной скорости сходимости.

EGP (Exterior Gateway Protocol / BGP): обмен префиксами между независимыми AS с применением маршрутных политик.



RIP (Routing Information Protocol): число хопов (hop count, максимум 15).

OSPF (Open Shortest Path First): стоимость (cost), обратно пропорциональная пропускной способности.

EIGRP: составная метрика (composite metric) с учётом пропускной способности (bandwidth) и суммарной задержки (delay).

Made with GAMMA

Три класса протоколов маршрутизации

Сравнительная характеристика алгоритмов распространения и представления топологии

Класс алгоритма	Что передаётся соседям	Представление о топологии	Характерные примеры
Distance Vector (дистанционно-векторный)	Вектор расстояний: сети и дистанции до них от соседа	«Маршрутизация по слухам»: только следующий узел и расстояние	**RIP v1/v2**, RIPng
Link-State (состояние связей)	Объявления о состоянии собственных каналов (LSA)	Полная карта области (LSDB) у каждого узла	**OSPF v2/v3**, **IS-IS**
Path Vector (вектор пути)	Префиксы сетей с полным списком автономных систем (AS-Path)	Граф взаимосвязи автономных систем и политики передачи	**BGP-4** (Border Gateway Protocol)

DV: ОБМЕН ТАБЛИЦАМИ

R1 передаёт R2: «Знаю сеть N с метрикой 1»; R2 наращивает метрику до 2 и верит R1.

LINK-STATE: КАРТА СВЯЗЕЙ

Узел описывает интерфейсы и рассылает копии всем; LSDB идентична.

PATH VECTOR: СПИСОК AS

Фильтрация петель: если собственная AS уже в AS-Path, маршрут отбрасывается.

Дистанционно-векторные протоколы (DVA)

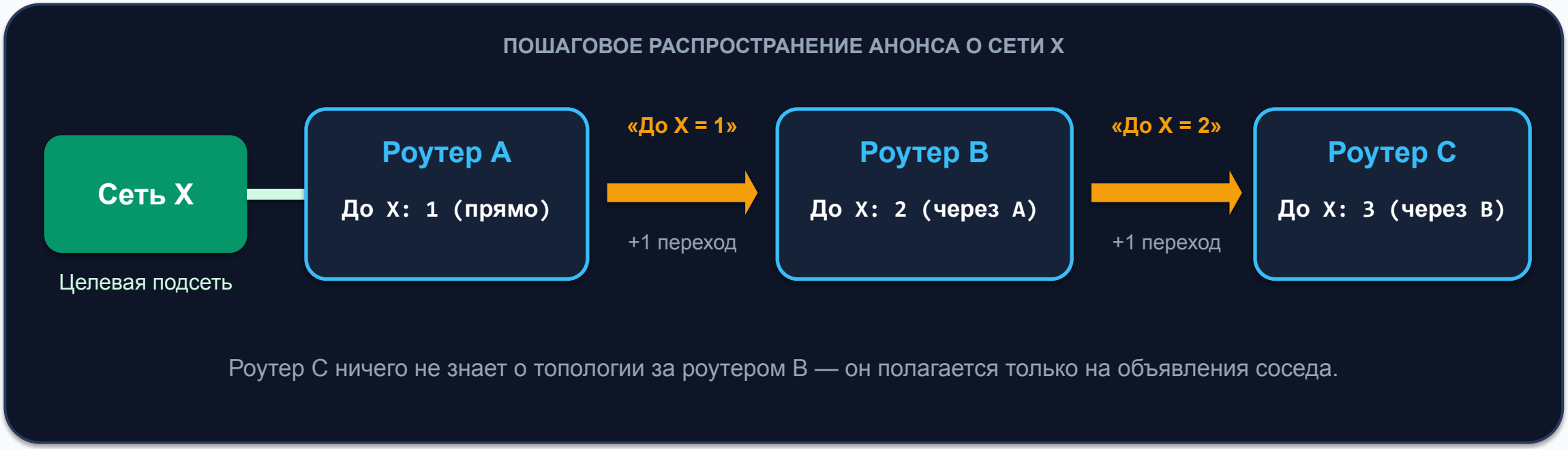
Роутер не видит всю карту сети целиком — он верит на слово своим непосредственным соседям.

Дистанция (Distance)

Насколько далеко целевая сеть (чаще всего — число переходов / роутеров).

Вектор (Vector)

В какую сторону идти — через какой интерфейс или какого соседа слать пакет.



Роутер C ничего не знает о топологии за роутером B — он полагается только на объявления соседа.

Протокол RIP: параметры и особенности

Классический представитель дистанционно-векторных протоколов (RIPv1, RIPv2, RIPng для IPv6).

15 шагов

Максимум переходов
(16 = сеть недостижима)

30 сек

Периодическая рассылка
всей таблицы целиком

UDP 520

Транспортный протокол
и номер порта

224.0.0.9

Мультикаст, VLSM и auth
в RIPv2 (IPv6 в RIPng)

✓ Преимущества RIP

- Настройка в 3 строки: быстрый старт для малых сетей.
- Экономия ресурсов: работает на самых слабых роутерах.
- Прозрачная логика: идеально для обучения и отладки.

✕ Недостатки и ограничения

- Медленная сходимость: 30 сек на каждый узел при сбое.
- Слепая метрика: 1 медленный модем «лучше» 2 гигабитных линий.
- Малый масштаб и петли: потолок 15 узлов и счёт до 16.

Петли маршрутизации и 5 механизмов защиты

При обрыве связи роутеры могут начать бесконечно пересылать пакеты по кругу, наращивая метрику.



Пакеты кружат между A и B до исчерпания TTL, пока метрика не достигнет 16.

1 Максимум метрики (16)

Искусственный потолок останавливает бесконечный счёт на 16 шагах.

2 Split Horizon

Расщепление горизонта: не анонсировать маршрут обратно его источнику.

3 Poison Reverse

Обратное отравление: слать обратно маршрут с метрикой 16 (недостижим).

4 Triggered Updates (Триггерные обновления)

При сбое роутер экстренно сообщает соседям сразу, не дожидаясь планового таймера в 30 секунд.

5 Hold-down Timer (Таймер удержания — 180 с)

После падения маршрута роутер замораживает запись на 180 сек и игнорирует ложные слухи о его доступности.

LSA и формирование карты сети

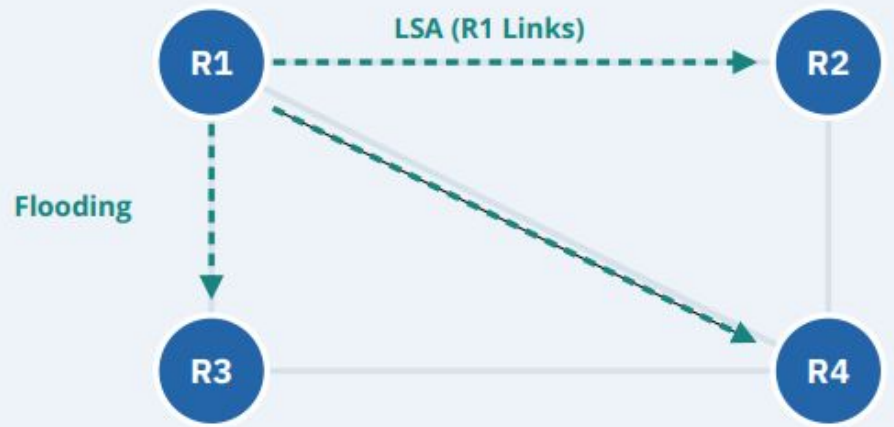
МЕХАНИЗМ LINK-STATE ADVERTISEMENT

В протоколах состояния связей (OSPF) каждый маршрутизатор генерирует **LSA** — формализованное сообщение о своих интерфейсах, IP-подсетях и стоимости подключений.

Лавинная рассылка (Flooding): полученный LSA ретранслируется всем соседям без изменений в пределах зоны.

БАЗА ДАННЫХ LSDB

После завершения синхронизации все маршрутизаторы внутри одной области обладают **идентичной базой LSDB** (Link-State Database) — единым слепком топологии.



Результат лавинной рассылки:
Каждый роутер сохраняет поступившие LSA в локальное хранилище. На узлах R1, R2, R3, R4 формируется идентичная топологическая база LSDB в пределах одной OSPF-зоны.

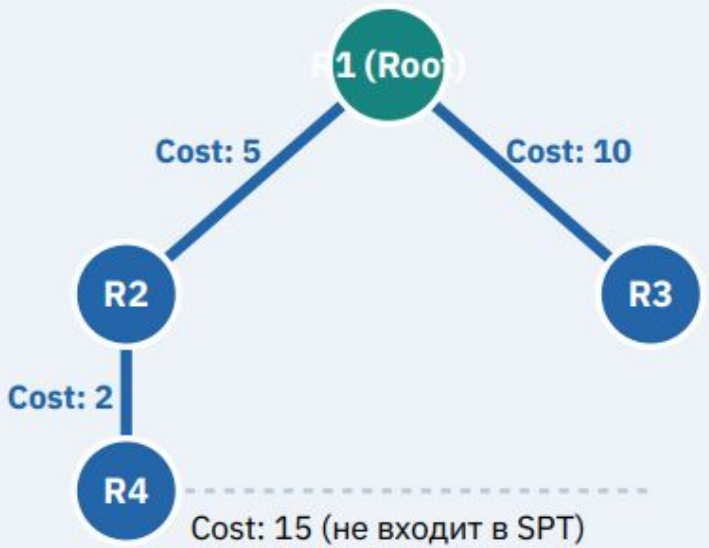
Алгоритм Дейкстры строит дерево кратчайших путей

РАСЧЁТ МАРШРУТОВ ИЗ LSDB

Имея полную топологическую карту, каждый маршрутизатор запускает алгоритм **SPF (Shortest Path First) Дейкстры**, помещая себя в корень дерева (root):

1. **Итеративный расчёт:** на каждом шаге выбирается узел с наименьшей накопленной стоимостью (metric/cost).
2. **Дерево кратчайших путей (SPT):** формируется ациклический граф оптимальных маршрутов от корня до всех известных сетей.
3. **Запись в RIB:** наилучшие пути к префиксам передаются в общую таблицу маршрутизации.

Масштабирование достигается делением сети на области (Areas): внутри зоны расчёт детализирован, между зонами передаются суммарные векторы.



Итог расчёта SPT для R1: До R4 выбран путь через R2 (стоимость 5+2=7), а не прямой линк R3–R4 (стоимость была бы 10+15=25).

Автономные системы (AS) и протокол BGP-4

Интернет — это десятки тысяч независимых сетей (AS), связанных единым протоколом внешней маршрутизации.



32-бит ASN (IANA)

Единое техническое управление: IGP (OSPF/RIP) внутри сети, BGP (EGP) на границах между AS.

Бизнес-политики (TCP 179)

Path Vector: выбор выгодного пути, а не просто кратчайшего, через LOCAL_PREF, MED, NEXT_HOP и AS_PATH.

Full View и защита RPKI

Около 1 млн IPv4-префиксов в глобальной таблице. Криптосертификаты RPKI защищают от BGP Hijacking.

Control Plane и Data Plane

АРХИТЕКТУРА СОВРЕМЕННОГО МАРШРУТИЗАТОРА

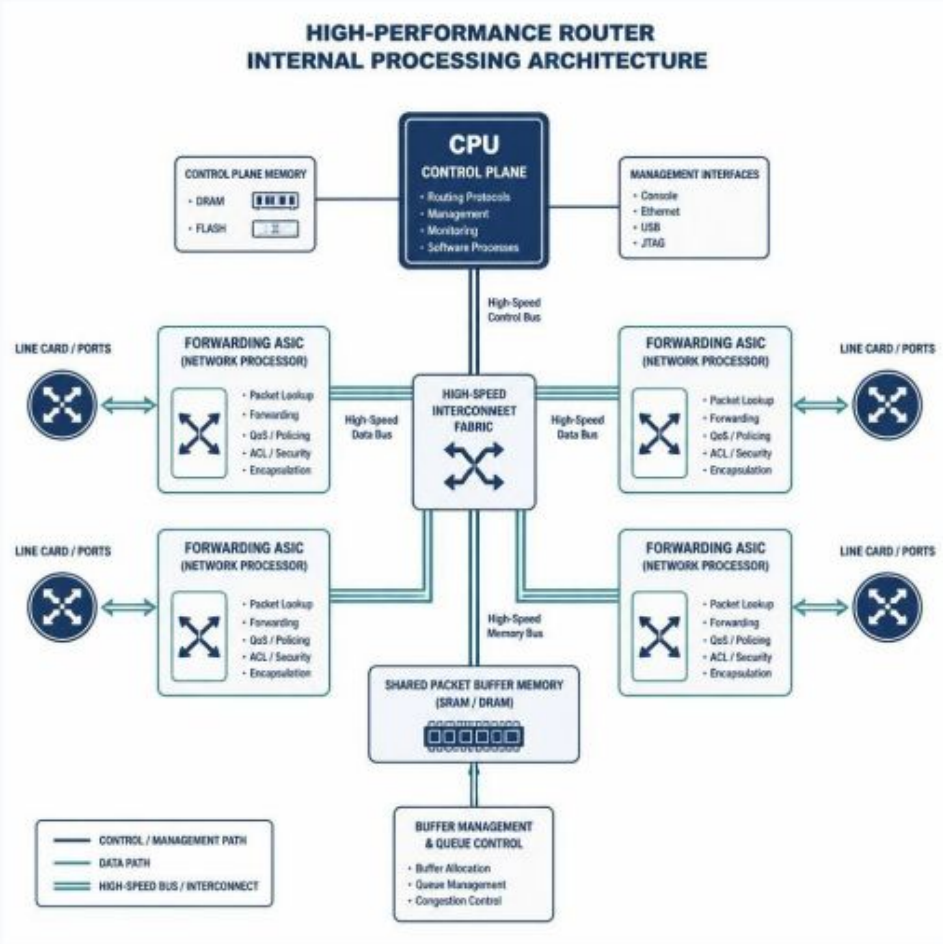
ПЛОСКОСТЬ УПРАВЛЕНИЯ · CONTROL PLANE

Интеллектуальная часть роутера. Выполняет протоколы (OSPF, BGP), строит базу **RIB** (Routing Information Base). Принимает решения о выборе лучших путей на уровне центрального процессора (CPU).

ПЛОСКОСТЬ ДАННЫХ · DATA PLANE (FORWARDING)

Исполнительная часть. Содержит **FIB** (Forwarding Information Base) — оптимизированную копию RIB. Обеспечивает продвижение транзитных пакетов между входными и выходными интерфейсами на линейной скорости портов.

На высокопроизводительных платформах FIB загружается в специализированные микросхемы ASIC и память TCAM, обеспечивая аппаратный поиск по префиксу за константное время.



Путь пакета от источника к получателю

Пошаговое продвижение IP-пакета через транзитные маршрутизаторы без NAT



Сегмент 1: ПК → R1

IP: 192.168.1.10 → 10.0.0.5
MAC: aaaa.aaaa → r111.1111

Сегмент 2: R1 → R2

IP: 192.168.1.10 → 10.0.0.5
MAC: r122.2222 → r211.1111

Сегмент 3: R2 → Сервер

IP: 192.168.1.10 → 10.0.0.5
MAC: r222.2222 → srv3.3333

IP-адреса источника и назначения сохраняются · L2 MAC-заголовки переписываются на каждом транзите

1. Шлюз. ПК сверяет маску: цель вне локальной сети, кадр идёт на MAC шлюза R1.

2. Проверка TTL. R1 деинкапсулирует L2, проверяет TTL: если TTL > 1, уменьшает на единицу и пересчитывает CRC.

3. Поиск в FIB. Маршрутизатор ищет самый длинный совпадающий префикс (LPM) и определяет выходной порт.

4. Переупаковка. Через ARP находится MAC next-hop, пакет инкапсулируется в новый Ethernet-кадр.