

Курс «Администратор Linux»

Маршрутизация в сетях IPv4

Занятие # 23

Алексей Цыкунов
Александр Румянцев



- Кто такие агрегаты
- Куда ведет blackhole
- Как можно роутить с помощью loopback
- Что такое multicast
- Что такое динамический роутинг
- Как работает OSPF
- Как настраивается quagga
- Зачем нужен BGP

Рекомендуемая схема нумерации для сетей

10 . 1 . 32 . 0 / 23

geo-id #1 vlan #132

Кстати, VLANы лучше нумеровать кратно 4 или для наглядности, кратно 10 - с учетом возможного расширения сети и geo-id

Агрегат - минимально возможная сеть включающая в себя все специфики

10.0.0.0/13 - Агрегат

10.1.0.0/16 - Специфик

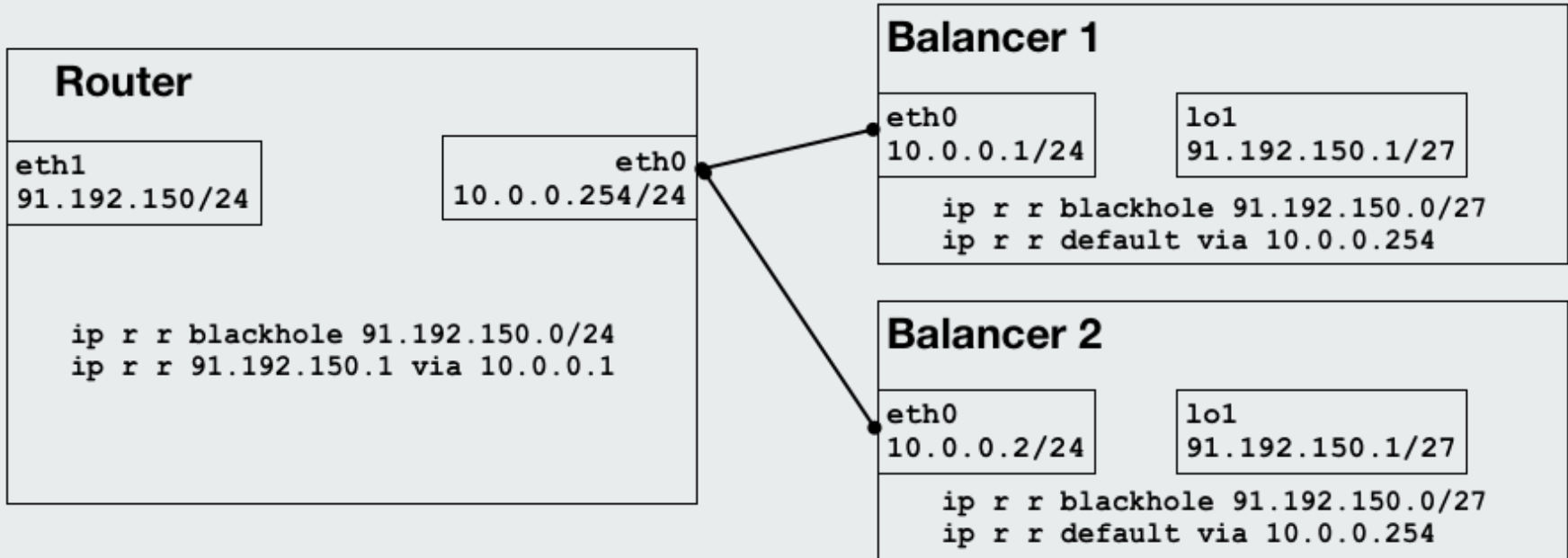
10.2.0.0/16 - Специфик

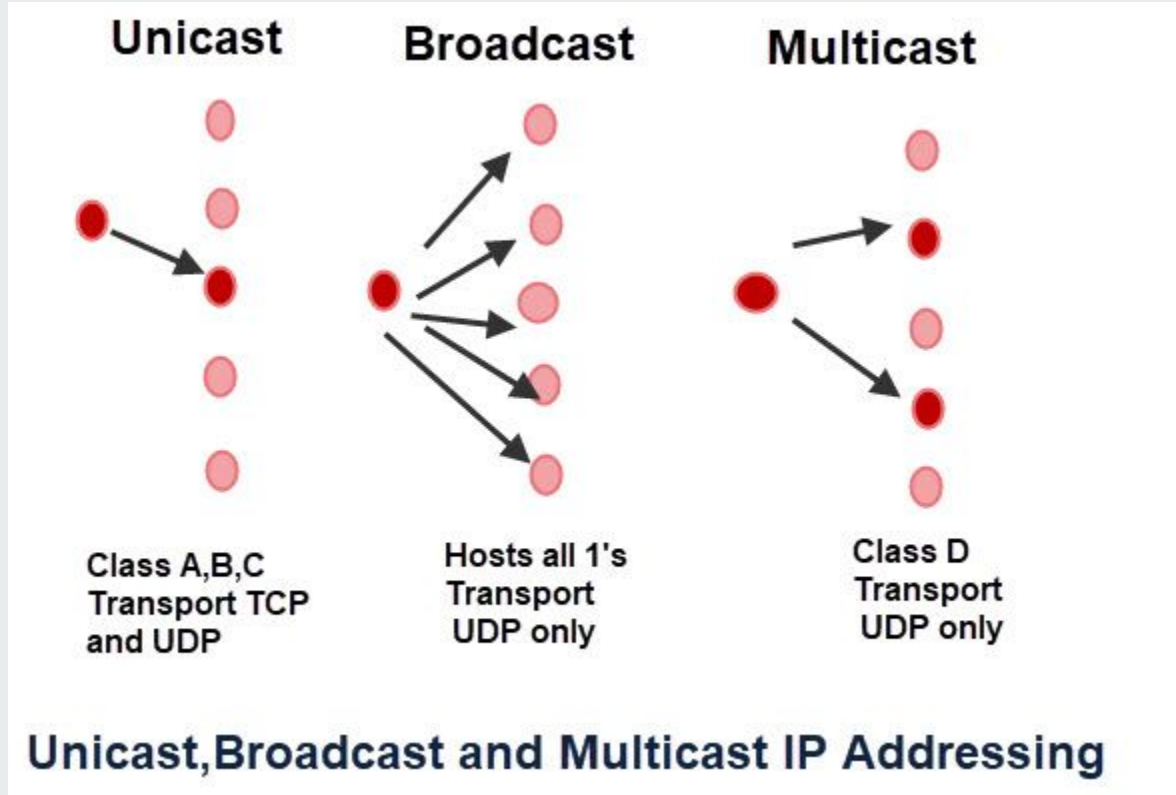
10.6.20.0/22 - Специфик

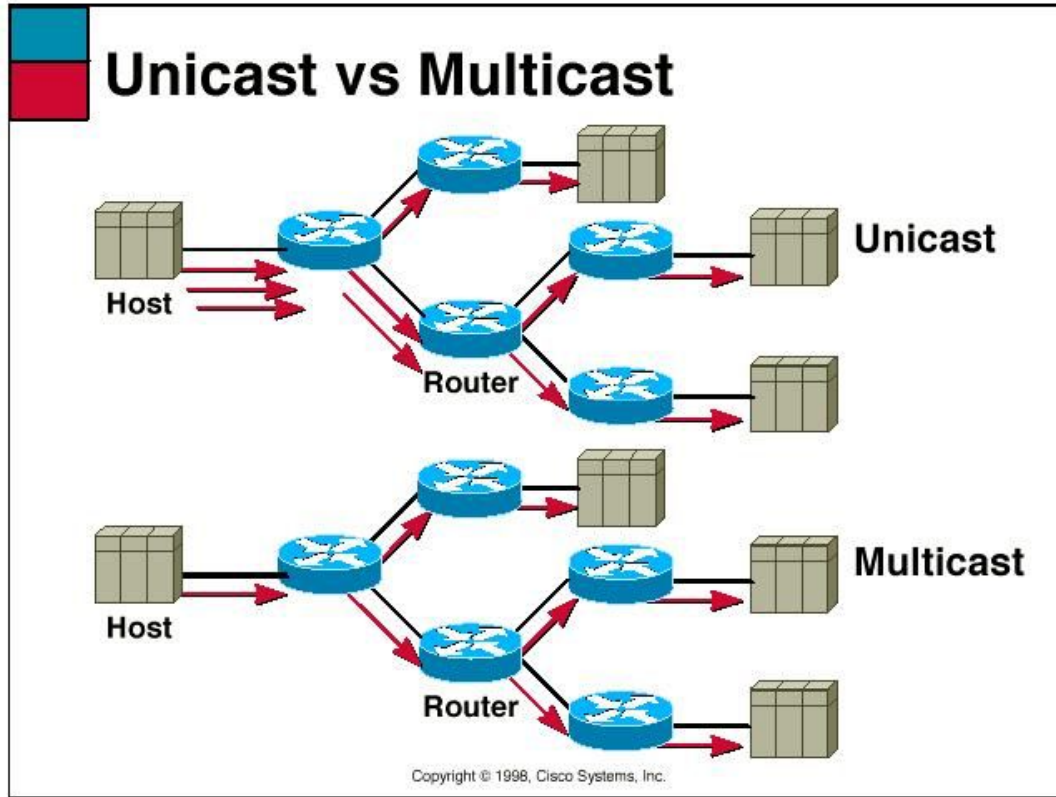
Агрегаты всегда должны "заворачиваться в null", что бы избежать проблем с кольцами, бродкастами и мусорным трафиком в маршрутизации

```
ip route add blackhole 10/8
```

Кроме того, null routing - самый дешевый способ фильтрации трафика







- Только UDP
- 224.0.0.0/4 (224.0.0.1 - 239.255.255.255)
- Группа - конкретный IP из данной подсети
 - Например - 224.0.2.1
- Для того чтобы принимать сообщения надо быть членом группы
- Для того чтобы отсылать сообщения не обязательно быть членом группы

- **Reserved Link-Local Addresses**
 - **224.0.0.0 – 224.0.0.255**
 - **Transmitted with TTL = 1**
 - **Examples:**
 - **224.0.0.1** **All systems on this subnet**
 - **224.0.0.2** **All routers on this subnet**
 - **224.0.0.5** **OSPF routers**
 - **224.0.0.13** **PIMv2 Routers**
 - **224.0.0.22** **IGMPv3**
- **Other Reserved Addresses**
 - **224.0.1.0 – 224.0.1.255**
 - **Not local in scope (Transmitted with TTL > 1)**
 - **Examples:**
 - **224.0.1.1** **NTP Network Time Protocol**
 - **224.0.1.32** **Mtrace routers**
 - **224.0.1.78** **Tibco Multicast1**

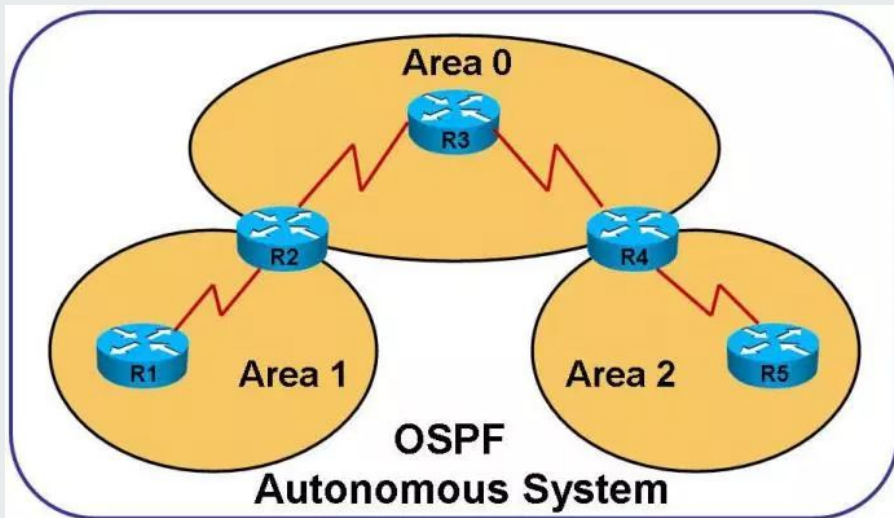
Автоматическое получение маршрутов и возможность их перестроения при изменении топологии

Interior Gateway Protocols

- Open Shortest Path First
- Enhanced Interior Gateway Routing Protocol

Работают на уровне L3, каждый роутер знает всю топологию своей области, отслеживается состояние соединений

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 (Dijkstra's algorithm).



1	HELLO	Обнаружение соседей
2	Database Description (DBD)	Синхронизация базы данных между роутерами
3	Link-State Request (LSR)	Запрос link-state записей
4	Link-State Update (LSU)	Посылка link-state записей
5	Link-State Acknowledgement (LSAck)	Подтверждение о получении

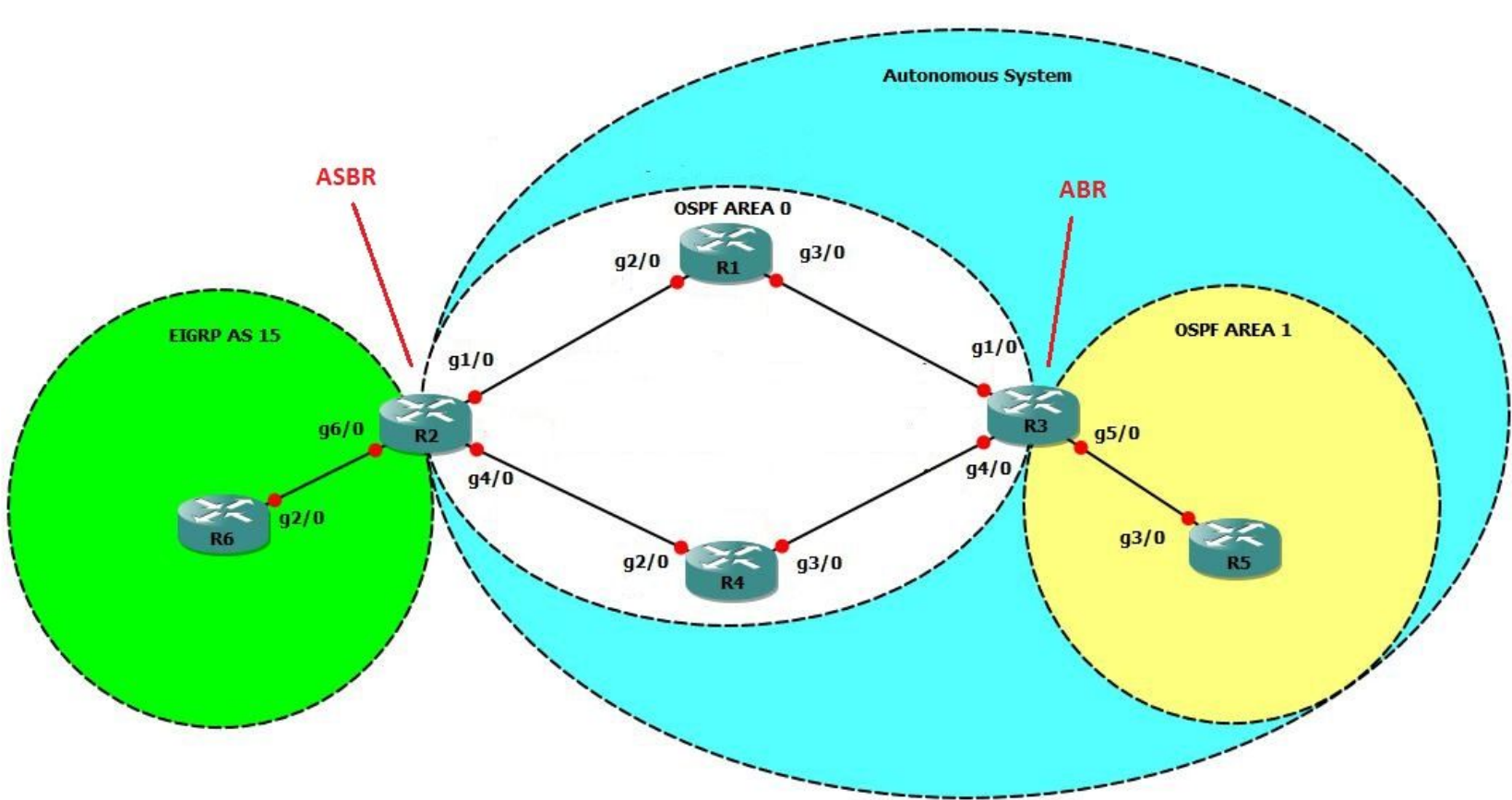
1. **Down:** Соседские отношения не установлены.
2. **Init:** Получен Hello-пакет.
3. **Two-Way:** Роутер увидел свой ID в полученном Hello-пакете.
4. **Exstart:** Определение ролей: Master и Slave.
5. **Exchange:** DBD отправлена.
6. **Loading:** Обмен LSR и LSU.
7. **Full:** Отношения установлены.

1. Обмен HELLO-пакетами
2. Формируется таблица состояний связей с соседями (link-state)
3. Формируют LSA - (router id, neighbor id, net/mask, net type, cost)
4. Маршрутизатор рассылает LSA своим соседям, те распространяют LSA дальше.
5. Каждый маршрутизатор, получивший LSA добавляет его в свою локальную табличку LSDB (Link State Database)
6. В LSDB скапливается информация, обо всех парах соединённых в сети маршрутизаторов
7. После обмена LSA, каждый маршрутизатор знает про все линки, на основании пар строится полная карта сети
8. На основании этой карты каждый маршрутизатор индивидуально ищет кратчайшие с точки зрения метрики маршруты во все сети и добавляет их в таблицу маршрутизации.

- **Link state database (LSDB)** – структура (база) данных для хранения данных топологии OSPF.
- **Shortest Path First (SPF)** – название алгоритма OSPF для анализа **LSDB** и определения лучшего маршрута (с наименьшей стоимостью) для каждого префикса.
- **Link State Update (LSU)** – пакет OSPF, в котором хранится детальная информация о топологии, в частности **LSA**.
- **Link State Advertisement (LSA)** – класс структуры данных OSPF, которых содержит информацию о топологии. **LSA** хранятся в **LSDB** и передаются по сети внутри **LSU**.

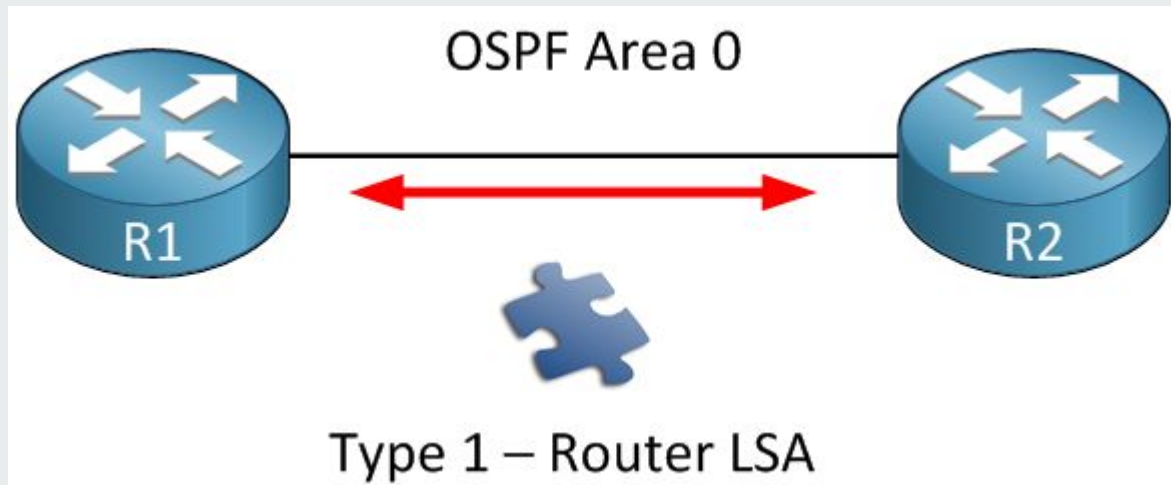
- **Area** — группа маршрутизаторов и их интерфейсов
- **Area Border Router (ABR)** — маршрутизатор, у которого интерфейсы подключены как минимум к двум разным **OSPF Area**, включая **Backbone Area (area 0)**.
- **Autonomous System Border Router (ASBR)** — маршрутизатор, который соединяет 2 или более автономные системы и используется в основном для анонсирования маршрутов из одной автономной системы в другую(-ие).
- **Автономная система** — набор маршрутизаторов под единым административным управлением (например управляемых одним администратором).

- **Backbone router** — маршрутизатор, у которого как минимум один интерфейс находится в **Backbone Area (area 0)**.
- **Internal router** — маршрутизатор, интерфейсы которого находятся только в одной **Area**.
- **Designated Router (DR)** — в multiaccess-сетях (в одной подсети может находиться более 2-ух маршрутизаторов) маршрутизатор, который выбирается среди других маршрутизаторов для генерации LSA, обмена топологиями итд
- **Backup Designated Router (BDR)** — маршрутизатор в multiaccess-сетях, который «наблюдает» за **Designated Router'ом (DR)** и занимает его место в случае, если **Designated Router (DR)** становится недоступным.



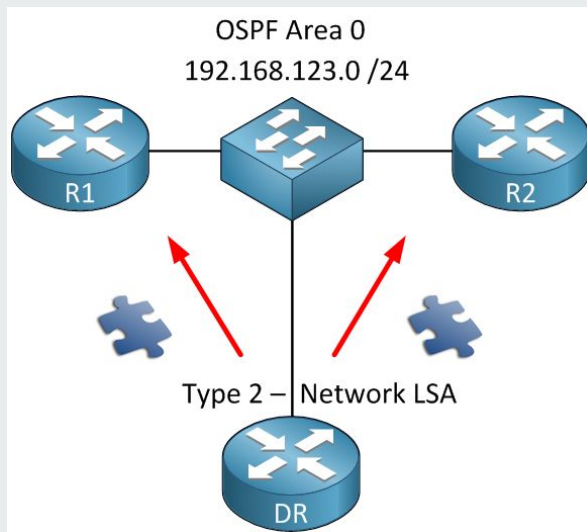
LSA Type 1 – Router LSA

Вещается каждым маршрутизатором только в пределах своей зоны (area). Содержит список напрямую подключенных к роутеру линков. Линк описывается двумя параметрами: IP-префикс на интерфейсе и тип линка

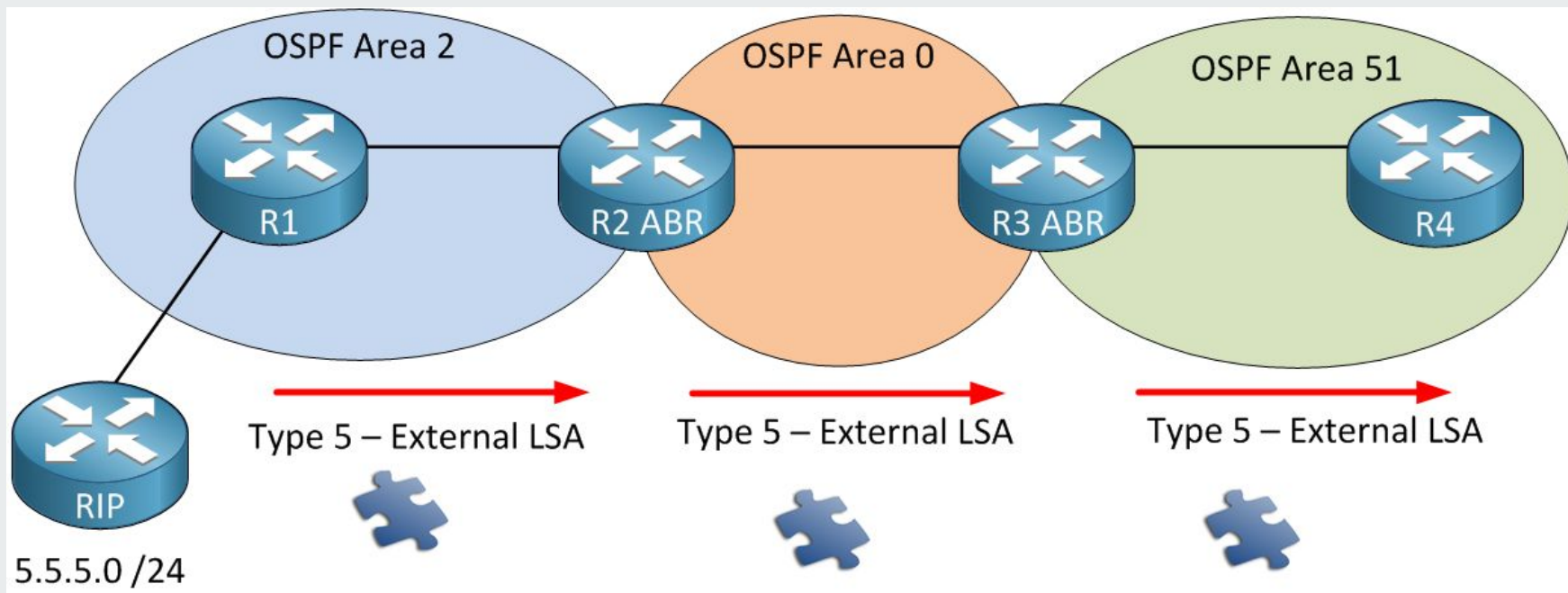


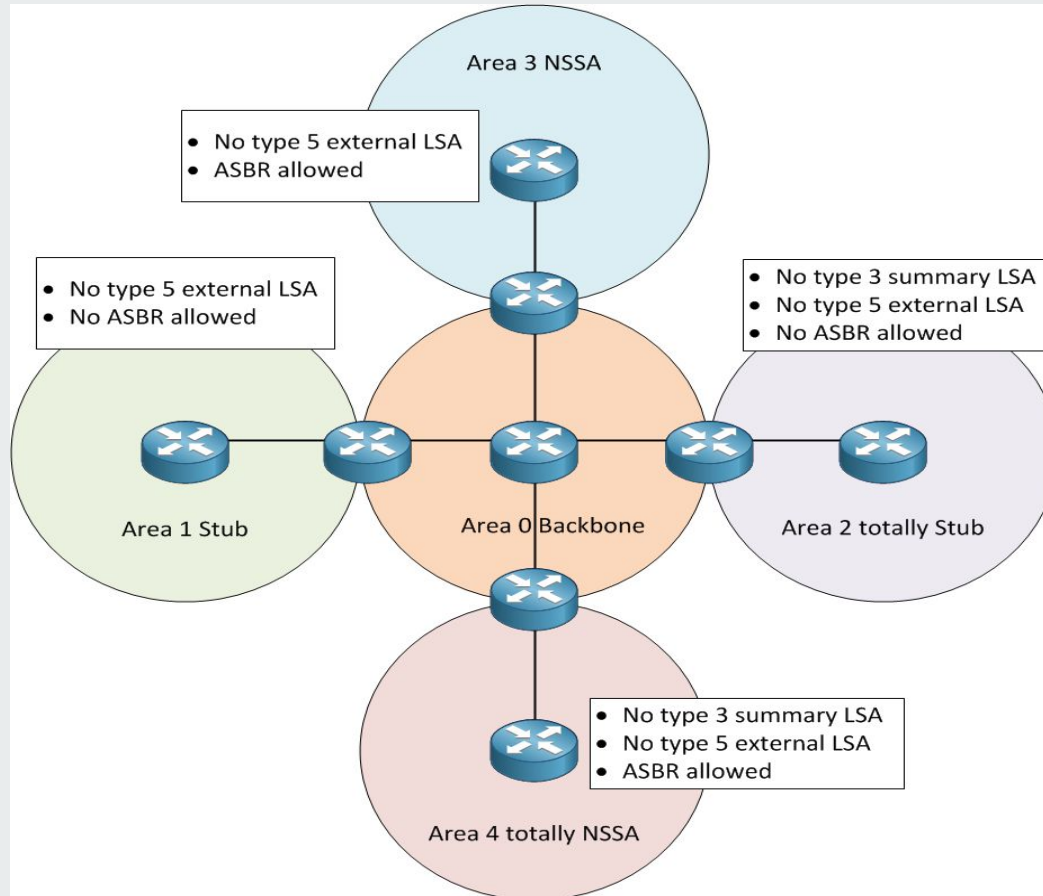
LSA Type 2 – Network LSA

Создана для много-доступных (multi-access) сетей. Генерируется DR'ом. Содержит список всех подключенных к сети маршрутизаторов, идентификатор DR'а, а также адрес и маску сети. Не выходит за пределы зоны, в которой была сгенерирована.



- Type 3 - Summary LSA
- Type 4 - Summary ASBR LSA
- Type 5 - Autonomous system external LSA





- **Backbone - Area 0**
- **Standart**
- **Stub area** – Запрещен ASBR и блокируются все External LSA Type5. Network LSA Type3 разрешены.
- **Not-so-stubby area** – Разрешен ASBR и Network LSA Type3. Блокируются все External LSA Type5.
- **Total Stub area** – Запрещен ASBR и блокируются все External LSA Type5 и Network LSA Type3.
- **Total Not-so-stubby area** – Разрешен ASBR и блокируются все External LSA Type5 и Network LSA Type3.

Из stub area в другие зоны можно попасть по дефолтному маршруту.

Некоторые правила, которые нужно знать при работе со stub и totaly stub зонами:

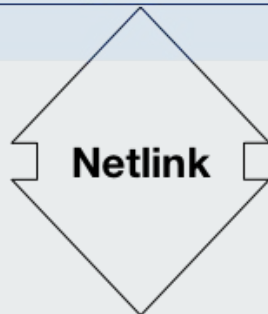
- В зоне должен быть хотя бы один ABR.
- Каждый маршрутизатор должен быть настроен как stub.
- В этих зонах не может быть ASBR.
- Backbone area не может быть stub или totaly stub.

Quagga (ex-Zebra)

Набор демонов,
реализующий
управление
сетью в linux

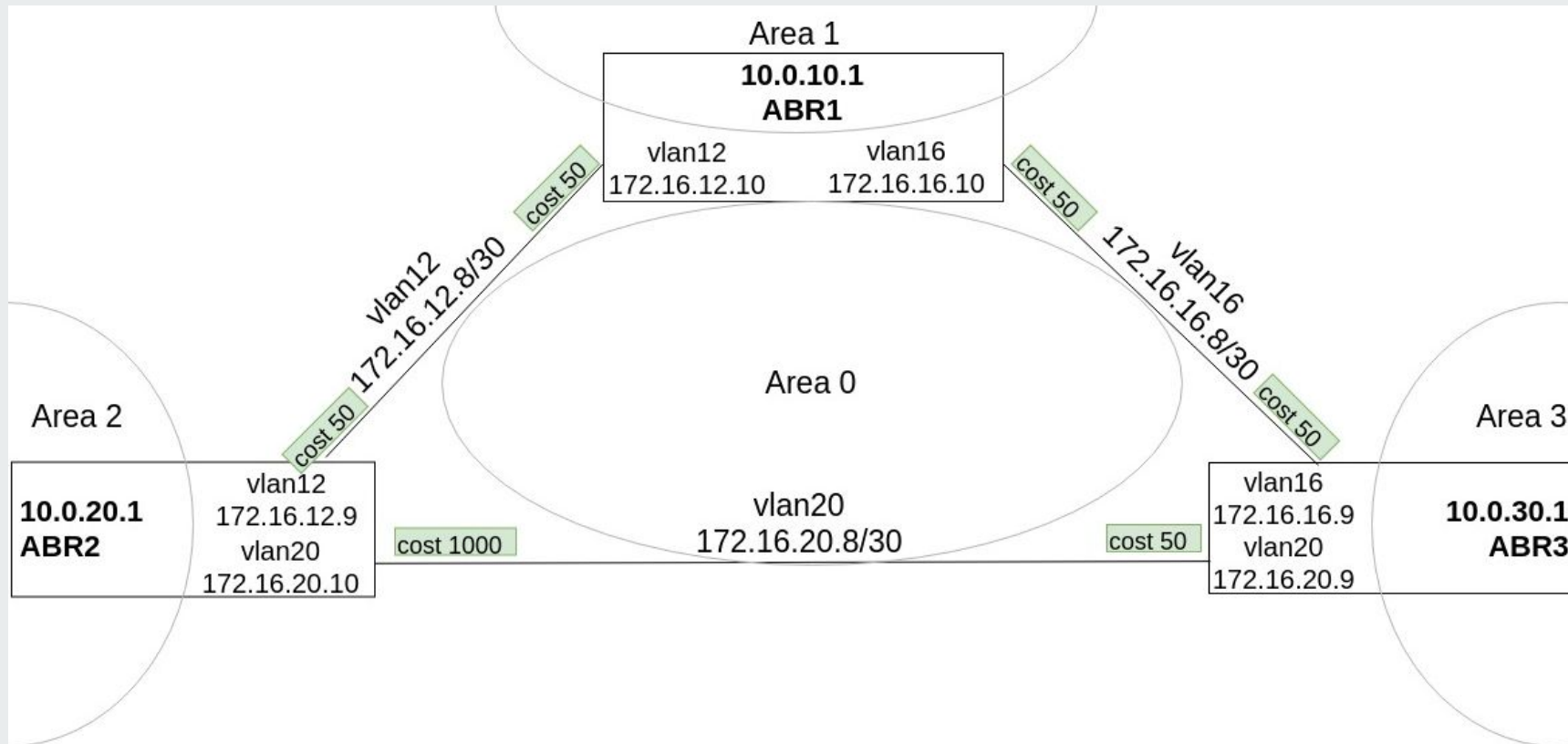


Возможно так же
управление
интерфейсами и
разнообразными
сетевыми настройками



Kernel Routing Table

Полностью копирует
управление и
функциональность
Cisco IOS



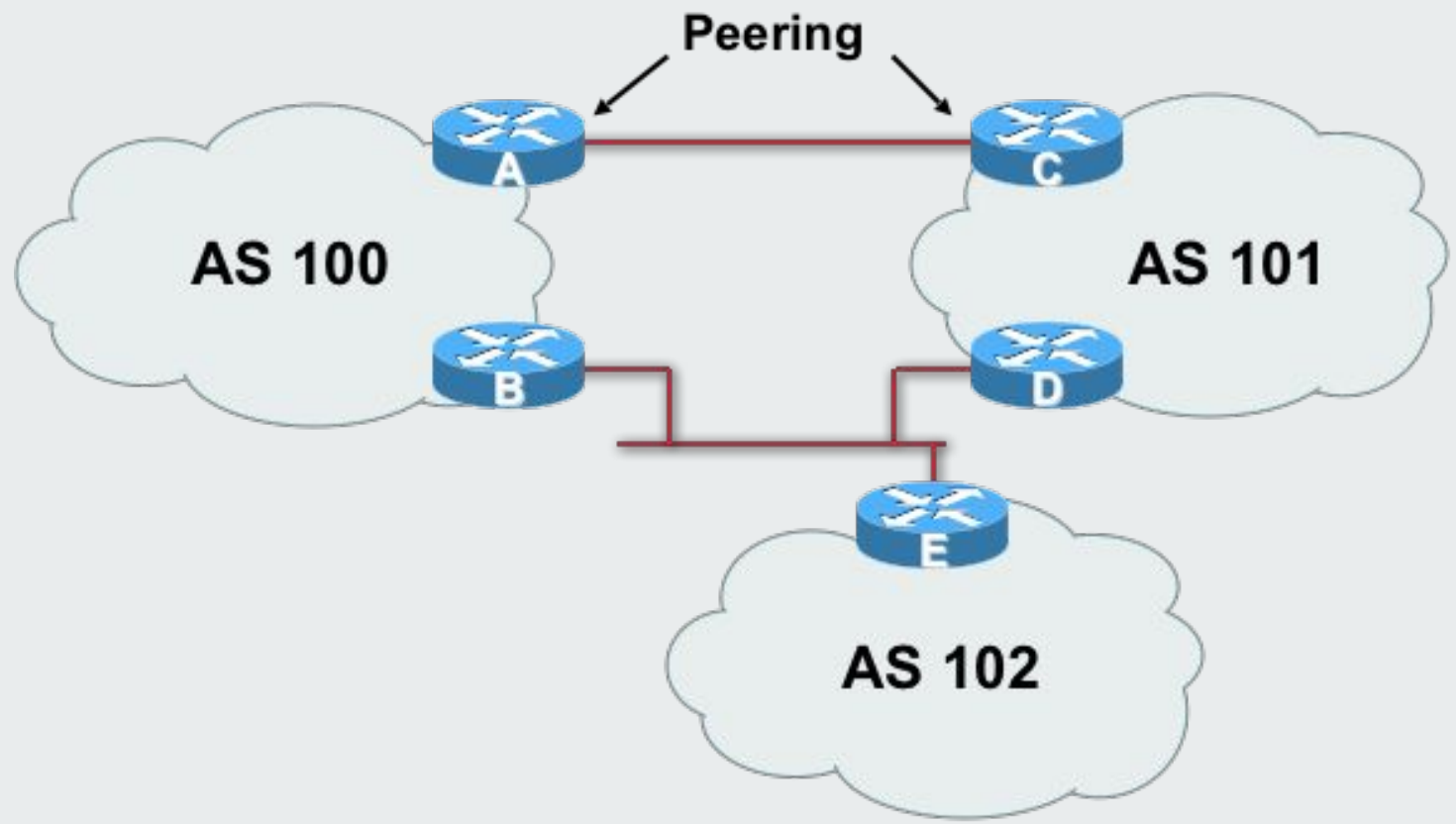
- **Exterior Gateway Protocol**
 - **Border Gateway Protocol**

Работает на уровне L4 (возможно управление маршрутизаторами с отдельно-стоящего BGP Route Server), состояние пиринга определяется по состоянию TCP-сессии. Может использоваться внутри AS/Area

Протокол обмена маршрутной информацией уровня провайдера.
Объединяет т.н. Автономные Системы (Autonomous System, AS)

AS похож на OSPF Area. Подразумевается, что все сети внутри AS так или иначе объединены с помощью IGP

В некоторых случаях BGP может использован внутри AS. Т.к. BGP в основном означает связь с провайдером, то для внутренних связей используют термин iBGP



Автономную систему хорошо иметь для независимости от ДЦ и в случае нескольких ДЦ. Минимальный размер сети, анонсированной через BGP не регламентируется протоколом, но в реальной жизни - /24. Поэтому минимальный размер AS тоже /24. Раньше адреса можно было получить непосредственно у RIPE, теперь ищите LIR, у которых еще остались блоки адресов.

Спасибо за внимание

Алексей Цыкунов

