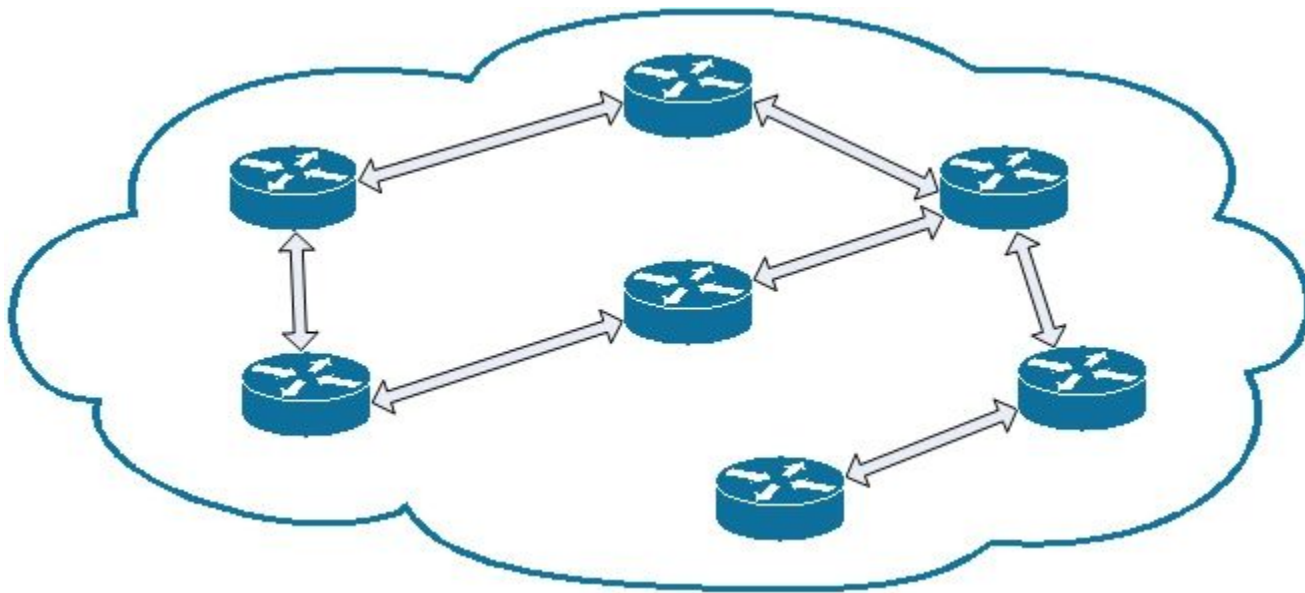


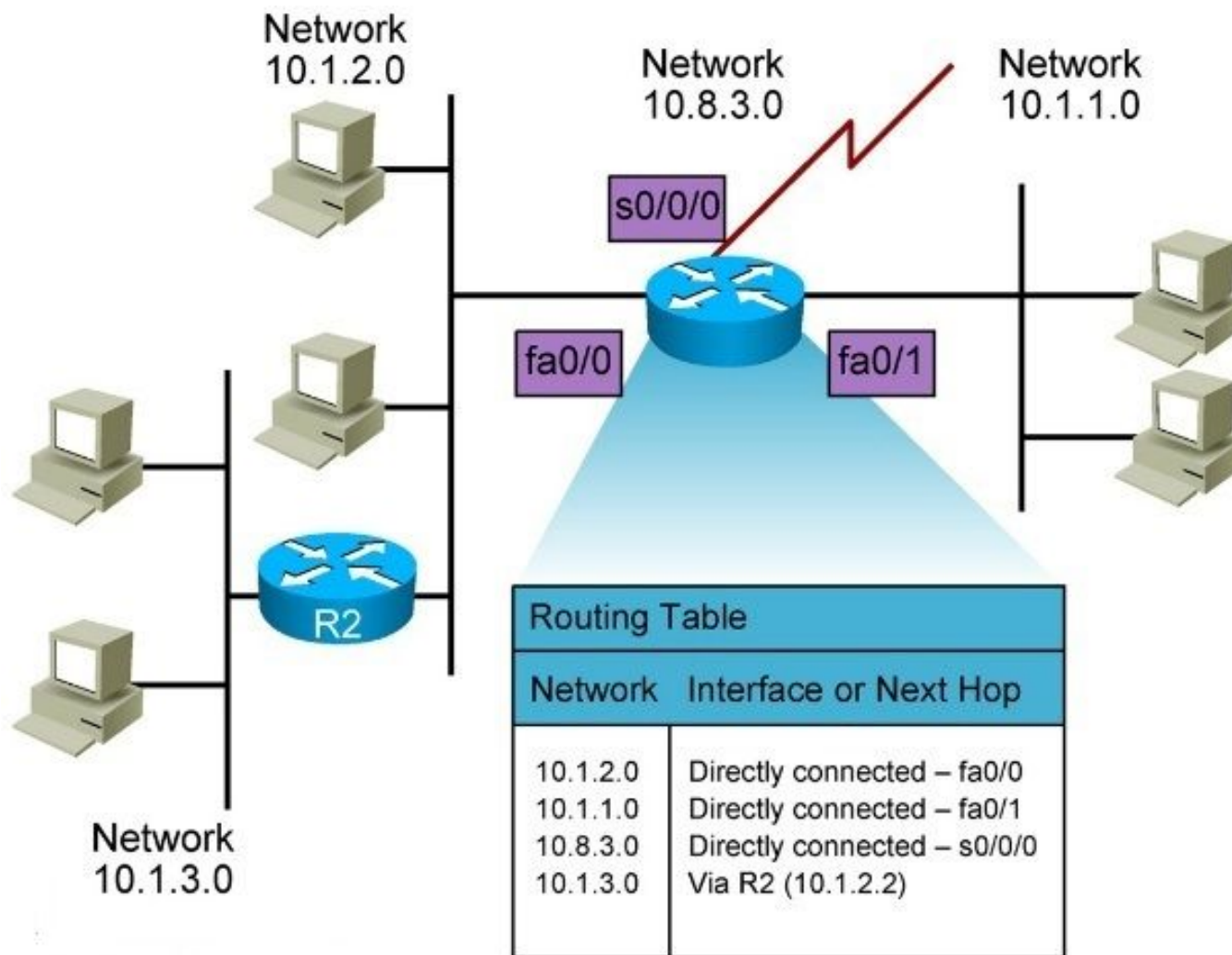
Безопасность протоколов маршрутизации



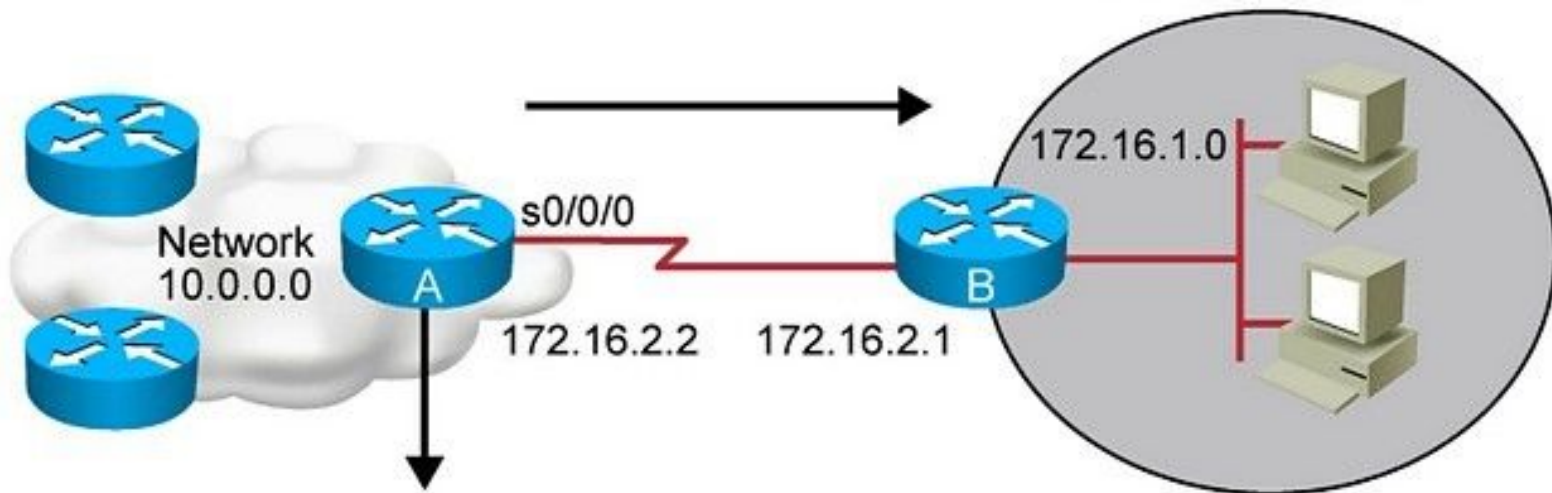
Понятие маршрутизации

- **Маршрутизация** — процесс определения лучшего пути, по которому пакет может быть доставлен получателю
- Возможные пути передачи пакетов называются **маршрутами**. Лучшие маршруты к известным получателям хранятся в **таблице маршрутизации**.

Принцип работы маршрутизации



Статическая маршрутизация

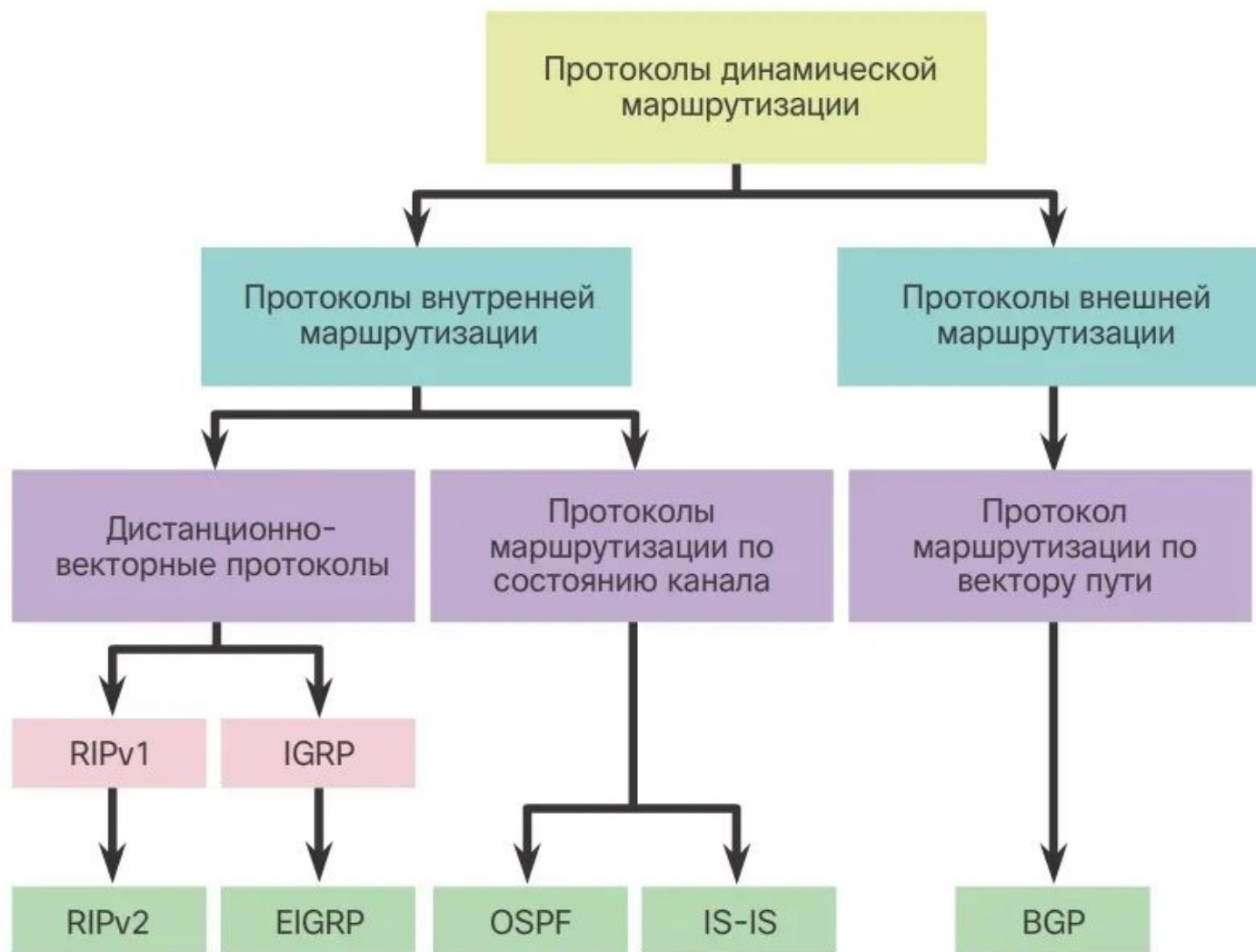


```
RouterX(config)# ip route 172.16.1.0 255.255.255.0 172.16.2.1
```

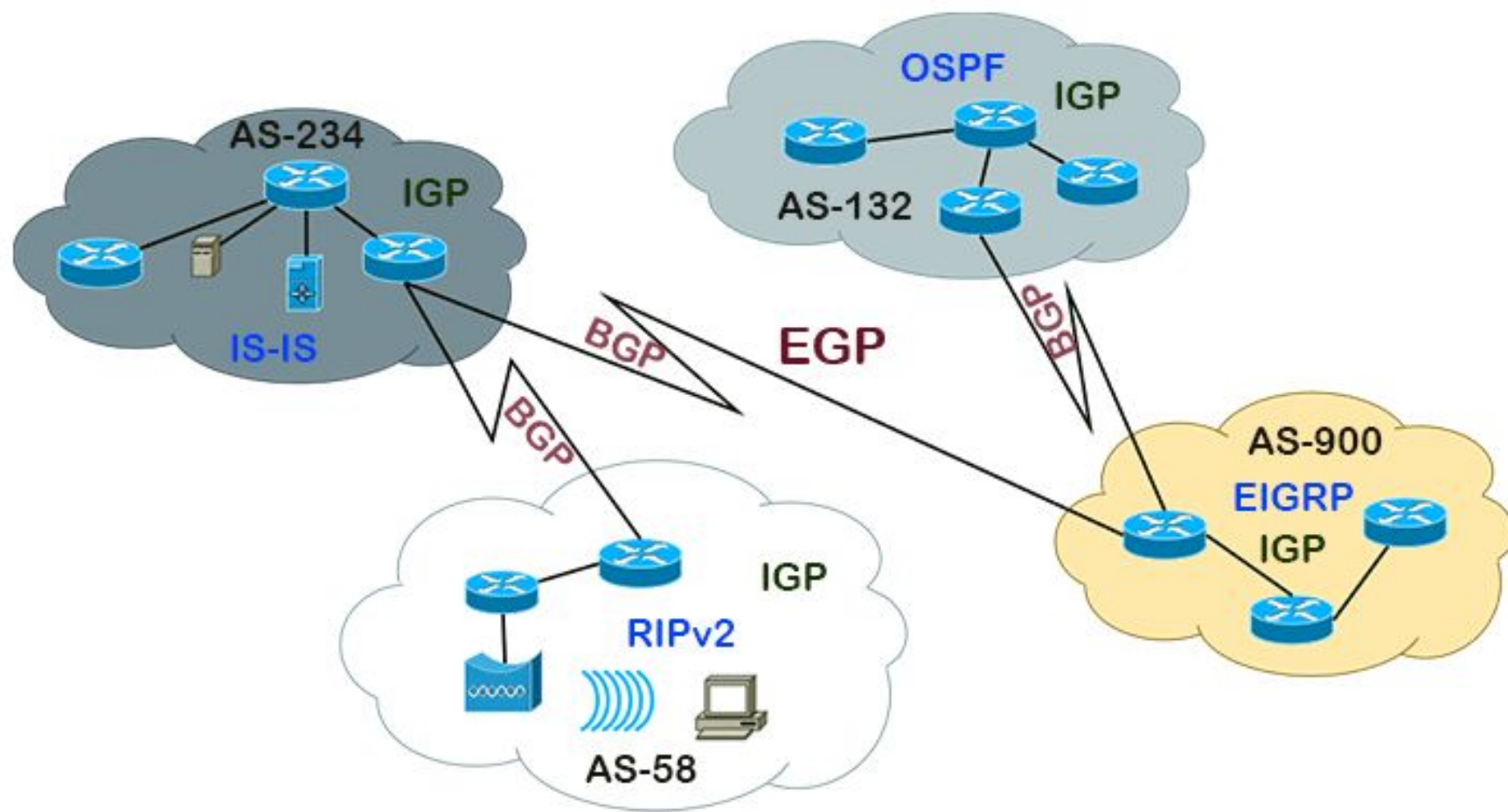
or

```
Router(config)#ip route 172.16.1.0 255.255.255.0 s0/0/0
```

Динамическая маршрутизация



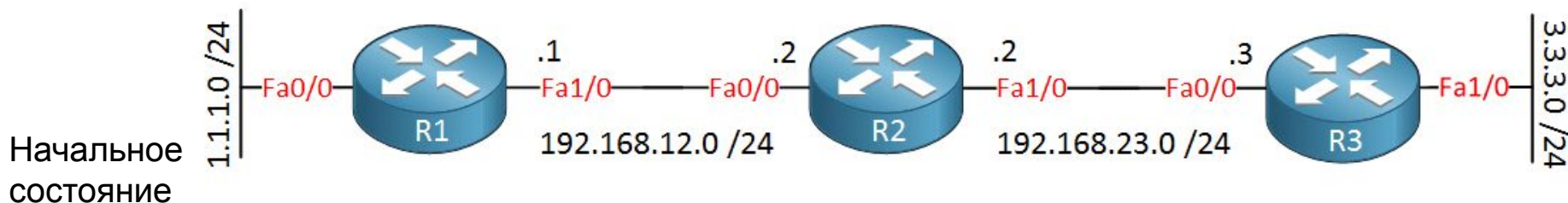
Внутренняя и внешняя маршрутизация, автономные системы



Сравнение протоколов маршрутизации

| Протокол | RIPv2 | EIGRP | OSPF | IS-IS | BGP |
|---------------------------------------|-----------------------------|--------------------------------------|--------------------|--------------------|-----------------------------|
| Использование | IGP | IGP | IGP | IGP | EGP / IGP |
| Тип | distance vector | гибридный | link state | link state | path vector |
| Метрика | число хопов | полоса пропускания / задержка | стоимость маршрута | стоимость маршрута | множество метрик (атрибуты) |
| Администр. дистанция (доверие) | 120 | внутр. 90, внеш. 170 (redistributed) | 110 | 115 | eBGP 20, iBGP 200 |
| Макс. длина маршрутной цепочки (hops) | 15 | 224 (default 100) | None | None | eBGP 1, iBGP None |
| Сходимость | медленная | очень быстрая | быстрая | быстрая | средняя |
| Обновление данных | Постоянно по всей топологии | Только изменения | Только изменения | Только изменения | Только изменения |

RIP - дистанционно-векторный протокол



Routing Table

| | | |
|------------------|-------|---|
| 1.1.1.0 /24 | Fa0/0 | 0 |
| 192.168.12.0 /24 | Fa1/0 | 0 |

Routing Table

| | | |
|------------------|-------|---|
| 192.168.12.0 /24 | Fa0/0 | 0 |
| 192.168.23.0 /24 | Fa1/0 | 0 |

Routing Table

| | | |
|------------------|-------|---|
| 192.168.23.0 /24 | Fa0/0 | 0 |
| 3.3.3.0 /24 | Fa1/0 | 0 |

После обмена маршрутами

Routing Table

| | | |
|------------------|-------|---|
| 1.1.1.0 /24 | Fa0/0 | 0 |
| 192.168.12.0 /24 | Fa1/0 | 0 |
| 192.168.23.0 /24 | Fa1/0 | 1 |
| 3.3.3.0 /24 | Fa1/0 | 2 |

Routing Table

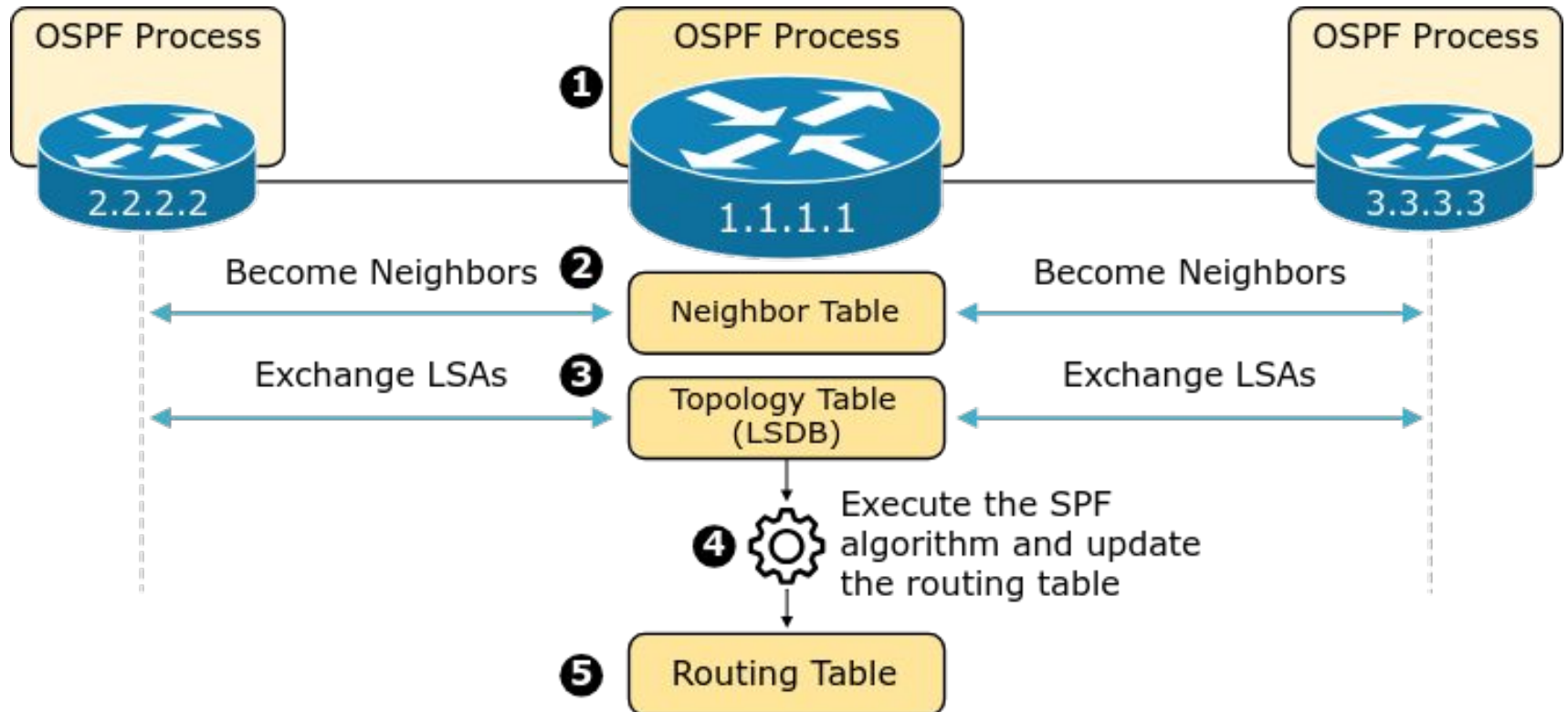
| | | |
|------------------|-------|---|
| 192.168.12.0 /24 | Fa0/0 | 0 |
| 192.168.23.0 /24 | Fa1/0 | 0 |
| 1.1.1.0 /24 | Fa0/0 | 1 |
| 3.3.3.0 /24 | Fa1/0 | 1 |

Routing Table

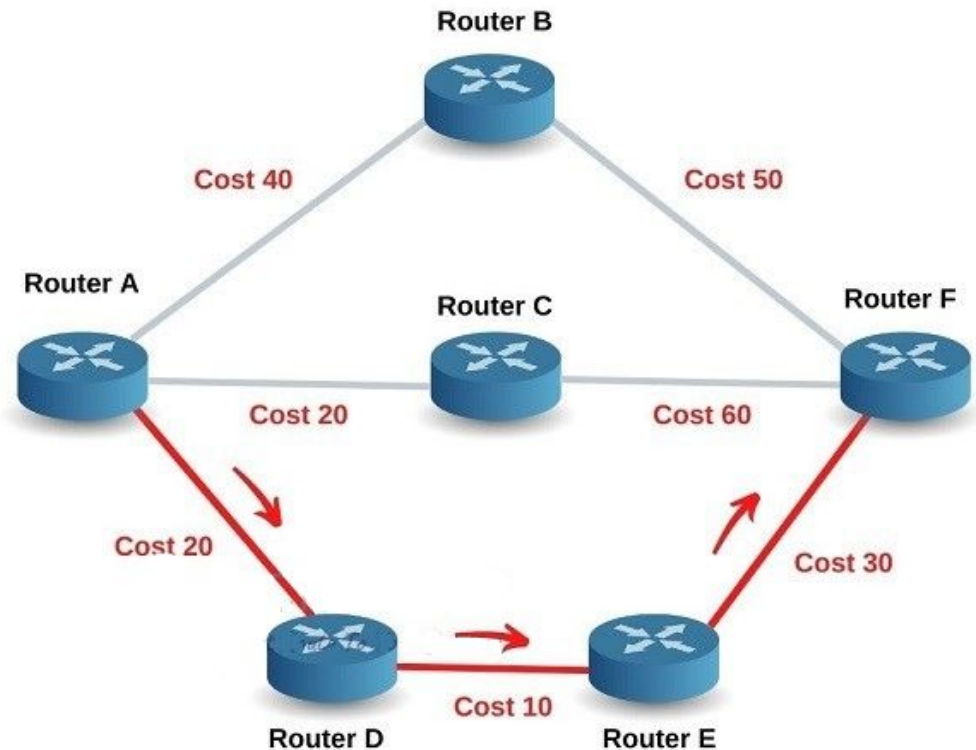
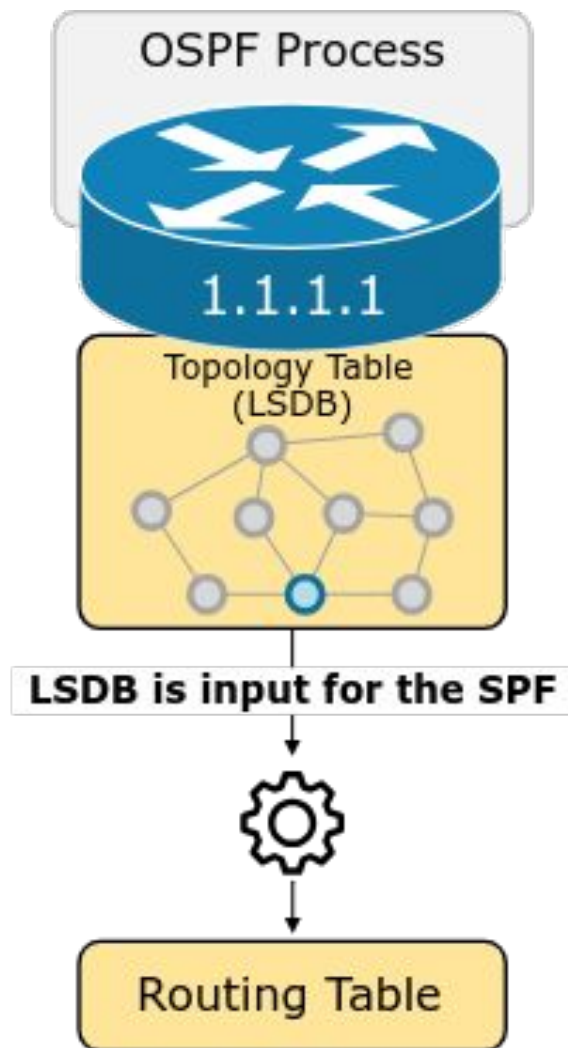
| | | |
|------------------|-------|---|
| 192.168.23.0 /24 | Fa0/0 | 0 |
| 3.3.3.0 /24 | Fa1/0 | 0 |
| 192.168.12.0 /24 | Fa0/0 | 1 |
| 1.1.1.0 /24 | Fa0/0 | 2 |

По умолчанию полная копия таблицы маршрутизации рассылается раз в 30 секунд (таймер Update)
При получении каждая метрика увеличивается на 1. Таблица обновляется, если получен маршрут с лучшей метрикой, чем имеющийся (либо отсутствующий в принципе).

OSPF - link-state протокол



OSPF - расчет кратчайшего маршрута (алгоритм Дейкстры)



Routes

Cost

Route 1 -> A - B - F

$40 + 50 = 90$

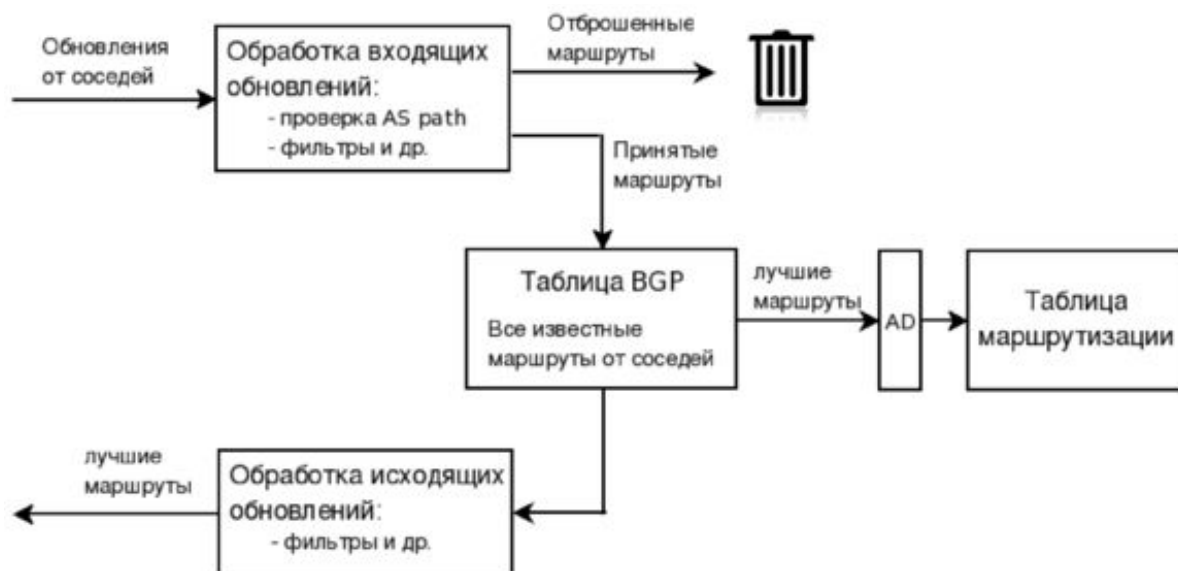
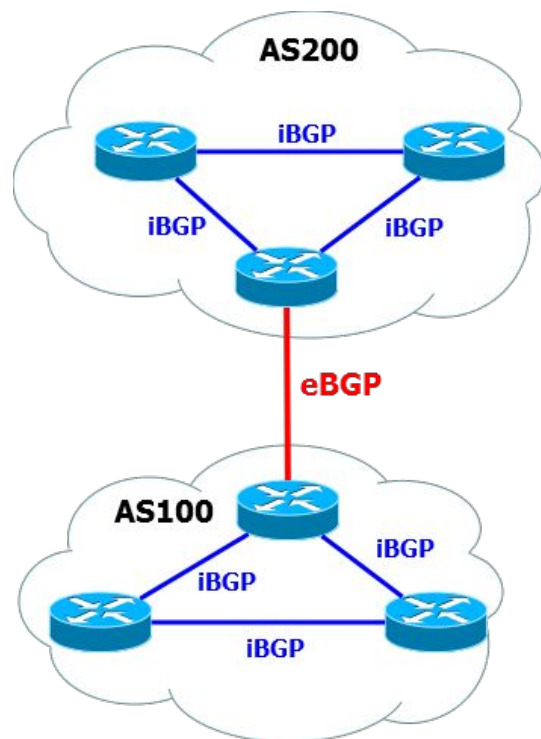
Route 2 -> A - C - F

$20 + 60 = 80$

Route 3 -> A - D - E - F

$20 + 10 + 30 = 60$

BGP - Border Gateway Protocol



- Использует TCP (port 179) - обеспечивает надежность
- Отправляет обновления только после изменений в сети
Периодически отправляет keeralive для проверки соединения
- Метрика протокола называется path vector (либо attributes)

Атаки на маршрутизацию

- Перехват маршрутных пакетов
- Фальсификация маршрутной информации
- Отказ в обслуживании
- Атаки на уровне управления

Защита

- Аутентификация сообщений протокола маршрутизации;
- Вынесение сети управления сетевым оборудованием в отдельный VLAN