



ЦЕНТР
ПРИКЛАДНЫХ
ИССЛЕДОВАНИЙ
КОМПЬЮТЕРНЫХ
СЕТЕЙ



2014

CEE-SEC(R)

Разработка ПО

Управление корпоративной сетью на основе SDN-технологий

Александр Шалимов

ЦПИКС, МГУ



<http://arccn.ru/>



ashalimov@arccn.ru



@alex_shali

@arccnnews

Что такое SDN/OpenFlow?

SDN = Software Defined Networking

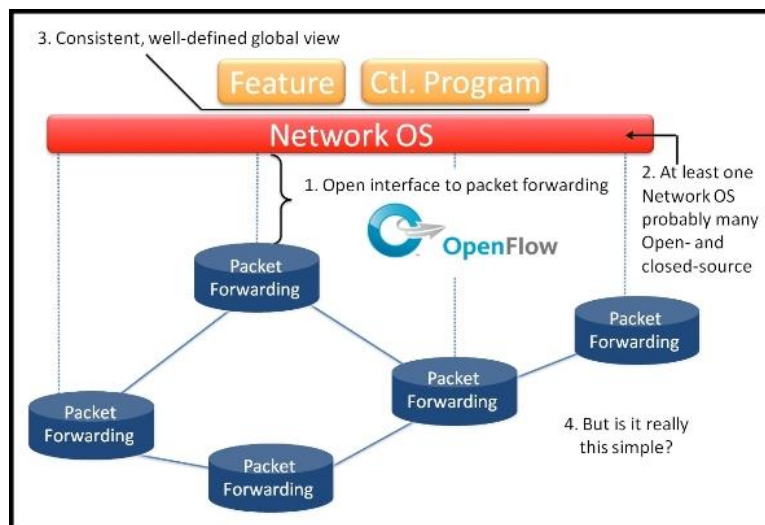
Внедрения



-
-
-

Основные принципы

- Физическое разделение уровня передачи данных от уровня управления сетевых устройств.
- Логически централизованное управление.
- Программируемость.
- Открытый единый интерфейс управления.

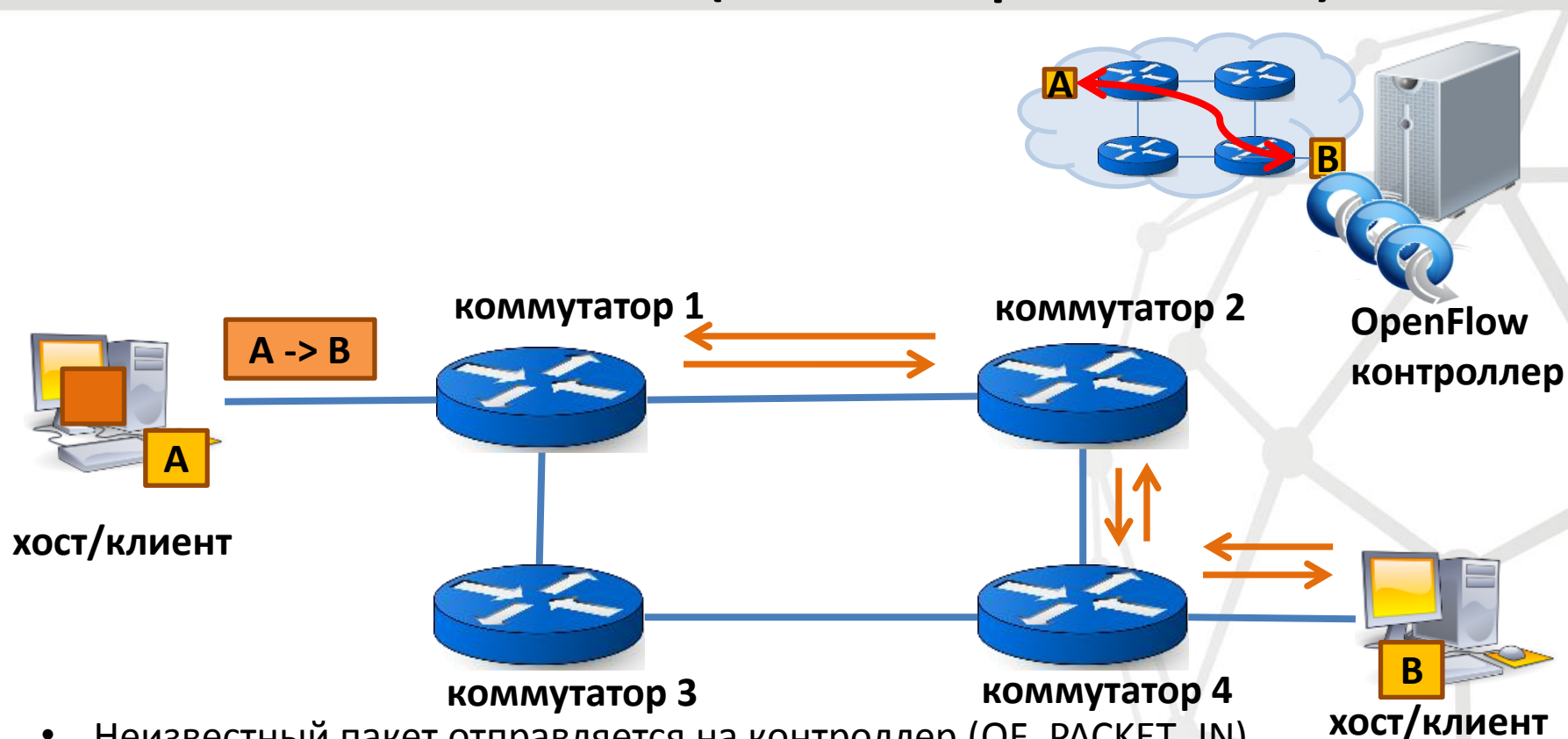


Преимущества

- Упрощение управления сетью (OPEX)
- Удешевление оборудования (CAPEX)
- Разработка ранее недоступных сервисов

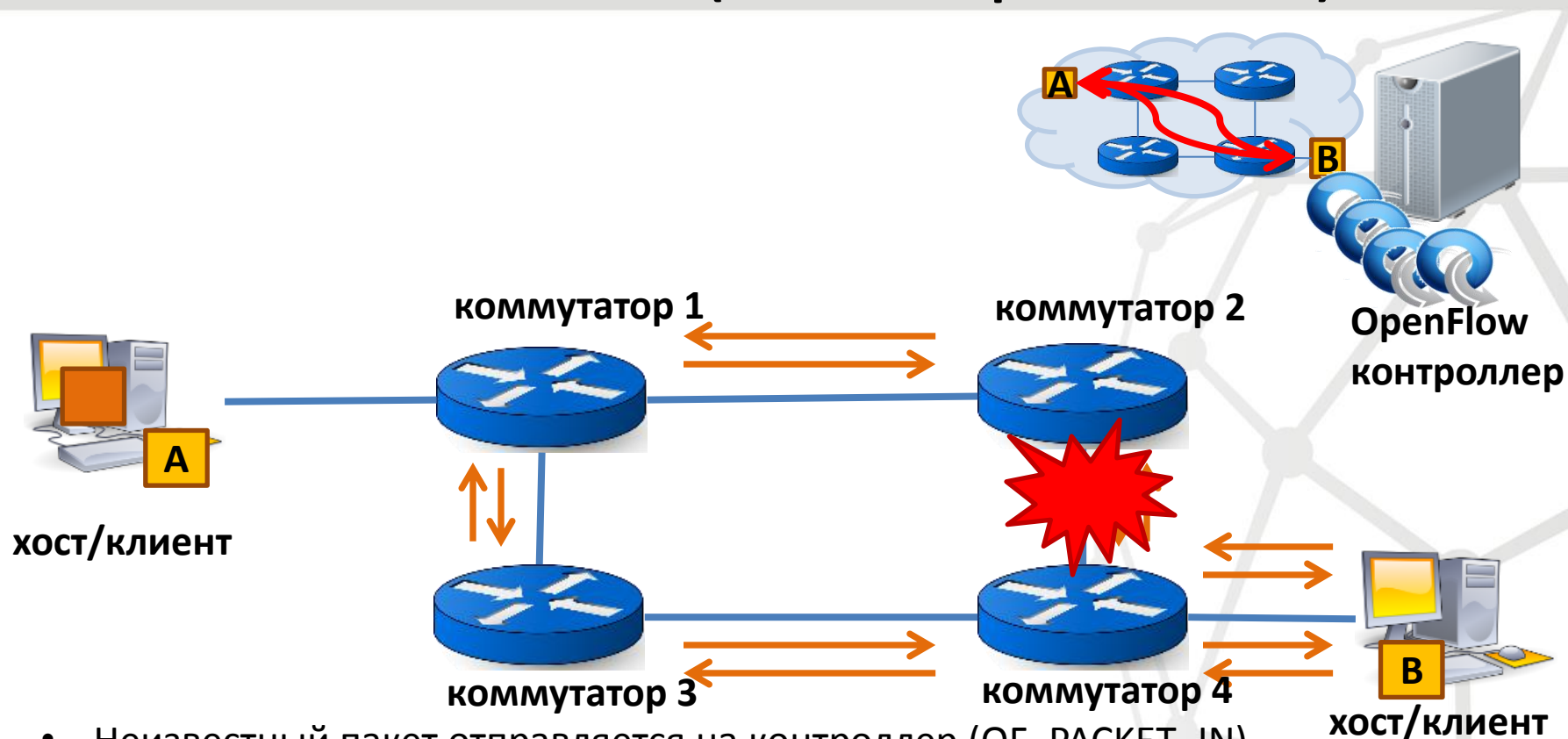
“SDN means thinking differently about networking”

Основы ПКС (SDN/OpenFlow)



- Неизвестный пакет отправляется на контроллер (OF_PACKET_IN).
- Контроллер вычисляет лучший маршрут через всю сеть (с наименьшей стоимостью и удовлетворяющий политикам маршрутизации).
- Соответствующие правила OpenFlow устанавливаются на коммутаторы + сразу и обратный маршрут (OF_PACKET_OUT/FLOW_MOD).

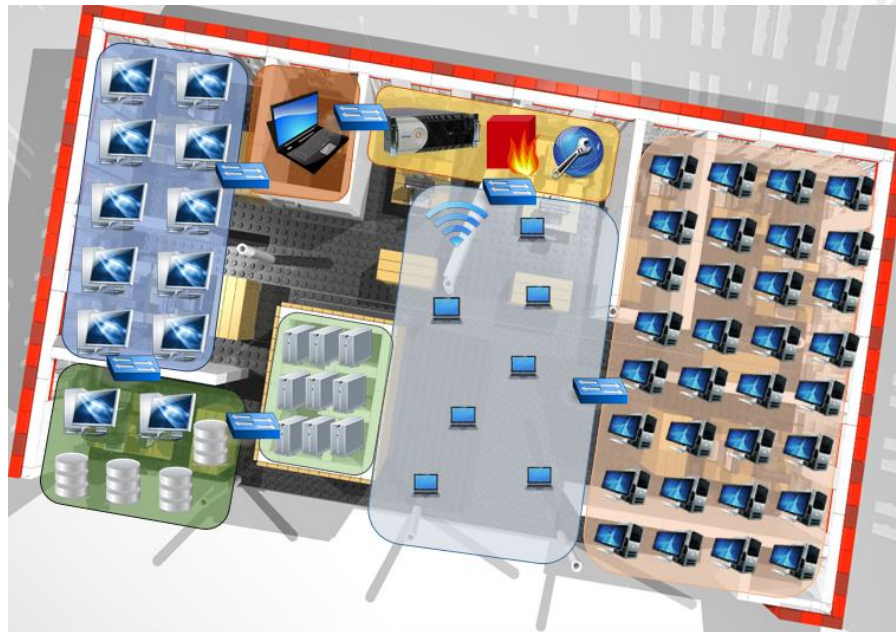
Основы ПКС (SDN/OpenFlow)



- Известный пакет отправляется на контроллер (OF_PACKET_IN).
- Контроллер вычисляет лучший маршрут через всю сеть (с наименьшей стоимостью и удовлетворяющий политикам маршрутизации).
- Соответствующие правила OpenFlow устанавливаются на коммутаторы + сразу и обратный маршрут (OF_PACKET_OUT/FLOW_MOD).
- **Динамическая переконфигурация в случае ошибки сети.**

Корпоративная сеть

- Современные компания имеют сложную сетевую инфраструктуру:
 - Большое количество сетевых элементов
 - Разветвленная топология
 - Набор различных политик маршрутизации и безопасности



Трудности администрирования

- Сетевые администраторы отвечают за поддержание работы сетевой инфраструктуры:
 - Сетевые инженеры руками переводят высокоуровневые политики в низкоуровневые команды
 - Ручная настройка всех сетевых устройств
 - Ограниченный инструментарий по управлению сетевыми устройствами
 - Переучивание под каждого вендора

```
Router Management
  1.  Configure Static-routes/ACLs
  2.  Configure RIP
  3.  Configure OSPF
  0.  Exit

Select Menu Number [0-3]: 1

router> enable
router# configure terminal
router(config)# ip route 5.5.5.5 255.255.255.255 2.2.2.2
router(config)# write
Configuration saved...
router(config)# _
```

Существующие системы управления

- Предназначены для мониторинга состояния: топология, характеристики каналов, загрузка каналов и задержка.
- Основы на протоколе SNMP.
- Конфигурация оборудования по-прежнему происходит в ручном режиме.

Примеры: Cisco Prime, HP OpenView, IBM Tivoli, OpenNMS.

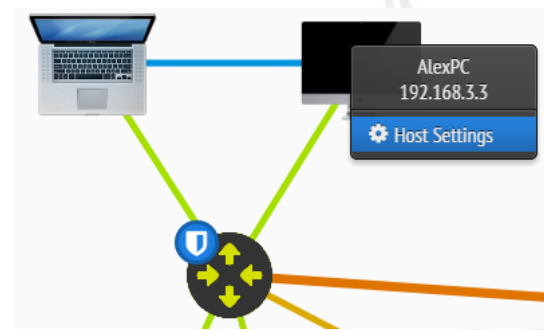
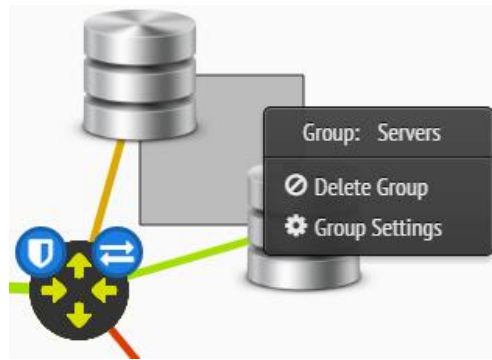
Цель

1. Сделать сеть управляемой без ручного доступа к оборудованию.
2. Повысить уровень абстракции управления сетью.

Идея: использовать для этого подход SDN и протокол OpenFlow

Семантическое управление сетью

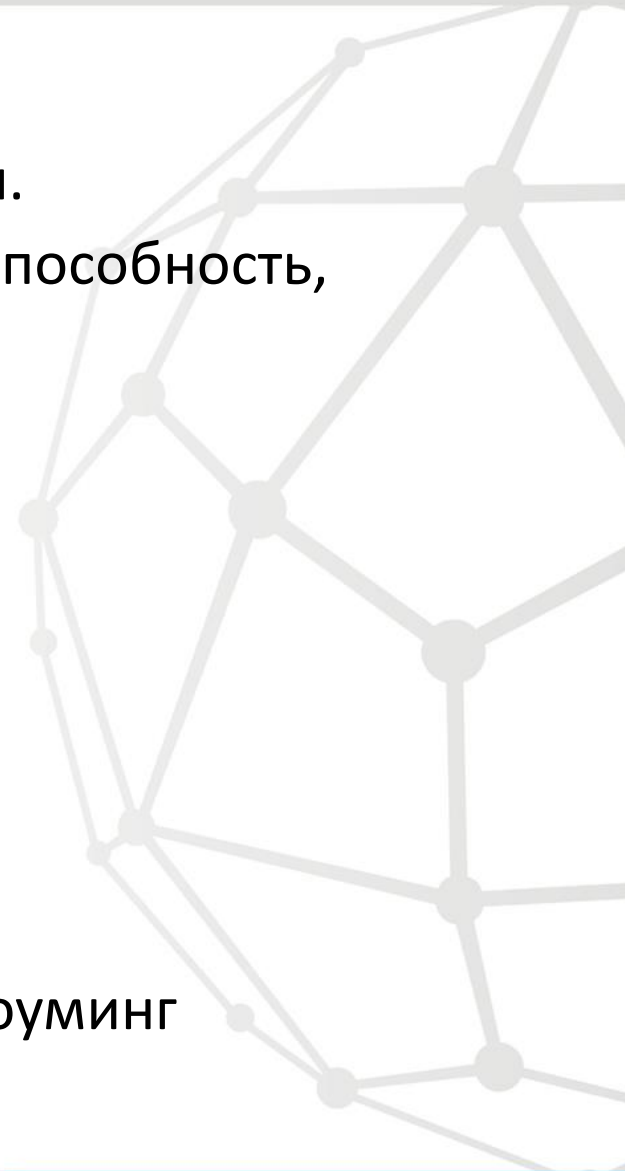
- **Имена.** Работа с именами хостов проще, чем запоминать связки IP и MAC адресов.
- **Группы.** Хосты объединяются в группы, удобно для задания одних политик. Вместо подсетей.
- **Пути.** Задавать маршруты через всю сеть сразу, а не для каждого устройства отдельно.



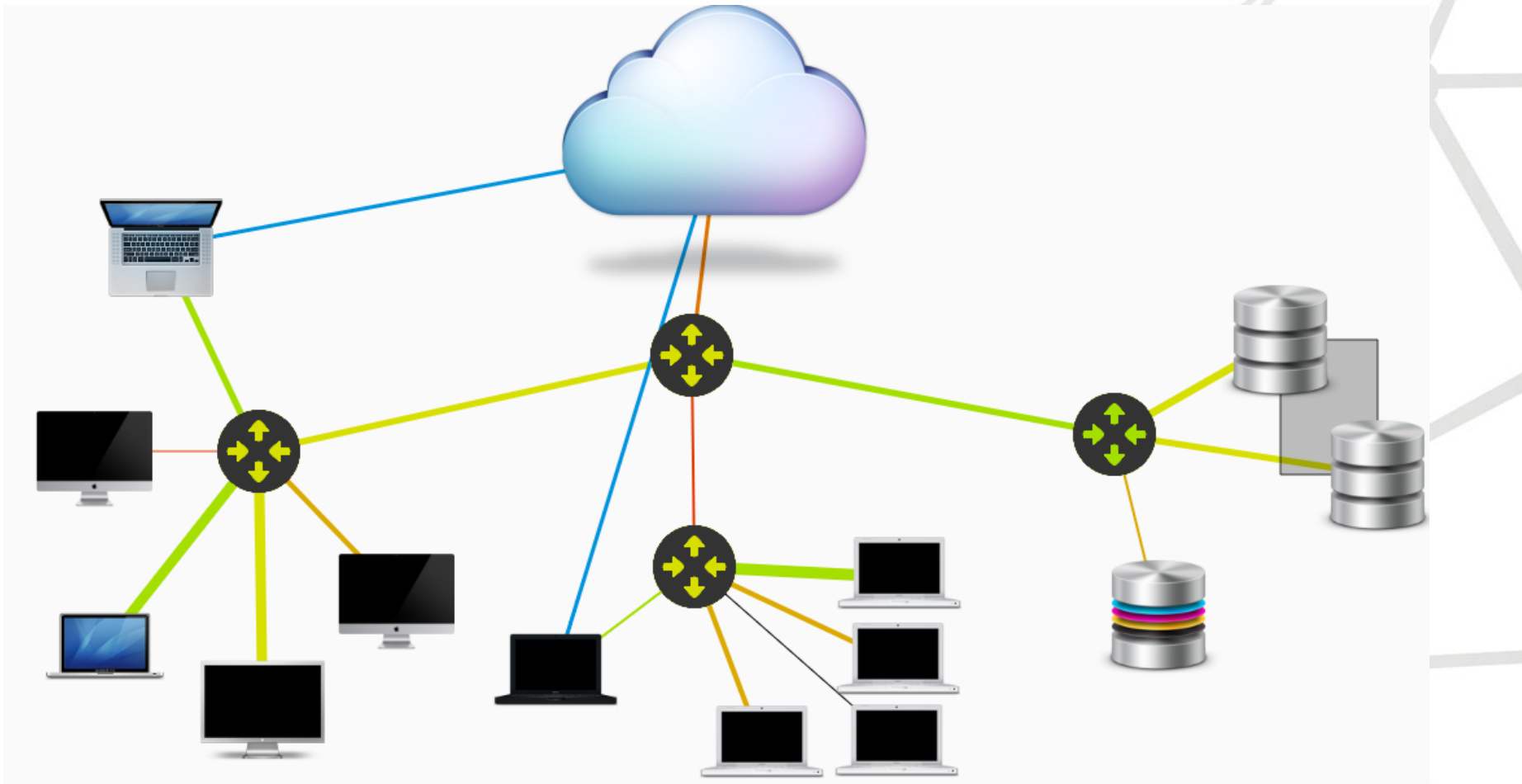
Бонус: В связи с тем, что теперь IP адреса скрыты, выбираем их сами, так как нам это удобно. Например, уменьшение правил, агрегирование потоков, снижение затрат на сбор статистики.

Основные функции

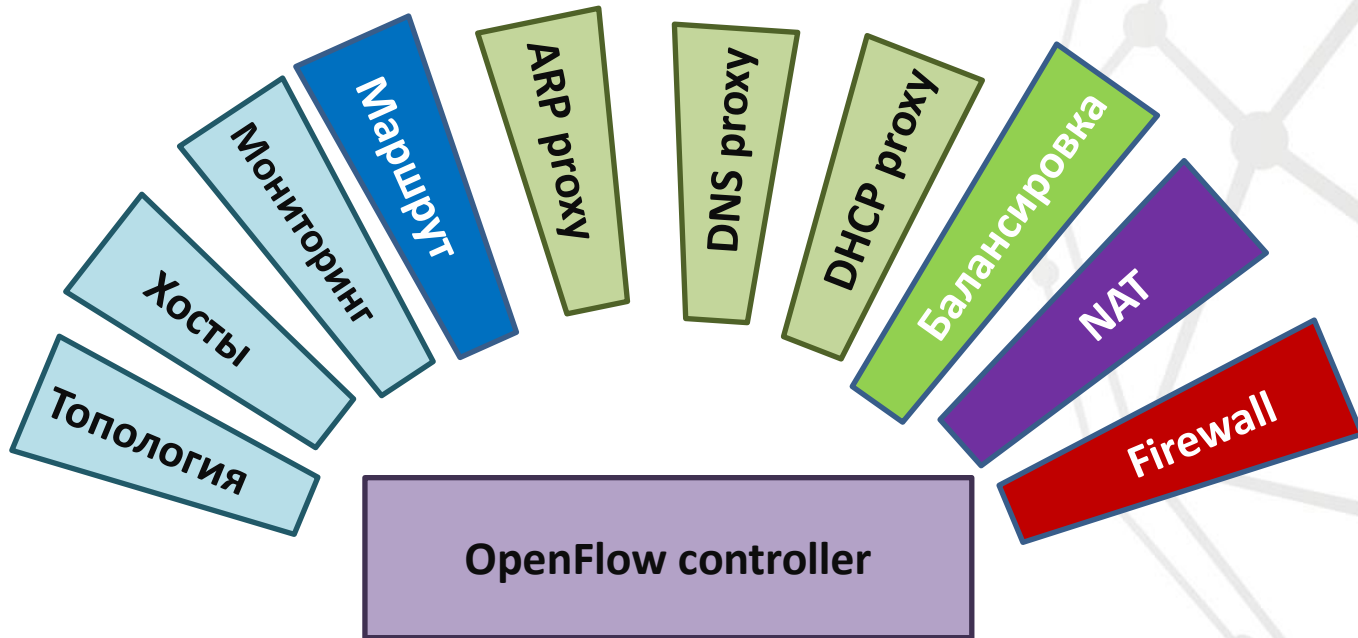
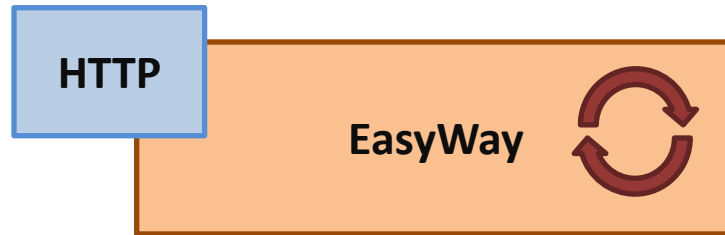
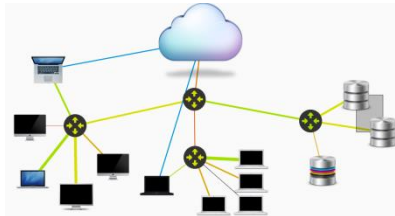
- Автоматическое определение топологии.
- Мониторинг загрузки сети (пропускная способность, задержки).
- Именованное.
- Группы.
- Выбор маршрутов.
- Поддержка QoS.
- Балансировка нагрузки.
- Файрволл и ограничения доступа.
- NAT
- Интеграция с WiFi сетями, бесшовный роуминг



Как это выглядит?



Реализация



Заключение

- SDN/OpenFlow позволяет значительно упростить управление сетью предприятия.
- Проект находится в открытом доступе
 - OpenFlow контроллер [arccn.github.io/runos](https://github.com/arccn/runos)
 - Система управления корпоративной сетью [arccn.github.io/easyway](https://github.com/arccn/easyway)





ЦЕНТР
ПРИКЛАДНЫХ
ИССЛЕДОВАНИЙ
КОМПЬЮТЕРНЫХ
СЕТЕЙ