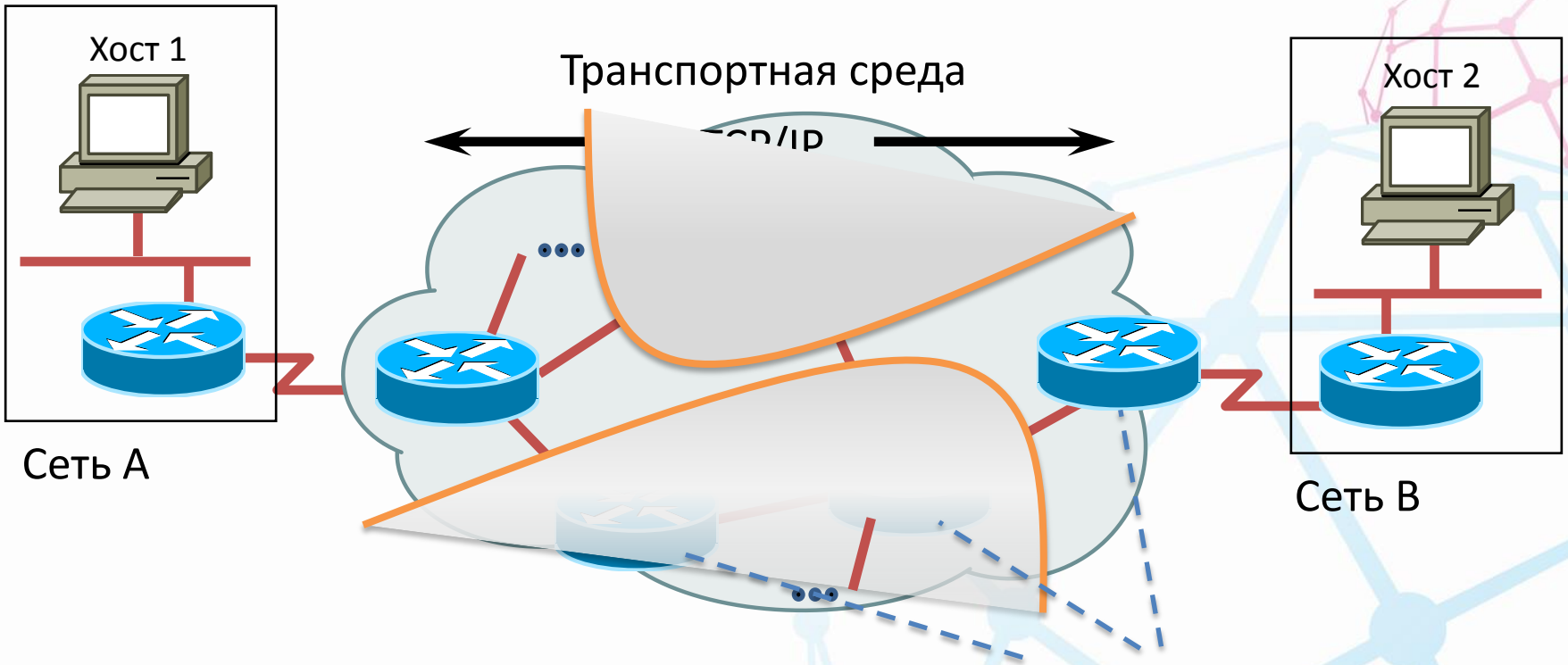
ЦЕНТР
ПРИКЛАДНЫХ
ИССЛЕДОВАНИЙ
КОМПЬЮТЕРНЫХ
СЕТЕЙ

Обеспечение сетевой безопасности с помощью программно-конфигурируемых сетей

***Смелянский Руслан Леонидович**, чл.-корр. РАН, профессор, директор по науке, Центра прикладных исследований компьютерных сетей, МГУ им. М.В.Ломоносова*

***Гамаюнов Денис Юрьевич**, к.ф.-м.н., с.н.с., и.о. зав. лабораторией безопасности информационных систем, факультет ВМК МГУ им. М.В.Ломоносова*

Традиционная TCP/IP сеть

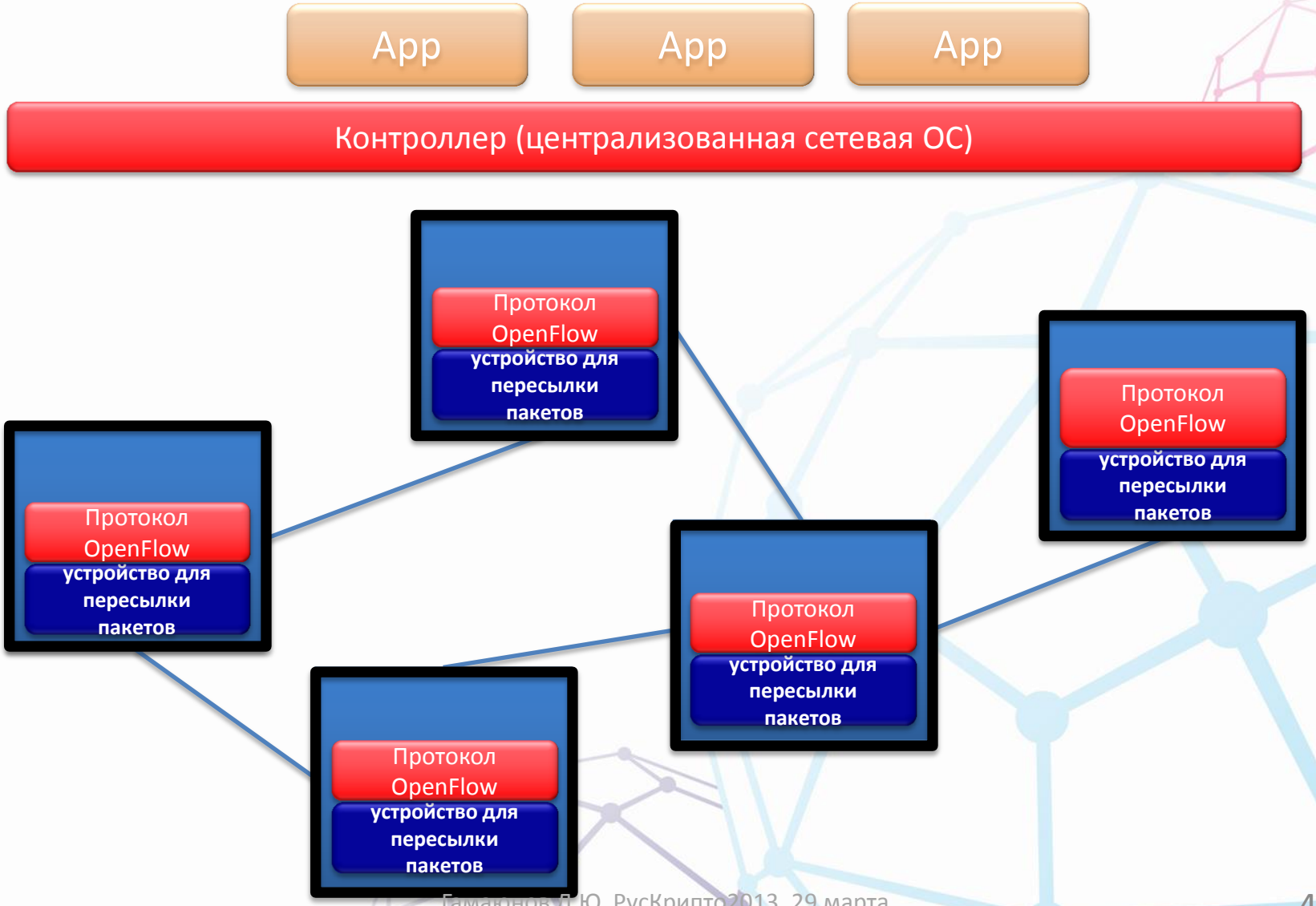


1. Построение маршрута (control path)
2. Реализация маршрута (data path)

} Функции каждого сетевого устройства

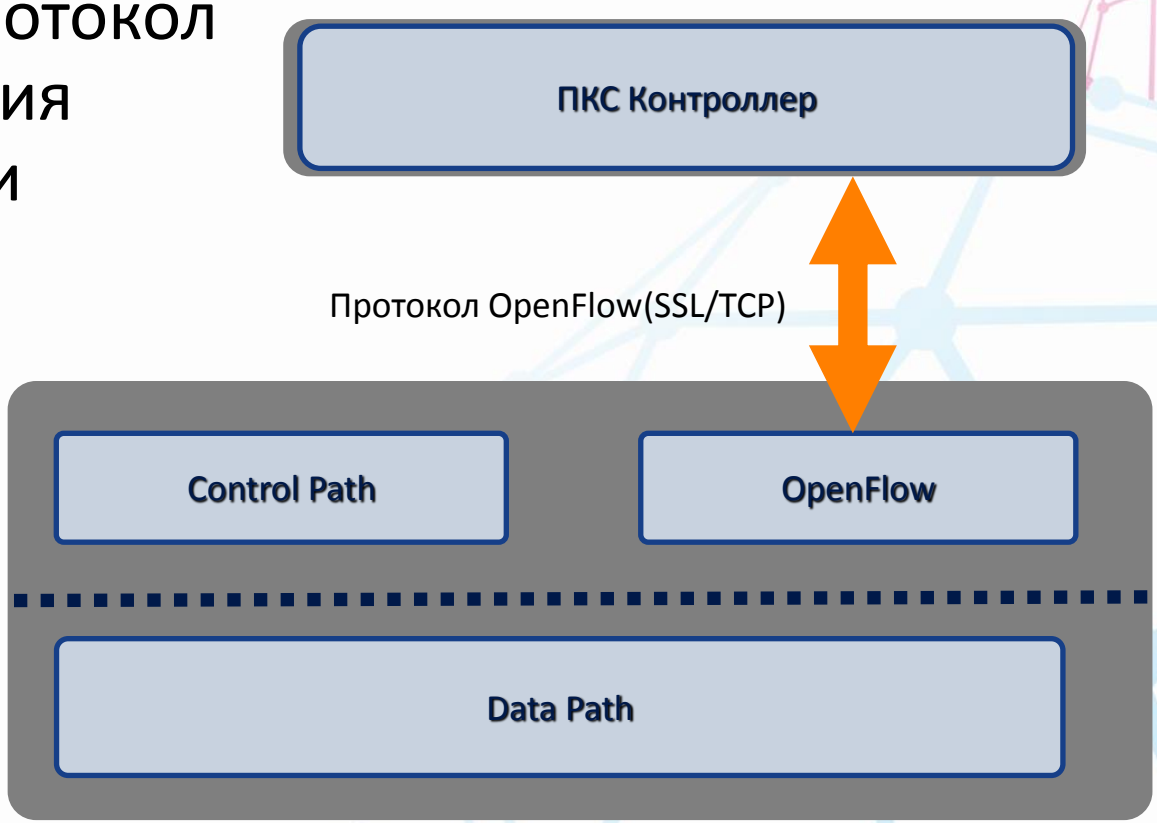
Логическая структура транспортной среды

Программно-Конфигурируемые Сети (ПКС)

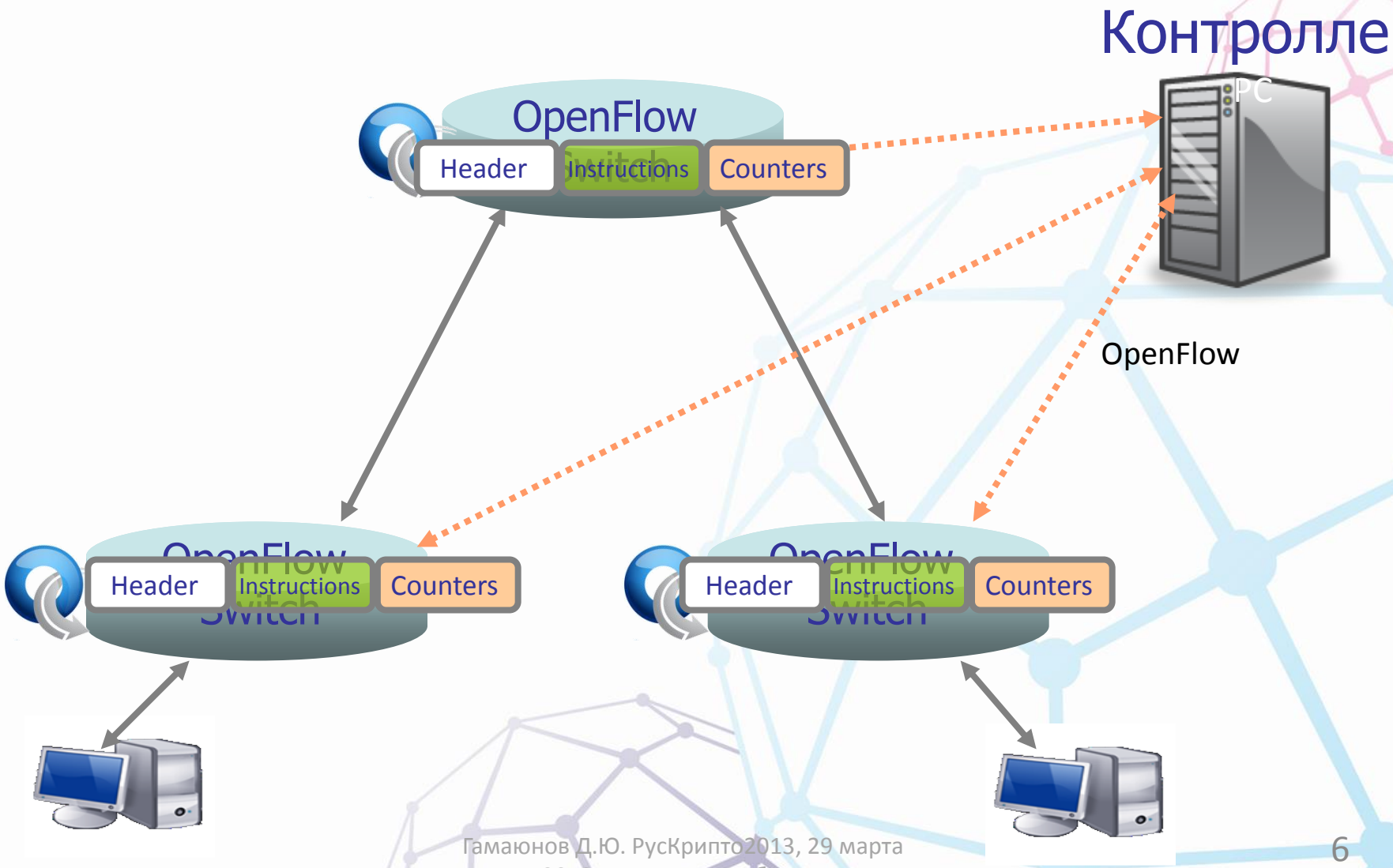


Логическая структура ПКС сети

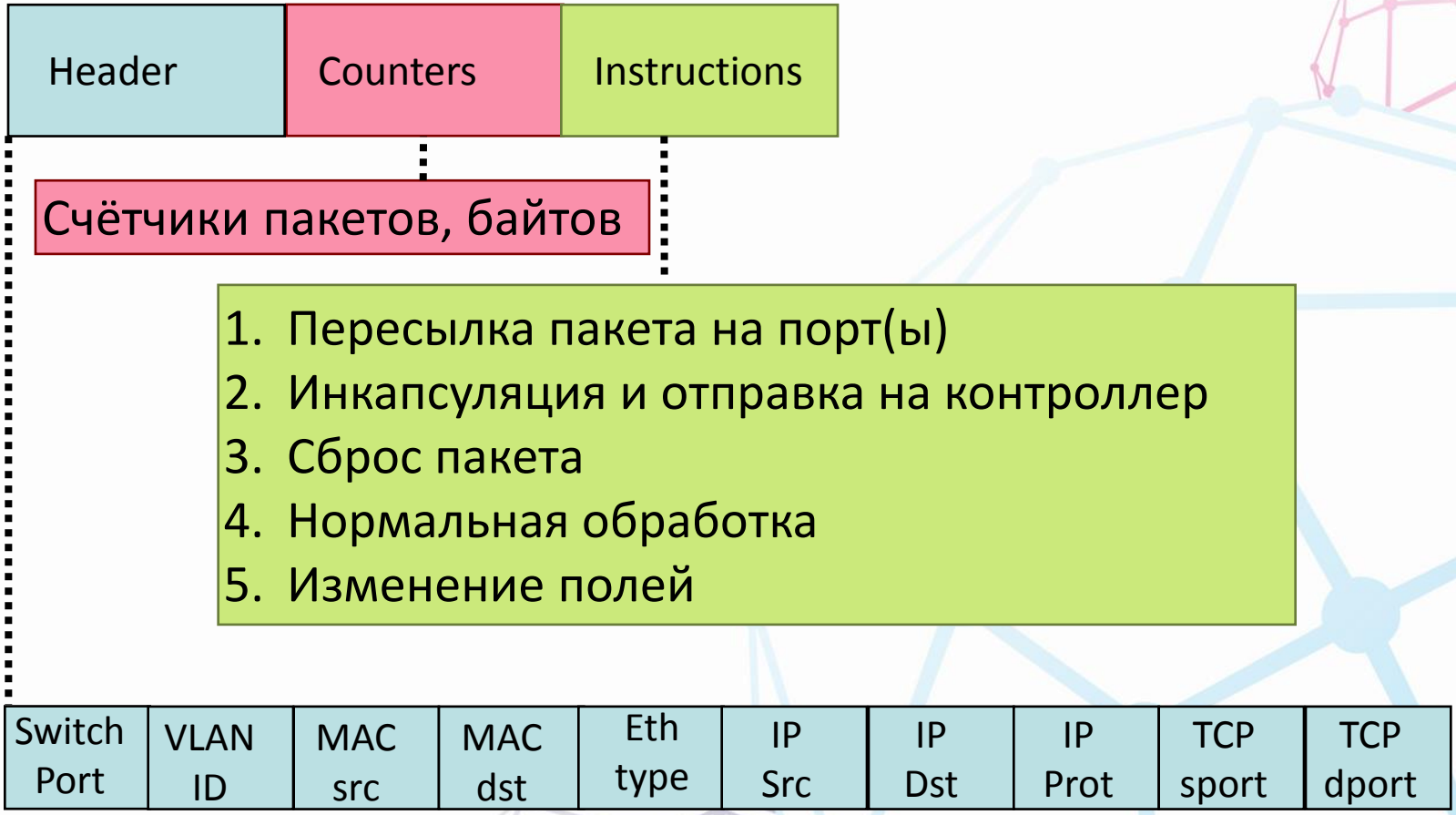
OpenFlow - протокол взаимодействия коммутатора и контроллера



Централизованное управление политиками форвардинга в сети



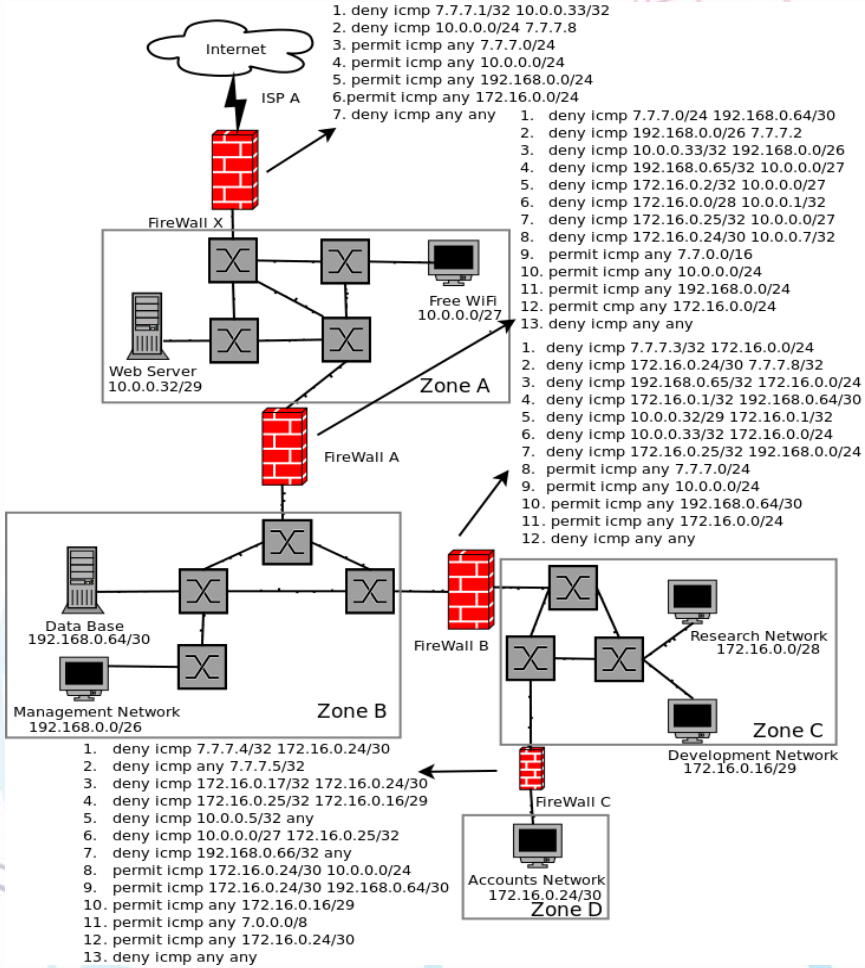
OpenFlow: управление потоками



+ маска, для обозначения значащих полей

Межсетевое экранирование средствами ПКС

- Традиционное решение задачи разделения доступа – выделенные устройства (МСЭ)
  - Высокая стоимость
  - Сложная задача администрирования
  - Производительность
- Переход к ПКС
  - Фильтрация на уровне Data Path
  - Управление и настройка на уровне Control Path
- **Как упростить переход?**



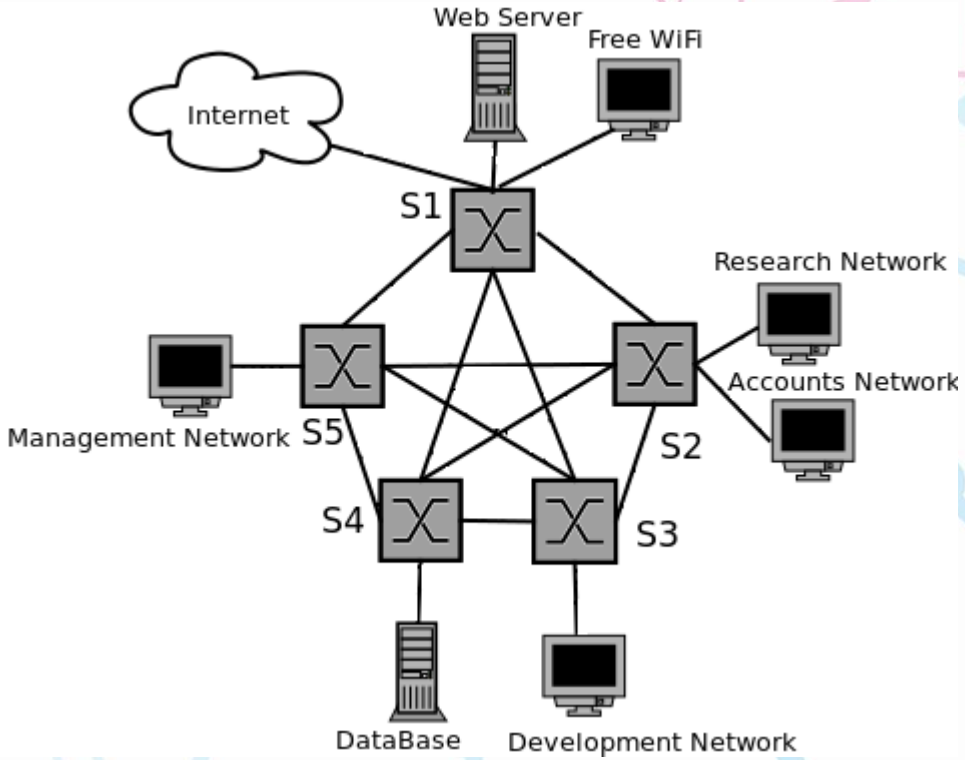
Алгоритм перехода к ПКС сети

- Оптимизация правил:
  - Поиск и удаление аномалий на каждом МСЭ в отдельности;
  - Поиск и удаление аномалий на МСЭ в совокупности;
- Построение единого логического (виртуального) МСЭ для каждой подсети в топологии;
- Подсчет минимального необходимо количества OF коммутаторов и выбор топологии ПКС сети;
- Трансляция правил фильтрации трафика для каждого OF коммутатора в политику ПКС сети

Результат : централизованная политика разграничения доступа для ПКС сети

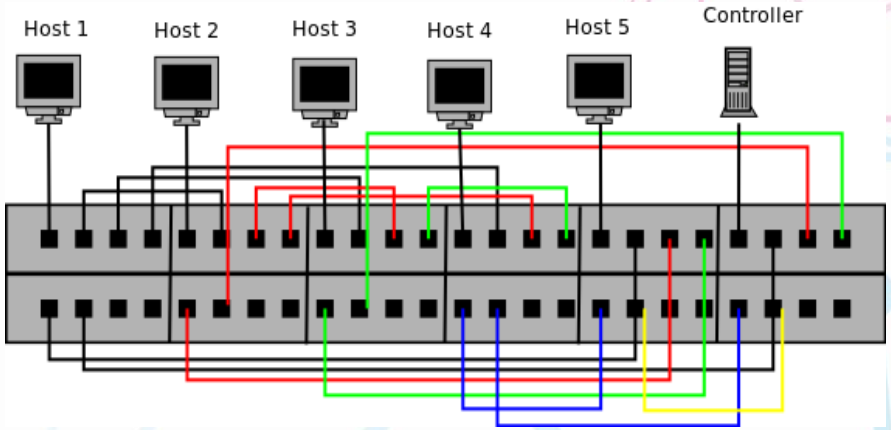
Целевая топология ПКС сети

- Сохранение графа связности узлов исходной сети
- Обеспечение связности через ПКС сеть
- Максимизация пропускной способности целевой топологии



Экспериментальная реализация

- Управляющее приложение на основе контроллера POX
- Вход – правила в формате Extended Cisco ACL
- Выход – политика для контроллера, управление коммутаторами NEC PF 5820



Номер испытания	Количество правил	Затрачиваемое время, мс
1	100	0.02
2	200	0.04
3	300	0.06
4	400	0.08
5	500	0.1

Время установки правил фильтрации на коммутатор.

Вариант реализации	Затрачиваемое время, мс
Классический	35
Рефлексивный	220 (первый пакет), 0.2 последующие пакеты

Величина задержки при передаче пакета.

Результаты и перспективы

- Оптимизация топологии
  - Уменьшено число устройств в data path
  - Число правил для каждого пакета существенно сокращено (для примера – 40 сопоставлений в традиционной топологии, и 7 в ПКС сети)
- Централизованное управление потоками трафика
  - Контроллер «видит» все входящие потоки, невозможность обходных путей
- Возможность балансировки нагрузки
  - Контроллеры с функциями балансировки нагрузки, обгнаружения и подавления DDoS атак
- Возможность анализа поведения всех устройств
  - Контроллеры с функциями IDS/IPS

Контакты

- Руслан Леонидович Смелянский, *чл.-корр. РАН, профессор, директор по науке, Центра прикладных исследований компьютерных сетей*

  e-mail: rsmeliansky@arccn.ru

  web: http://www.arccn.ru/

- Денис Юрьевич Гамаюнов, *к.ф.-м.н., с.н.с., и.о. зав. лабораторией безопасности информационных систем, факультет ВМК МГУ им. М.В.Ломоносова*

  e-mail: gamajun@seclab.cs.msu.su

  web: http://seclab.cs.msu.su/