

**РАЗРАБОТКА ЭФФЕКТИВНОГО
АЛГОРИТМА БЕЗОПАСНОСТИ
ДЛЯ ПРОГРАММНО-
КОНФИГУРИРУЕМОЙ СЕТИ-
ЧАШИН Ю. Г., АЗИЗОВА Д. Г.,
БАБЕНКО А. А., 2022**

АКТУАЛЬНОСТЬ

Компьютерные сети стали логическим результатом эволюции компьютерных и телекоммуникационных технологий.

❖ Они являются частным случаем распределённых компьютерных систем

❖ Могут рассматриваться как средство передачи информации на большие расстояния, для чего в них применяются методы кодирования и мультиплексирования данных, получившие развитие в различных телекоммуникационных системах.

Объект исследования

система управления коммутатором на основе
протокола OpenFlow.

Предмет исследования

описание технологии
программно-конфигурируемых сетей.

Цель работы:

- ❖ изучение программно-конфигурируемых сетей как одного из возможных этапов и направлений развития сетевых технологий
- ❖ разработка системы управления коммутатором на основе протокола OpenFlow.

ЗАДАЧИ

- ❖ дать понятие программно-конфигурируемым сетям; отметить достоинства и недостатки программно-конфигурируемых сетей;
- ❖ осуществить обзор нового стандарта OpenFlow, изучить его главные характеристики, объяснить особенности архитектуры и отметить преимущества объединенной эксплуатации протокола с программно-конфигурируемыми сетями;
- ❖ определить, до какой степени программно-конфигурируемые сети могут решить проблемы управления сетевой безопасностью;
- ❖ отметить главные достоинства использования программно-конфигурируемых сетей в современных условиях

Практическая значимость работы

определяется в возможности динамически конфигурировать компоненты сетевой инфраструктуры и задавать оптимальные параметры передачи данных для различных типов сетевого трафика при применении протокола OpenFlow для настройки коммутатора.

Предпосылки создания технологий программно – конфигурируемых сетей.

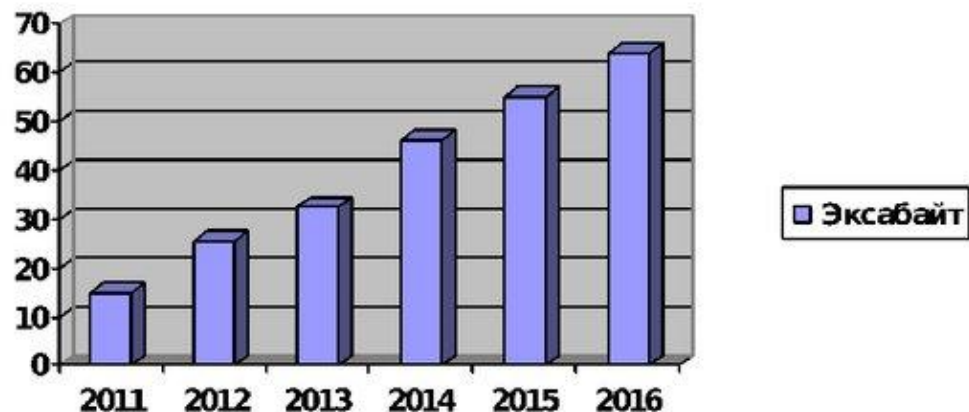


Рисунок 1.1 – График роста трафика за 2011 – 2016 год

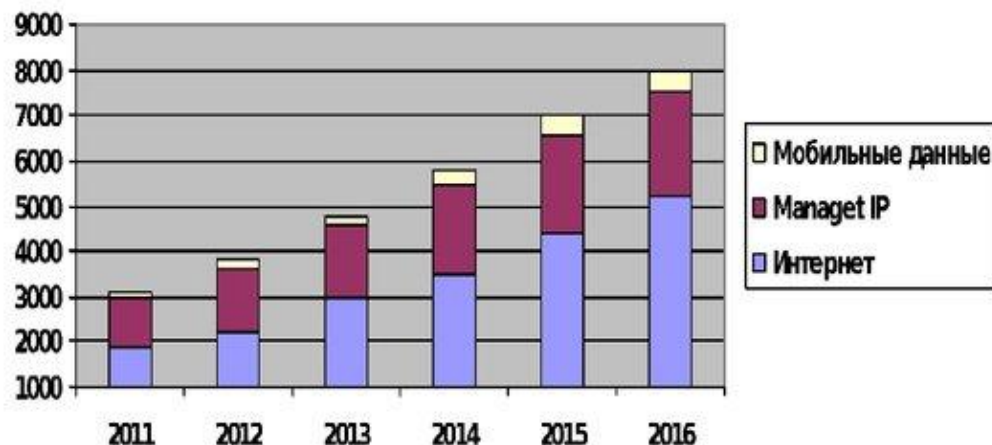


Рисунок 1.2 – График глобального обмена файлами

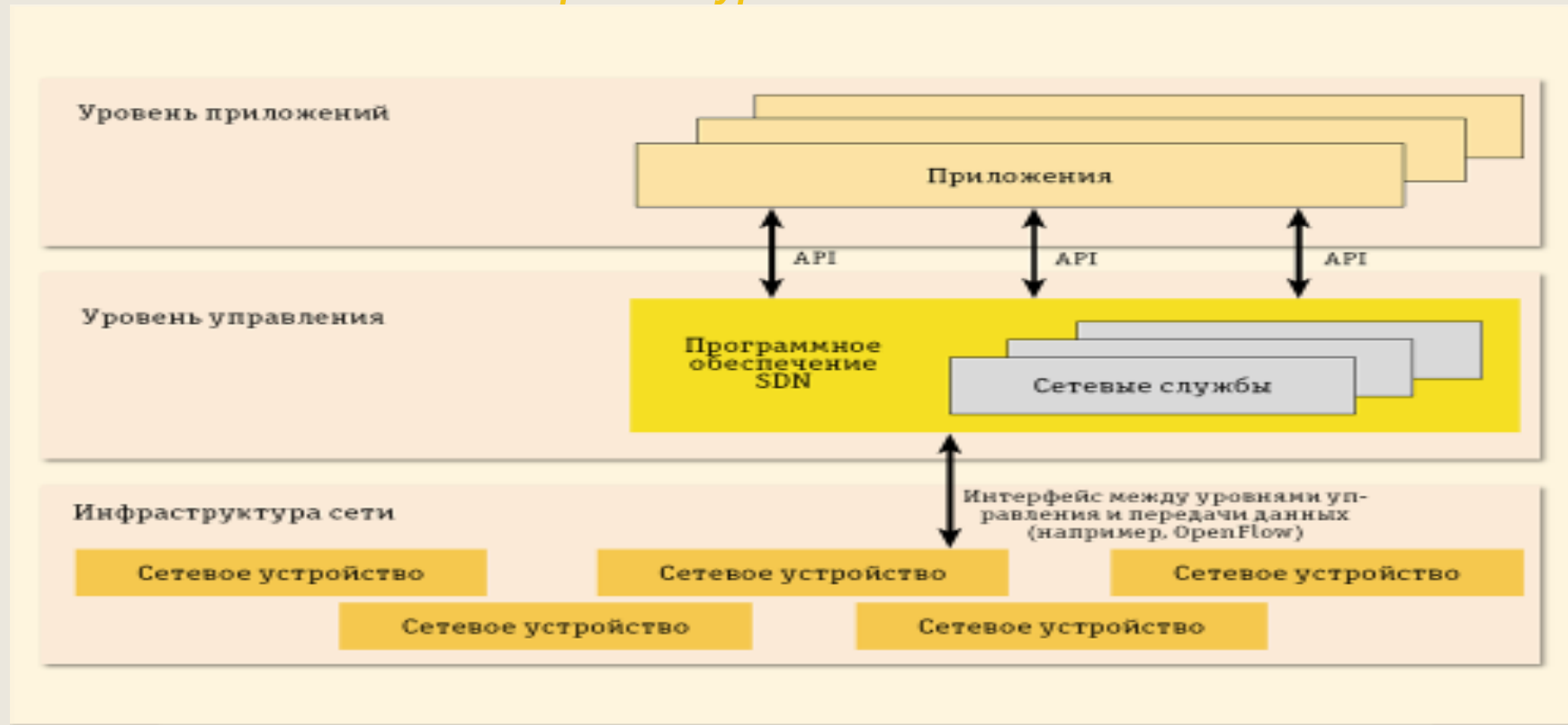
Объем трафика в Интернете за последние пять лет вырос втрое, а пропускная способность современных каналов связи не в состоянии удовлетворять потребности пользователей.

Начиная с 2011 года ежегодные темпы роста пропускной способности сетей во всем мире составляли около 60%, однако исследования специалистов IEEE показывают, что пропускную способность каналов связи требует увеличивать вдвое раз в два года.

Средняя скорость мобильных соединений с 2012 по 2017 год вырастет в 7 раз. Этот показатель стал важнейшим фактором, поддерживающим рост объема мобильного трафика.

ПРОГРАММНО-КОНФИГУРИРУЕМАЯ СЕТЬ SDN

Архитектура SDN



В архитектуре SDN выделяется три уровня :

- ❖ инфраструктурный уровень, предоставляющий набор сетевых устройств (коммутаторов и каналов передачи данных);
- ❖ уровень управления, включающий в себя сетевую операционную систему, которая обеспечивает приложениям сетевые сервисы и программный интерфейс для управления сетевыми устройствами и сетью;
- ❖ уровень сетевых приложений для гибкого и эффективного управления сетью.

Программно – конфигурируемая сеть

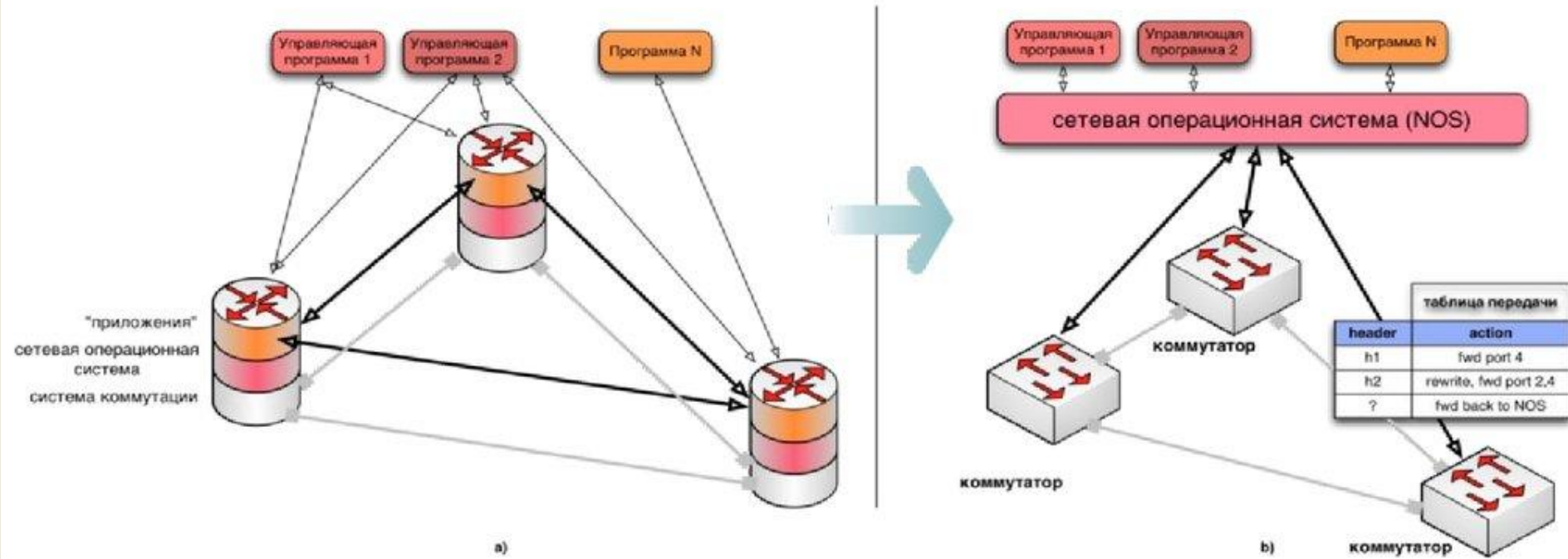
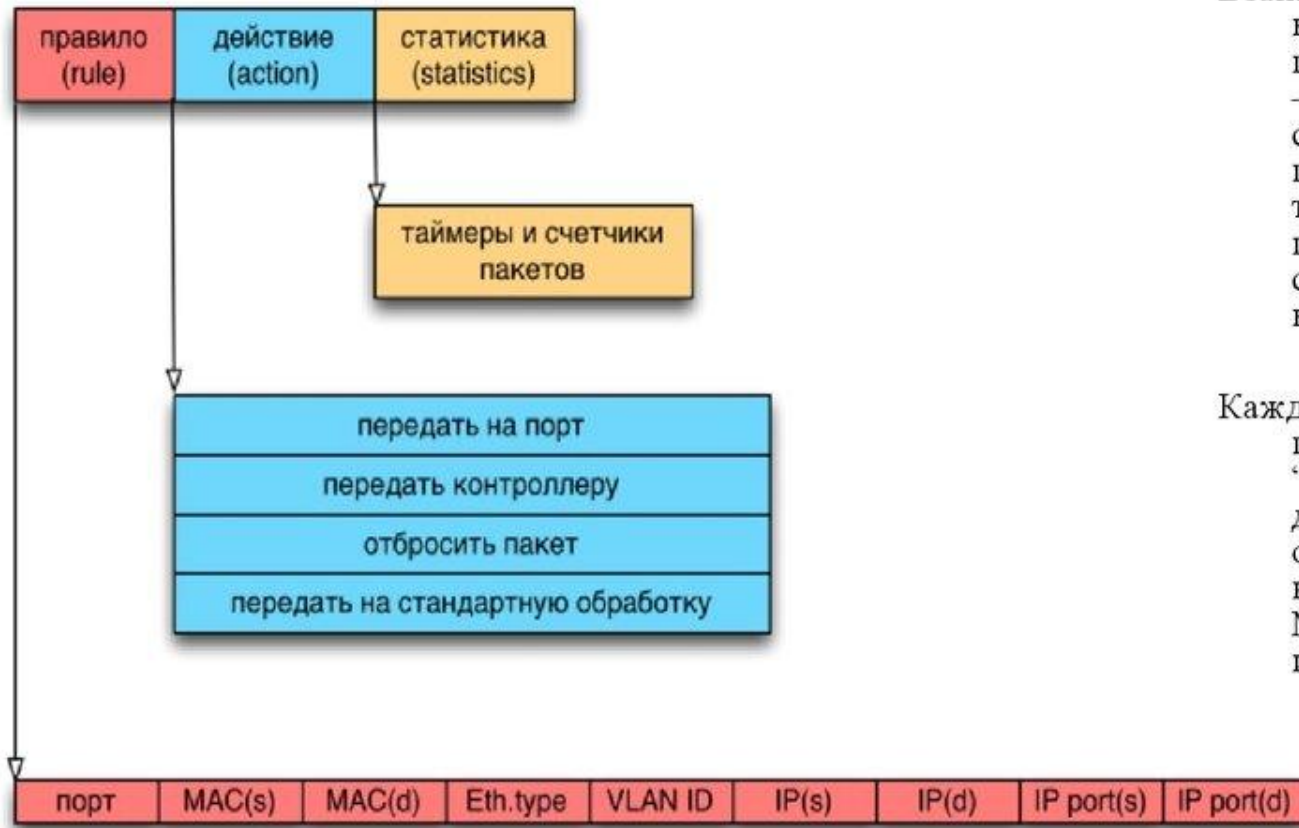


Рисунок 2.2 – Разделение системы управления и передачи в архитектуре SDN. (a) Традиционная архитектура с автономными сетевыми элементами, (b) архитектура SDN с централизованной управляющей функцией.

Концепция SDN предусматривает передачу управляющих функций центральному серверу – так называемому контроллеру, таким образом заменяя традиционную распределяемую модель маршрутизации на централизованную.

В отличие от традиционной сети, где маршрутизация – это распределенный итеративный процесс, при котором рабочая топология сети вычисляется совместно всеми устройствами, в SDN – это программа моделирования сети с заданными параметрами.

Обзор стандарта OpenFlow 1.3



Взаимодействие контроллера с коммутатором осуществляется посредством протокола OpenFlow – каждый коммутатор должен содержать одну или более таблиц потоков (flow tables), групповую таблицу (group table) и поддерживать канал (OpenFlow channel) для связи с удаленным контроллером – сервером.

Каждая запись абстрактной таблицы передачи OpenFlow является “правилom” и связана с потоком данных (flow). Поток определяется заголовком пакета – например, комбинацией адресов MAC, IP и номеров портов источника и получателя данных

Рисунок 3.2 – Структура таблицы передачи, OpenFlow

МЕХАНИЗМ РАБОТЫ коммутатора OpenFlow

- ❖ Передача пакета, принадлежащего потоку, в указанный порт.
- ❖ Инкапсулирование и передача пакета, принадлежащего потоку, контроллеру. Пакет доставляется через защищённое соединение после того, как инкапсулируется и отправляется контроллеру.
- ❖ Отбросить пакет, принадлежащий потоку.

Протокол конфигурации и управления OpenFlow

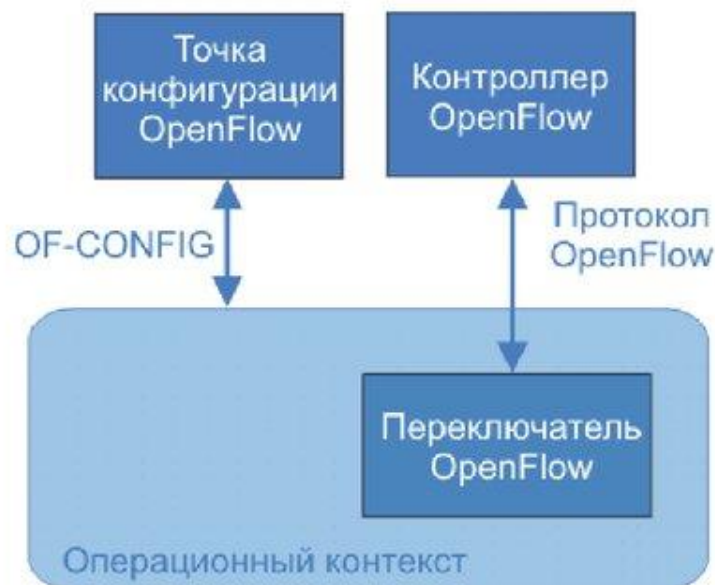


Рисунок 3.4 – Точка конфигурации OpenFlow взаимодействует с операционным контекстом используя конфигурацию и протокол управления (OF-CONFIG).

Протокол OpenFlow предполагает, что в технологии OpenFlow обмен данными был сконфигурирован с учетом необходимых данных, таких как IP-адреса контроллеров. Целью протокола конфигурации OpenFlow (OF-CONFIG) является предоставление возможности удаленного конфигурирования обмена данными.

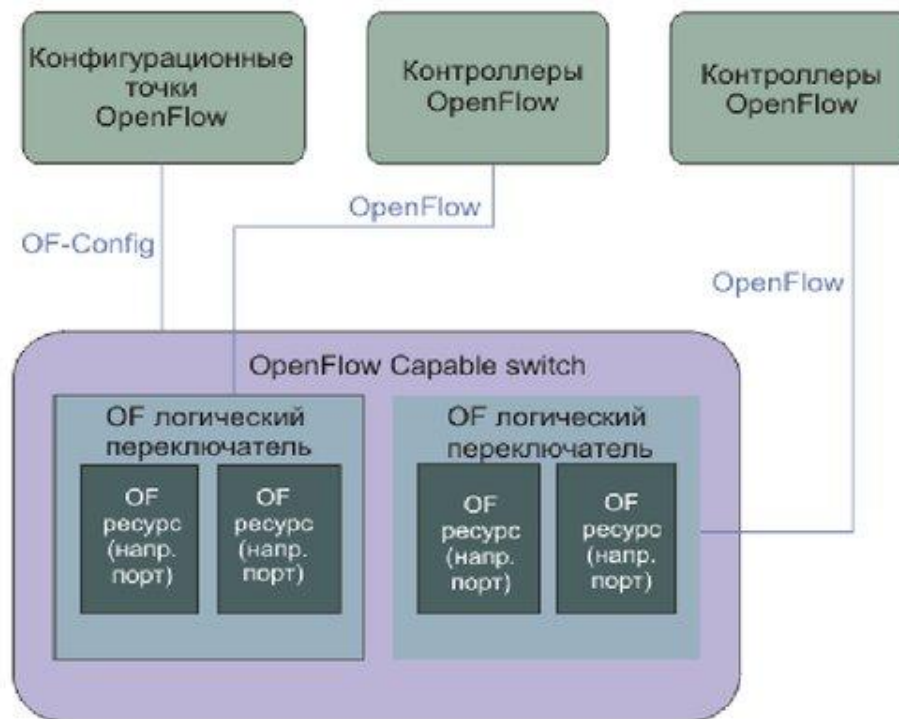


Рисунок 3.5 – Взаимодействия между компонентами спецификации протоколов OF-CONFIG и OpenFlow

Логические переключатели OpenFlow

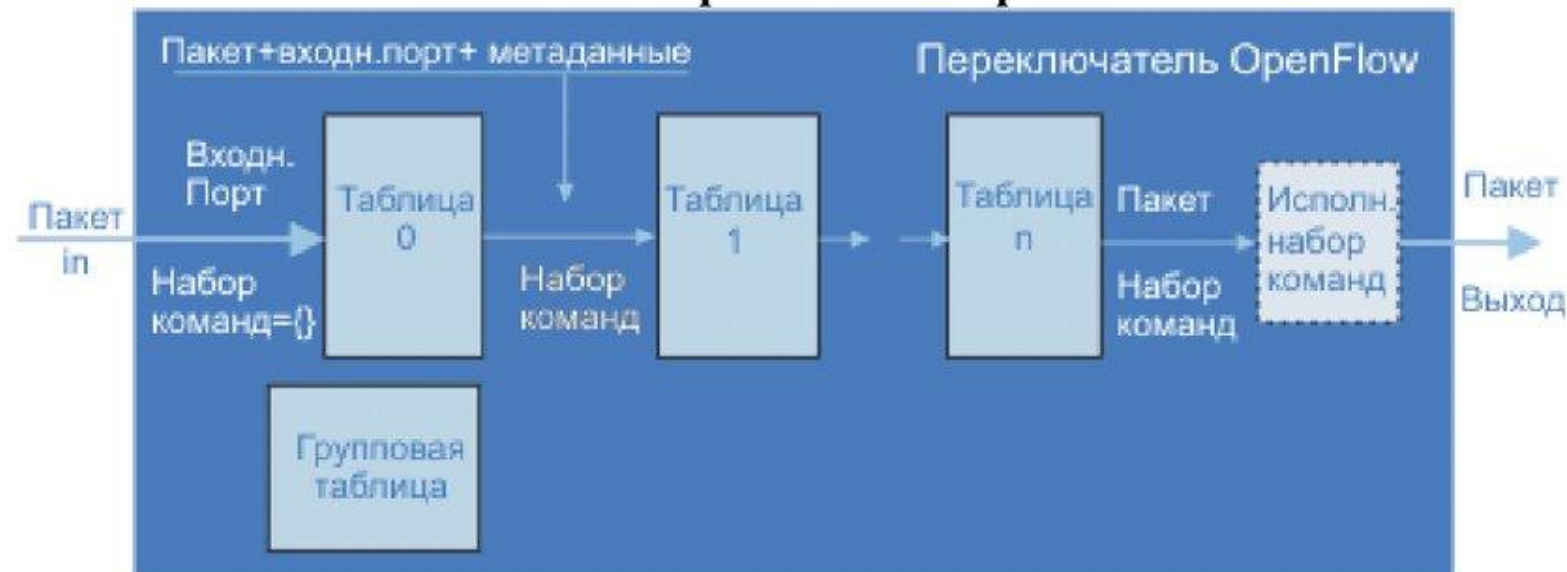


Рисунок 3.6 - Внутренние устройства переключателя OpenFlow

Таблицы пронумерованы, начиная с 0. Пакет будет передан для анализа следующей таблице, если он прошел фильтрацию предыдущей. Если пакет соответствует критериям отбора, выполняется определенный набор команд. При этом пакет может быть просто переадресован следующей таблице с помощью команды (goto). Каждая таблица переадресации коммутатора OpenFlow содержит набор записей, каждая из которых состоит из полей сравнения, счетчиков и набора инструкций, которые следует выполнить для каждого отобранного пакета. Таблица переадресации (Flow Table) состоит из списка свойств и является логическим контекстом.

Проверка начинается сначала для нулевой таблицы и может продолжаться с привлечением дополнительных таблиц. Сравнение пакетов с эталонами производится в соответствии с уровнем приоритета. Если соответствие в таблице найдено, выполняется соответствующий набор команд. Если соответствия в таблице переадресации не найдено, дальнейшие действия зависят от конфигурации: пакет может быть переадресован контроллеру, отброшен или может быть продолжена сверка для следующей таблицы.

ПРОГРАММНО-КОНФИГУРИРУЕМЫЕ СЕТИ В УПРАВЛЕНИИ СЕТЕВОЙ БЕЗОПАСНОСТЬЮ

- ❖ Безопасность в сетях традиционной инфраструктуры
- ❖ Инфраструктура
- ❖ Программное обеспечение
- ❖ Протоколы

ПЕРСПЕКТИВЫ РАЗВИТИЯ ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЕЙ

- ❖ Увеличение эффективности распределения сетевых ресурсов;
- ❖ Достижение максимально возможной сбалансированности нагрузки;
- ❖ Возможность разделить различные потоки и задать им индивидуальные правила обработки и управления трафиков в рамках единой сети;
- ❖ Возможность операторам в зависимости от поставленных целей задавать необходимые значения параметров и характеристики, что делает администрирование максимально удобным и простым;
- ❖ При необходимости можно будет тестировать все нововведения в рамках существующей физической сети для внесения корректировок перед применением их на практике

Выводы:

Программно-конфигурируемые сети позволяют решать задачи:

- ❖ Повышения пропускной способности каналов, упрощения управления сетью
- ❖ Перераспределения нагрузки, повышения масштабируемости сети
- ❖ Повышения безопасности сетей
- ❖ Снижения капитальных затрат
- ❖ Увеличения надежности функционирования сети с помощью централизованного управления конфигурацией сетевых параметров на уровне пользователей, устройств и приложений
- ❖ Динамической подстройки емкости виртуальной сети и других параметров под растущие потребности клиента без изменения физической топологии
- ❖ Создания изолированных виртуальных сетей для каждого клиента на базе единой физической инфраструктуры.

Спасибо за внимание!