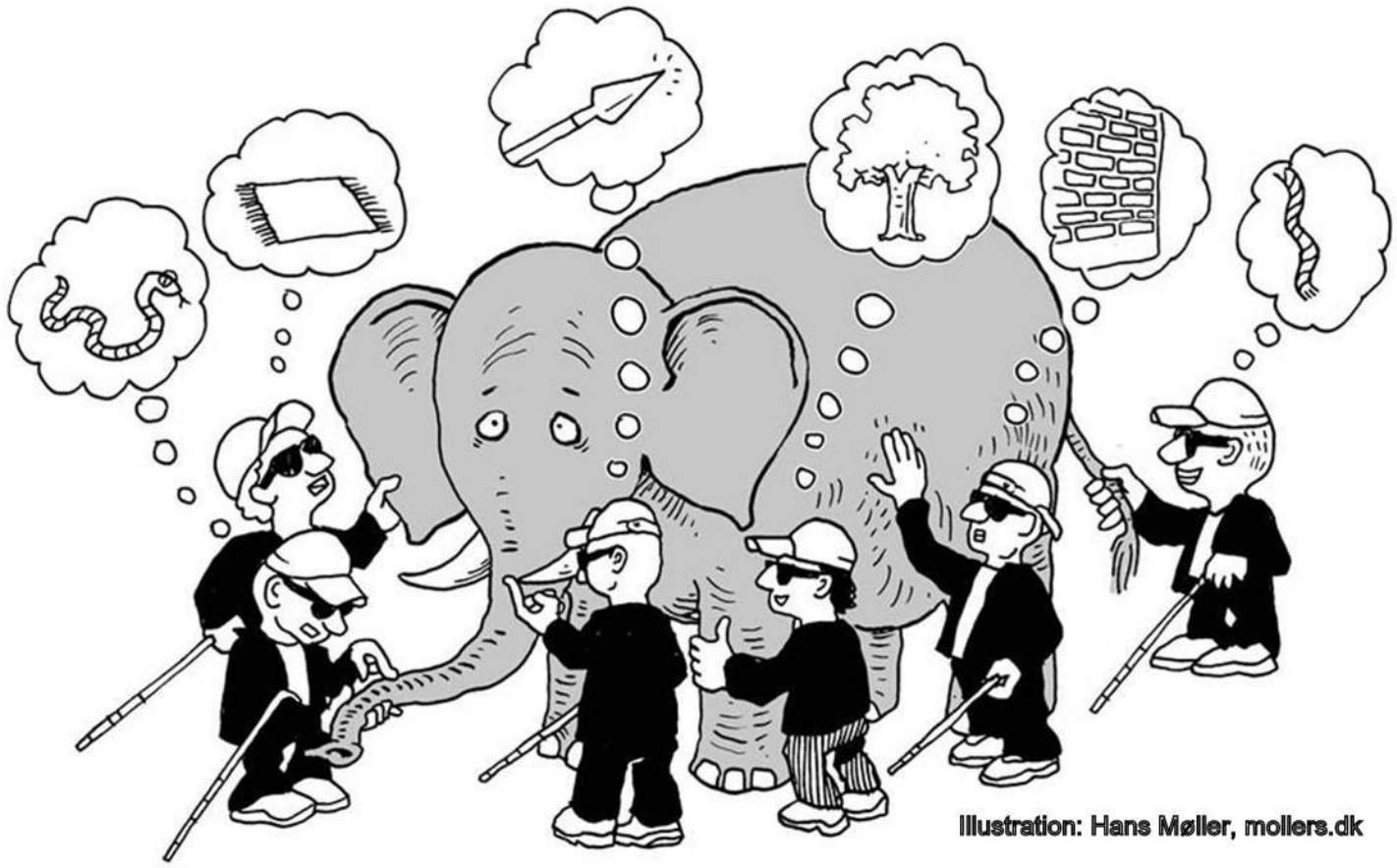
Программируемая сеть, думающая за вас: ночной кошмар или светлое будущее?!

Михаил Кадер, Cisco
mkader@cisco.com
security-request@cisco.com

Что такое Software Defined Network (SDN)?

Что такое программируемые сети (SDN)?



Множество определений

- Openflow
- Контроллер
- Openstack
- Оверлейные сети
- Сетевая виртуализация
- Автоматизация
- API
- Ориентированные на приложения
- Виртуальные сервисы
- Открытый vSwitch
- …

Терминология: SDN, OpenFlow, OpenStack, оверлейные сети….

Что такое программно управляемая сеть (SDN)?

"…В архитектуре SDN **разделены уровни управления и передачи данных,** обеспечена логическая централизация интеллектуальных сетевых механизмов и информации о состоянии сети, а низлежащая сетевая инфраструктура абстрагирована от приложений…"

Примечание. Как программное управление, так и автоматизация возможны и без SDN.

Источник: www.opennetworking.org

Что такое OpenFlow?

"…открытый стандарт, определяющий взаимодействие между разделёнными уровнями управления (контроллер) и передачи данных (агент)…"

Примечание. В SDN не обязательно используется OpenFlow.

Источник: www.opennetworking.org

Что такое OpenStack?

ПО с открытым исходным кодом для создания частных и публичных облаков; включает сервисы вычислений (Nova), сетевые сервисы (Quantum) и сервисы хранения (Swift).

Примечание. Может использоваться в SDN-сетях и не-SDN-сетях.

Источник: www.openstack.org

openstack

Что такое оверлейная сеть?

Оверлейная сеть создается на основе существующей сетевой инфраструктуры (физической или виртуальной) с помощью сетевого протокола. В качестве примеров протоколов оверлейных сетей можно привести GRE, VPLS, OTV, LISP и VXLAN.

Примечание. Может использоваться в SDN-сетях и не-SDN-сетях.

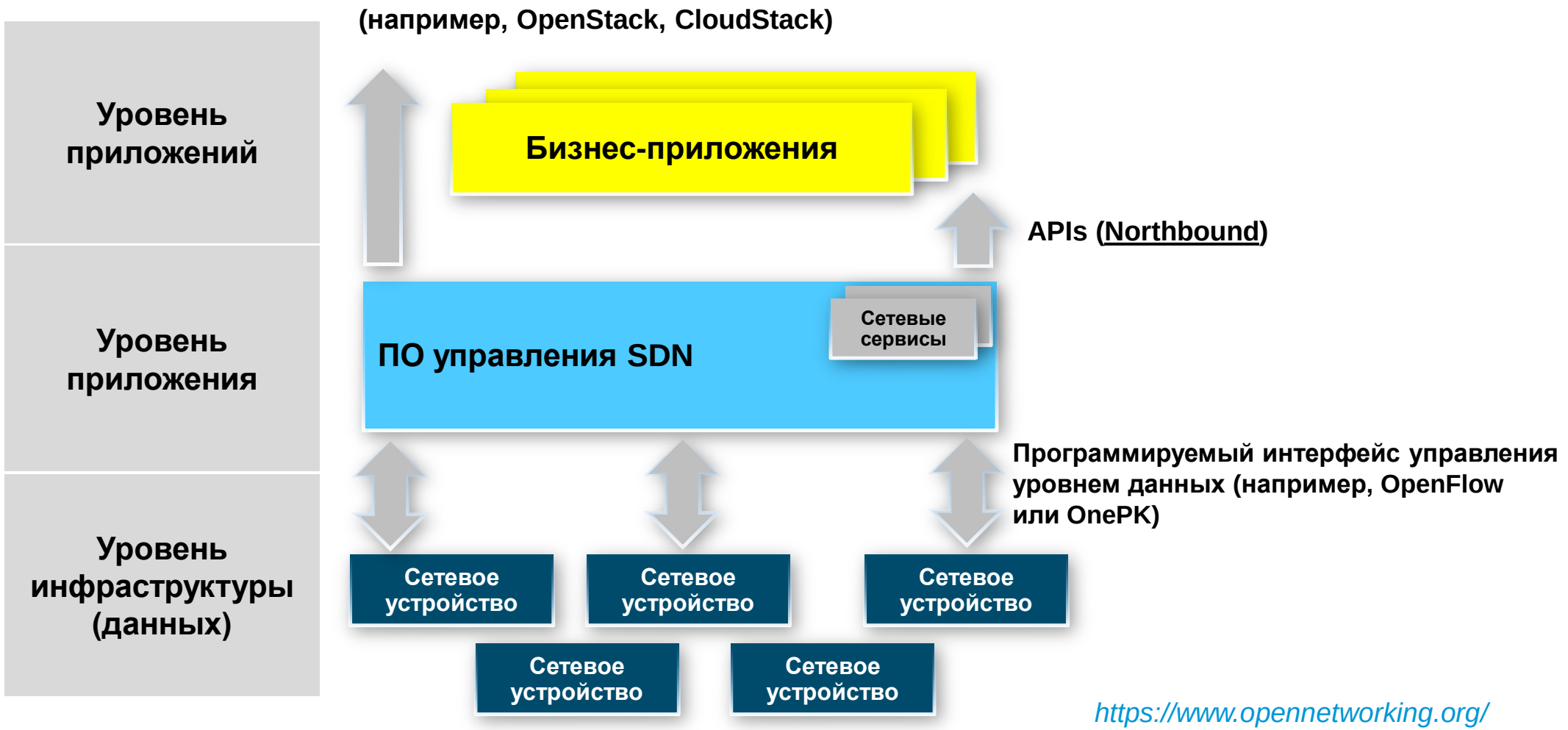
2 уровня – «Как передавать» и «Что передавать»

Уровень обработки	Где запускается	Показатели функционирования	Типы процессов и задач
Уровень управления	ЦПУ коммутатора	Тысячи пакетов в секунду	Протоколы маршрутизации (например, OSPF, IS-IS, BGP), Spanning Tree, SYSLOG, AAA (Authentication Authorization Accounting), NDE (Netflow Data Export), CLI (Command Line interface), SNMP
Уровень передачи данных	Специальный аппаратный ASIC	Миллионы или миллиарды пакетов в секунду	Коммутация L2 и L3 (IPv4 | IPv6), MPLS forwarding, VRF Forwarding, маркировка QOS (Quality of Service), классификация, Policing, сбор Netflow, ACL (Access Control Lists)

Уровень управления (Control Plane) и уровень передачи данных (Data Plane)

Два фундаментальных термина для понимания концепции SDN

Архитектура классической SDN: сетевые устройства передают трафик, не «думая» ни о чем



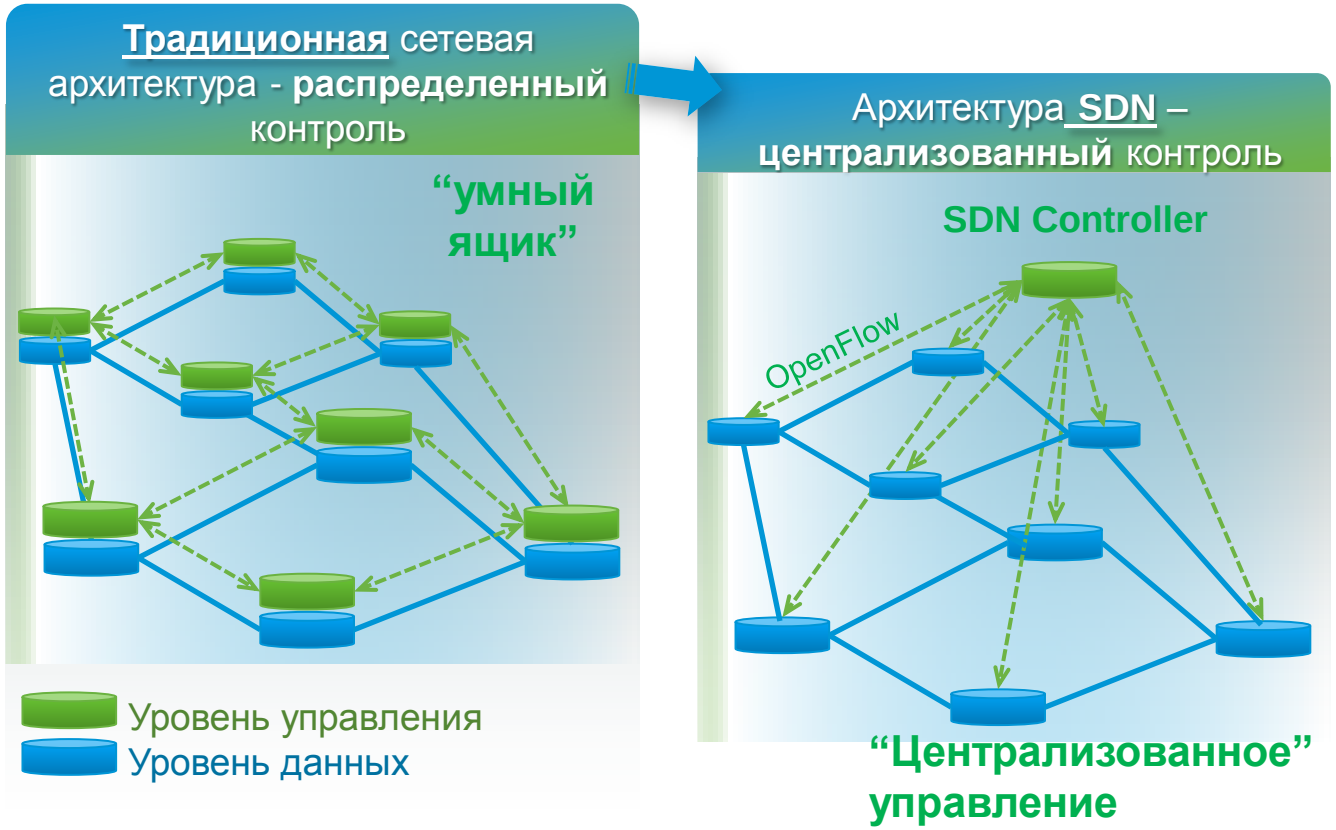
https://www.opennetworking.org/

Приложения, программирующие сетевое поведение

- Правила обработки пользовательского трафика задают сами приложения
  - Реализация собственных алгоритмов
  - Возможность избавиться от ненужных функций на сетевом уровне
- Управление трафиком в реальном времени
  - Оптимизация сети для различных приложений со специфичными требованиями
- Изоляция
  - Разделение сети между различными приложениями
- Унифицированные сетевые политики
  - Автоматизация и централизация сетевого управления
  - Эластичность сети
- Быстрое внедрение новых сервисов и процессов

В чем отличие SDN от традиционного построения сети?

- Переход от управления сетью на базе отдельного устройства к централизованному управлению
- Рост сетевой функциональности
- Адаптация к динамически изменяющимся потребностям
- Возможность изменений в реальном времени
- Еще дешевле и проще в управлении, чем современные сети



Классическая SDN – не панацея!

Что облегчает SDN?

- Сетевая виртуализация
- Изменение цепочки обработки трафика и реализация новых сервисов
- Применение политик
  - 5-tuple
  - (ограниченный) AVC
  - Фильтрация URL
  - Проверка репутации
- Сетевые сервисы
  - Балансировка нагрузки
  - QoS

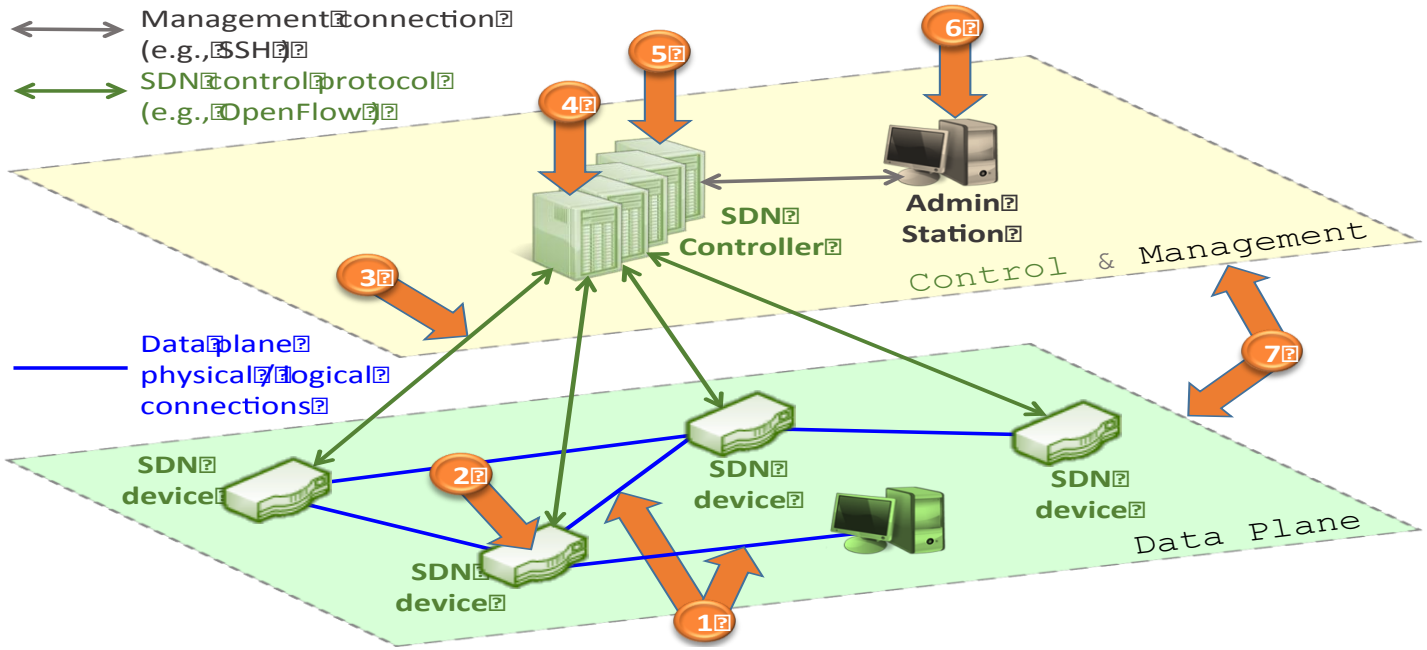
Что пока под вопросом

- Inter-domain
  - BGP
  - LISP
- Мультипакетные сервисы
  - Stateful inspect
  - DPI
- Производительность
  - Задержки обработки пакетов
  - Масштабирование контроллера
- Доступность
  - Сложность переноса логики из действующей сети в контроллер
  - Требуется кластеризация
- Зрелость технологии

Безопасность SDN

Вектора атак на SDN

- Канал от пользовательского до сетевого устройства
- Сетевое устройство
- Протокол управления сетевыми устройствами (OpenFlow, onePK)
- Контроллер SDN
- Станция управления
- Приложения
- API



- С точки зрения доступности, конфиденциальности, целостности, подотчетности, неотказуемости…

Особенности обеспечения безопасности классической SDN

- Классическая SDN базируется на публичных стандартах и интерфейсах
  - Хороши известный вектор для атаки
- Внешний доступ к внутренним ресурсам сетевого устройства
- Каскадное распространение проблемы/уязвимости по всей SDN
- Отказ в облуживании на контроллер
- Легкость тестирования сценариев атак для злоумышленника
- Компрометация контроллера = компрометация всей сети

Спасибо!