

Программно-конфигурируемые сети (SDN)  
как возможный фундамент  
Сетей Будущего после 2020 года.  
Исследования по данному направлению в  
рамках деятельности МСЭ-Т

Фарид Нахли,  
Начальник отдела развития ИКТ  
ОАО «Гипросвязь»

# Содержание

1. Развитие технологий, предопределивших появление программно-конфигурируемых сетей
2. История появления и эволюция программно-конфигурируемых сетей
3. Принцип разделения функций управления и функций передачи данных
4. Начало и ход стандартизации SDN в рамках деятельности Сектора стандартизации МСЭ

1. Развитие технологий, предопределивших появление программно-конфигурируемых сетей
2. История появления и эволюция программно-конфигурируемых сетей
3. Принцип разделения функций управления и функций передачи данных
4. Начало и ход стандартизации SDN в рамках деятельности Сектора стандартизации МСЭ

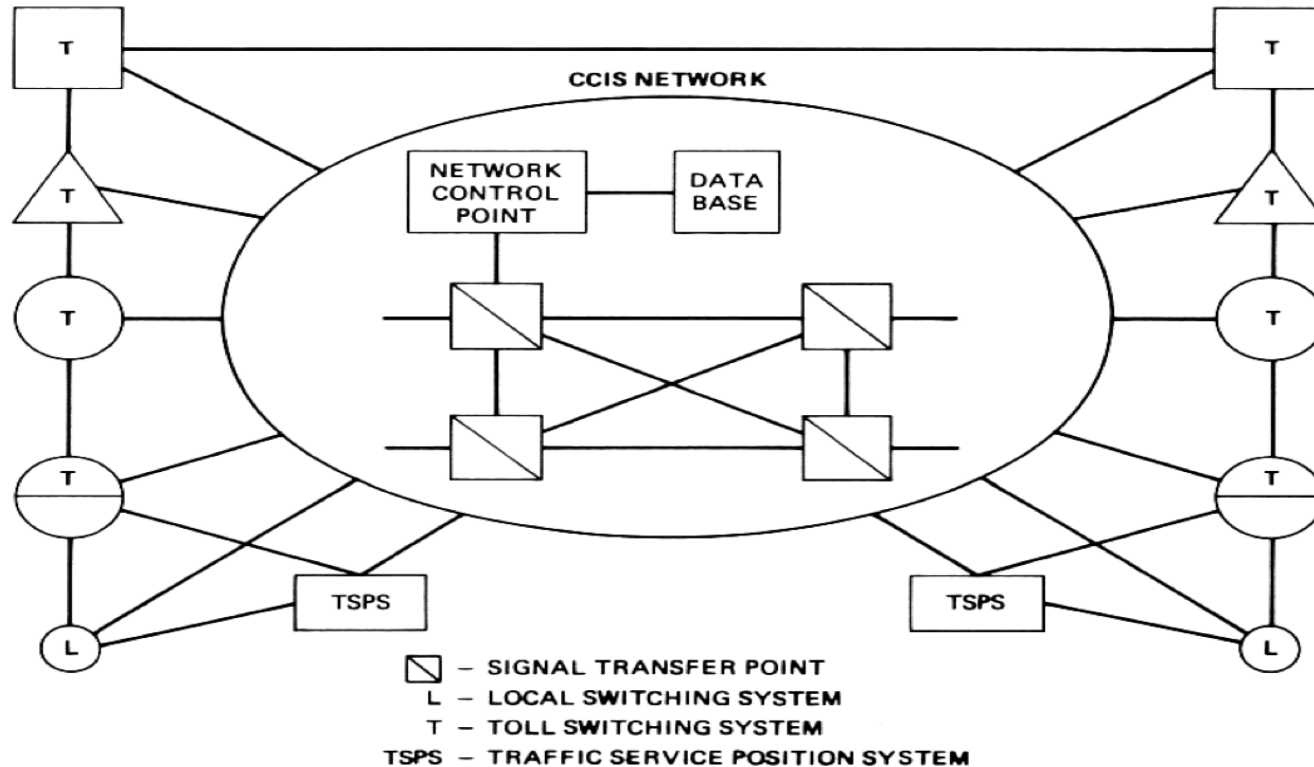
# Сопутствующие технологии

- **Централизованное управление сетью:** впервые стало применяться в 1980-х
- **Возможность программирования в сетях:** появилась в активных сетях в 1990-х
- **Виртуализация сетевых ресурсов:** появилась в 1990-х

Источник: Georgia Institute of Technology, Dr. Nick Feamster

# Централизованное управление сетью

В 1981 году с целью повышения эффективности управления и ускорения внедрения новых услуг был предложен принцип точки сетевого управления (Network Control Point, NCP)



Источник: Bell System Technical Journal, Vol. 61, No. 7 (1982)

# Централизованное управление сетью

В результате внедрения такого подхода были получены следующие преимущества:

- Сокращение затрат за счет возможностей уменьшения времени удержания канала и возможности запроса состояния канала перед отправкой запроса на его использование
- Быстрое внедрение новых услуг за счет существенно возросшей гибкости и масштабируемости
- Появление возможности непосредственного мониторинга состояния всей сети
- Возможность независимого развития инфраструктуры и услуг на основе анализа загруженности сети и объема и характера пользовательских данных

Источник: Georgia Institute of Technology, Dr. Nick Feamster

# Активные сети

## Что такое активные сети:

- Сети, в которых коммутационное оборудование выполняет вычислительные операции над пакетами
- Примеры – трассировочное ПО, firewall, proxy, application servers

## Мотивация и история развития:

- Активно продвигались DARPA research community в 1994-1995
- Для ускорения инноваций, в том числе по инициативе пользователей
- Активное оборудование могло использоваться с устаревшим
- Каждый программируемый коммутатор мог выполнять дополнительные вычисления

Источник: Georgia Institute of Technology, Dr. Nick Feamster

# Активные сети

## Не получили широкого распространения:

- Неподходящее время для их появления, не существовало ЦОДов и облачных решений
- Высокая стоимость аппаратной части
- Не были проработаны вопросы безопасности
- В качестве потенциального программиста рассматривались конечные пользователи, хотя это должен быть администратор сети
- Вопросы совместимости

При разработке протокола **OpenFlow** были учтены допущенные ошибки, он позволяет просто обновлять ПО, а также содержит в себе необходимые базовые функции

Источник: Georgia Institute of Technology, Dr. Nick Feamster



# Виртуализация сетевых ресурсов

## Что такое виртуализация:

- Построение нескольких сетевых топологий на одной инфраструктуре
- Примеры: VLAN, VMWare, Nicira и др.

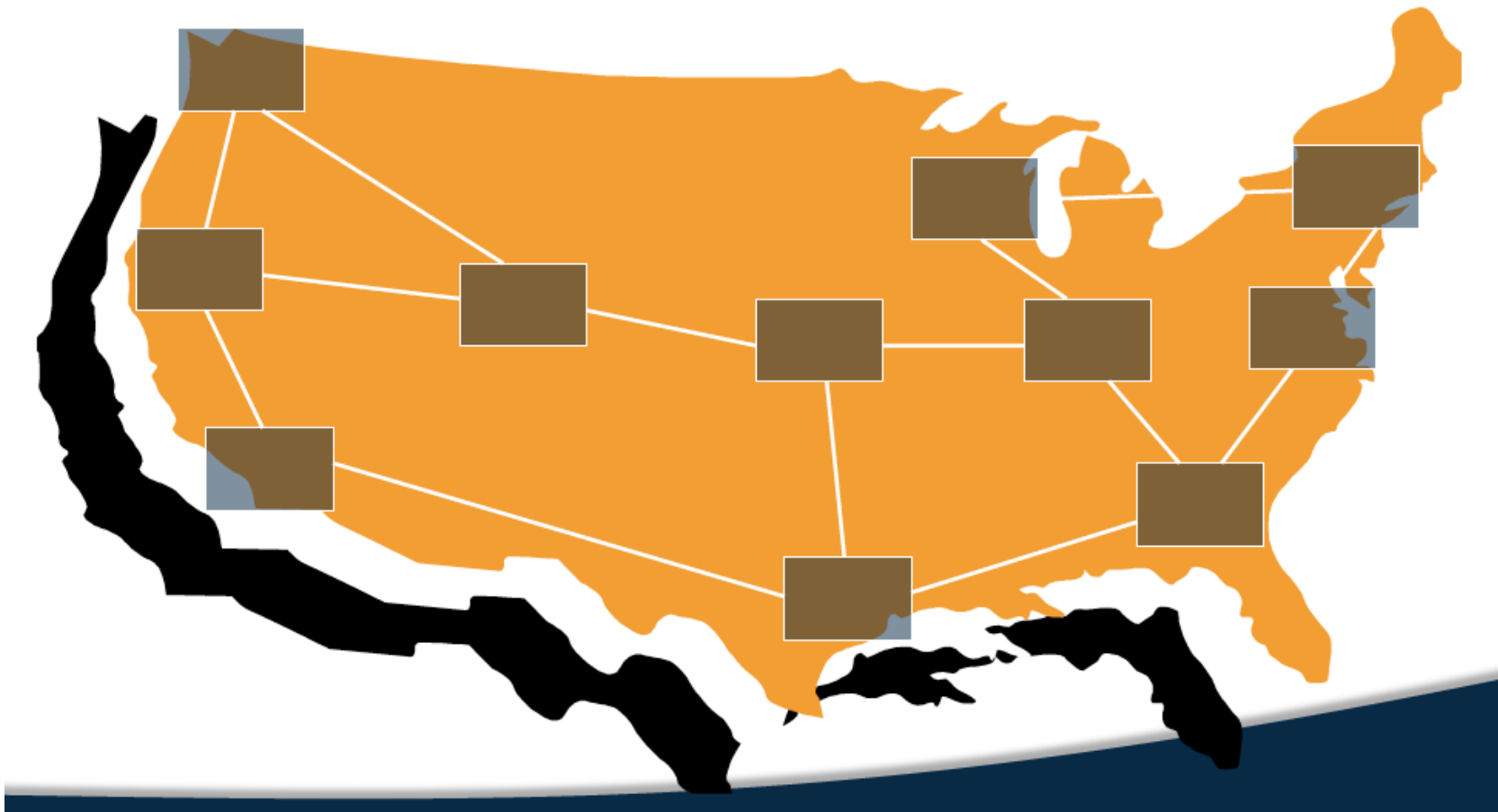
## Преимущества:

- Много логических маршрутизаторов на одной платформе
- Изоляция разных типов ресурсов (память, процессор, полоса пропускания)
- Настраиваемое ПО
- Типовые процессоры для выполнения функций управления

Источник: Georgia Institute of Technology, Dr. Nick Feamster

# Виртуализация сетевых ресурсов

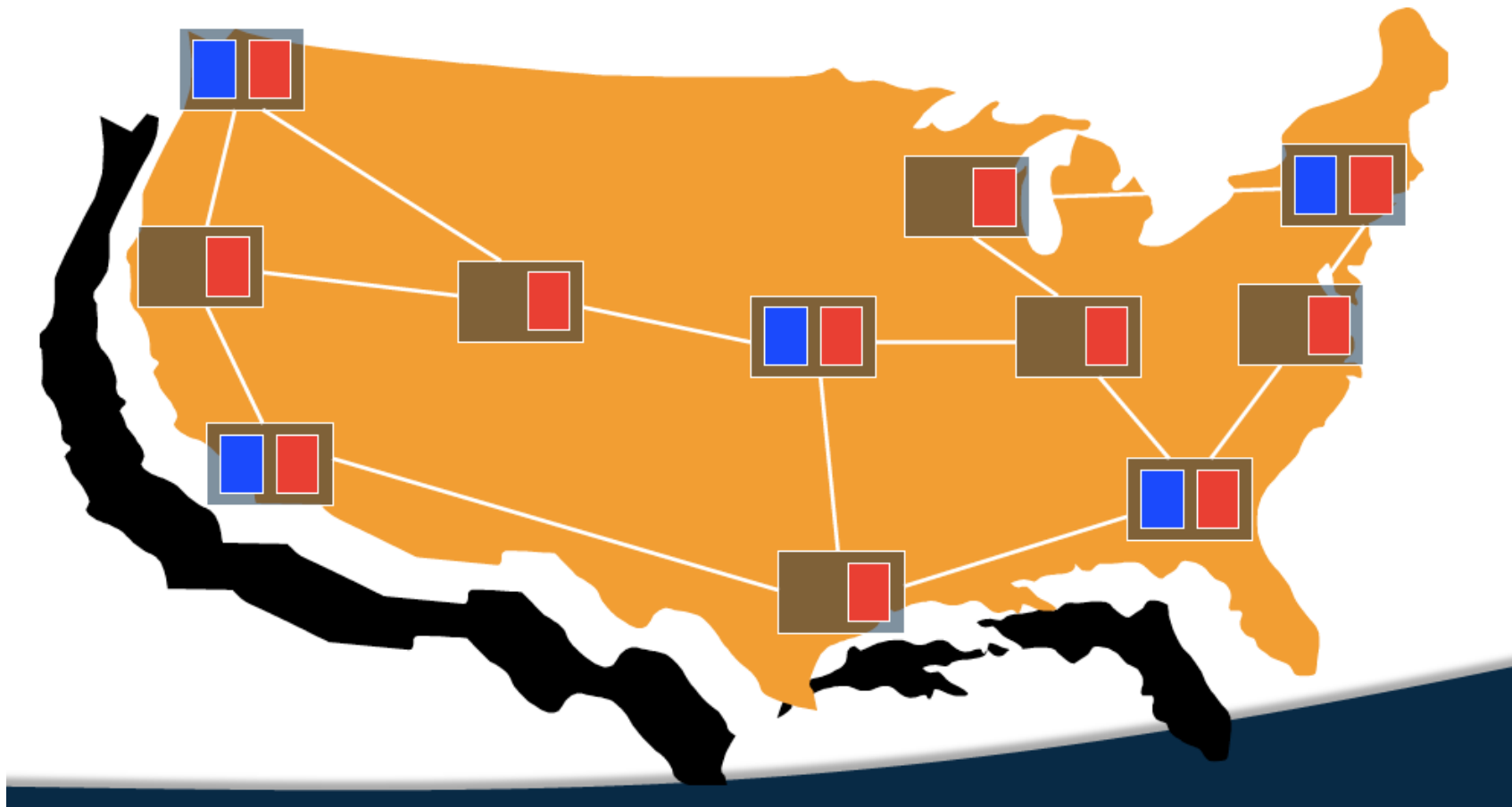
## Пример фиксированной инфраструктуры



Источник: Georgia Institute of Technology, Dr. Nick Feamster

# Виртуализация сетевых ресурсов

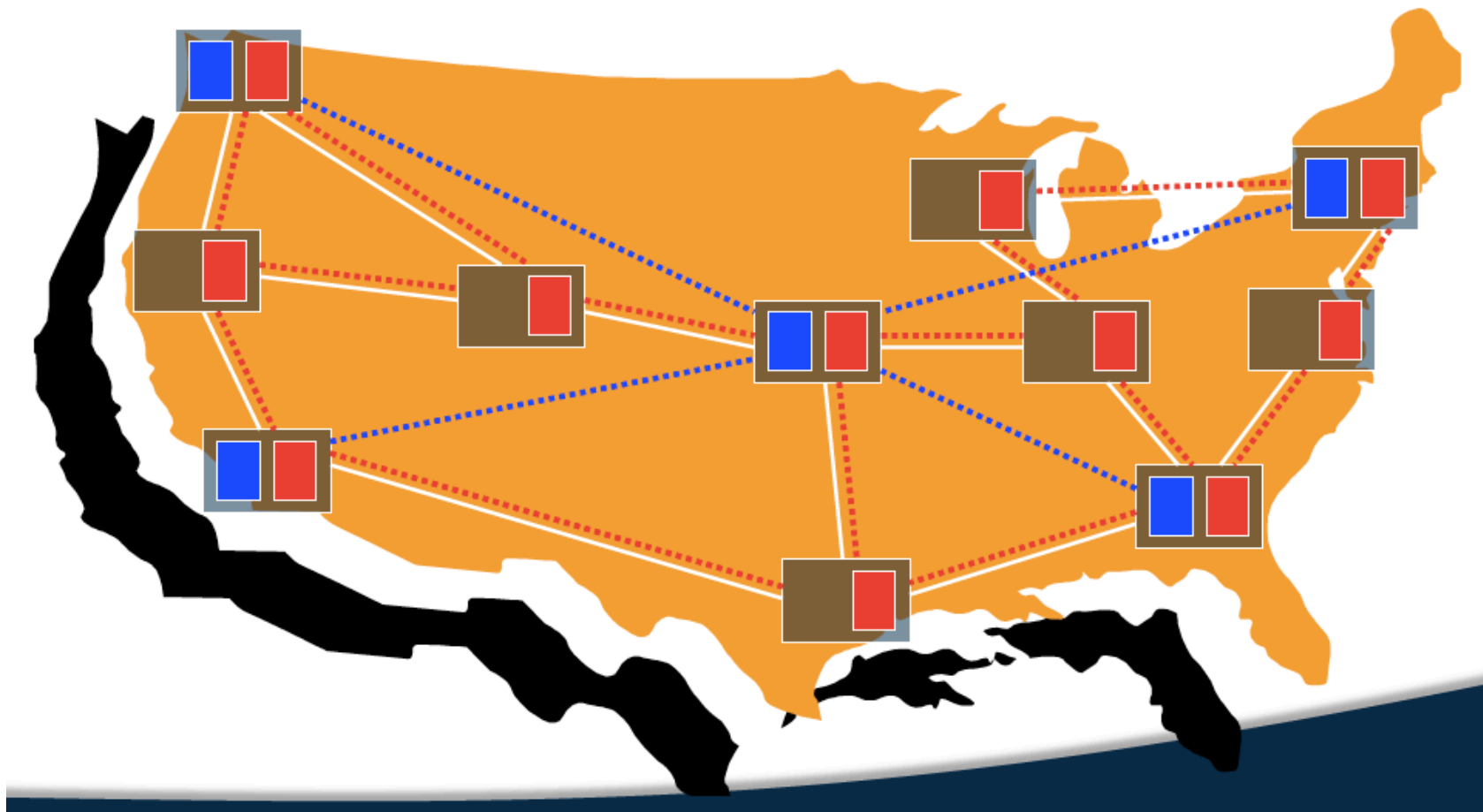
## Пример совместного использования инфраструктуры



Источник: Georgia Institute of Technology, Dr. Nick Feamster

# Виртуализация сетевых ресурсов

## Произвольная виртуальная топология



Источник: Georgia Institute of Technology, Dr. Nick Feamster

1. Развитие технологий, предопределивших появление программно-конфигурируемых сетей

2. История появления и эволюция программно-конфигурируемых сетей

3. Принцип разделения функций управления и функций передачи данных

4. Начало и ход стандартизации SDN в рамках деятельности Сектора стандартизации МСЭ

# История появления SDN

В последние годы наблюдается повышенный интерес к программно-конфигурируемым сетям, но стоит отметить, что лежащие в основе идеи развивались **уже более 20 лет**.

В некоторых вопросах SDN возвращаются к идеям из **ранних телефонных сетей**, например, в четком разделении функций контроля и функций передачи данных для упрощения сетевого администрирования. В тоже время **открытость, предоставляемая OpenFlow** позволяет упростить процесс инноваций на таких сетях.

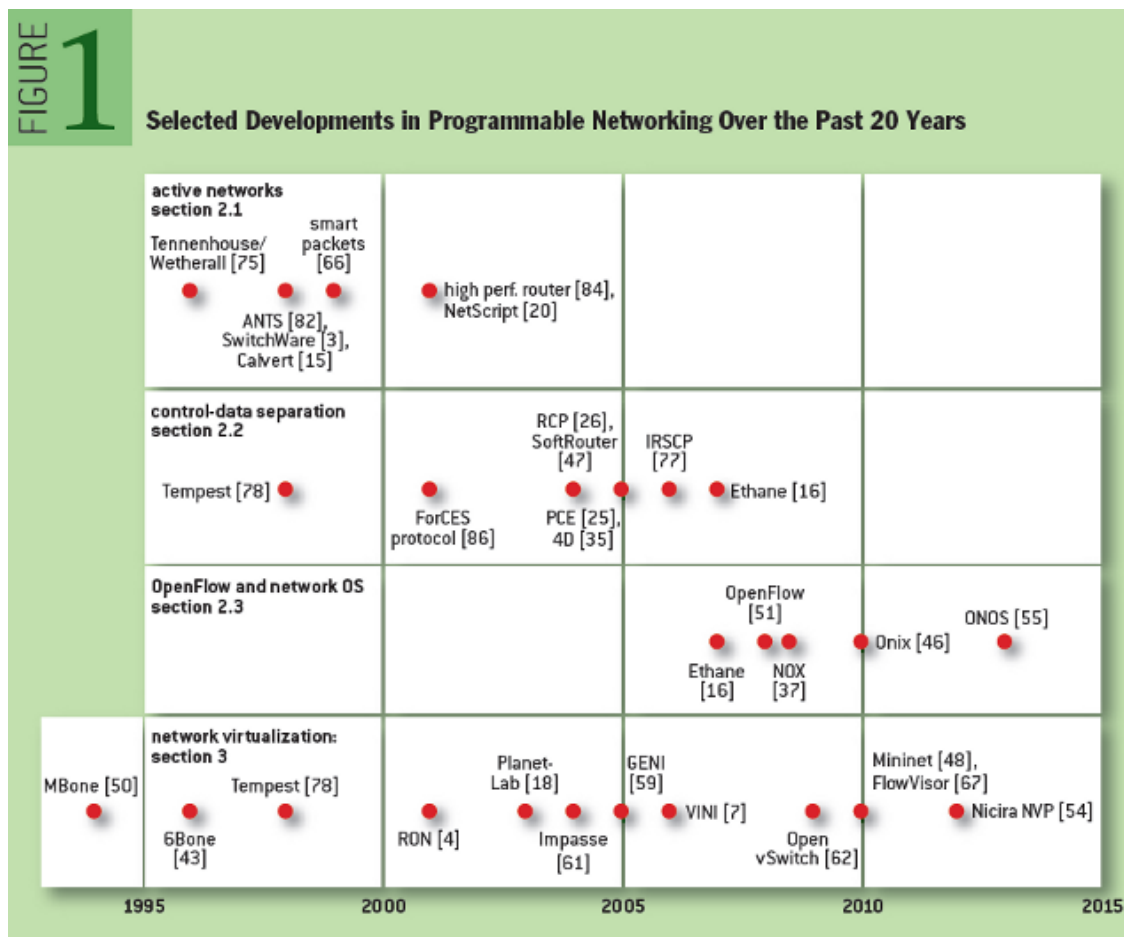
Другими словами, идеологи SDN используют **ряд хорошо известных принципов и подходов построения сетей**.

**Термин SDN** получил широкую распространенность в **2009 году**.

Источник: <http://queue.acm.org/detail.cfm?id=2560327>

# История появления SDN

Проекты по направлению программно-конфигурируемых сетей за последние 20 лет



Источник: <http://queue.acm.org/detail.cfm?id=2560327>

# История появления SDN

## I. Этап активных сетей:

- Более широкие возможности внедрения новых приложений, ученым были нужны новые возможности, были предприняты первые попытки сделать сети программно-конфигурируемыми
- Толчок со стороны технологий: снижение стоимости вычислений, интерес инвесторов
- Практическая необходимость: недовольство операторов сложностями развертывания новых технологических решений

## Вклад данного этапа:

- Программируемые функции сетей
- Виртуализация сетевых ресурсов
- Демультимплексирование на уровне приложений

Источник: <http://queue.acm.org/detail.cfm?id=2560327>



# История появления SDN

## II. Этап разделения функций контроля и передачи данных:

- Прагматичный подход – необходимость упростить решение задач инжиниринга трафика
- Толчок со стороны технологий: появление открытых интерфейсов между функциями контроля и передачи данных (например, ForCES), логическая централизация управления
- Необходимость решения проблем администрирования

### Вклад данного этапа:

- Логическая централизация функций контроля с открытыми интерфейсами в сторону маршрутизаторов и коммутаторов
- Распределенное управление состоянием контроллеров

Источник: <http://queue.acm.org/detail.cfm?id=2560327>

# История появления SDN

## III. Протокол OpenFlow:

- Функциональное обобщение – больше функций возлагается непосредственно на контроллеры, ограничивая гибкость, но увеличивая быстроту внедрения
- Технологически подходящий момент с точки зрения производителей чипсетов, оборудования, операторов и исследователей
- Начало использования в университетских сетях и ЦОДах

## Вклад данного этапа:

- Обобщение сетевых функций
- Появление понимания сетевой ОС: функции данных с открытыми API, плоскость управления состоянием
- Распределенные функции управления состоянием

Источник: <http://queue.acm.org/detail.cfm?id=2560327>

1. Развитие технологий, предопределивших появление программно-конфигурируемых сетей
2. История появления и эволюция программно-конфигурируемых сетей
3. Принцип разделения функций управления и функций передачи данных
4. Начало и ход стандартизации SDN в рамках деятельности Сектора стандартизации МСЭ

# Принцип разделения функций

## **Функции контроля и функции передачи данных:**

- Функции контроля – логика контроля процесса маршрутизации (например, протокол маршрутизации, конфигурации middlebox)
- Функции передачи данных – маршрутизация трафика в соответствии с заданной логикой (например, L3 маршрутизация, L2 коммутация)

## **Целесообразность разделения функций:**

- Независимость в развитии, т.е. программные решения контроля сети могут развиваться независимо от аппаратной части
- Выполнение функций контроля высокоуровневым ПО, что упрощает поиск ошибок и проверку состояния

Источник: Georgia Institute of Technology, Dr. Nick Feamster

# Принцип разделения функций

## Возможные применения:

- ЦОДы – переход к виртуализации, L2 маршрутизация
- Маршрутизация – улучшенный контроль над логикой принятия решений
- Корпоративное применение – решение вопросов безопасности
- R&D – совместное использование с существующими сетями

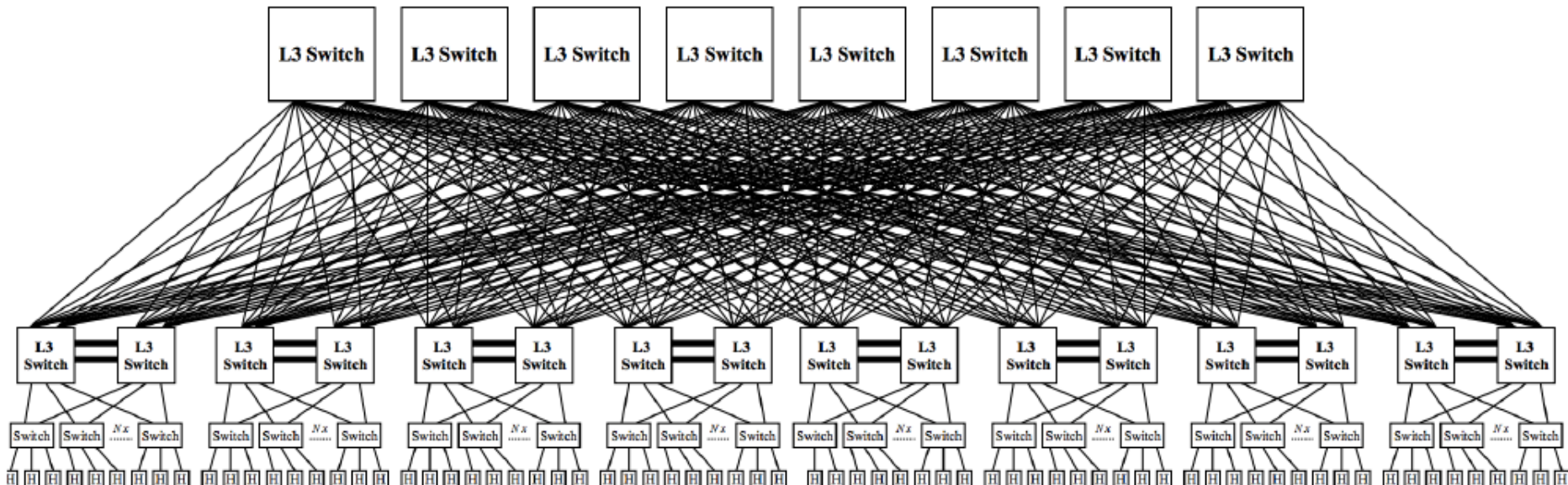
## Ограничения, которые необходимо преодолеть:

- Масштабируемость – количество контроллеров, которые должны отвечать за принятие решений маршрутизаторами и коммутаторами
- Надежность и безопасность – что произойдет, если контроллер откажет или будет взломан

Источник: Georgia Institute of Technology, Dr. Nick Feamster

# Пример: ЦОДы Yahoo

- Задача – 20 000 серверов в кластере = 400 000 виртуальных машин, необходимость быстрой балансировки нагрузки при изменениях в трафике, гарантированная целостность
- Решение – программное управление коммутаторами из центральной базы данных

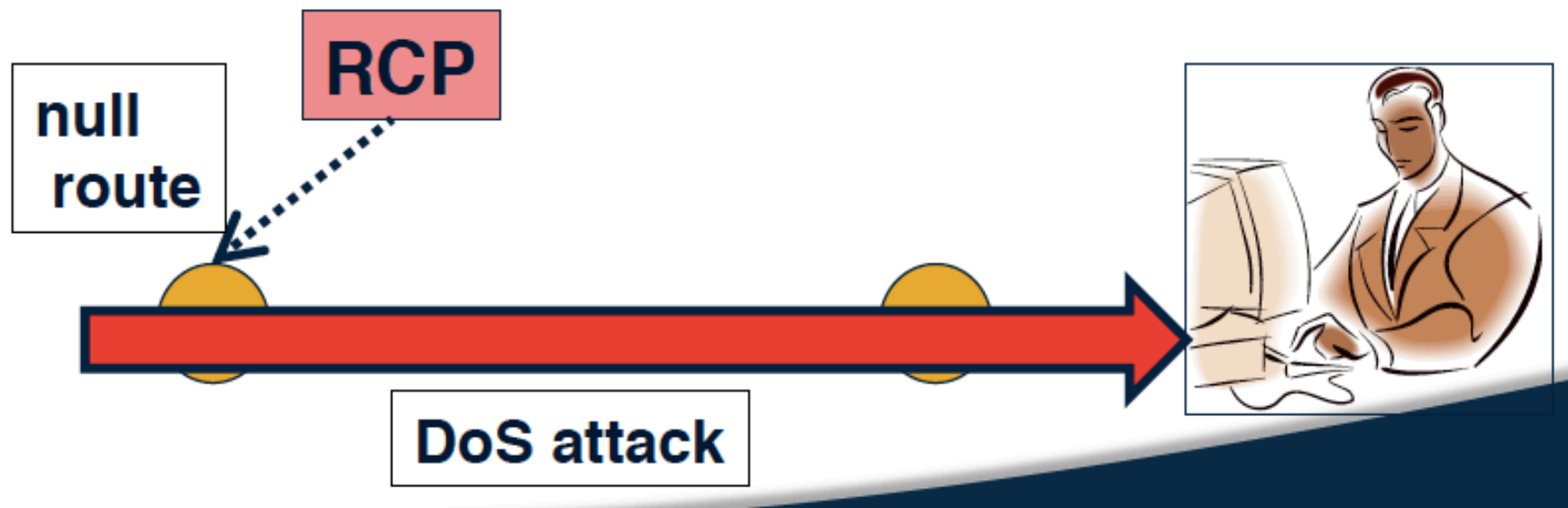


Источник: SDN in Warehouse-©-Scale Data Centers, Igor Gashinsky (<http://goo.gl/u9bWq>)

# Пример: Безопасность в сети AT&T

## Предотвращение сетевых атак:

- Измерительная система выявляет атаку
- Определяются точка входа и жертва атаки
- Вредоносный трафик отбрасывается в точке входа



Источник: Jennifer Rexford

# Возможности: междоменная маршрутизация

## Улучшение работы BGP:

- Сейчас существует ряд ограничений – выбор маршрута выполняется путем фиксированной последовательности шагов, возможности контроля входящего/исходящего трафика ограничены, сложно встроить вспомогательную информацию
- Решение – контроллеры могут обновлять состояние напрямую
- Применения – упрощенная балансировка трафика при плановом обслуживании пограничного маршрутизатора, непосредственный контроль пользователя над выбором маршрута, улучшенная безопасность междоменной маршрутизации за счет возможности выбора известных маршрутов

Источник: Jennifer Rexford



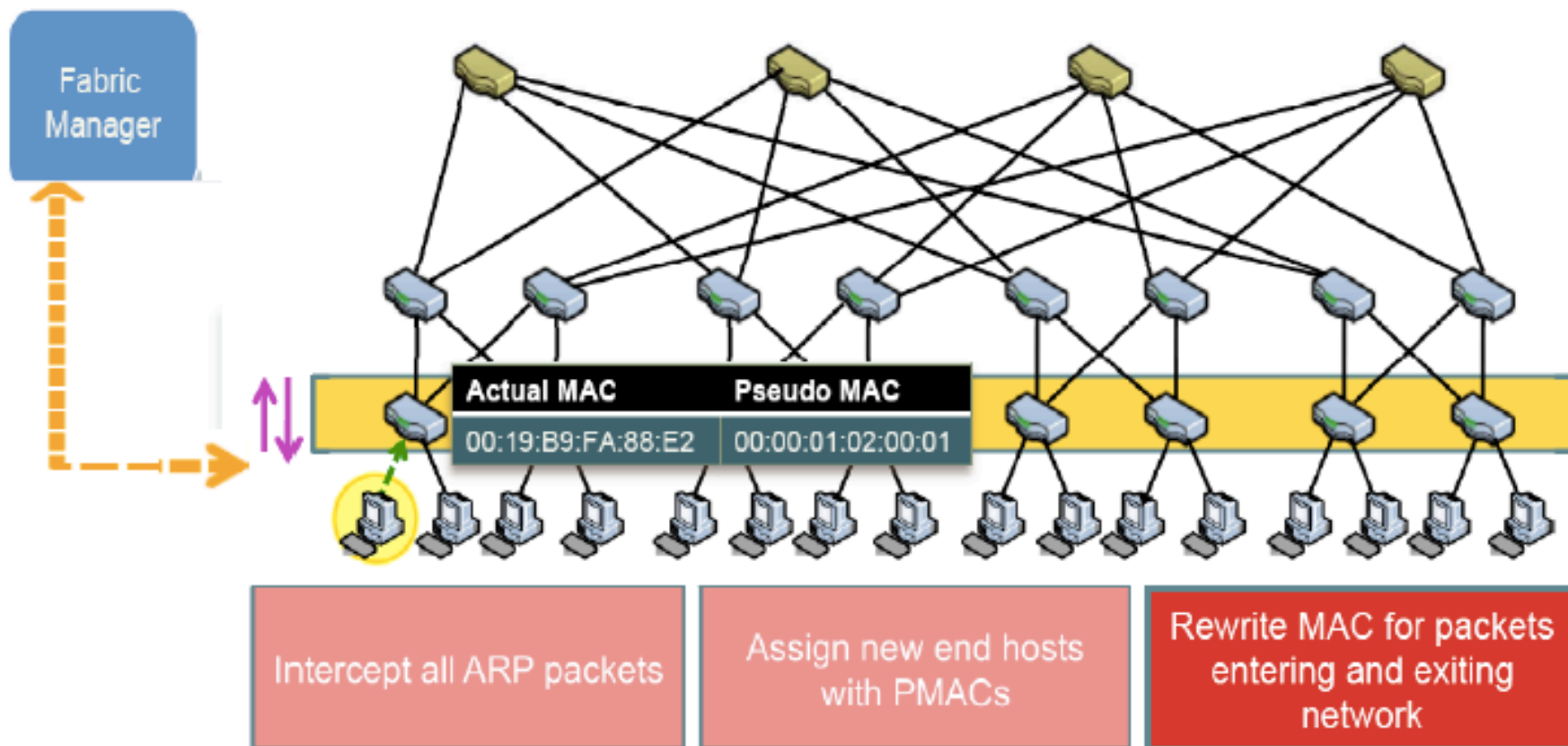
# Возможности: адресация в ЦОДах

## Как лучше реализовать адресацию в ЦОДах:

- L2 – проще конфигурировать/администрировать, но ограничена масштабируемость
- L3 – можно использовать существующие протоколы маршрутизации
- Оптимальное решение – совместить решения, использовать псевдо MAC-адреса, зависящие от топологии вместо независимы
- Для управления – Fabric manager перехватывает ARP-запросы и переписывает реальные MAC-адреса на псевдо

Источник: Georgia Institute of Technology, Dr. Nick Feamster

# Возможности: адресация в ЦОДах



Источник: Georgia Institute of Technology, Dr. Nick Feamster

# Другие возможности

- Динамический контроль доступа
- Улучшение возможностей перехода к новым решениям
- Балансировка нагрузки на сервера
- Виртуализация сетевых ресурсов
- Совместное использование нескольких беспроводных точек доступа
- Энергоэффективная работа сети
- Адаптивный мониторинг трафика
- Обнаружение DDoS-атак

Источник: Georgia Institute of Technology, Dr. Nick Feamster

## Ограничения: масштабируемость (на примерах решений RSP и ONIX)

**Проблема:** контроллер должен хранить маршруты и осуществлять вычисления для каждого маршрутизатора, которых может быть несколько тысяч

### **Пример решения в RSP:**

- Исключить избыточность – хранить только одну копию каждого маршрута и избегать избыточных вычислений
- Ускорить поиск – система индексации для быстрого поиска маршрутов
- Выполнять только маршрутизацию BGP

### **Пример решения в ONIX:**

- Декомпозиция – хранить только определенную часть NIB в памяти
- Агрегация – например, один контроллер на каждое здание и общий суперконтроллер

Источник: Georgia Institute of Technology, Dr. Nick Feamster

## Ограничения: надежность (на примерах решений RCP и ONIX)

**Проблема:** необходимо обеспечить надежную работу в случае отказа контроллера, а также добиться целостности в вычислениях нескольких контроллеров

### **Пример решения в RCP:**

- Дублирование контроллеров, при этом они работают в независимом режиме, но по идентичному алгоритму
- Получение информации о каждом сегменте, к которому подключен контроллер

### **Пример решения в ONIX:**

- Приложения несут ответственность за отслеживание отказа сетевого оборудования
- Координация распределена между несколькими идентичными контроллерами

Источник: Georgia Institute of Technology, Dr. Nick Feamster

1. Развитие технологий, предопределивших появление программно-конфигурируемых сетей
2. История появления и эволюция программно-конфигурируемых сетей
3. Принцип разделения функций управления и функций передачи данных
4. Начало и ход стандартизации SDN в рамках деятельности Сектора стандартизации МСЭ

# МСЭ-Т и SDN

Предпосылкой для начала работ по стандартизации SDN в МСЭ стало **собрание технических директоров крупнейших компаний отрасли**, которое состоялась 18 ноября 2012 года в г. Дубае. В коммюнике по итогам встречи отмечалось, что направление SDN должно стать одним из приоритетных направлений развития Сетей Будущего. В собрании принимали участие представители таких компаний как **Cisco, Ericsson, Etisalat, Fujitsu, Huawei, KDDI, NEC, NSN, NTT, Orange FT Group, RIM, Telecom Italia, Telecom South Africa и Verizon.**

Как следствие, на ВАСЭ-12 была принята **Резолюция 77** «Работа по стандартизации в области организации сетей с программируемыми параметрами в Секторе стандартизации электросвязи МСЭ», поручившая **ИК-13 и КГСЭ** организовать проведение необходимых работ для стандартизации SDN.

# МСЭ-Т и SDN

Раздел веб-сайта МСЭ, посвященный SDN <http://www.itu.int/en/ITU-T/sdn/Pages/default.aspx>

## Software-defined Networking (SDN)

YOU ARE HERE HOME > ITU-T > SOFTWARE-DEFINED NETWORKING (SDN)

SHARE    

The World Telecommunication Standardization Assembly (WTSA-12) in Dubai, UAE, 20-29 November, conferred on ITU-T a strong mandate to expand and accelerate its work in the SDN domain by adopting [Resolution 77 - Standardization work in ITU-T for software defined networking](#). This followed a meeting of the Chief Technology Officer (CTO) Group, 18 November 2012 where SDN was emphasized as a strategic priority (see Communiqué [here](#)). In addition the Global Standards Symposium (GSS-12) held the day preceding WTSA-12, 19 November 2012, attached similar weight to the topic; acting on the recommendations of the CTO Group by taking SDN as one of its points of focus and feeding the conclusions of its SDN discussion into WTSA-12.

SDN is considered a major shift in networking technology which will give network operators the ability to establish and manage new virtualized resources and networks without deploying new hardware technologies. ICT market players see SDN and network virtualization as critical to countering the increases in network complexity, management and operational costs traditionally associated with the introduction of new services or technologies. SDN proposes to decouple the control and data planes by way of a centralized, programmable control-plane and data-plane abstraction. This abstraction will usher in greater speed and flexibility in routing instructions and the security and energy management of network equipment such as routers and switches.

### STUDY GROUPS



### JOINT COORDINATION ACTIVITY (JCA)



#### Events

#### News

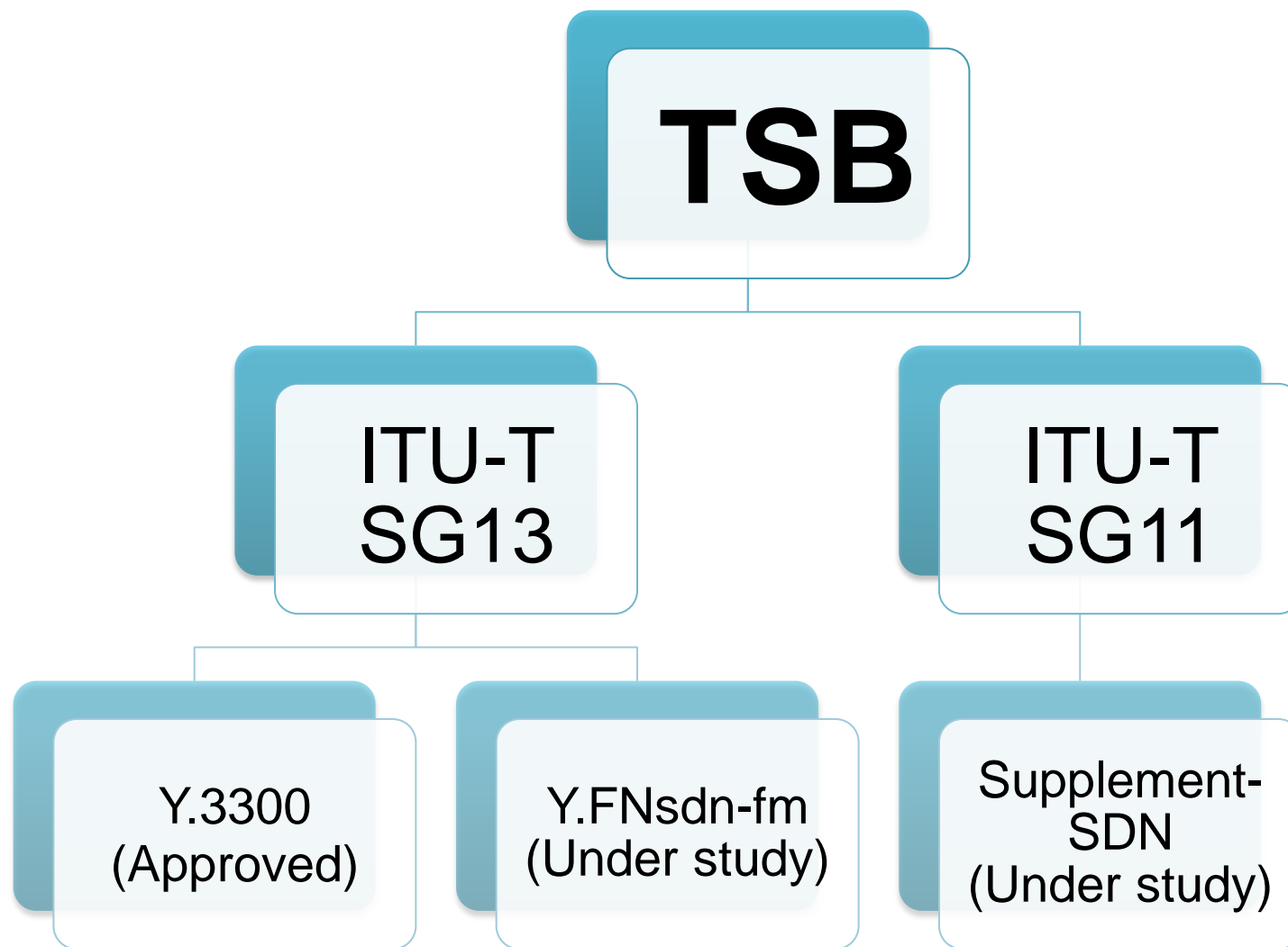
- ▶ Meeting of [SG11](#), including WP2/11 "[SDN and resource control](#)"  
09-16 July 2014, Geneva, Switzerland
- ▶ Meeting of [SG13](#), including WP3/13 "[SDN and networks of future](#)"  
07-18 July 2014, Geneva, Switzerland
- ▶ [JCA-SDN meeting](#)  
11 July 2014, Geneva, Switzerland

#### Past events

- ▶ [JCA-SDN meeting](#)  
19 February 2014, Geneva, Switzerland
- ▶ Meeting of SG11/WP2 "[SDN and resource control](#)"  
21 February 2014, Geneva, Switzerland
- ▶ Meeting of SG13/WP3 "[SDN and networks of future](#)"  
28 February 2014, Geneva, Switzerland
- ▶ Meeting of SG11/WP2 "[SDN and resource control](#)"  
7-13 Nov 2013, Kampala, Uganda
- ▶ Meeting of SG13 "Lead SG on SDN".  
This includes activities of its WP3/13 "[SDN and networks of future](#)"  
4-15 November 2013, Kampala, Uganda



# МСЭ-Т и SDN



# МСЭ-Т и SDN

**Y.3300** – Структура программно-конфигурируемых сетей. Рекомендация описывает структуру программно-конфигурируемых сетей и определяет базовые принципы SDN. Приведены основные определения, цели, высокоуровневые возможности и архитектура SDN. В Приложении также содержатся предложения по дальнейшему развитию стандартизации SDN.

Базовый текст – <http://www.itu.int/md/T13-SG13-140228-TD-WP3-0193>

**Y.FNsdn-fm** – Требования формальных спецификаций и методов проверки SDN. В документе описаны требования по использованию формальных спецификаций и способов проверки в контексте применения SDN как решения Сетей Будущего. В среде SDN неполное или вредоносное ПО может привести к нарушению функционирования оборудования. Адаптация формальных методов позволит повысить надежность таких сетей.

Базовый текст – <http://www.itu.int/md/T13-SG13-140228-TD-WP3-0194>

**Supplement-SDN** – Структура сигнализации в сетях SDN. В документе будут определены требования к сигнализации в сетях SDN, а также требования к интерфейсам и информации, передаваемой протоколами сигнализации. Определение этих требований позволит перейти к разработке протоколов сигнализации для SDN. Выполняемая работа будет согласовываться с работой ИК-13 МСЭ-Т.

Базовый текст – <http://www.itu.int/md/T13-SG11-140709-TD-GEN-0432/en>

# Спасибо за внимание!

# Thank you for your attention!

Фарид Нахли  
Начальник отдела развития ИКТ  
ОАО «Гипросвязь»

Тел.: +375 17 237-34-95  
Факс: +375 17 285-77-27  
E-mail: [nahli@giprosvjaz.by](mailto:nahli@giprosvjaz.by)