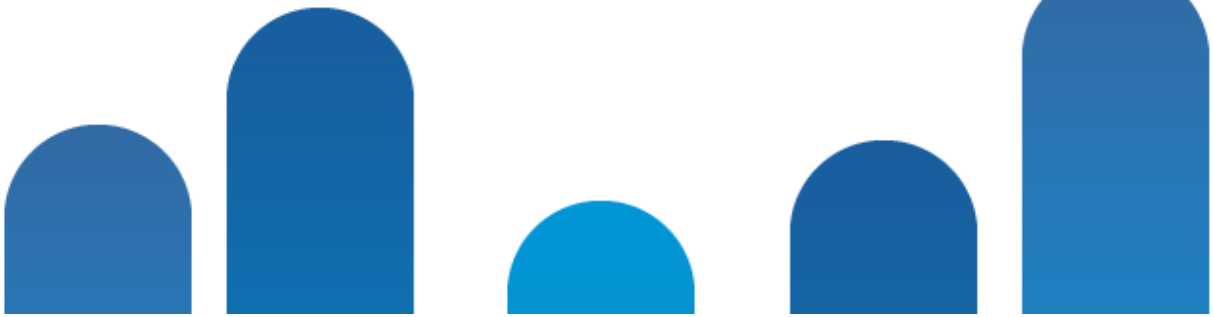
Cisco Expo 2012

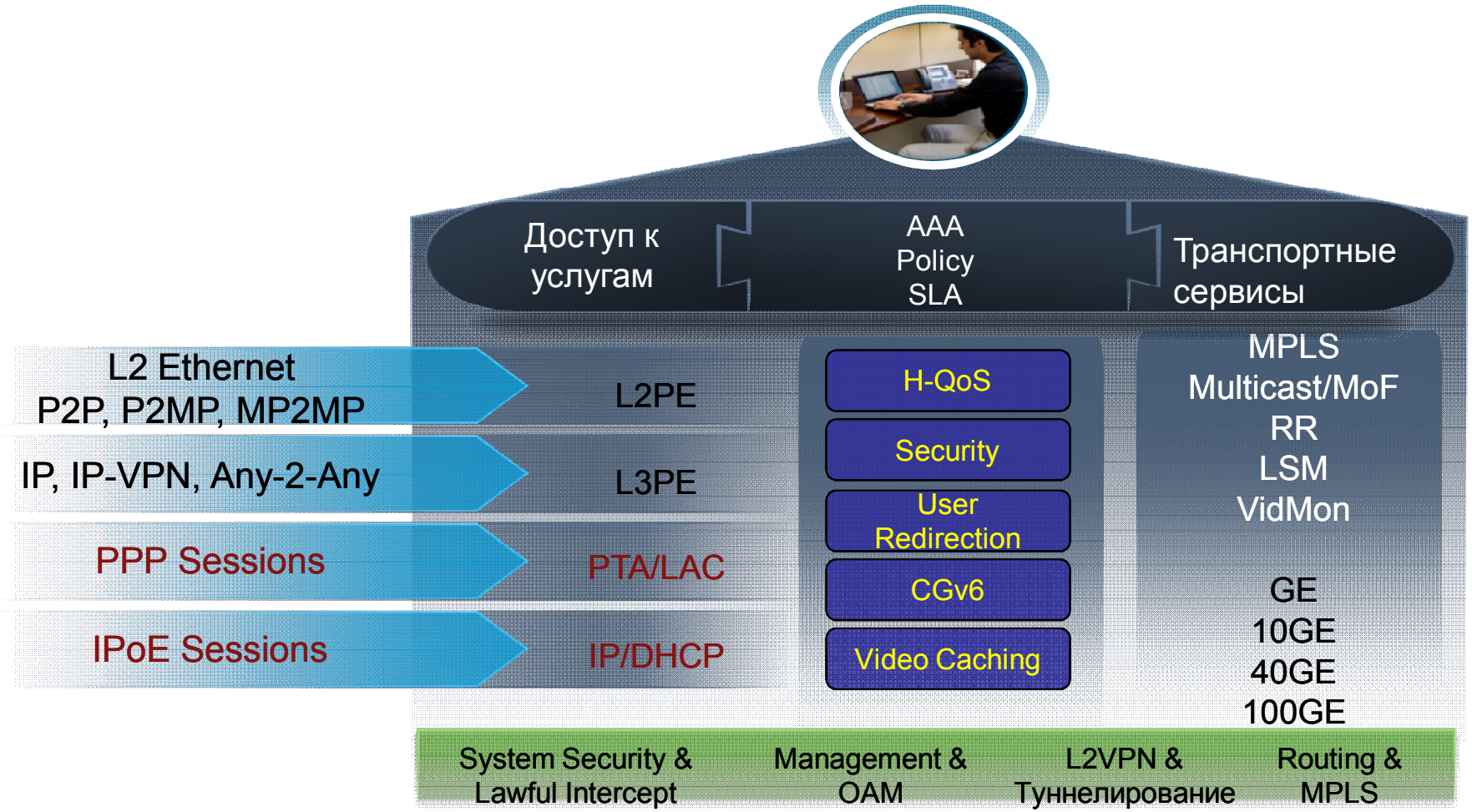
ASR 9000 как высокопроизводительный BNG: функционал и сценарии применения

Андрей Идлис
Системный инженер-консультант



BUILT FOR THE HUMAN NETWORK

BNG функционал на ASR 9000

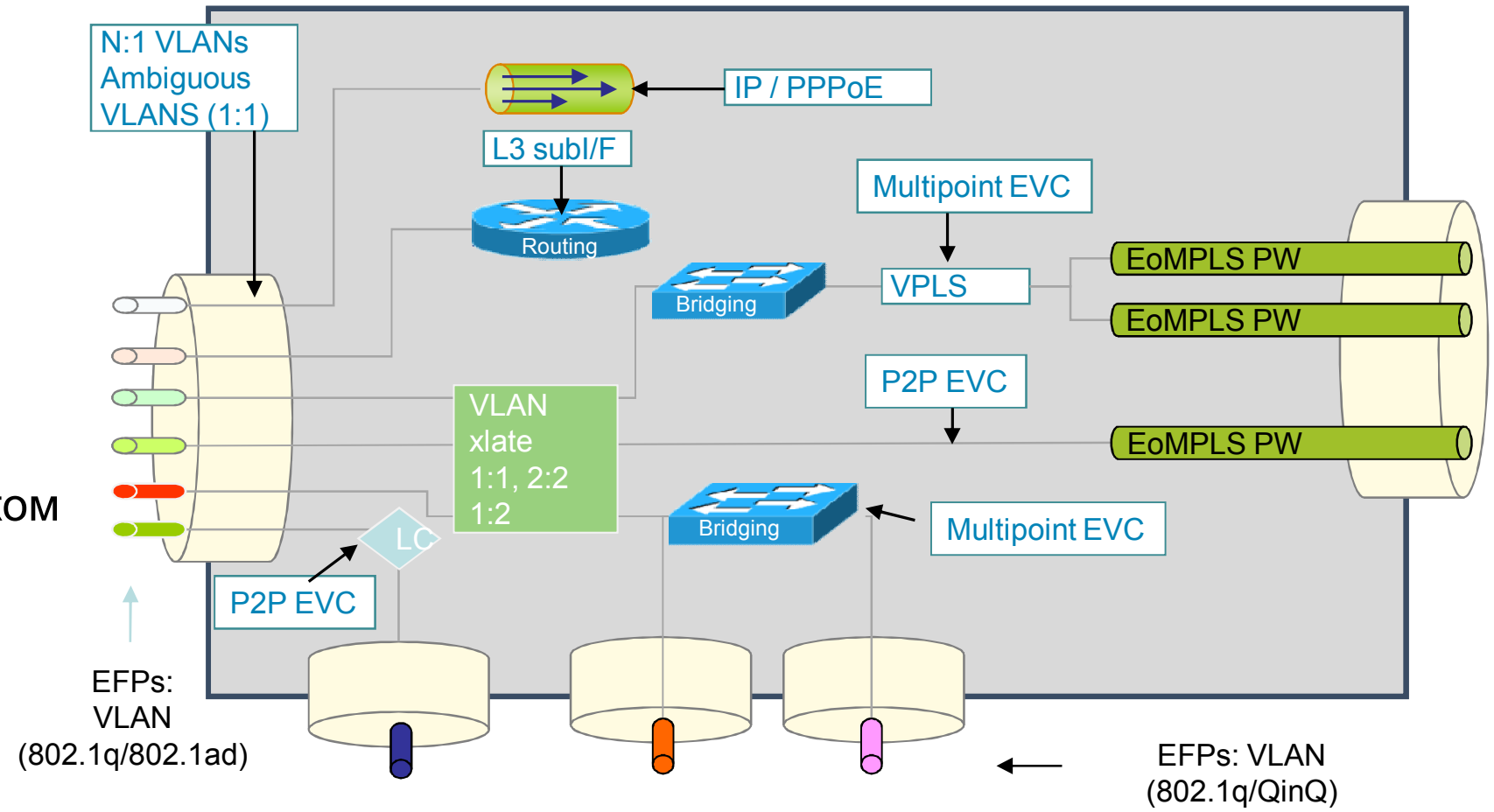


ASR 9000
IOS XR®

BNG интерфейсы являются частью EVC инфраструктуры

+ EFP Interfaces
+ L3 Interfaces
+ BNG Interfaces

на одном физическом порту



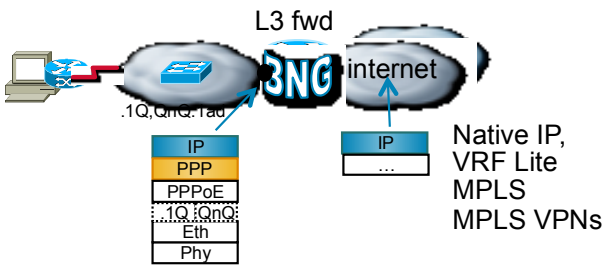
Сценарии применения

Розница

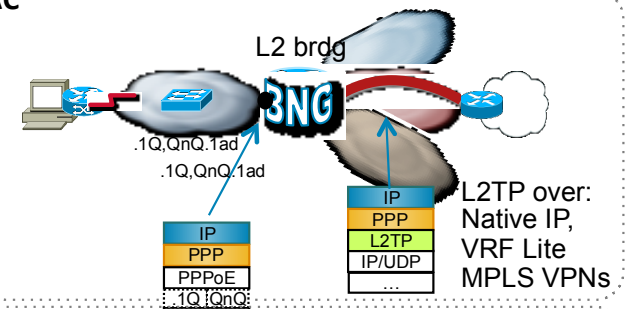
Услуги для других Операторов (опт)

PPP сессии

PTA



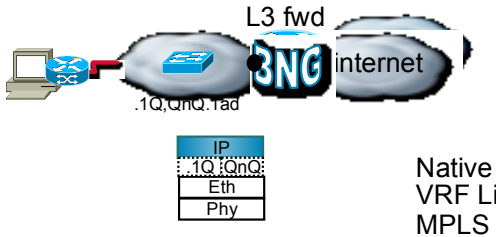
LAC



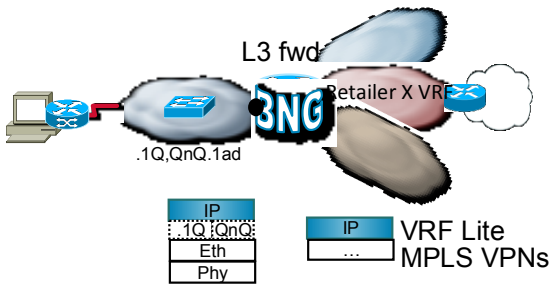
PTA

IP сессии

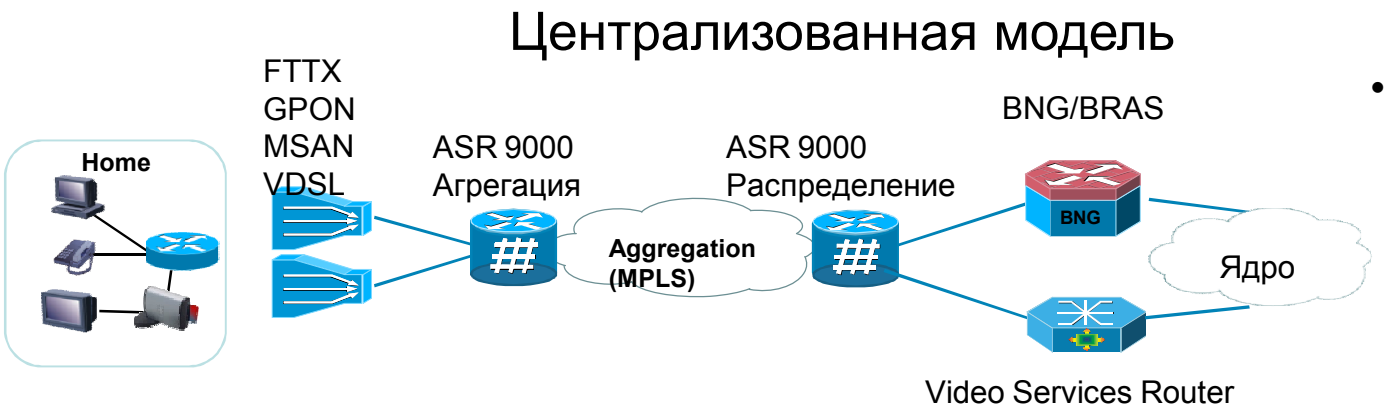
IP–Layer2 Connected



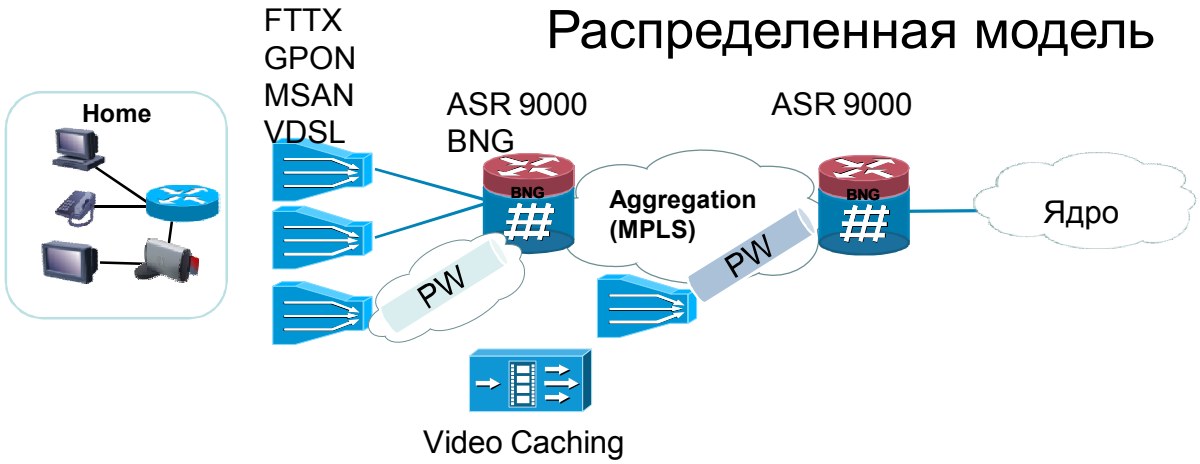
IP–Layer2 Connected



Централизованная и Распределенная модели агрегации

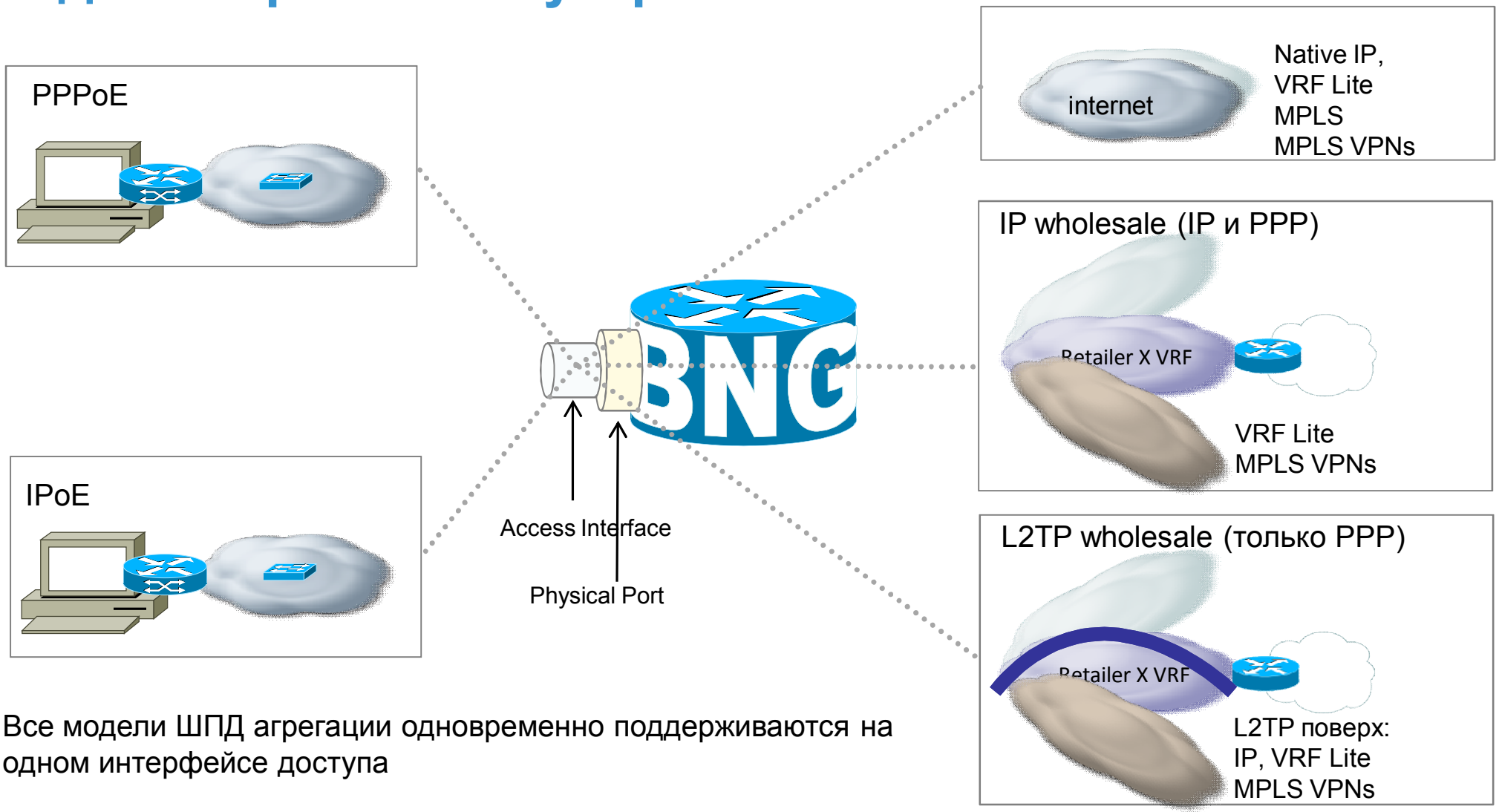


- Традиционная модель ШПД агрегации
- Централизованная модель с несколькими сервисными границами:
  - BNG для Интернета и голоса
  - Video Services router для Video и IP TV



- BNG нового поколения
- Единая распределенная сервисная граница
- Больше полоса на абонента
- Фокус на Triple-Play
- Можно интегрировать кеширование видео (CDS)

Единое граничное устройство

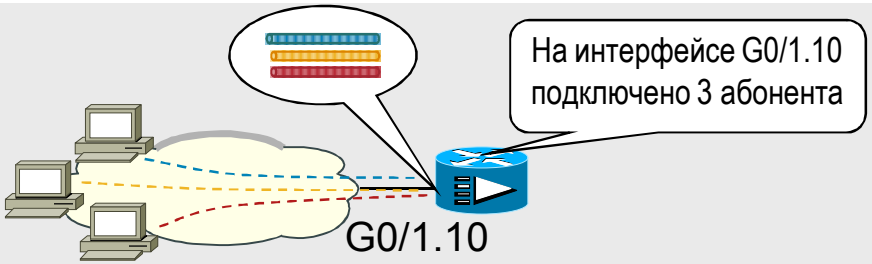
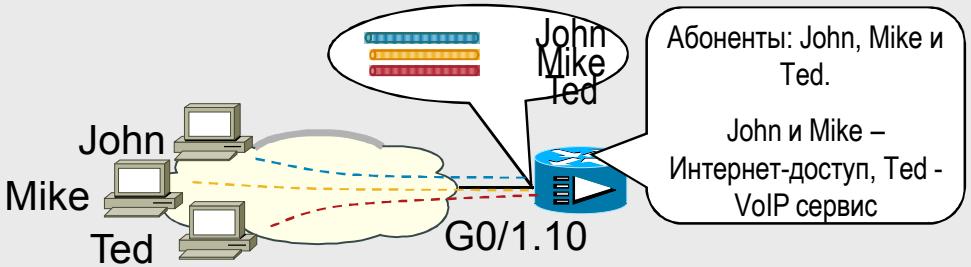
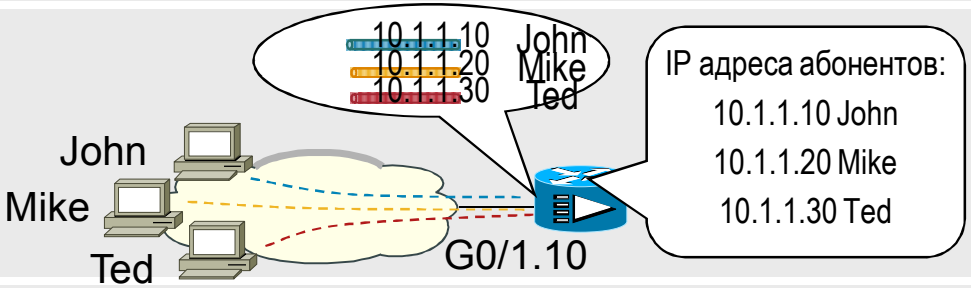
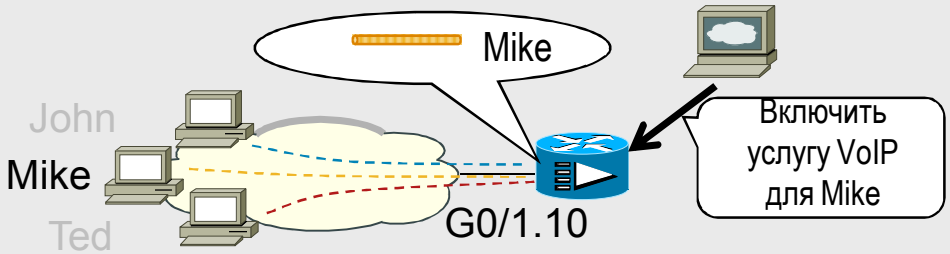


Все модели ШПД агрегации одновременно поддерживаются на одном интерфейсе доступа

Работа с абонентскими сессиями

Cisco Expo 2012

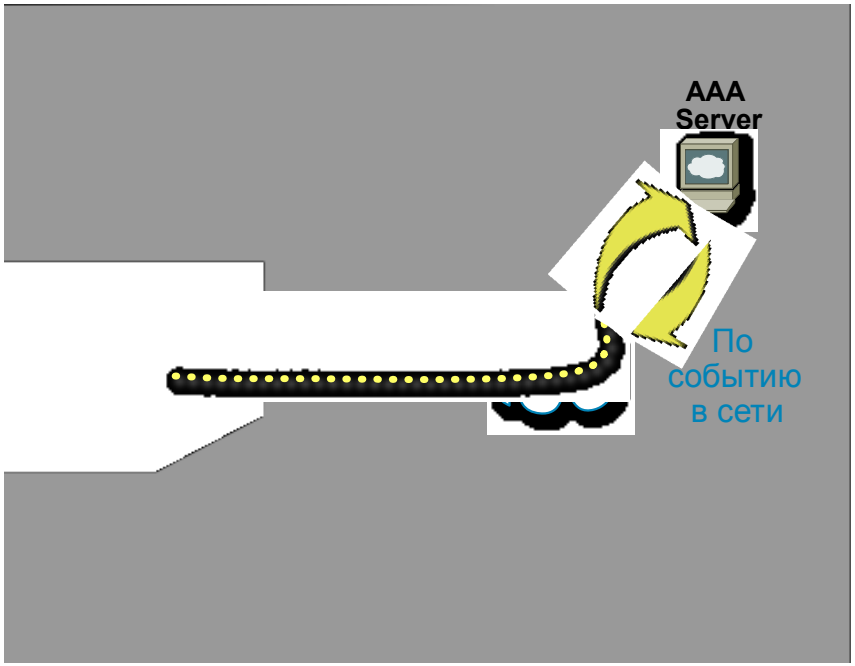
Основные функции BNG

Идентификация абонента		Создание виртуальной конструкции – сессии абонента
Аутентификация и авторизация абонента		Аутентифицировать абонента и назначить ему индивидуальные политики обслуживания
Управление IP адресами		Назначить каждому абоненту уникальный адрес (возможно из разных пулов)
Динамическое управление политиками		Динамическое изменение списка доступных услуг

Динамическое применение политик

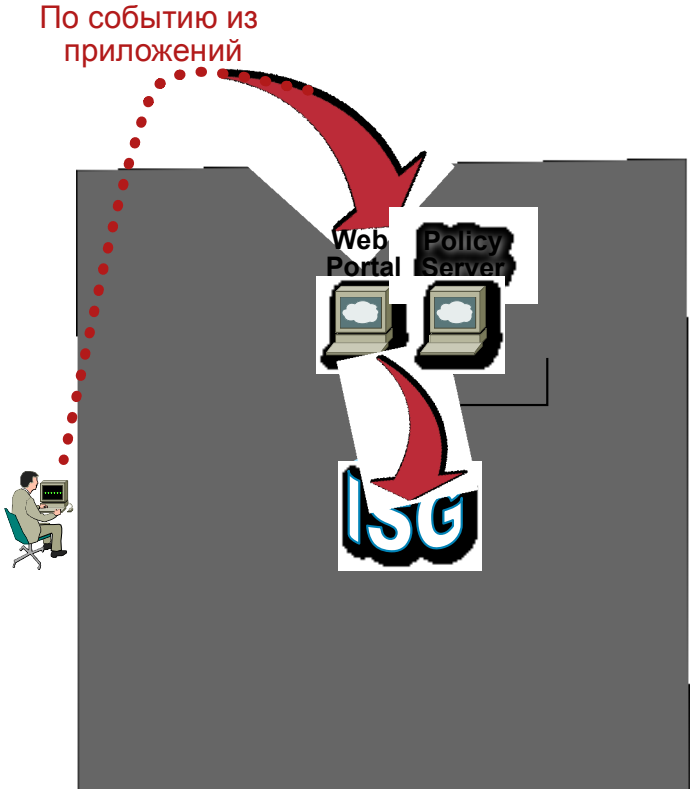
pull

(например, автоматический запрос сервисного профиля при установлении сессии)



push

(например, «турбо кнопка»)



Интерфейс с внешними системами

Протокол RADIUS для аутентификации абонентов и загрузки описаний сервисов

Расширение протокола RADIUS (Change of Authorization, **RFC 3576**). Открытый интерфейс для динамического изменения политик и сервисов

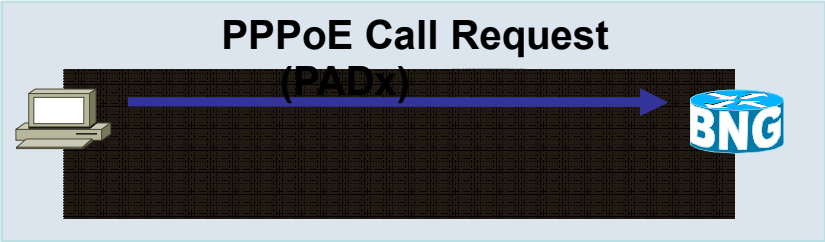
Policy PULL

Policy PUSH

Инициация динамических сессий

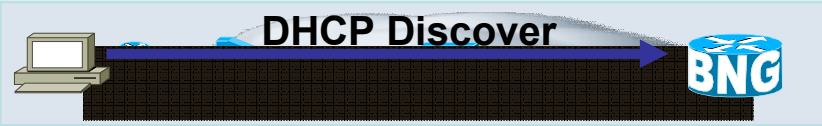
- Сессии инициируются по проявлению активности абонента – First Sign of Life (FSOL)
- Для сессий разных типов возможны разные FSOL

PPP сессии



- Получение **PADR** сообщения
  - Session-start event
- Трафик абонента идентифицируется по MAC + PPP session ID

IP сессии

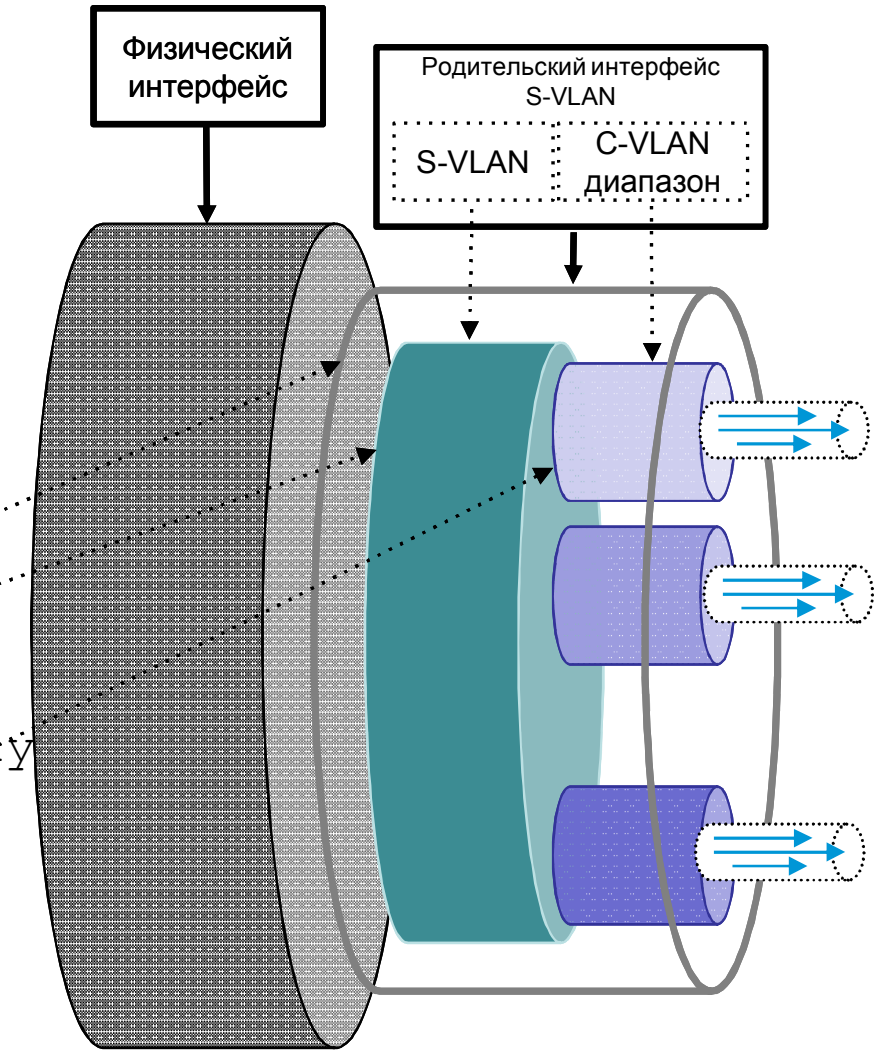


- Получение **DHCP Discover** сообщения
  - Session-start event
- Трафик абонента идентифицируется по MAC адресу
- BNG должен являться DHCP Proxy
  - DHCP proxy = DHCP relay который:
  1. создает и поддерживает DHCP bindings
  2. «Притворяется» DHCP сервером для абонента

- Трафик абонента идентифицируется по MAC адресу
- Нет средств мониторинга состояния сессии (нет DHCP обмена), завершение сессии должно быть через CoA или CLI или по idle-timeout

Динамическое создание VLAN

- Динамическое создание множества абонентских VLAN для 1:1 модели агрегации
- Поддержка сценариев PPPoE и IPoE
- VLAN создается при проявлении активности абонента - First Sign of Life (PPPoE PADI, DHCP Discover)



Пример 1:

```
interface Bundle-Ether100.10
  encapsulation dot1q 100 second-dot1q any
```

Пример 2:

```
interface Bundle-Ether100.10
  encapsulation dot1ad 100 dot1q 300-475
```

Аутентификация сессии

Аутентификация: доступ к сетевым ресурсам предоставляется только легитимным абонентам

Способы аутентификации:

- **Механизмы аутентификации, обеспечиваемые протоколом доступа**:
  - PPP: CHAP/PAP
- **Transparent Auto Logon (TAL):**
  - Аутентификация на основе идентификаторов, извлекаемых непосредственно из абонентского трафика, например: MAC/IP address, DHCP Option 82, DHCP Option60, C-VLAN/S-VLAN, PPPoE Tags...
- **Web Logon**

Аутентификация не является обязательной, но используется в подавляющем большинстве случаев

Transparent Auto Logon

Шаг 1: Определяем формат username:

```
aaa attribute format USERNAME_FORMAT
 format-string "%s:%s:%s@bng.cisco.com" remote-id circuit-id vendor-class-id
```

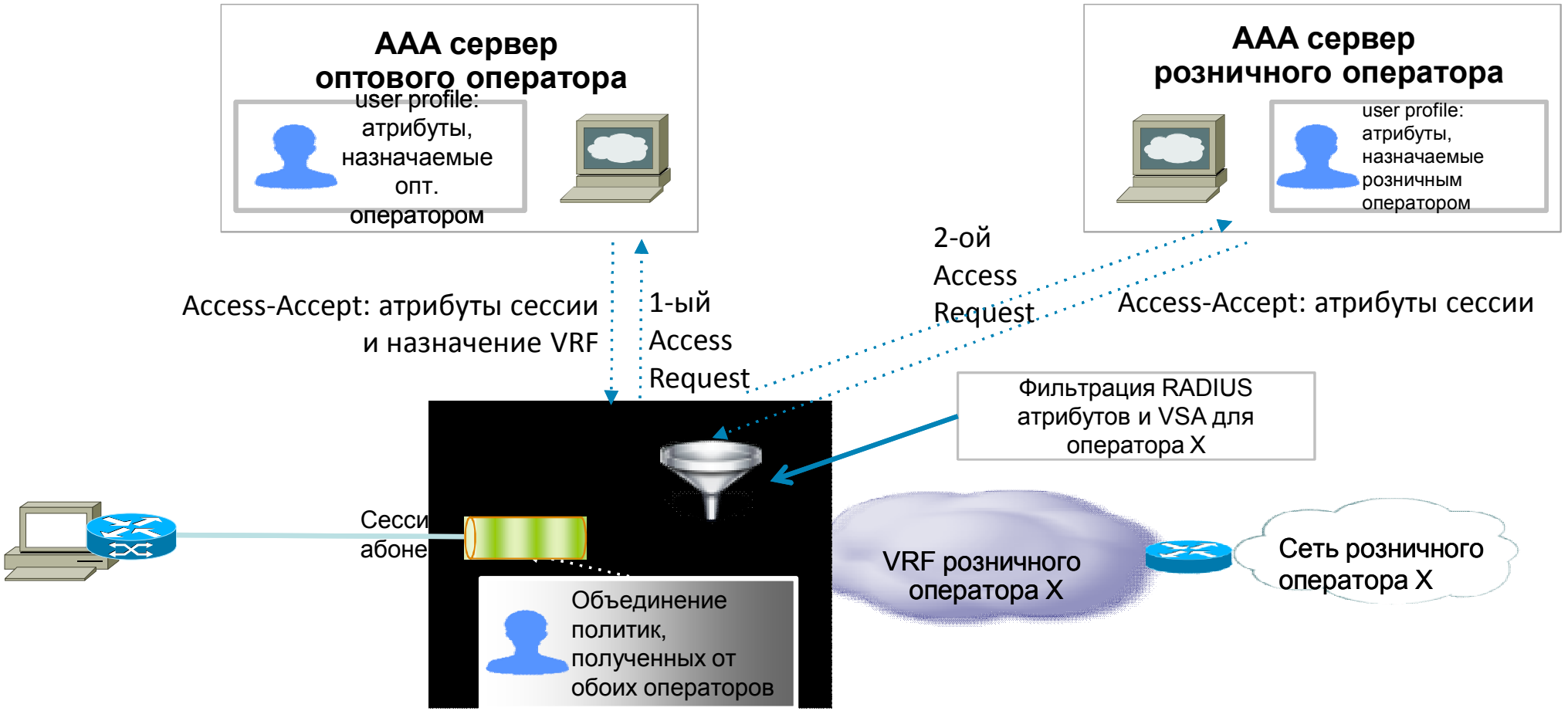
Шаг 2: Указываем шаблон username, используемый для аутентификации

```
<…>
  20 authorize aaa list default format USERNAME_FORMAT password <pwd>
<…>
```

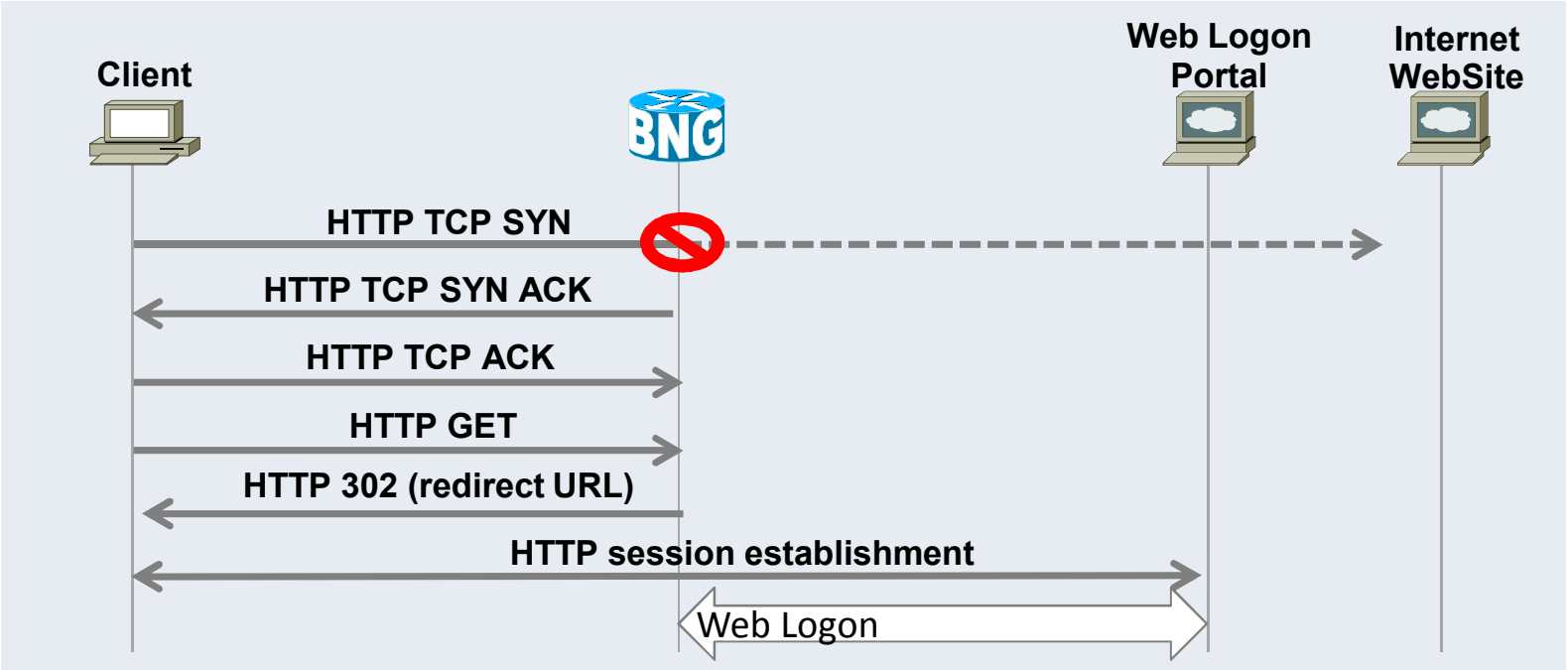
Источники информации для заполнения поля username:

- DHCP Option 82
- DHCP Option 60
- PPPoE Tags (PPPoE Intermediate Agent)
- Phy-slot
- Phy-subslot
- Phy-port
- Outer-vlan-id
- Inner-vlan-id

Двойная аутентификация сессии – double dip



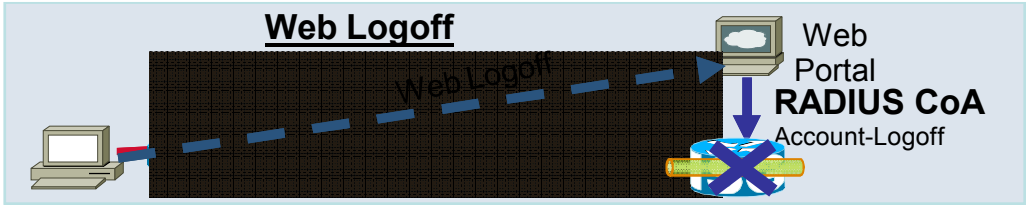
Web Logon: функция HTTP redirect



- BNG перехватывает TCP обмен при установке HTTP сессии абонента с веб-сайтом и устанавливает HTTP сессию с абонентом
- BNG возвращает абоненту сообщение HTTP 302 (Redirect), содержащее URL портала оператора
- Клиент устанавливает HTTP сессию напрямую с порталом

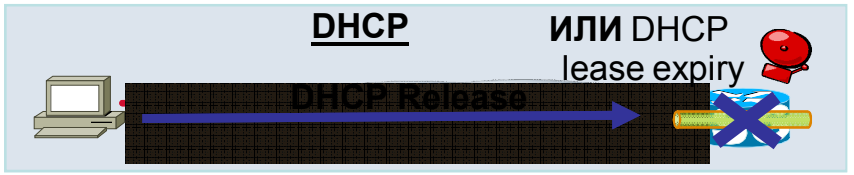
Завершение (разрыв) сессии

Универсальные механизмы – IP и PPP сессии



Только для PPP сессий

Только для IP сессий



DHCP – инициированные сессии

Как «рестартовать» IPoE сессию

- IPoE сессии инициируются **ТОЛЬКО** при получении **DHCP discover**
- Однако сессия может быть терминирована ранее истечения DHCP Lease:

  CoA Account-Logoff, PoD, CLI, перезагрузка шасси маршрутизатора …

- **Трафик абонента будет сбрасываться, пока не начнется процесс переполучения IP адреса (до половины Lease Time)**

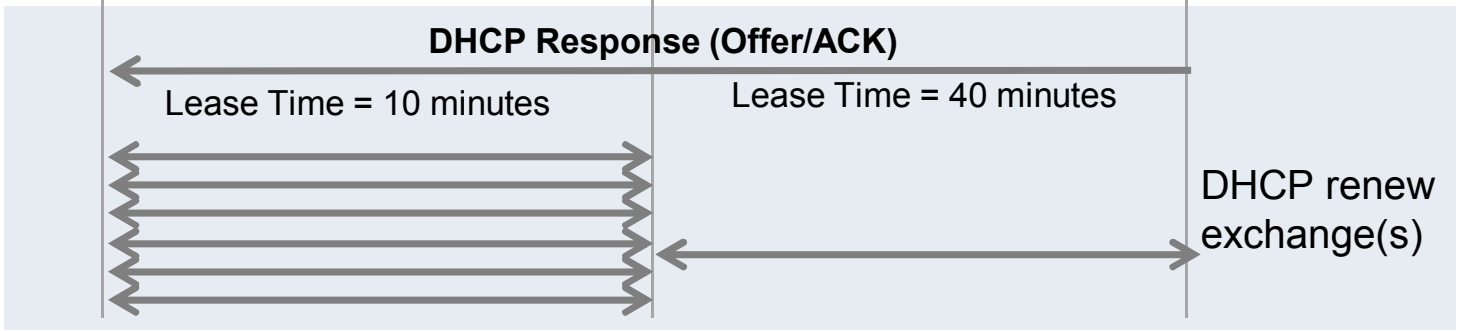
Вариант 1

Уменьшить Lease Time на DHCP сервере

DHCP Сервер работает с короткими Lease Time; повышенная нагрузка на DHCP сервер

Вариант 2

DHCP Lease Proxy



DHCP Сервер работает со стандартными Lease Time

DHCP Proxy на BNG конвертирует их в короткие Lease Time для абонента

Политики (сервисы) для сессии абонента

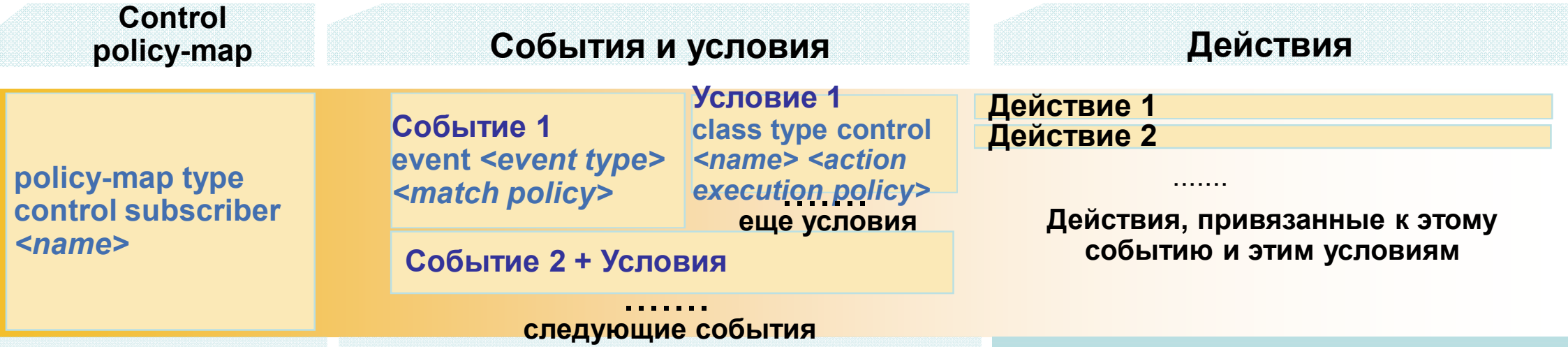
- Применяются к абонентской сессии

Функции		
	Установление сессии	associated unnumbered interface MTU Параметры PPP протокола (параметры NCP/LCP, методы аутентификации)
	Управление сессией	Keepalives: PPP Keepalives Timeouts: Idle (только помечает сессию, но не удаляет ее) Absolute (только для PPP)
	Traffic Conditioning	QoS: MQC: HQoS, pQoS IGMP/QoS correlation (только для PPP) Access Loop overhead (только для PPP) Security: Per User ACLs uRPF
	Traffic Forwarding Control	Назначение IP адресов (PPP addr-pool, DHCP class) HTTP Redirection ACL Based Forwarding (ABF) VRF mapping L2TP mapping (PPP only) Multicast replication in session (PPP only)
	Traffic Accounting	PostPaid Interim Broadcast

Описание политик (сервисов)

	Место хранения	Способ загрузки
	**AAA Server** ▪ Конфигурируются специальные **Сервисные профили** ▪ Используются стандартные и Vendor Specific RADIUS атрибуты ▪ Загрузка по мере необходимости	1 ▪ Необходимо активировать Premium HSI сервис ▪ Сервисный профиль не описан на BNG 2 RADIUS Access-request Username: Premium_HSI Password: <service pwd> 3 RADIUS Access-accept Определение сервисного профиля ▪ Сервис активируется ▪ Сервисный профиль кешируется, пока есть хоть одна сессия с этим сервисом 4
	**BNG** ▪ Профиль преднастраивается на самом BNG `dynamic-template type { ppp | ipsubscriber | service } <name>`	▪ Описание сервиса постоянно хранится в конфигурации BNG

Управление сессий абонента - Control Policy



Применяется на интерфейсе доступа (в сторону абонентов)

Управляет всем жизненным циклом сессии

Возможные типы событий:

- **Session-start**: старт новой сессии (PPPoE или IPoE)
- **Session-activate**: стартовал LCP (PPPoE)
- **Authentication/Authorization failure**: отказ авторизации
- **Authentication/Authorization no response**: нет ответа от Radius сервера
- **Service-stop**: CoA запрос на отключение сервиса
- **Account-Logon**: CoA запрос Account Logon
- **Account-Logoff**: CoA запрос Account Logoff
- **Timed-policy-expiry**: Истечение ранее установленного таймера

Набор действий для данного {события и условий}

Упорядоченный список действий:

- do-all
- do-until-failure
- do-until-success

Варианты действий:

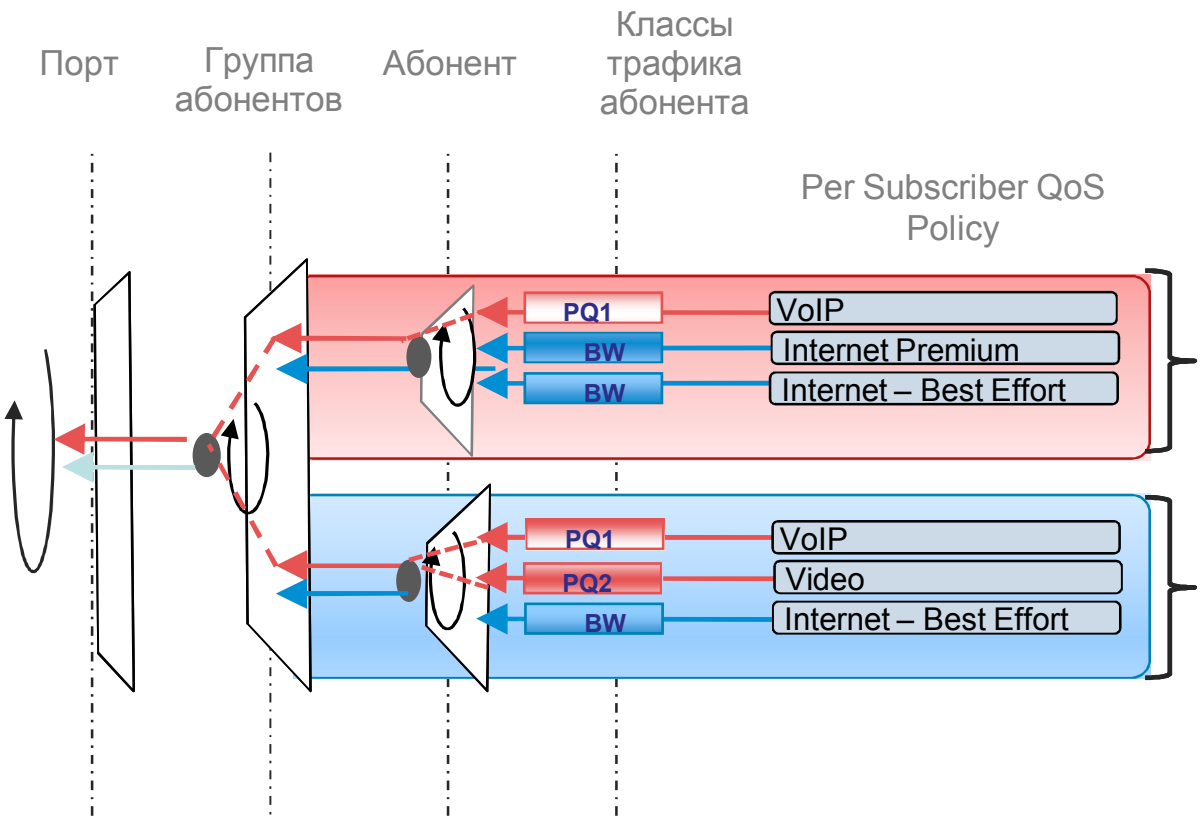
- **Activate**: Применить сервис для сессии
- **Deactivate**: Отменить сервис для сессии
- **Authenticate/Authorize** : Аутентифицировать сессию (PPP CHAP/TAL)
- **Set-timer/Stop-timer**: старт/стоп таймера
- **Disconnect**: Разорвать сессию

Функции QoS

Cisco Expo 2012

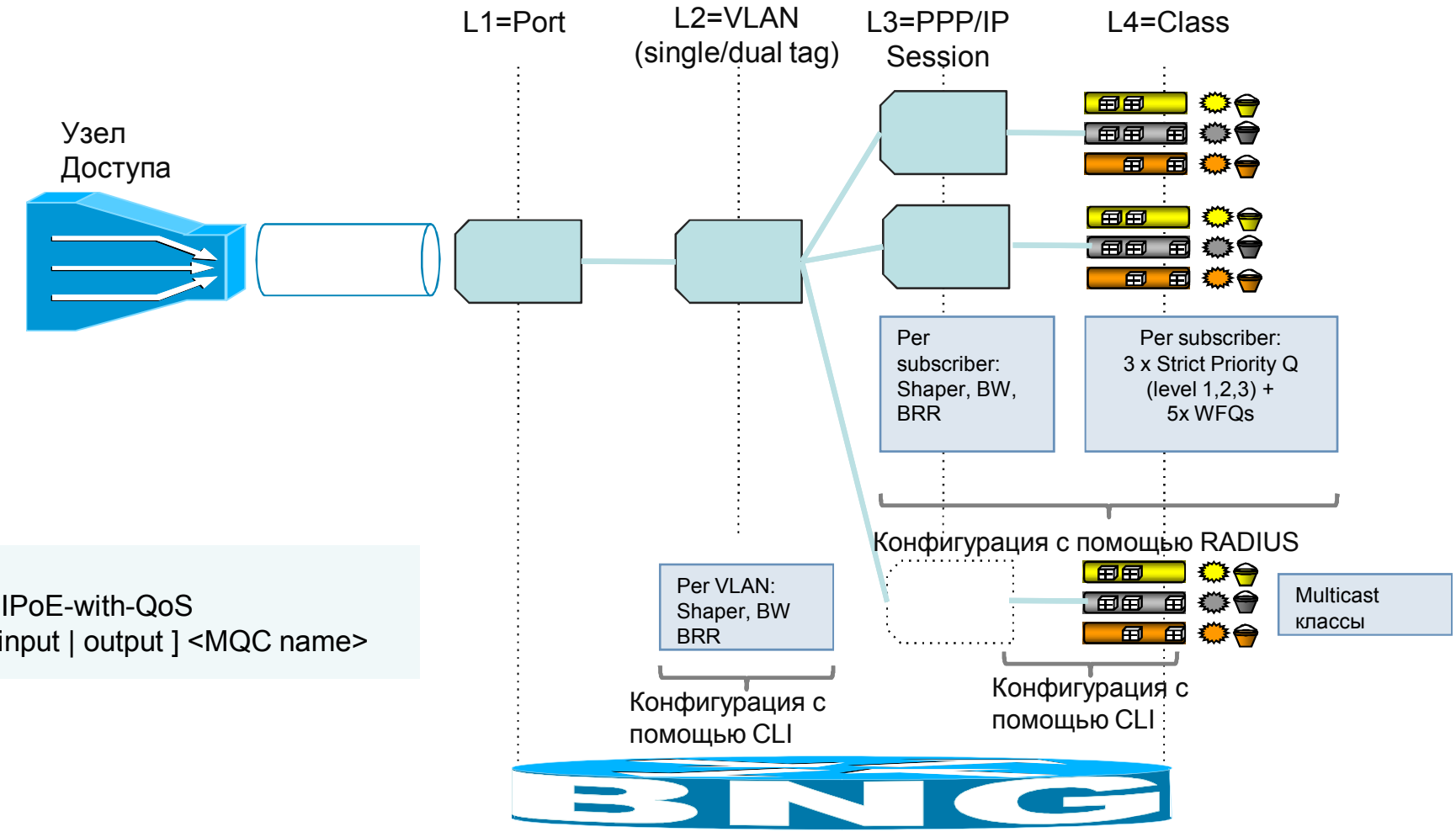
H-QoS для абонентской сессии

4 уровня иерархии



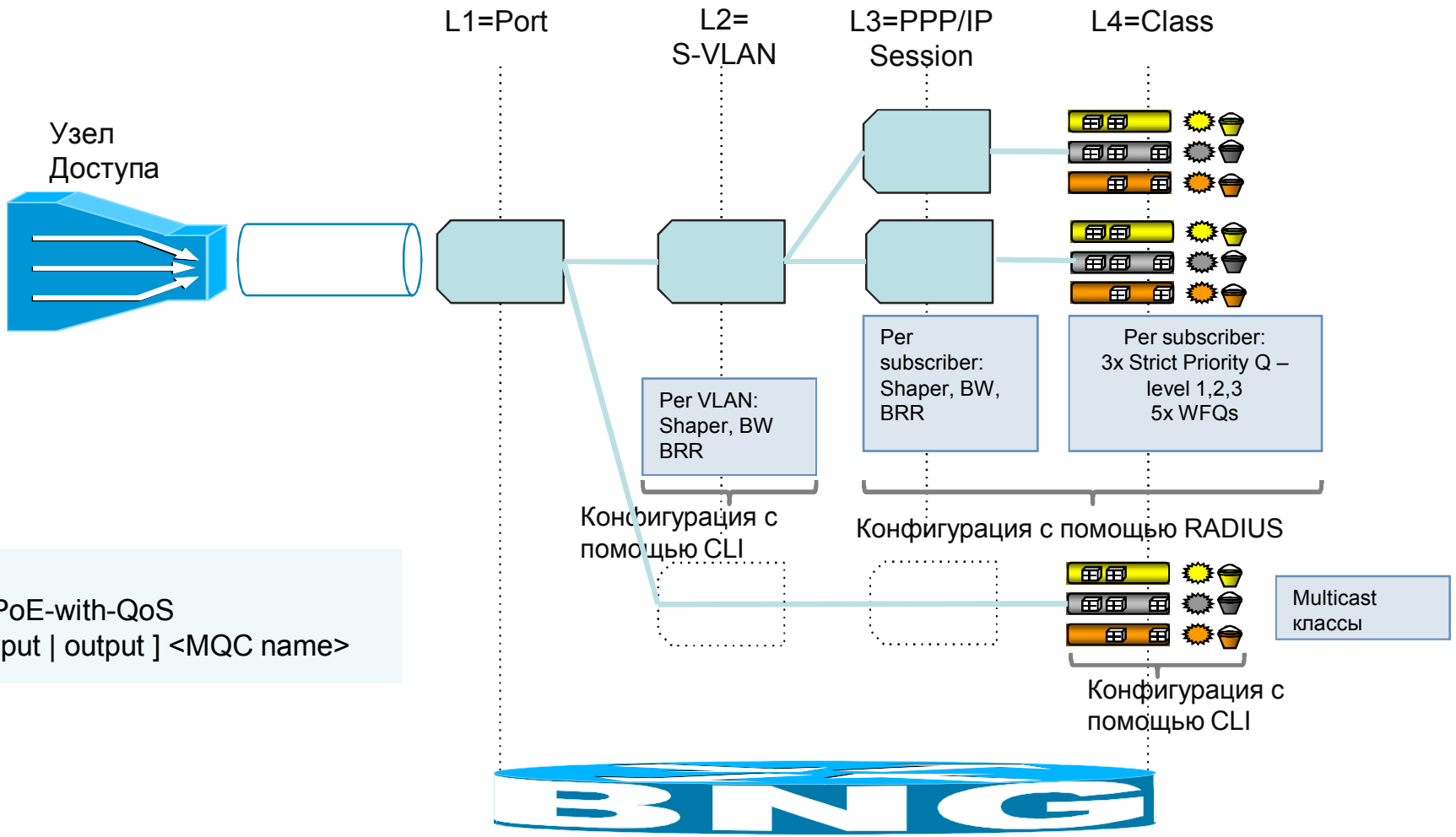
- Иерархический QoS для всех абонентов
- 8 очередей на абонента
- Strict Priority очереди
- WRED
- 2R3C policers, иерархический полисинг
- 4-х уровневый H-QOS
- Priority очереди с функцией priority propagation для качественной передачи голоса и видео с минимальными задержками и джиттером

4-уровневый QoS в модели N:1 VLAN



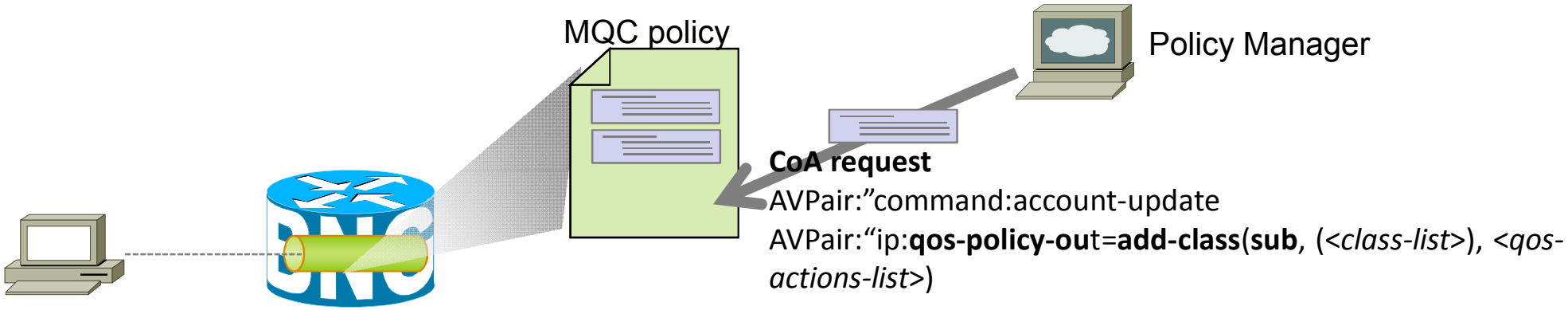

```
dynamic-template
  type ipsubscriber IPoE-with-QoS
    service-policy [ input | output ] <MQC name>
```

4-уровневый QoS в модели 1:1 VLAN




```
dynamic-template
  type ipsubscriber IPoE-with-QoS
    service-policy [ input | output ] <MQC name>
```

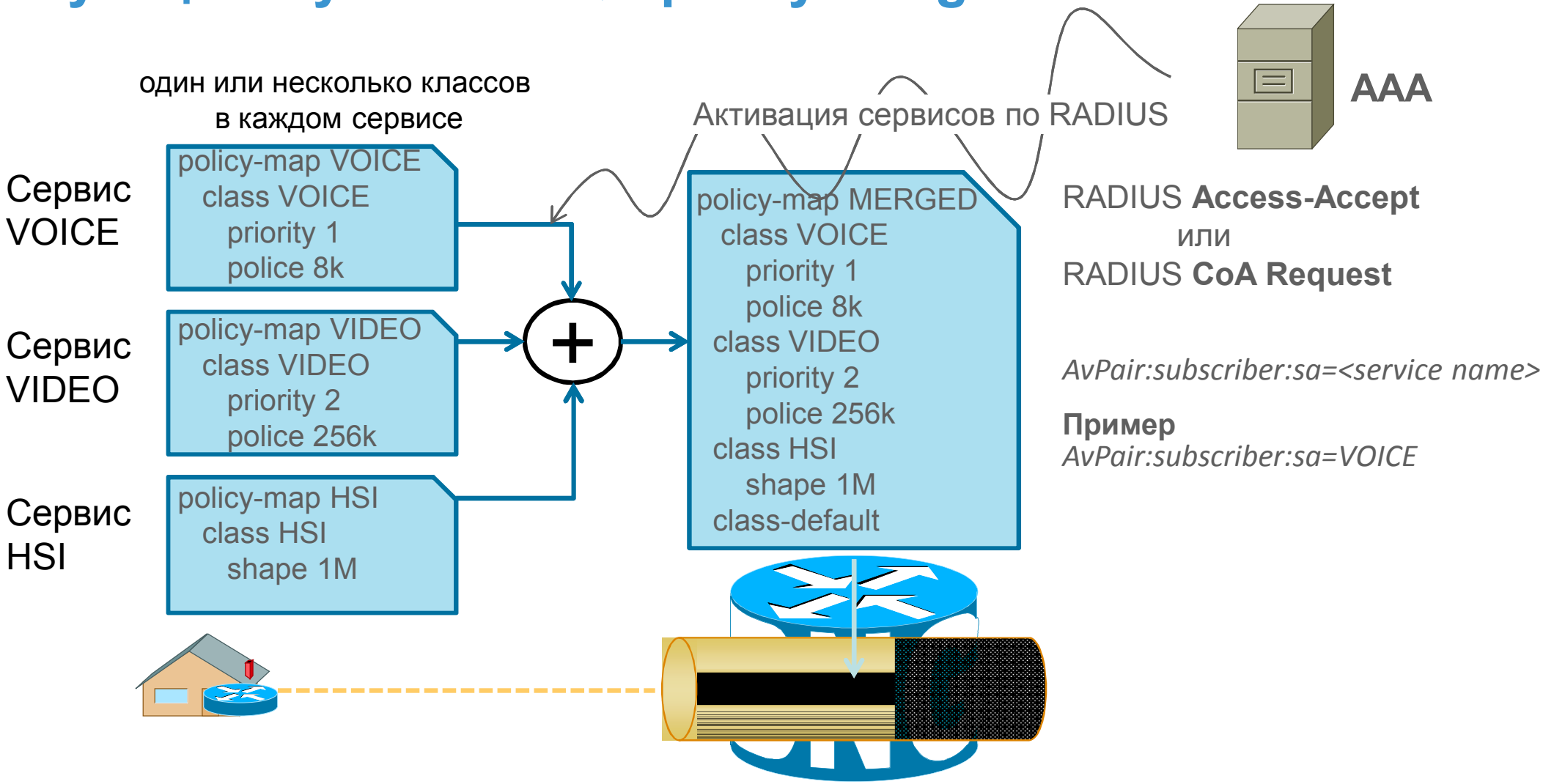
Параметризация QoS - pQoS



- Динамическое создание и модификация MQC политик для абонентских сессий
  - Создание MQC политик
  - Добавление/удаление MQC классов и actions в политике
    - class-map должен быть преднастроен на BNG
- Работает через RADIUS
  - RADIUS CoA Account Update
  - RADIUS Access-Accept

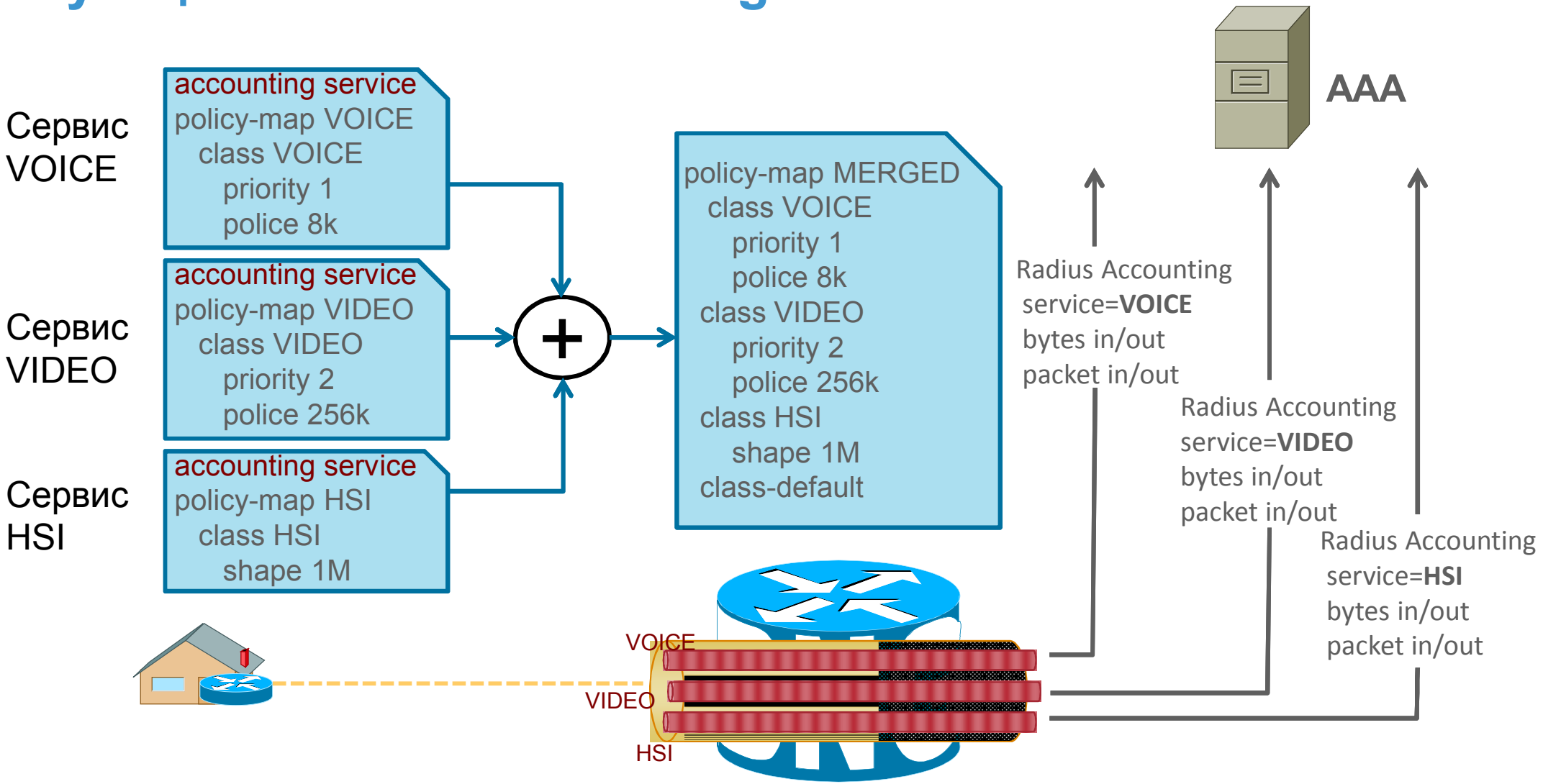
Функция Dynamic MQC policy merge

IOS XR 4.3.1



Функция Service Accounting

IOS XR 4.3.1



Функции безопасности

Cisco Expo 2012

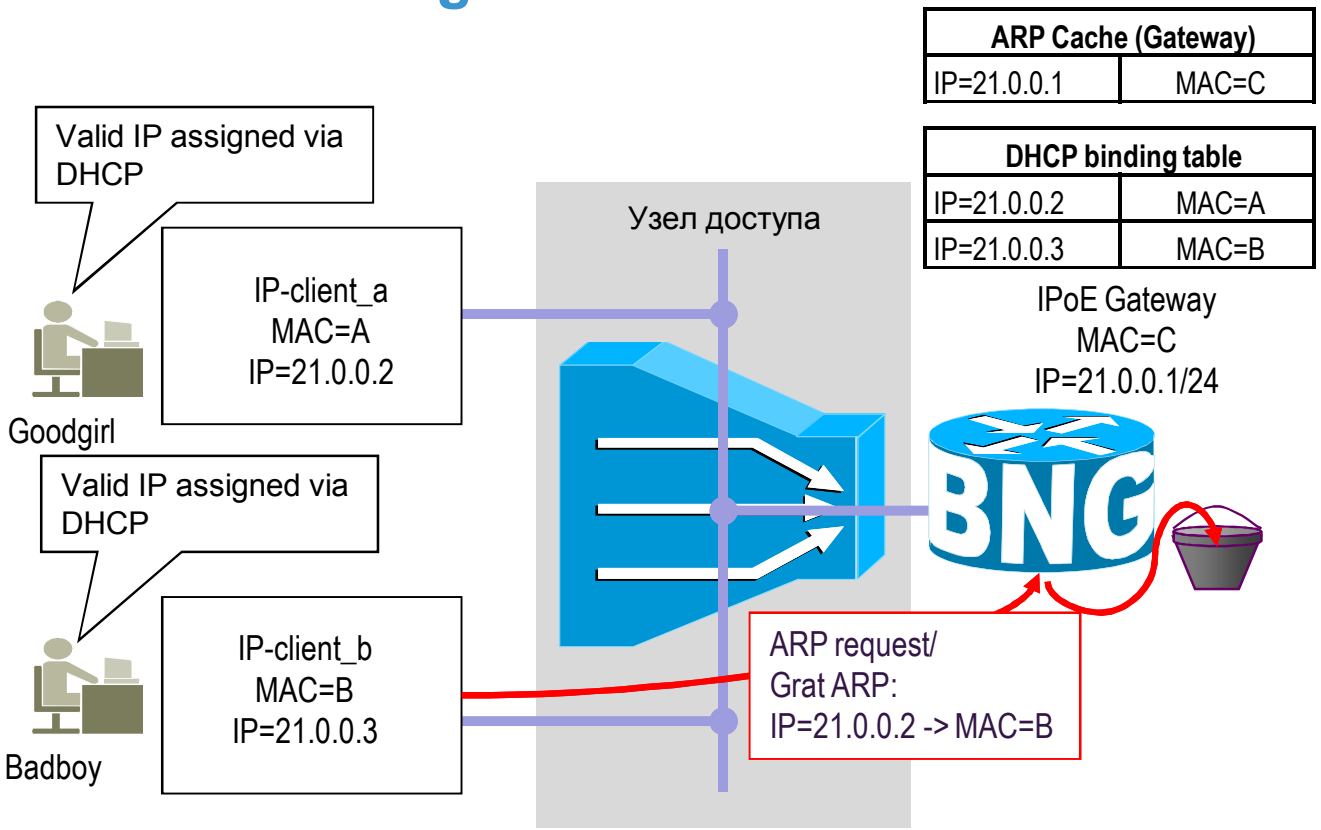
Функции безопасности

- Unicast Reverse Path Forwarding (uRPF)
- Необходимо контролировать IP Source Address при получении трафика от абонентов (*входящий* трафик)
  - Исходящий трафик относится к сессии на основе IP DA
- IP SA трафика, полученного сессией, должен соответствовать назначенному для этой сессии IP адресу
  - PPPoE Sessions: MAC + PPP Session ID + IP
  - IP Sessions: MAC + IP

```
dynamic-template type { ppp | ipsubscriber |service }  <tmpl_name>
   ipv4 verify unicast source reachable-via rx
```

- Списки ACL
  - ACL могут быть применены к сессии в обоих направлениях
  - L3 Only

ARP Security
ARP Poisoning Protection



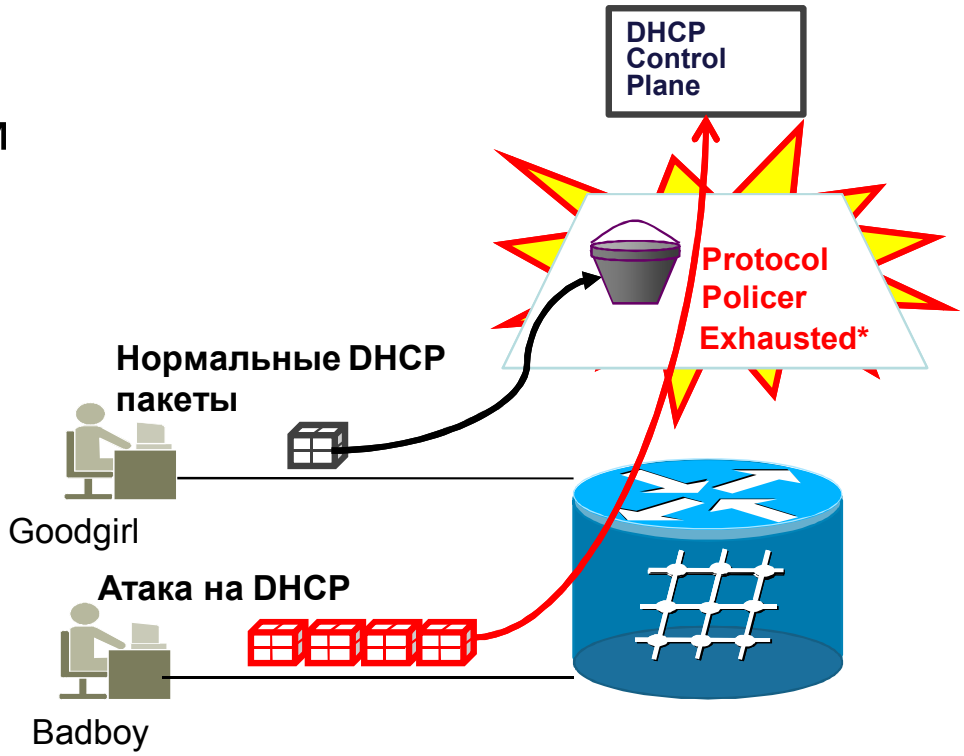
- Badboy отправляет поддельные ARP сообщения, чтобы модифицировать ARP кэш BNG
- ARP сообщения не приводят к изменению ARP кэша BNG
  - Но BNG, естественно, отвечает на ARP запросы абонентов
- BNG строит ARP кэш на основе информации DHCP Proxy binding table, а не ARP обмена с абонентами
- Попытка перехвата трафика не удалась

Защита плоскости управления BNG

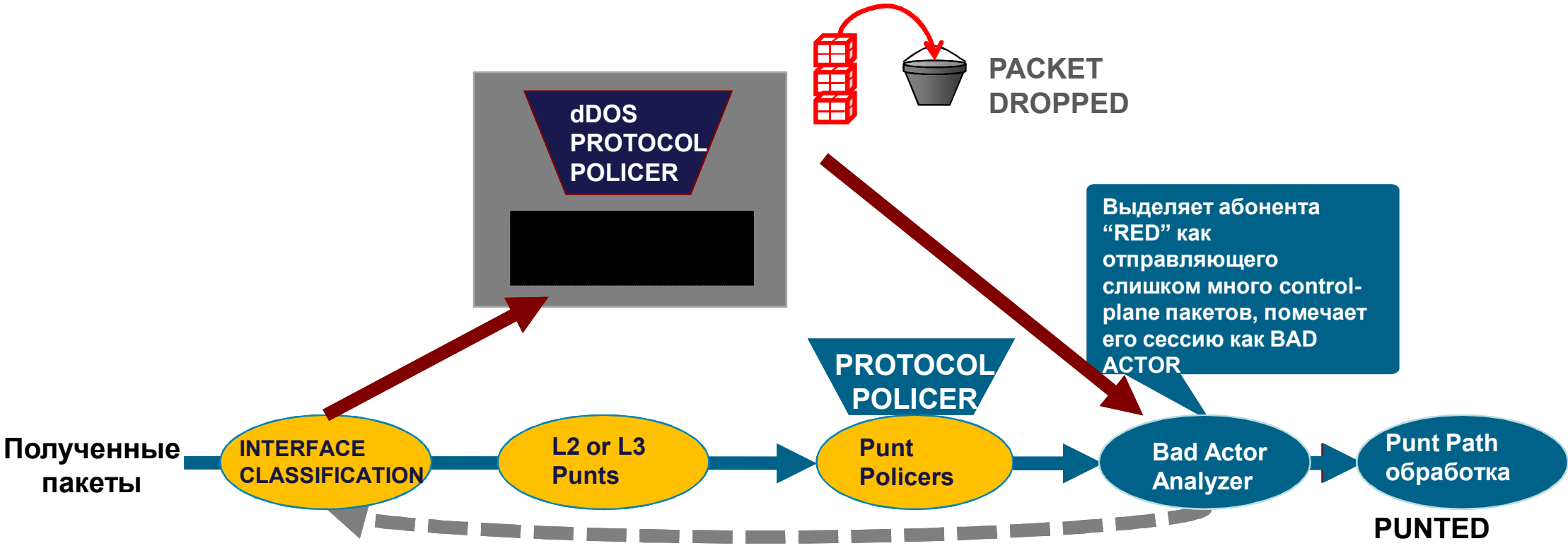
- Предотвращение dDOS атак
  - **Первая ступень защиты**: IOS XR Control Plane Protection
    - Защита на уровне определенного сетевого протокола
  - **Вторая ступень защиты**: Адаптивный CoPP
    - Интеллектуальная защита для протоколов установления/контроля абонентских сессий (DHCP, ARP, PPPoE Control Packets)

Адаптивный CoPP

- LPTS policing работает с общим трафиком (всех сессий)
  - ⇒ Top Talkers (или Bad Actors) могут негативно влиять на предоставление сервиса остальным абонентам
- **Адаптивный CoPP** определяет Bad Actors и полисит их трафик, позволяя нормальным абонентам получать сервис
  - ⇒ Полисинг с учетом знания об абоненте



Адаптивный CoPP: как это работает



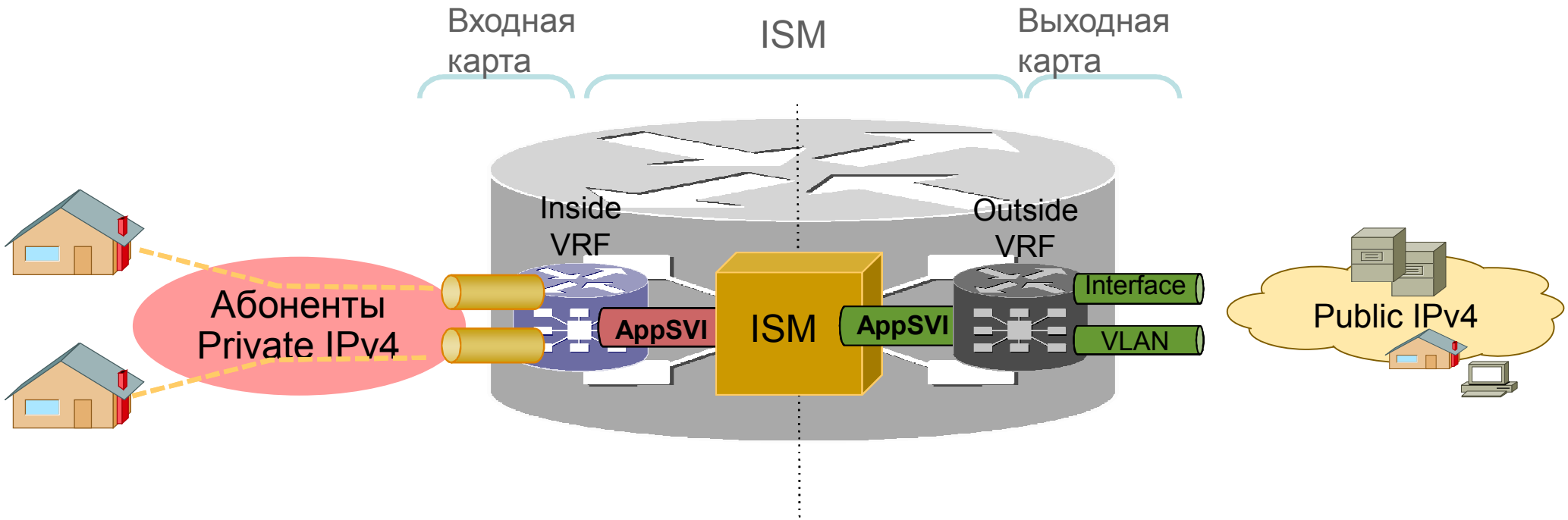
- Определяется поток (сессия), от которой поступает слишком много протокольных пакетов
- dDOS protocol policer помечает абонента как Bad Actor и генерирует SYSLOG сообщение

  Если сессии с этим mac-адресом не существует, в TCAM программируется MAC Source Address как Bad Actor
- NPU проверяет флаг Bad Actor при обработке пакетов, и для Bad Actor применяются более строгие полисеры – на определенное время (15 мин по умолчанию)

CGN и IPv6 функционал

Cisco Expo 2012

Интеграция BNG и CGN функционала

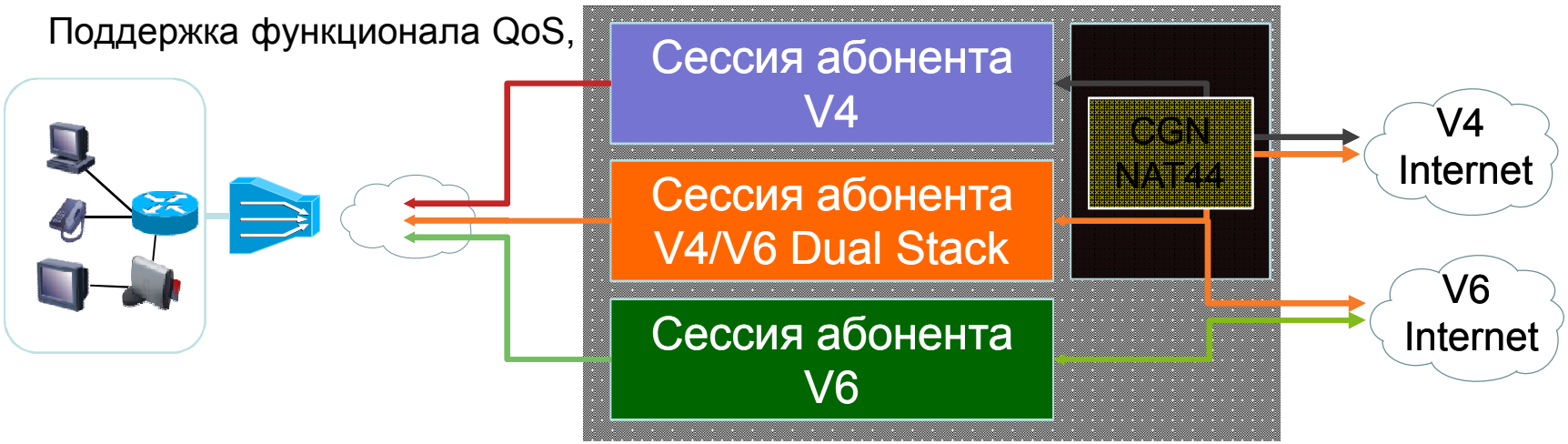


- Интеграция BNG функционала с CGN функционалом ISM модуля
- Carrier Grade NAT в соответствии со стандартами (RFC4787, RFC5382, RFC5508)
- Производительность ISM модуля:
  20M трансляций, 1M трансляций/сек, ~15Gbps трафика

IPv6 и Dual-Stack сессии

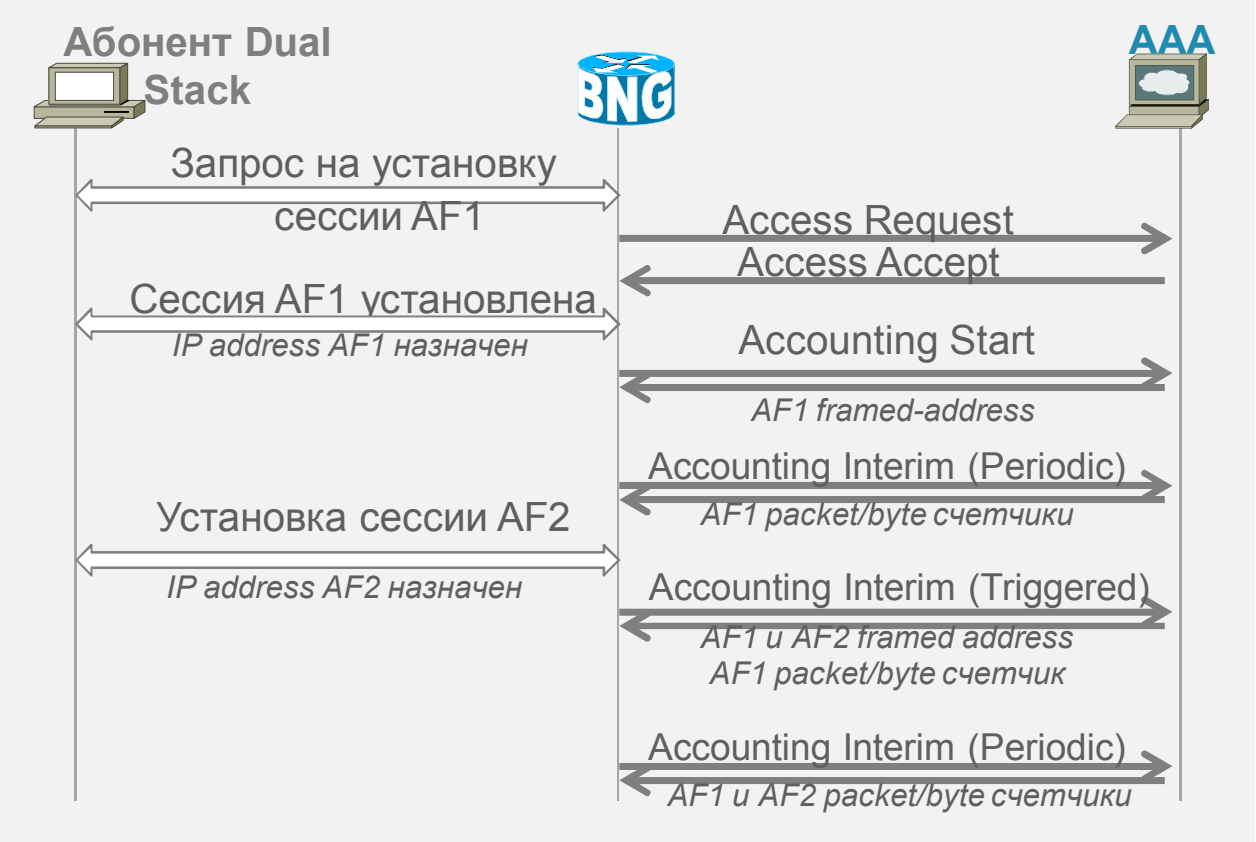
IOS XR 4.3.0

- v4/v6 Dual Stack сессии
  - Одна сессия абонента
  - Аутентификация выполняется один раз
  - Единый Accounting
    - Счетчики для V4 и V6
- Методы назначения v6 адресов
  - DHCPv6 Сервер
  - DHCPv6 Proxy
  - DHCPv6 RADIUS proxy
  - DHCP v6 NA и PD
- Поддержка функционала QoS,
- Единый VRF для V4 и V6
- Интеграция BNG и CGN функционала
  - ISM модуль для CGN функционала
  - NAT44 для V4 абонентов
  - NAT44 для V4 трафика Dual-Stack абонентов
  - Поддержка DS-Lite AFTR для абонентов DS-Lite



Сессия Dual Stack абонента

IOS XR
4.3.0



Аутентификация выполняется один раз – при установке первой Address Family (AF)

Одно сообщение accounting start
- Содержит framed address для установленной AF

Регулярный interim accounting включает статистику по установленной AF

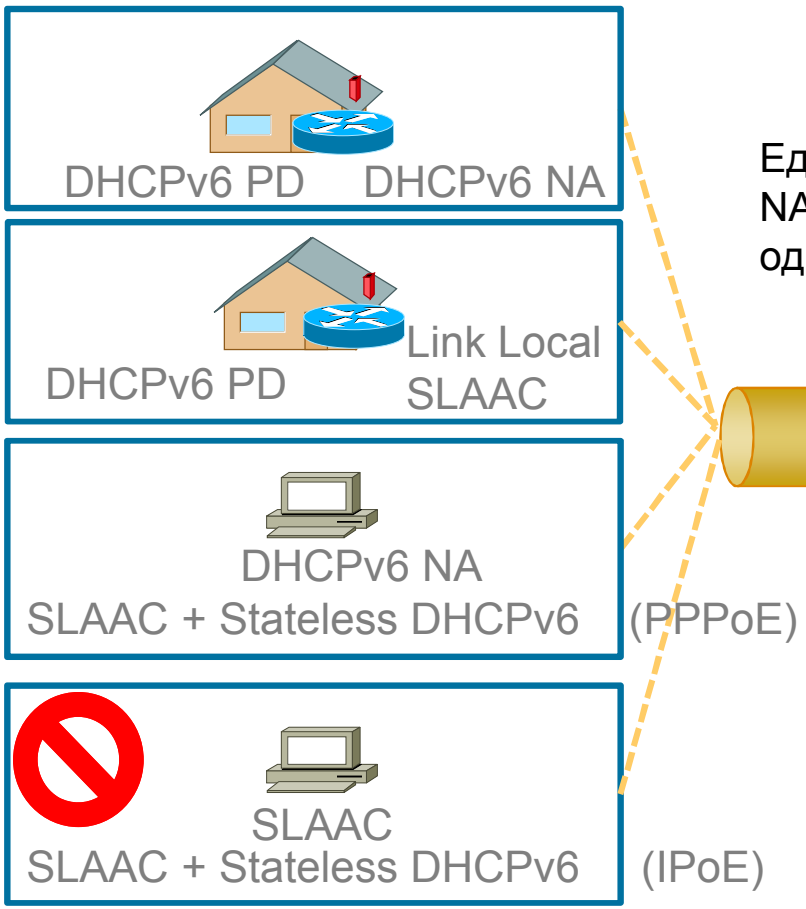
Отдельный interim accounting отправляется при установке второй AF
- Содержит framed address для двух AF

Регулярный interim accounting включает статистику по двум AF
- Отдельные и суммарные счетчики

Методы назначения IPv6 адресов

IOS XR
4.3.0

Назначение IPv6 адресации абоненту



Единая сессия для
NA и PD адресов
одного абонента

Управление IPv6 адресацией

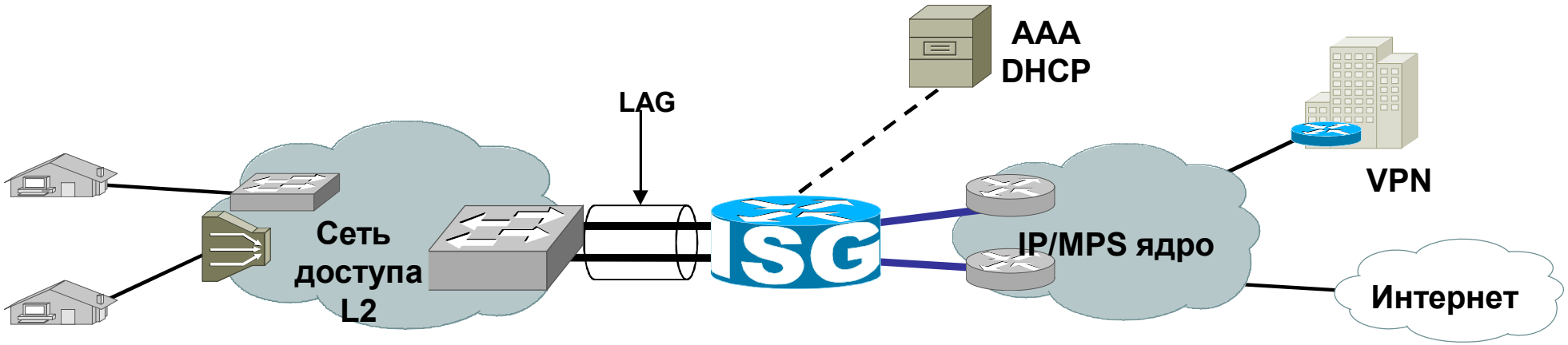
Резервирование и отказоустойчивость

Cisco Expo 2012

Способы обеспечения отказоустойчивости

- Отказоустойчивость внутри устройства BNG
  - Резервирование компонентов: RSP, блоки питания, вентиляция
  - SSO/ISSU
  - Резервирование интерфейсов подключения: Link Aggregation (LAG)
- Резервирование на уровне устройств
  - Два независимых устройства (Stateless)
  - Кластер из двух устройств (Stateful)

Резервирование внутри устройства BNG

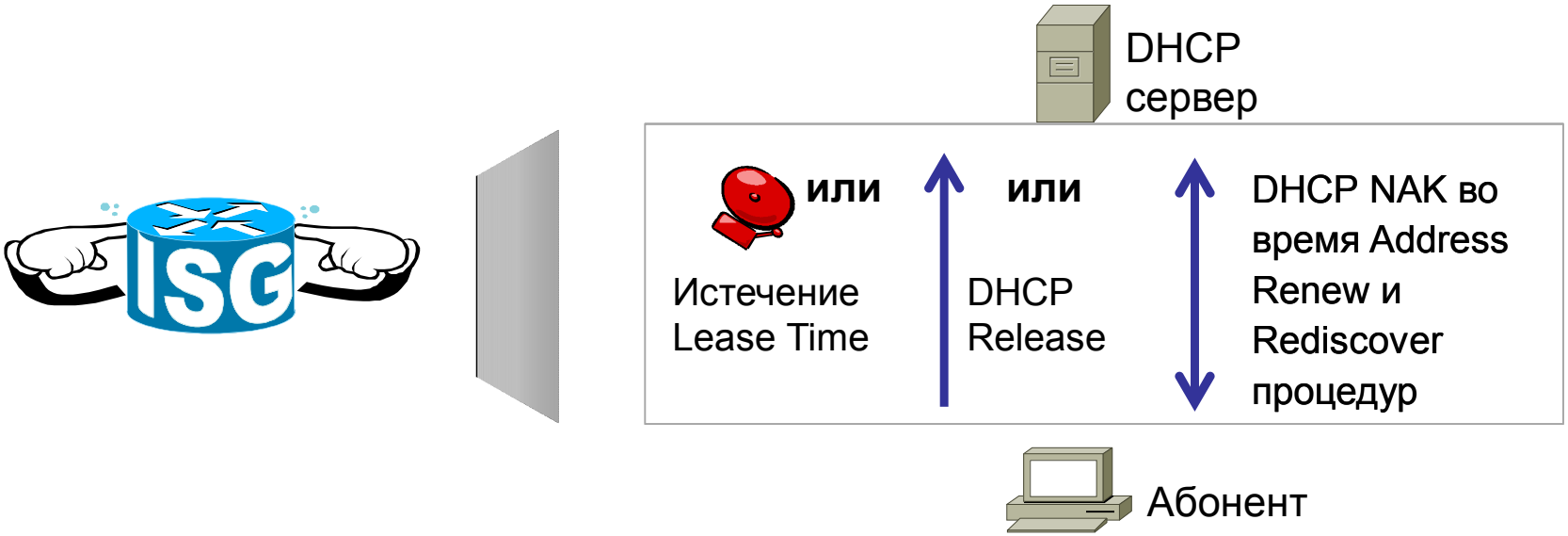


- LAG (Bundle-Ethernet)
- Выход из строя активного интерфейса – прозрачное переключение текущей сессии на оставшиеся интерфейсы
- Для корректной работы механизмов QoS требуется модификация алгоритма балансировки на бандле:

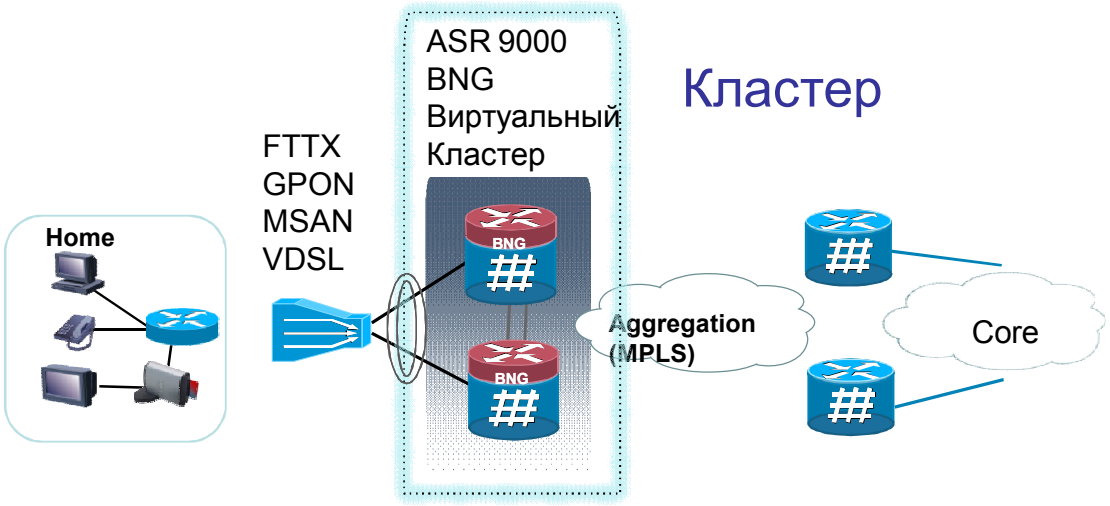
```
interface bundle-ether 1
  bundle load-balancing hash dst-ip
```

Stateless резервирование: два шасси

- Резервирование для PPPoE сессий в целом проще, чем для IPoE сессий
- Дизайн обязательно должен обеспечивать «симметрию» трафика – трафик от абонента и к абоненту должен проходить через один и тот же BNG
- Для переустановления сессии абонент должен отправить DHCP Discover!
- Время переключения определяется величиной Lease Time
- Абонент (как правило) не имеет средств мониторинга состояния IPoE сессии (в отличие от PPPoE)

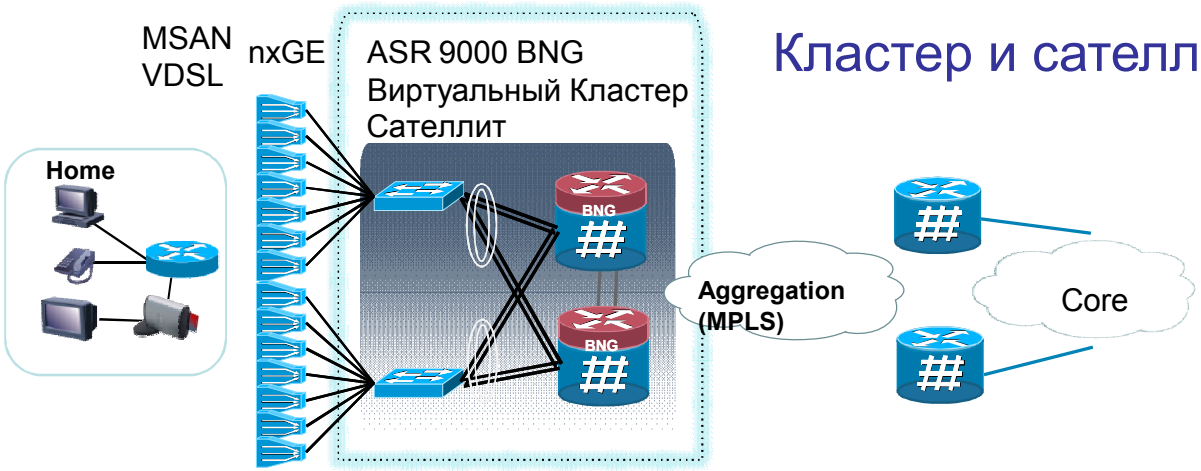


Кластер ASR 9000 nV как единое резервированное BNG устройство



Кластер

- Гео-резервирование
- Dual Homing
- Работа как с одним шасси
- Stateful Failover
- Active/active LAG в сторону доступа и ядра



Кластер и сателлит

- Гео-резервирование
- Большая плотность 1GE портов
- Работа как с одним шасси (кластер и сателлиты)
- Сателлиты представлены как линейные карты
- Простая топология, нет Spanning Tree

Масштабируемость

Cisco Expo 2012

Требования к аппаратуре для поддержки BNG

Шасси:	ASR 9001, ASR 9006, ASR 9010 ASR 9922 (4.3.1)
RSP:	A9K-RSP440-SE

Access Facing карты (BNG)	Typhoon Service Edge карты:
	• A9K-24X10GE-SE
	• A9K-36X10GE-SE (4.3.1)
	• A9K-MOD80/160-SE с интерфейсами:
	  • A9K-MPA-2x10GE
	  • A9K-MPA-4x10GE
	  • A9K-MPA-20x1GE

Core Facing карты (Uplink)	Любая линейная карта
Поддержка технологии nV (кластер)	Да
Поддержка технологии nV (сателлит)	Да (4.3.0)

Параметры масштабирования

Сегодня:

- 64 000 сессий на шасси (для ASR 9001 32 000 сессий)
- 64 000 сессий на LC
- Скорость установки сессий: 100-300 сессий в секунду

Планы на будущее:

- 128 000 сессий на шасси ASR 9006/9010 (4.3.0)
- 192 000 сессий на шасси ASR 9006/9010 (4.3.1)

Также рекомендуем посетить

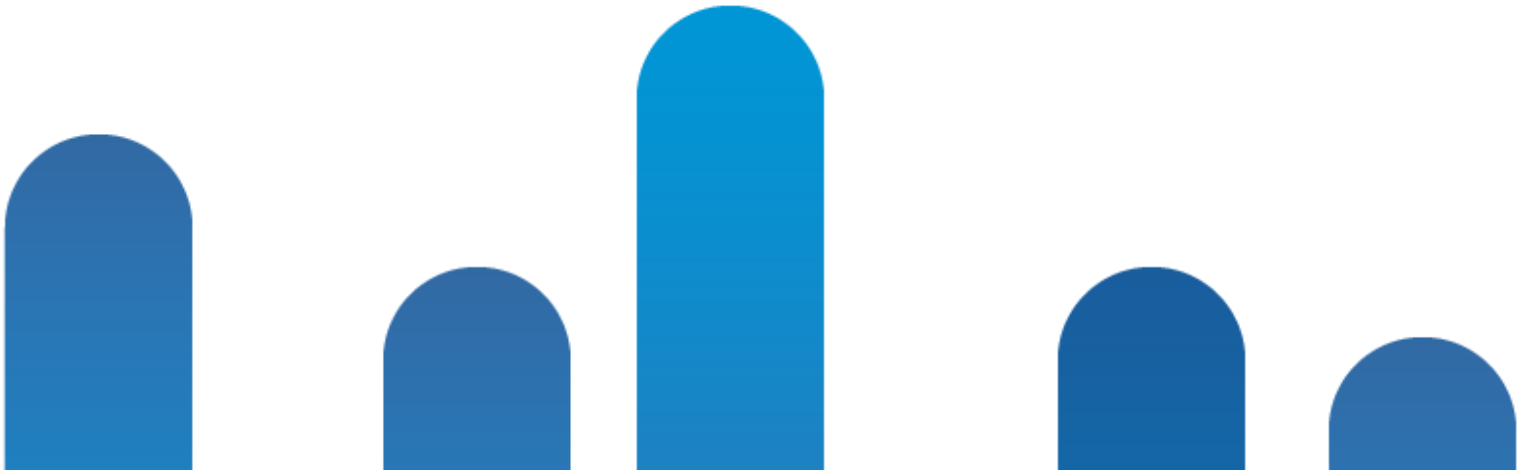
- **ASR 9000 nV технология - кластеры и сателлиты**
- **Архитектура Cisco Unified MPLS: Внедрение MPLS на всех уровнях сети**
- **Реализация технологии “Операторский NAT” в продуктах Cisco**

- **Открытая дискуссия** по технологиям для операторов связи
  - 21 ноября, среда, 18 часов, Конгресс-зал Правый
  - Готовьте свои вопросы!
- **Демо-стенд «Решения для операторов связи»** (демо-зона, комната 5)
  - ASR 9000 с интерфейсами 100GigabitEthernet
  - Технология сетевой виртуализации ASR 9000 nV
  - Carrier Grade v6 на базе маршрутизатора Cisco ASR 9000 с модулем ISM
  - И многое другое!

Спасибо!

Заполняйте анкеты он-лайн и получайте подарки в Cisco Shop: **http://ciscoexpo.ru/expo2012/quest**

Ваше мнение очень важно для нас!



BUILT FOR THE HUMAN NETWORK

cisco