Андрей Идлис
Cisco Systems

Развертывание сети ШПД на базе Ethernet-доступа: вопросы и ответы

Часть 1. Быстрее, шире, доступнее. Архитектура сети ШПД

Сеть широкополосного доступа (ШПД) является частью инфраструктуры любого «розничного» оператора. Существуют различные технологии доступа, модели предоставления услуг, архитектурные подходы к строительству таких сетей.

Решения, принятые оператором на начальном этапе развертывания сети, оказывают существенное влияние на дальнейшее ее функционирование и развитие, на возможность оказывать те или иные услуги, на структуру капитальных и операционных затрат оператора; а исправление ошибок, допущенных на этапе планирования ШПД, после того как сеть построена и введена в эксплуатацию, — дело сложное и дорогостоящее. Поэтому так важно тщательно проанализировать плюсы и минусы каждого подхода, взвесить все «за» и «против», прежде чем сделать выбор в пользу использования конкретной архитектуры. Чтобы помочь читателям, приступающим к развертыванию сетей ШПД на базе Ethernet-доступа, избежать серьезных ошибок, в этой статье мы расскажем о подходах, используемых в индустрии в настоящий момент, о достоинствах и недостатках различных вариантов.

Архитектурные решения, предлагаемые в рамках этой статьи, основаны на рекомендациях международных организаций по стандартизации, таких как Broadband Forum (рекомендация TR-101), MetroEthernet Forum и других. Кроме того, при написании статьи использовались руководства по построению сетей IP NGN от компании Cisco: специальное подразделение внутри Cisco ведет постоянную работу по тестированию различных архитектурных вариантов построения сетей ШПД, выпускаемые по результатам тестирования руководства описывают детали сетевого дизайна вплоть до листингов конфигурации применяемого оборудования.

Архитектура сети ШПД

Обычно при построении любых сетей стараются придерживаться иерархического подхода, и сети ШПД с этой точки зрения не являются исключением. Можно выделить четыре основных уровня, в том или ином виде присутствующих в любой сети ШПД. Это:

- Уровень доступа.
- Уровень агрегации.
- Уровень предоставления услуг (сервисный уровень).
- Уровень магистрали.

Рассмотрим их предназначение.

Уровень доступа, как следует из его названия, обеспечивает физический доступ абонента к сети. Все существующие технологии доступа обычно подразделяются на три класса — проводные, кабельные и беспроводные. К проводным относятся сети xDSL, PON и Ethernet. В данной статье мы рассматриваем исключительно Ethernet-доступ, однако с точки зрения архитектуры сети, то есть организации VLAN, логических принципов подключения абонентов, обеспечения резервирования и т.д., все типы проводных (да и беспроводных) сетей доступа весьма похожи. Поэтому многие принципы, изложенные в статье, также можно отнести и к другим технологиям доступа.

Далее следует уровень агрегации. Его задача — подключение уровня доступа к уровню предоставления услуг и к ядру сети. Географические размеры сети агрегации различаются и зависят от плотности абонентов, имеющейся оптической инфраструктуры и т.п.: как правило, она покрывает крупный город или область. Сеть может быть построена как полностью на втором уровне модели OSI (то есть, проще говоря, с использованием коммутаторов), так и с использованием технологий IP/MPLS (с применением IP/MPLS маршрутизаторов).

Сеть агрегации, построенная полностью на втором уровне, обычно обходится дешевле в развертывании, но, как правило, сложнее в эксплуатации. Те из читателей, кто работал с большими коммутируемыми сетями, представляют себе сложности, а именно большие широковещательные домены или проблемы поиска неисправностей в протоколе STP. Кроме того, данные сети имеют меньшие возможности масштабирования, поэтому такой подход можно рекомендовать только для относительно небольших сегментов агрегации.

Сеть агрегации, построенная на базе технологии IP/MPLS, обеспечивает необходимую гибкость, простоту эксплуатации и хорошие возможности масштабирования. Особо стоит отметить, что использование IP/MPLS в агрегации позволяет применять комбинированный подход к доставке трафика: часть трафика можно маршрутизировать на третьем уровне модели OSI (например, видеотрафик, особенно его multicast-составляющую), а другую часть (например, интернет-трафик) — туннелировать на втором уровне до сервисной границы с помощью технологий Ethernet over MPLS или VPLS.

Оператор может пойти по пути развертывания агрегации с использованием коммутации на втором уровне модели OSI с тем, чтобы перейти на технологию IP/MPLS в будущем, по мере роста абонентской базы и, соответственно, сегмента агрегации. Оборудование производства Cisco, например, предлагает возможность осуществить такой вариант с полным сохранением инвестиций: для перехода на IP/MPLS в коммутаторах агрегации не требуется никаких аппаратных изменений, необходимо всего лишь приобрести дополнительную программную лицензию.

Задача сервисного уровня заключается не в передаче трафика как такового, а в организации сервиса, то есть того, за что в итоге и платит абонент. Сервисный уровень осуществляет аутентификацию и авторизацию абонента — определяет список сервисов, которые может (и должен) получать абонент. Далее оборудование сервисного уровня обеспечивает выполнение параметров контракта с абонентом по сервисам, на которые абонент подписан, например, ограничивает скорость доступа в Интернет до контрактных величин; и здесь же формируется статистика для биллинга абонента или обеспечивается контроль потребления услуг абонентами, работающими по предоплате. На сервисном уровне формируется понятие абонентской сессии, то есть своеобразного «виртуального сетевого интерфейса» к абоненту, осуществляется выдача IP-адресов.

Собственно, на уровне IP-протокола абонент взаимодействует именно с сервисным уровнем.

Оборудование, реализующее функции сервисного уровня, принято называть терминами BRAS (Broadband Remote Access Server, термин стандарта Broadband Forum TR-59) или BNG (Broadband Network Gateway, термин стандарта Broadband Forum TR-101). Оба употребляются в индустрии взаимозаменяемо, в настоящей статье принято обозначение BRAS.

Устройство BRAS — это, по сути, маршрутизатор, обладающий специальным дополнительным функционалом по работе с абонентскими сессиями и позволяющий выполнить следующее:

- Аутентификацию абонента во внешней системе.
- Авторизацию абонента, то есть получение списка сетевых сервисов и их параметров, на которые подписан абонент, во внешней системе.
- Создание абонентской сессии — виртуального интерфейса в сторону абонента, применение к этому интерфейсу необходимых параметров для реализации выбранных сервисов (например, ограничение скорости доступа в Интернет), назначение IP-адреса абоненту.
- Передачу во внешнюю систему биллинга данных об использовании абонентами ресурсов (например, общий трафик в байтах, переданный абоненту, или проведенное в сети время).

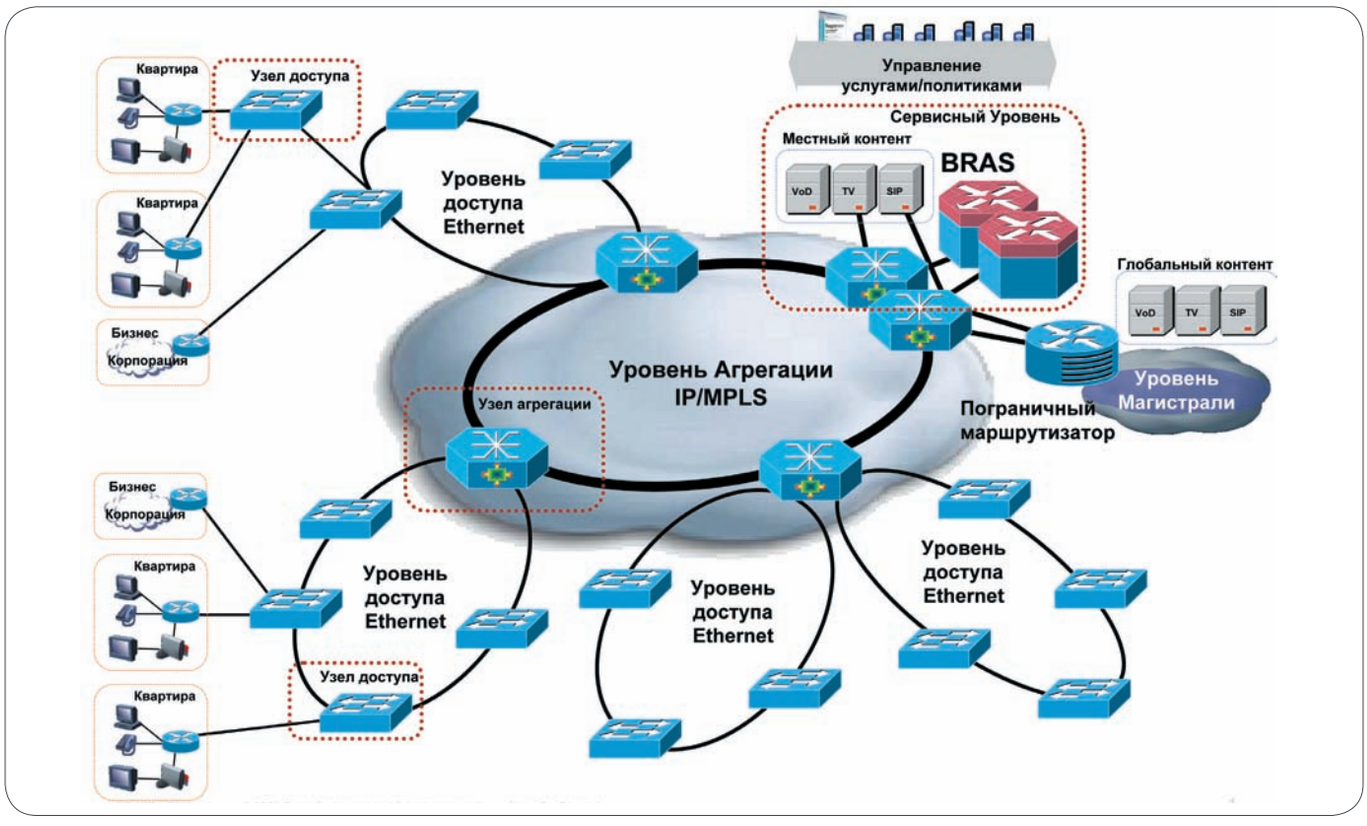
Существуют и другие, расширенные, функции управления абонентскими сессиями, которые могут быть реализованы устройством BRAS. К ним можно отнести, например, контроль квот с последующим автоматическим отключением абонента от сети или перенаправление абонента на специальный портал для клиентов, тарифицируемых по предоплате.

Функции сервисного уровня могут быть вынесены на отдельное специализированное оборудование, как правило, располагающееся в этом случае между уровнем агрегации и уровнем магистрали, или возложены на оборудование уровня агрегации. В последнем случае термин BRAS означает не выделенный маршрутизатор сервисного уровня, а соответствующий набор функционала по управлению абонентскими сессиями, реализованный на маршрутизаторе уровня агрегации.

Стоит заметить, что не все типы услуг в принципе нуждаются в выделенном сервисном уровне (и в полном наборе функций BRAS). Как правило, услуги можно разделить на два класса: транспортные (или сетевые) и услуги приложений. К услугам первого типа относятся, например, доступ в Интернет, доступ к корпоративному VPN, к собственному игровому серверу оператора и т.д. Они тарифицируются по скорости доступа или количеству переданных байт. Тарификация, как и доступ к услуге, выполняются собственно сетью, а именно устройством BRAS.

Примерами услуг второго типа — услуг приложений — являются такие сервисы, как IP-телефония или IPTV. Они управляются и тарифицируются соответствующими прикладными системами (например, доступ к услуге VoIP управляется регистрацией абонентского терминала на SIP Proxy сервере, а тарификация обеспечивается программным коммутатором вызовов VoIP — SoftSwitch). Сеть всего лишь обеспечивает транспорт (с соответствующими гарантиями качества обслуживания) от абонентского терминала до прикладной системы. Поэтому такие

Рис. 1. Общая архитектура сети ШПД



приложения не нуждаются в выделенном уровне сервисной границы. Минимально необходимая часть функций сервисной границы (а это, фактически, только выдача IP-адресов и обеспечение IP-связанности с соответствующей прикладной системой) всегда может быть возложена на оборудование агрегации, даже если оно не в состоянии реализовать полный набор функций BRAS. В этом случае часть трафика абонента, в частности — видеотрафик, может обслуживаться без использования ресурсов BRAS, что позволяет оптимизировать капитальные затраты при строительстве сети ШПД.

Уровень магистрали предназначен для быстрой и надежной передачи трафика на межрегиональном уровне. Фактически, магистраль связывает между собой сети агрегации, построенные в разных городах. Если оператор эксплуатирует сеть только в одном городе или области, уровень магистрали может вообще отсутствовать в явном виде, являясь, по сути, подключением к вышестоящему магистральному оператору.

Общая архитектура типичной сети ШПД приведена на рис. 1.

Организация сервисов. Использование VLAN. Функции CPE

Рассмотрим вопрос организации сервисов на всей цепочке от абонентского оборудования (CPE) через оборудование доступа и агрегации до оборудования сервисной границы (BRAS). Мы будем ориентироваться на предоставление трех базовых сервисов — VoIP, IPTV и доступа в Интернет.

Основным стандартом в этом вопросе, которому в той или иной мере соответствует большинство ШПД-сетей, является TR-101, принятый организацией Broadband Forum. Стандарт рассматривает технические аспекты реализации сервисов Triple Play в сетях ШПД, построенных на базе Ethernet-технологий, специфицирует определенные архитектурные модели и определяет функциональные требования к оборудованию CPE, доступа, агрегации и BRAS, необходимые для успешной реализации предлагаемых архитектурных моделей.

Далее в статье мы обсудим основные вопросы этих архитектур — режим работы CPE (routed или bridged), организацию VLAN в сети (VLAN на пользователя или VLAN на сервис), организацию подачи мультикаст-трафика и прочее.

Использование VLAN

Сеть доступа и агрегации обеспечивает подключение абонента к сервисному уровню (уровню предоставления услуг). Услуги, реализованные с помощью выделенной сервисной границы, как правило, требуют обеспечить подключение абонента к оборудованию сервисного уровня на втором уровне модели OSI. В сети доступа и агрегации такие подключения выполняются посредством набора VLAN. Услуги приложений могут использовать оборудование агрегации в качестве упрощенной сервисной границы, и соответствующий VLAN как средство подключения пользовательского терминала к узлу агрегации необходим только на уровне доступа.

Существуют две базовые модели использования VLAN в сетях доступа и агрегации: «VLAN на пользователя» и «VLAN на сервис/группу пользователей». В стандарте TR-101 используется иная терминология — модели 1:1 и N:1; и этой, второй, терминологией мы и будем пользоваться в настоящей статье.

Модель 1:1 предполагает, что каждому абоненту соответствует свой персональный VLAN на всей сети доступа и агрегации вплоть до уровня сервисной границы (см. рис. 2).

Модель N:1, напротив, заключается в том, что один общий VLAN используется для некоторой группы абонентов (см. рис. 3).

Каждая из этих схем имеет свои достоинства и недостатки. Рассмотрим их подробнее.

Начнем с модели 1:1, или «VLAN на абонента». К числу ее безусловных достоинств относится довольно высокая степень изоляции абонентов друг от друга на всей сети доступа и агрегации. Поскольку каждый абонент в этой модели имеет фактически свой выделенный VLAN типа «точка-точка», в котором находятся всего лишь два хоста — он сам (его CPE) и соответствующий ему интерфейс на BRAS, вопросы изоляции абонентов друг от друга и контроля их трафика решаются автоматически. Абонент может передавать трафик только на выделенный ему логический интерфейс BRAS, проверка легитимности использования IP/MAC адреса абонента осуществляется исключительно на BRAS. Модель 1:1 позволяет обеспечить четкую идентификацию порта подключения абонента на устройстве BRAS — по номеру VLAN-абонента.

С другой стороны, эта модель предполагает наличие большого числа VLAN в сети доступа и агрегации. Поскольку пространство номеров VLAN ограничено (на номер VLAN в стандарте 802.1q выделено 12 бит, таким образом, мы имеем 4095 уникальных значений номеров VLAN), для внедрения этой модели приходится применять двойную 802.1q инкапсуляцию, то есть QinQ-инкапсуляцию (иерархическую нумерацию VLAN). Как правило, второй, верхний VLAN тег в этой схеме определяет коммутатор доступа или кольцо коммутаторов доступа. Кроме того, эта модель требует назначения индивидуального номера VLAN каждому абоненту, то есть требует от оператора, во-первых, изначального планирования множества номеров VLAN в сети и, во-вторых, выделения и назначения индивидуального номера на момент подключения абонента, увеличивая трудозатраты на выполнение такого подключения. Альтернативой тут могла бы быть разработка схемы нумерации VLAN, позволяющей провести так называемый препровиженинг оборудования доступа, то есть изначально присвоить уникальные номера VLAN всем портам коммутаторов доступа. Такие схемы часто применяются операторами DSL-сетей доступа. Однако, как показывает практика, разработать подходящую схему для Ethernet-доступа оказывается или довольно сложно, или вообще невозможно. Связано это с тем, что Ethernet-доступ носит более распределенный характер, коэффициент использования портов коммутаторов доступа сильно различается от дома к дому, периодически в кольцо требуется подключить новый коммутатор, что может сломать принятую изначально схему, и т.д.

Модель 1:1 также предполагает наличие единой сервисной границы для всех услуг, предоставляемых абоненту. Так как весь трафик абонента по выделенному ему VLAN доставляется до устройства BRAS, все сервисы (в том числе видео-по-запросу или VoIP) требуется подавать через BRAS, что не всегда является экономически правильным

Рис. 2. Модель «VLAN на абонента», или 1:1

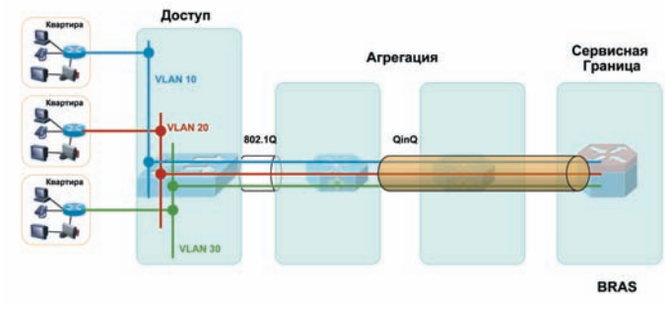
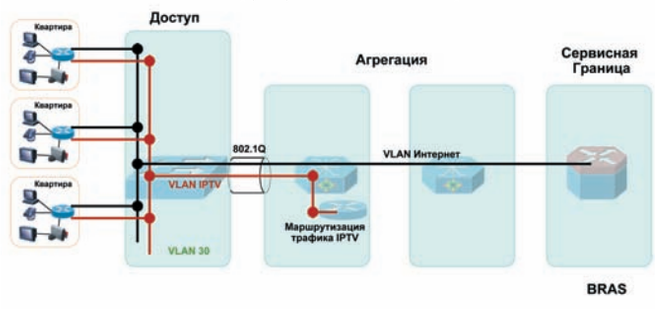


Рис. 3. Модель «VLAN на группу пользователей/сервис» или N:1



решением. Из-за использования большого числа VLAN сложнее становятся схемы резервирования BRAS устройств, схемы подачи multicast-трафика. Подробнее об этом мы расскажем в следующих разделах статьи.

Вторая модель, N:1 или «VLAN на сервис», предполагает, что для группы абонентов, подключенных к общему сервису, выделяется один общий VLAN, который соединяет эту группу абонентов с виртуальным интерфейсом, организованным на оборудовании, выполняющем функции сервисной границы для этого сервиса. Это может быть, например, интерфейс на BRAS для сервиса доступа в Интернет или интерфейс на оборудовании агрегации для сервиса IPTV. Для подачи этой же группе абонентов другого сервиса может использоваться как этот же, так и отдельный, второй общий VLAN. Модель «VLAN на сервис», в отличие от модели выделенных VLAN, существенно проще с точки зрения управления пространством номеров VLAN. Число VLAN в сети существенно уменьшается, во многих случаях позволяя отказаться от необходимости стекирования тегов VLAN (то есть в модели N:1 можно обойтись без применения технологии QinQ). Упрощается технология подключения абонента — все порты коммутаторов доступа настраиваются одинаково, не требуется индивидуальных настроек номеров VLAN. Отказ от технологии QinQ позволяет упростить технологию подачи мультикаста. Наиболее важным достоинством модели N:1, на наш взгляд, является возможность строить сеть с множеством сервисных границ, то есть VLAN, предназначенный для обеспечения доступа в Интернет, может «приземляться» на BRAS, а VLAN, предназначенный для услуг IPTV — непосредственно на устройстве уровня агрегации, снижая нагрузку на BRAS и уменьшая общую стоимость сети для оператора связи.

Однако в модели N:1 необходимо решить ряд вопросов, относящихся к безопасности и защите пользователей друг от друга. Поскольку группа абонентов находится в одном VLAN, без принятия специальных мер абоненты могут получить возможность обмениваться трафиком напрямую через сеть доступа и агрегации, что не всегда устраивает оператора связи. Основная проблема прямого обмена трафиком между абонентами «ниже» уровня сервисной границы заключается в том, что этот обмен не контролируется оператором, то есть не производится аутентификация абонента, тарификация, ограничение скорости трафика и т.д., поскольку все эти действия выполняются «выше», на уровне сервисной границы.

Второй вопрос, который теперь ложится на оборудование доступа и агрегации — контроль использования IP- и MAC-адресов. В предыдущей модели использование абонентом выданного именно ему, а не соседу, IP-адреса, контролирует оборудование сервисной границы, то есть, например, BRAS для услуги доступа в Интернет. Первая задача — запрет локального обмена трафиком между абонентами там, где это нежелательно — решается применением функций Split Horizon Forwarding на коммутаторах доступа. Этот класс функций имеет различные названия у разных производителей, но суть всегда заключается в том, что трафик, полученный от абонента (от абонентского порта), не может быть отправлен в другой абонентский порт коммутатора. Вторая задача — контроль использования IP- и MAC-адресов — решается группой из трех функций, применяемых на коммутаторах доступа: DHCP Snooping, Dynamic ARP Inspection и IP Source Guard.

DHCP Snooping — базовая функция, на основе которой функционируют следующие две. Она «подсматривает» DHCP-обмен клиента с сервером DHCP и запоминает MAC-адрес абонента и выданный ему IP- адрес в специально создаваемой таблице. На основе этой таблицы работают функции Dynamic ARP Inspection и IP Source Guard. Эти функции проверяют ARP- и IP-пакеты, поступающие в сеть от абонента, на корректность, то есть проверяют тот факт, что абонент использует именно тот IP-адрес, который был ему выдан по DHCP.

Отметим здесь, что при условии реализации функции Split Horizon Forwarding в сети доступа и агрегации эти три функции не обязательно выполнять на коммутаторе доступа, а можно возложить на оборудование BRAS. Такой подход позволяет использовать более простое оборудование в сети доступа.

Оборудованию BRAS может понадобиться идентификация порта подключения абонента. В модели «VLAN на абонента» этой идентификацией является, по сути, номер индивидуального VLAN абонента. Здесь же в одном VLAN находятся несколько абонентов, поэтому такой способ, очевидно, не подходит.

Однако существует решение этой проблемы и в модели N:1. В зависимости от используемого протокола доступа (IP или PPP, подробнее об этом — далее) используются механизмы DHCP Option 82 или PPPoE Intermediate Agent. Оба эти механизма действуют похожим образом. В случае применения протокола IP коммутатор доступа перехватывает DHCP Discover запросы от клиентов и вставляет в DHCP опции этого пакета опцию 82, идентифицирующую коммутатор доступа и порт этого коммутатора. Затем пакет DHCP Discover попадает на BRAS, который способен проанализировать опцию 82 и получить из нее идентификацию порта подключения абонента. Для протокола PPP коммутатор доступа перехватывает PPPoE PADI-запросы на установление PPPoE сессии и добавляет в опции этого пакета соответствующую информацию. Далее PADI-пакет отправляется на BRAS, где и происходит анализ этой информации.

Как мы видим, каждый из подходов — «VLAN на абонента» и «VLAN на группу абонентов» — имеет свои достоинства и недостатки; краткая сравнительная таблица приведена ниже.

Таким образом, для абонентов частного сектора наиболее разумным представляется использование модели N:1, в то время как обслуживание бизнес-абонентов удобнее осуществлять в модели 1:1. В одной сети доступа могут применяться обе модели одновременно.

Во второй части материала будут рассмотрены варианты протоколов доступа, аутентификация и авторизация абонентов, а также режимы работы в сети абонентских устройств.

Таблица

Параметр	Модель 1:1	Модель N:1
Организация VLAN	VLAN на каждого абонента	VLAN на группу абонентов
Организация сервисов (Internet, IPTV, VoIP)	Все сервисы используют один VLAN, выделенный для абонента, и реализуются на одном сервисном устройстве (BRAS)	Разные сервисы могут использовать общий VLAN, возможно также выделение отдельного VLAN под каждый сервис. Разные сервисы могут быть реализованы на разном сервисном оборудовании
Кол-во VLAN в сети доступа	Большое	Малое
Применение двойного тегирования QinQ в сети доступа/агрегации	Необходимо	Нет необходимости
Индивидуальные настройки порта коммутатора доступа	Да, необходимо настроить персональный номер VLAN абонента	Нет, типовая конфигурация портов
Запрет локальной коммутации трафика между абонентами	Да, путем помещения каждого абонента в отдельный VLAN	Да, путем применения функции Split Horizon Forwarding на коммутаторе доступа
Контроль использования IP-адресов абонентами	Выполняется на BRAS	Выполняется на коммутаторе доступа с помощью DHCP Snooping, Dynamic ARP Inspection, IP Source Guard или на BRAS
Идентификация порта подключения абонента	По номеру VLAN	С помощью DHCP Option 82 или PPPoE Intermediate Agent в случае использования PPP