Оптимизация оказания услуг 3-PLAYна сети широкополосного доступа.

Централизованный контроль подписки на услуги и консолидированная точка доступа

Подготовлено сотрудниками Juniper Networks Россия:
Василием Мухиным, Системный инженер, vmukhin@juniper.net



Представительство
Juniper Networks в России
Смоленская пл., д. 3,
Смоленский Пассаж, 14ый этаж,
121099, Москва, Россия
Тел.: +7 095 981-34-88
Факс: +7 095 937-82-90

СОДЕРЖАНИЕ

СОДЕРЖАНИЕ 2
СПИСОК ИЛЛЮСТРАЦИЙ 3
ВВЕДЕНИЕ 4
ВОПРОСЫ ВЫБОРА СЕТЕВОЙ МОДЕЛИ 5
Точка предоставления услуг 5
Модель доставки услуг 7
Принцип преемственности старых услуг 8
Типы подключения: PPPoE против DHCP 9
Multicast – поддержка трафика групповой рассылки 10
ПРЕИМУЩЕСТВА ЦЕНТРАЛИЗОВАННОГО ПОДХОДА 11
Снижение интеллектуальной роли DSLAM по отношению к IP 11
Вопросы масштабирования и обслуживания 11
Вопросы управления адресным пространством 13
Вопросы надежности 14
Вопросы безопасности: Защита от подмены адресов 14
Усовершенствованная модель QoS 15
Независимость от технологии доступа и производителя 16
МОДЕЛИ ПРЕДОСТАВЛЕНИЯ УСЛУГ: C-VLAN против S-VLAN 17
Эксплуатационные преимущества 18
Преемственность старой модели предоставления услуг 19
Гибкость по отношению к методу аутентификации 19
Планирование персонифицированного SLA при помощи ИЕРАРХИЧЕСКОГО QoS 20
Вопросы Масштабирования 21
Общие рекомендации по выбору модели доступа 22
КЛАССИЧЕСКАЯ BSR-МОДЕЛЬ И ДУАЛИСТИЧЕСКИЙ ПОДХОД BSA/BSR 23
Единая BSR-платформа управления правилами обслуживания и IP-маршрутизации 23
Эмуляция BSR: Распределенная модель BSA/BSR 25
ТРЕБОВАНИЯ К СОВРЕМЕННЫМ СЕТЯМ ШИРОКОПОЛОСНОГО ДОСТУПА 29
Исходные данные. Предположения 29
Общие требования к архитектуре сети 30
Требования к BSR в централизованной модели доступа 31
Требования к уровню сети доступа 33
Требования к уровню CPE 33
BSR НА БАЗЕ МАРШРУТИЗАТОРОВ JUNIPER E-СЕРИИ 35
ОПЫТ ПОСТРОЕНИЕ СЕТЕЙ ДОСТУПА 36
ЗАКЛЮЧЕНИЕ 39
ПРИЛОЖЕНИЕ 1: ДОПОЛНИТЕЛЬНЫЕ МАТЕРИАЛЫ 40

Copyright © 2006, Juniper Networks, Inc.

СПИСОК ИЛЛЮСТРАЦИЙ

Рис. 1 Вид типовой домашней сети в ближайшем будущем 5
Рис. 2 Элементы сети доступа 6
Рис. 3 Пример использования модели C-VLAN. 8
Рис. 4 Классическая архитектура сети доступа на основе ATM 9
Рис. 5 BSR в роли единой точки предоставления услуг 13
Рис. 6 Сквозной контроль QoS в решении Juniper 16
Рис. 7 Пример реализации модели C-VLAN 17
Рис. 8 C-VLAN против S-VLAN на сервисной границе 18
Рис. 9 Построение иерархических правил управления очередями на BSR 20
Рис. 10 Рекомендованный вид архитектуры для сети широкополосного доступа 23
Рис. 11 Пример использования платформы E-серии для центрального BSR. 24
Рис. 12 Процессы маршрутизации и QoS в модели BSR 24
Рис. 13 Распределенная архитектура BSA/BSR 26
Рис. 14 Процессы маршрутизации и QoS в модели BSR/BSA 27
Рис. 15 Линейка маршрутизаторов Juniper с функциональность BSR. 35
Рис. 16 Пример сети широкополосного города с населением 4 млн. 37
Рис. 17 Пример сети широкополосного города с населением 1 млн. 38
Рис. 18 Пример сети широкополосного города с населением 500 тыс. 39

Copyright © 2005, Juniper Networks, Inc.

ВВЕДЕНИЕ

Развитие современных сетей широкополосного доступа связано с желанием операторов связи предоставить своим абонентам новые сервисы в дополнение к уже существующей услуге высокоскоростного доступа в Интернет. Это позволило бы операторам привлечь новых пользователей и получить дополнительную прибыль от продажи услуг, которые, как правило, покрывались операторами спутникового ТВ, традиционной телефонии, кабельного телевидения. Однако предоставление новых сервисов на существующей инфраструктуре ведет к чрезмерному увеличению операционных затрат и под час просто невозможно из-за отсутствия необходимых механизмов качества обслуживания. Данный факт заставляет операторов связи и поставщиков решений задуматься о возможности миграции к новой инфраструктуре, которая позволит эффективно и с наименьшими затратами внедрять и эксплуатировать новые сервисы, такие как:

- Широко вещательное цифровое телевидение (IPTV)
- Видео по запросу
- Интерактивные компьютерные игры
- Услуги для корпоративного сектора
- VPN access,
- firewall or intrusion prevention,
- Voice over IP (VoIP).

Постепенно с ростом количества и размера домашних сетей на первый план будут выходить услуги, связанные с обеспечением сетевой безопасности.

Все чаще архитектура сетей широкополосного DSL-доступа основывается на использовании технологии Ethernet, обеспечивая тем самым, возможность миграции к инфраструктуре, позволяющей оказывать разнообразные услуги на высоких скоростях передачи данных. Существенными вопросами при такой миграции являются вопросы управления подписчиками, услугами и определения границ сети отвечающей за маршрутизацию трафика между подписчиками и сервисами на основе IP-адресов. Должна ли эта функциональность быть сосредоточена на центральном узле или, скажем, распределена на множестве периферийных устройств широкополосного доступа (DSLAM) в непосредственной близости к подписчику? Некоторые хорошо зарекомендовавшие себя подходы оказываются плохо применимы в

Copyright © 2006, Juniper Networks, Inc.

условиях новой инфраструктуры и требований со стороны новых типов сервисов.

Ethernet является той средой, которая при минимальном отношении стоимость / полоса пропускания позволяет строить высоконадежные сети доступа с поддержкой необходимого уровня качества обслуживания (QoS) в пакетных сетях, провиженинга (авто-конфигурации), передачи трафика групповой рассылки (multicast) для приложений и сервисов реального времени. На следующем рисунке схематично представлена картина того, как будет устроена типовая домашняя сеть в обозримом будущем.

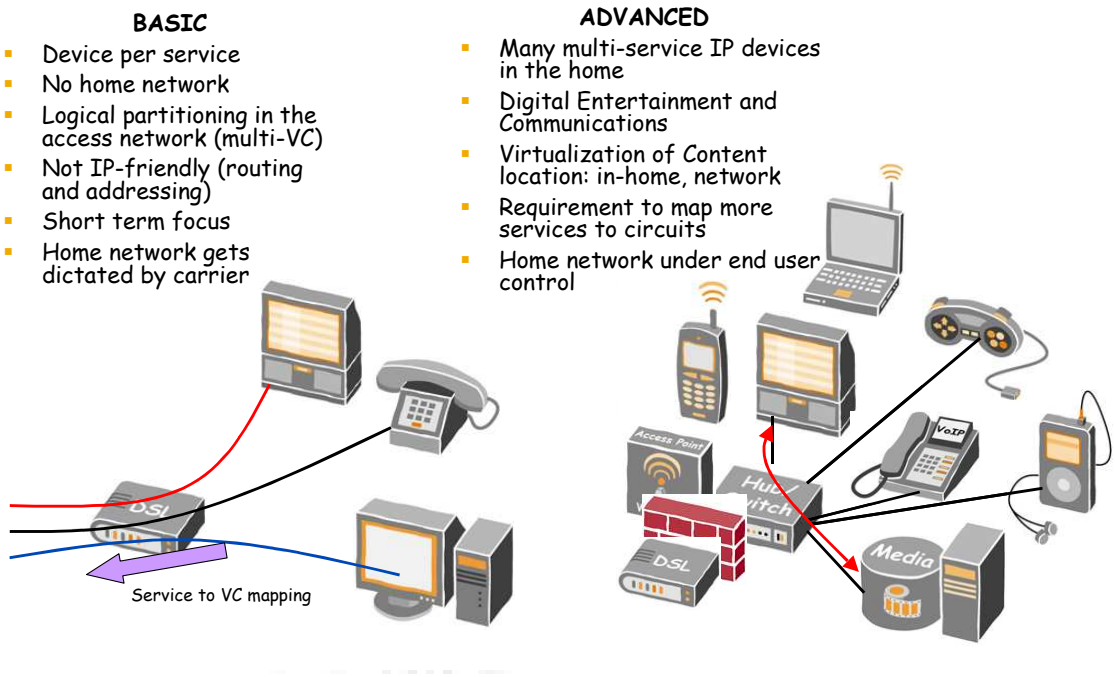


Рис. 1 Вид типовой домашней сети в ближайшем будущем

ВОПРОСЫ ВЫБОРА СЕТЕВОЙ МОДЕЛИ

Точка предоставления услуг

Выбор точки предоставления услуг на сети доступа будет иметь далеко идущие последствия и во многом определит величину капитальных и операционных затрат оператора на развитие сети и ее последующую эксплуатацию соответственно.

Copyright © 2005, Juniper Networks, Inc.

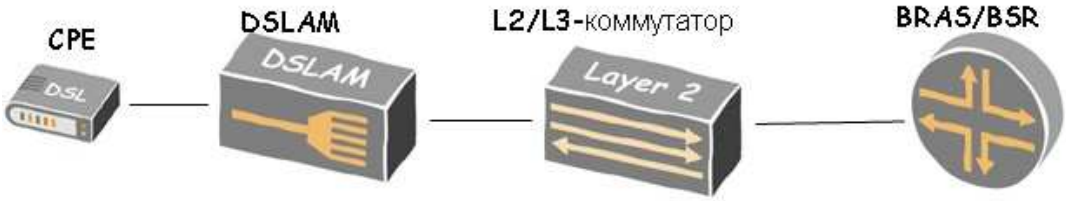
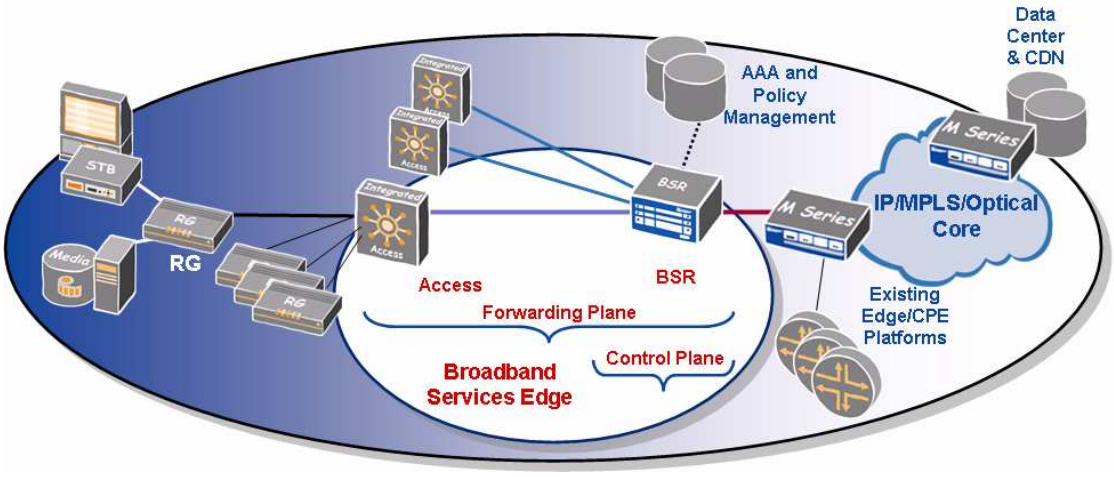


Рис. 2 Элементы сети доступа

Скажем, вынос данного функционала непосредственно на устройство доступа DSLAM приведет к необходимости внедрения чрезвычайно дорогой системы управления подпиской, которую будет крайне сложно масштабировать с ростом количества устройств доступа. Рост капитальных затрат будет так же обусловлен необходимостью установки дорогих интеллектуальных устройств доступа, с развитыми (L2/L3) механизмами качества обслуживания на уровне подписчика, механизмами обслуживания трафика широковещательной рассылки (IP TV) (репликация, IGMP proxy/snooping) и т.д.Терминирование пользовательских сессий на DSLAM-е приведет к нехватке процессорных ресурсов или к чрезмерной стоимости устройства доступа. Одним словом, такой подход в условиях современных сетей создает больше проблем, чем решает их.

В противоположность, консолидация точки предоставления услуг на специализированном центральном устройстве (Broadband service router – BSR) позволяет упростить и сделать более эффективным процесс управления сетью и существенно сократить операционные расходы и высвободить необходимые ресурсы на DSLAM-е.



Связка DSLAM-а, работающего на втором уровне модели OSI, и BSR

Copyright © 2006, Juniper Networks, Inc.

представляется идеальной комбинацией. Не дорогие устройства доступа с дешевыми 1 GE или 10 GE портами и поддержкой минимально необходимого функционала на уровне IP и высокопроизводительный L3 BSR на основе платформы E-серии компании Juniper, являются базой для построения оптимального решения для современной сети широкополосного доступа, нацеленной на предоставление Triple-Play услуг. Наличие *иерархического* механизма качества обслуживания на BSR (в частности на маршрутизаторах E-серии компании Juniper) полностью нивелирует те не многие преимущества, которые может предложить распределенная модель доступа.

Модель доставки услуг

Следующим основополагающим принципом, с которым необходимо определиться является принцип распределения виртуальных частных сетей на уровне доступа между подписчиками и сервисами.

Первым и наиболее распространенным в построенных на сегодня сетях является подход, Shared VLAN (разделяемой частной сети). Под каждый тип сервиса выделяется отдельный VLAN, доступ к которому имеет каждый пользователь, подписанный на данный сервис. Основное преимущество подхода связано с простотой реализации. Главные недоставки – проблемы разграничения доступа пользователей друг к другу (сетевая безопасность), и невозможность обеспечить персонифицированный уровень качества обслуживания для каждого подписчика. В принципе этого уже достаточно, для того чтобы отказаться от этого подхода для построения 3-Play инфраструктуры.

Следующий способ связан с выделением отдельного VLAN (C-VLAN = Customer VLAN) для каждого подписчика и размещение трафика от разных сервисов, на которые подписан клиент, в этом C-VLAN-е.

И, наконец, последним способом, является выделение отдельного VLAN-а для каждого отдельного сервиса (S-VLAN), на который подписан конкретный пользователь. С одной стороны этот способ является наиболее привлекательным с точки зрения разграничения доступа и управления качеством обслуживания, однако на практике означает необходимость поддержки огромного числа S-VLAN-ов на BSR и, как следствие, ограничения по масштабируемости сети.

Компромиссным вариантом является подход C-VLAN. При этом каждый сервис в рамках одного C-VLAN обеспечивается гарантированным уровнем обслуживания в соответствии с SLA (Service Level Agreement), это возможно благодаря *иерархическому* механизму качества обслуживания на маршрутизаторах E-серии. В принципе, на платформе E-серии может быть

Copyright © 2005, Juniper Networks, Inc.

реализован доступ на основе S-VLAN, например, в случае если приложения, отвечающие за тот или иной сервис, находятся в физически различных сетях/средах.

На рисунке ниже проиллюстрирована Ethernet-DSL архитектура с консолидированным центром доступа на BSR, использующая модель доступа с одним VC на участке CPE/RG-DSLAM-BSR (C-VLAN)

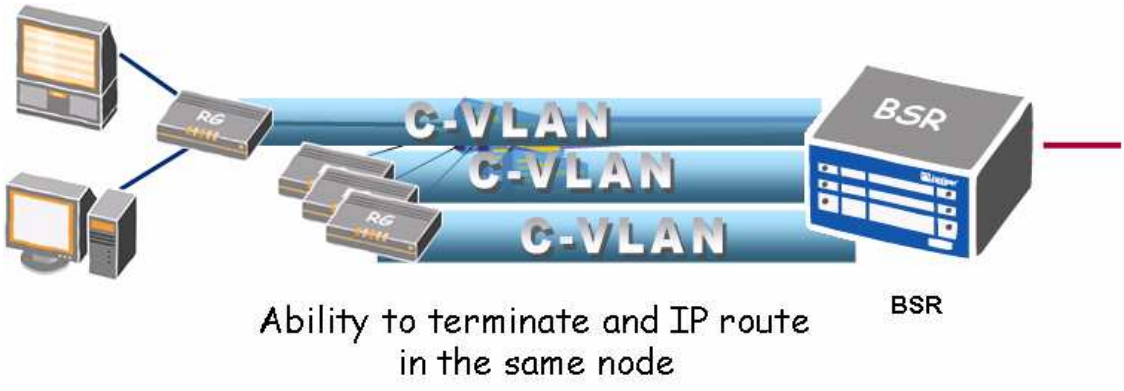


Рис. 3 Пример использования модели C-VLAN

Из соображения снижения капитальных затрат, наиболее предпочтительным является построение простого уровня доступа работающего на втором уроне (L2) стандартной модели OSI. Использование модели C-VLAN позволяет заранее на этапе установки пред-конфигурировать порты DSLAM-ом для использования соответствующих VLAN-ов, тем самым, избежав необходимости их настройки в процессе эксплуатации (в отличие от модели S-VLAN) и как следствие сократить операционные расходы и сделать их более предсказуемыми. Кроме того, такой подход позволит оператору сохранить определенную независимость в выборе производителя для устройств уровня доступа.

Принцип преемственности старых услуг

Решение для сетей DSL-доступа на основе ATM и сегодня успешно применяется многими операторами. Типовая архитектура базируется на использование DSLAM-ов и ATM-коммутатора для агрегации трафика на втором уровне. Далее пользовательские сессии – PPP или DHCP-сессии, как правило, терминируются на BRAS-е, который отвечает за предоставление транспортных сервисов с использованием MPLS, L2TP и т.д. Существует масса нюансов связанных с конкретной реализацией, но типовая схема соответствует описанной выше.

Copyright © 2006, Juniper Networks, Inc.

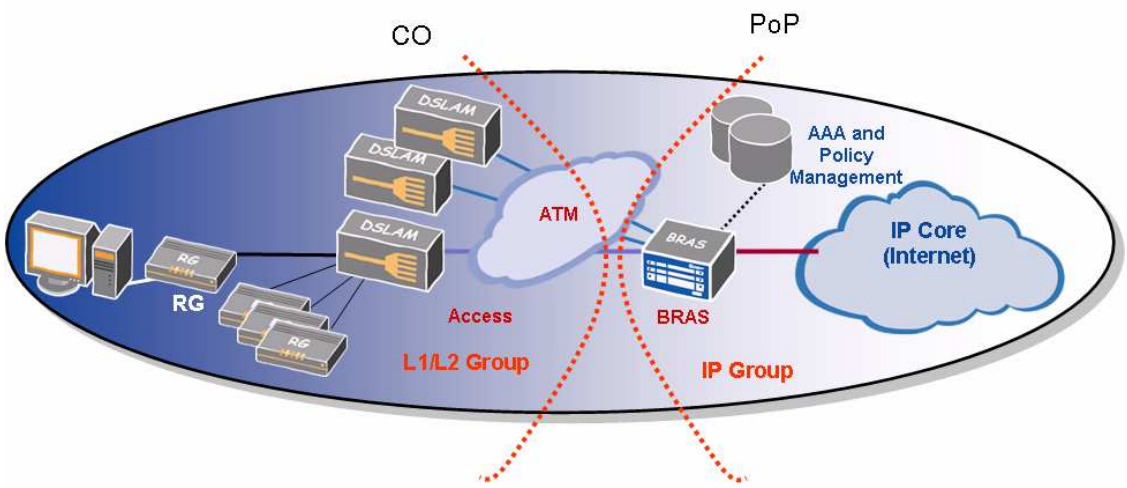


Рис. 4 Классическая архитектура сети доступа на основе ATM

Очевидно, что процесс миграции в сторону новой инфраструктуры не может быть единовременным. Построенные широкополосные сети доступа, рассчитанные только на высокоскоростной доступ в Интернет (на основе как ATM, так и Ethernet) будут поддерживаться операторами и в обозримом будущем. Подход, продвигаемый Juniper, учитывает этот факт в полной мере и гарантирует органичное сосуществование старой архитектуры и различных технологий доступа с централизованным решением на основе BSR E-серии и обеспечивает плавный процесс миграции подписчиков. Решение предусматривает внедрение сервисов с добавленной стоимостью, включая firewall, IDS, SSL и установку пограничного контроллера VOIP сессий (Session Border Controller - SBC).

Типы подключения: PPPoE против DHCP

Dynamic Host Control Protocol (DHCP) и Point-to-Point Protocol over Ethernet (PPPoE) являются наиболее распространенными протоколами, которые используются в широкополосных сетях доступа. Каждый протокол обладает рядом преимуществ и недостатков, которые необходимо иметь в виду.

PPPoE ориентирован на сессионные подключения точка-точка между CPE и BSR и имеет более развитые по сравнению с DHCP механизмы аутентификации пользователей, в то время как DHCP позволяет устанавливать менее чувствительное по отношению к сбоям подключения. В случае организации DSL доступа каждый подписчик идентифицируется физической линией/(номером порта и устройства доступа), т.к. для каждого такого подключение выделен отдельный VLAN, то именно метка - VLAN-tag (внутренняя метка VLAN-а в случае стекирования) может служить

Copyright © 2005, Juniper Networks, Inc.

идентификатором клиента, для этого задействуются механизмы RADIUS в случае PPPoE или Option 82[1] в случает DHCP.

Не смотря на существующие различия в подходах, на наш взгляд, было бы не верно противопоставлять один подход другому. В рамках новой инфраструктуры должны поддерживаться как PPPoE, так и DHCP-протокол, дополняющие друг друга и расширяющие портфель услуг операторов связи.

Multicast – поддержка трафика групповой рассылки

Механизма групповой рассылки (далее – Multicast) широко применяется для доставки мультимедийного контента, в частности широковещательного видео поверх IP-инфраструктуры (IP TV). Эффективное распространение IP TV трафика (репликация трафика, в точке как можно более близкой к конечному подписчику) на участке DSLAM-BSR как правило, решается за счет организации выделенного Multicast VLAN-а (MC-VLAN). Соответственно репликация трафика в направлении конкретного подписчика осуществляется непосредственно на DSLAM-е, на основе IGMP-запросов (на DSLAM необходима поддержка механизмов IGMP-snooping и IGMP-proxy). Для того чтобы сократить время переключения между каналами, DSLAM так же будет отвечать за предоставление или запрет доступа подписчику к соответствующей группе широковещательной рассылки/ТВ-каналу, в то время как BSR должен быть сконфигурирован в режиме static IGMP. В данном режиме BSR будет передавать весть IP TV трафик (все IP TV каналы) в направлении соответствующего L2 сегмента в не зависимости от полученных запросов не подписку.

Таковы общие вопросы, связанные принципами организации современных сетей доступа, рассчитанных на предоставление множества различных сервисов. Эти и другие связанные вопросы более подробно рассматриваются в последующих главах.

[1] DHCP Option 82 позволяет «relay agent»-у добавить в клиентский DHCP-запрос информацию о себе и в таком виде переправить на сервер. Сервер, в свою очередь, может использовать эти данные при назначении клиенту IP-адреса и прочих правил доступа.

Copyright © 2006, Juniper Networks, Inc.

ПРЕИМУЩЕСТВА ЦЕНТРАЛИЗОВАННОГО ПОДХОДА

Очень частая точка зрения, с которой приходится сталкиваться, заключается в утверждении, что для обеспечения максимально эффективного и качественного предоставления услуг необходимо вынести точку предоставления сервиса как можно ближе к конечному пользователю. И действительно, использование интеллектуальных IP DSLAM-ов позволило бы эффективно обслуживать Multicast трафик и применять правила IP QoS на границе сети в непосредственной близости к подписчику. С другой стороны существует множество других требований, связанных с обслуживанием DSL доступа, с управлением подпиской пользователей на множество различных услуг. Этим требованиям на много эффективнее можно удовлетворить, перенеся соответствующий функционал с границ сети на BSR. В конечном итоге (при прочих равных условиях) мерой эффективности для оператора связи следует считать простоту управления, величину операционных расходов, масштабируемость всей сети в целом.

Снижение интеллектуальной роли DSLAM по отношению к IP

Вынос интеллектуальной роли по отношению к обработке протокола IP подписки на услуги за пределы DSLAM позволяет максимально удешевить этот элемент сети доступа и сделать его максимально пригодным для массового использования. Тенденции, связанные с увеличением скорости доступа, ведут к неизбежному снижению протяженности последней мили. Соответственно по мере переноса DSLAM-ом ближе к конечному пользователю будет снижаться плотность портов на одном устройстве, и увеличиваться число самих DSLAM-ов до десятка тысяч.

Вопросы масштабирования и обслуживания

Централизованная архитектура легче поддается обслуживанию, упрощается процесс локализации и скорость обнаружения сбоев. Трудно спорить с фактом, что легче обслуживать несколько крупных IP-узлов чем сотни (а в некоторых случаях и тысячи) распределенных точек присутствия образующих IP-сеть. Чем больше сеть, тем больше будет проявляться дынный фактор. К примеру, сеть, имеющая миллион подписчиков, может быть построена с использованием 50-ти BSR сконцентрированных на относительно не большом количестве узлов. Каждый BSR будет обслуживать сотни устройств доступа и десятки тысяч пользователей. Однако и в случае небольших сетей, предусматривающих внедрение системы управления подпиской и персонифицированных SLA,

Copyright © 2005, Juniper Networks, Inc.

централизованный подход оказывается более выгодным.

Альтернативный подход связанный, с распределением функции идентификацией и терминированием пользовательских сессий на уровне DSLAM, увеличит количество IP-устройств с 50 до нескольких тысяч, соответственно увеличатся расходы на обслуживание, поиск неисправностей, замену программного обеспечения и т.д.

Устойчивость и надежность решения на уровне доступа, прежде всего, будет зависеть от простоты самих DSLAM-ов. Практика показывает, что добавление экстрафункций на уровне доступа ведет к возникновению дополнительных проблем (зачастую проявляющихся самым неожиданным образом и в самые неожиданные моменты). Выявление одного такого случая повлечет замену программного обеспечения на тысяче устройств. Так же необходимость внедрения в перспективе новых функций (например, поддержка IPv6) приведет к аналогичной ситуации.

В рамках продвигаемого подхода Juniper предлагает ограничиться на уровне DSLAM-ов минимальным набором функций:

- IP DHCP Relay;
- IGMP Snooping, IGMP proxy;
- репликация трафика Multicast;
- поддержка стекирования меток VLAN.

Весь функционал, связанный с управлением IP QoS, правилами маршрутизации, контролем доступности сетевых ресурсов (Connection Admission Control), выделением IP-адресов выносится на BSR, таким образом, что BSR выступает в роли единой точки предоставления услуг.

Copyright © 2006, Juniper Networks, Inc.

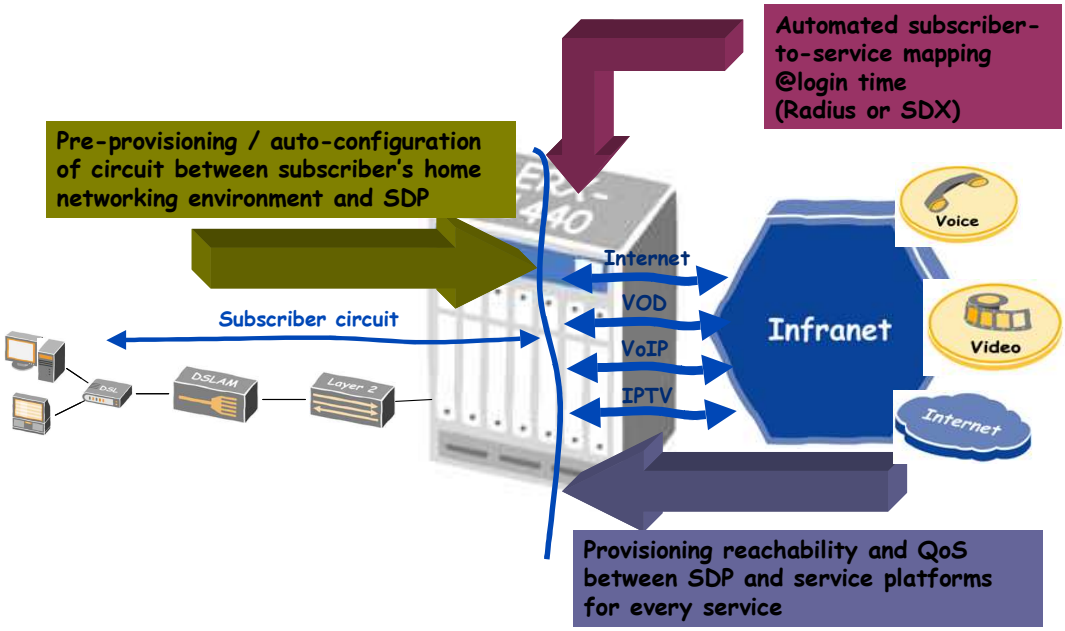


Рис. 5 BSR в роли единой точки предоставления услуг

Ключевое преимущество централизованного подхода, который предлагает Juniper, заключается в возможности организации авто-конфигурирования и механизма само-подписки пользователя на новые сервисы, что сводит практически к нулю манипуляции, которые должен выполнить администратор сети для подключения нового пользователя. Централизованная система управления пользователями и услугами (RADIUS или SDX-300) упрощает процесс управления сетевыми ресурсами, сбором статистики и предоставляет открытые интерфейсы в сторону уже существующих у оператора систем поддержки бизнес процессов/билинговой системой.

Вопросы управления адресным пространством

В случае централизованного подхода BSR отвечает за динамическое распределение IP-адресов для пользователей подключенных сразу группе DSLAM-ов. В случае если за распределение адресов отвечает каждый DSLAM в отдельности, то разделение адресного пространства на дополнительные пулы приводит к их не оптимальному расходованию и необходимости настройки динамических протоколов маршрутизации – OSPF или BGP – между множеством DSLAM-ов. Появление подобного IP-сегмента на уровне доступа может добавить масштабируемости и управляемости сети в целом.

Copyright © 2005, Juniper Networks, Inc.

Сетевая инфраструктура, предполагающая меньшее количество IP-адресов м меньшее количество устройств требующих установки, обслуживания и управления, позволит сократить оператору как операционные затраты, так и затраты на капительное строительство. Наиболее эффективным способом управления распределением адресов это сохранение на DSLAM функциональности DHCP-relay, которая позволит им перехватывать широковещательные DHCP-запросы пользовательских устройств и перенаправлять их на BSR.

Вопросы надежности

Традиционный аргумент, который приводится в пользу распределенной модели, заключается в том, что централизованный подход предполагает наличие единой точки отказа для всех подписчиков. Это утверждение базируется на несколько искаженном представлении о централизованной модели, которая включает в себя лишь одни большой BSR, через который проходит весь трафик сети. В реальных сетях, как правило, устанавливается несколько BSR-ов отвечающих за определенный географический регион и дублирующих друг друга. Необходимый уровень надежности в сети доступа может быть достигнут путем использования на DSLAM двух физических подключений в направлении DSR.

Высокий уровень отказоустойчивости просто необходим в устройствах отвечающих за распределение IP-адресов, не только для того чтобы обеспечить бесперебойность передачи данных, но и для того чтобы сохранить целостность системы по отношению к базе данных содержащей перечень выданных адресов в случае сбоя. Данная проблема наиболее ярко проявится в случае распределенной архитектуры, когда за управление адресным пространством отвечает DSLAM.

В свою очередь BSR наделен функцией, которая позволяет поддерживать целостность записей в базе DHCP даже после перезагрузки устройства.

Вопросы безопасности: Защита от подмены адресов

Возможность контроля за соответствием принадлежности сетевых адресов их действительным владельцам позволяет существенно сократить число сетевых атак в сети, как направленных против подписчиков сети, так и на нарушение работоспособности самой сети (DoS). При наличии сети второго уровня между DSLAM и BSR весь трафик с необходимостью проходит через BSR (отсутствие прямого взаимодействия между подписчиками гарантируется за счет разделения трафика разных

Copyright © 2006, Juniper Networks, Inc.

пользователей на уровне VLAN-tag). Механизм контроля значения адреса источника на каждом порту BSR гарантирует подписчиков от использования злоумышленником чужих IP/MAC адресов, а так же возможность быстрой идентификации источника атаки в случае возникновения таковой.

Усовершенствованная модель QoS

Согласно рекомендации TR-0592 функциональность, связанная с идентификацией и подпиской пользователь на сервисы, не должна быть реализована на уровне DSLAM-а, а все сервисы должны доставляться пользователю внутри единого VC (virtual circuit). Рекомендация гласит, что размещение данного функционала, должно быть выполнено ближе к BSR, для того чтобы обеспечить контроль трафика подписчиков в точке, максимально приближенной к источнику предоставления услуги.

С другой стороны, внедрение сложных механизмов QoS на уровне IP и на уровне приложений повлечет за собою модернизацию аппаратной платформы и как следствие сильное удорожанием устройств и это очевидным образом скажется на стоимости проектов, которые могут включать тысячи DSLAM-ов.

Промежуток сети между DSLAM и BSR не имеет ни малейшего «представления» о том, кому из пользователей принадлежит проходящий трафик и единственная возможность, которая существует на данном уровне – это применить механизм QoS в целом ко всему трафику, агрегированному на порту DSLAM. Однако именно на этом промежутке сети происходит жесткая конкуренция между различными типами трафика в направлении от источника к подписчику. Необходимый уровень обслуживания трафика в расчете на каждого абонента может быть достигнут при помощи внедрения механизмов: иерархических/вложенных правил приоритезации и управления очередями; контроля за наличием свободных ресурсов сети под запрашиваемые услуги и динамического QoS для приложений IP TV и VoD.

Рекомендованное Juniper решение для сквозного (end-to-end) контроля параметров качества обслуживания полностью совместимо с рекомендациями dsl-форума TR-059 и проиллюстрировано на следующем рисунке.

[2] TR-059 другое название документа *DSL Evolution – Architecture Requirements for the Support of QoS Enabled IP Services.*

Copyright © 2005, Juniper Networks, Inc.

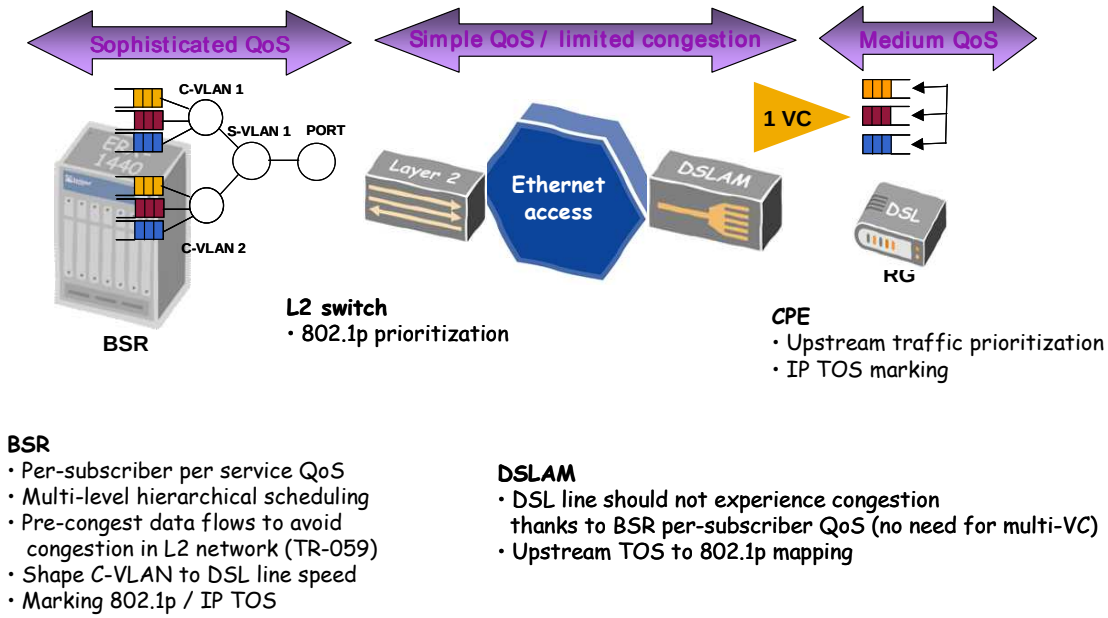


Рис. 6 Сквозной контроль QoS в решении Juniper

Применение вложенных/иерархических правил QoS на BSR для каждого отдельного подписчика гарантирует, что на ниже лежащих каналах (между DSLAM и BSR, а так же DSLAM - CPE) не возникнет переполнений по трафику в направление к пользователю.

Независимость от технологии доступа и производителя

Важной характеристикой, продвигаемого решения с единой сервисной границей и точкой доступа, является независимость от технологии используемой на уровне доступа. Централизованное решение по управлению подпиской столь же эффективно работает для сетей доступа Metro Ethernet, Passive Optical Networks (PON), HFC/Cable или WiFi/WiMax, как и для DSL.

Кроме свободы в выборе технологии доступа оператор получает некоторую независимость в выборе производителя оборудования для уровня доступа, т.к. основные требования (с точки зрения сетевой архитектуры и управления подпиской) минимизированы и сводятся к трем упомянутым выше:

- IP DHCP Relay,

Copyright © 2006, Juniper Networks, Inc.

- IGMP Snooping, IGMP proxy,
- репликация трафика Multicast.

МОДЕЛИ ПРЕДОСТАВЛЕНИЯ УСЛУГ: C-VLAN против S-VLAN

Как организовать доставку услуг абоненту на уровне доступа (промежуток сети CPE-DSLAM-BRAS) и последней мили, консолидировать ли весь трафик в рамках одного VLAN/VC или использовать модель, в которой для каждого сервиса будет выделен свой собственный L2 домен (VLAN/VC)? - вопрос который постоянно возникает в любом проекте построения широкополосной сети доступа.

Первый способ принято называть модель доступа C-VLAN (Customer VLAN), который предусматривает выделение единственного C-VLAN-а для всех сервисов, на которые подписан абонент. Второй подход соответственно носит название S-VLAN (Service VLAN), где для каждого абонента предусматривается выделения множества VLAN-ов - одного под каждую услугу. В последнем случае предполагается так же организация множества VC между DSLAM и CPE.

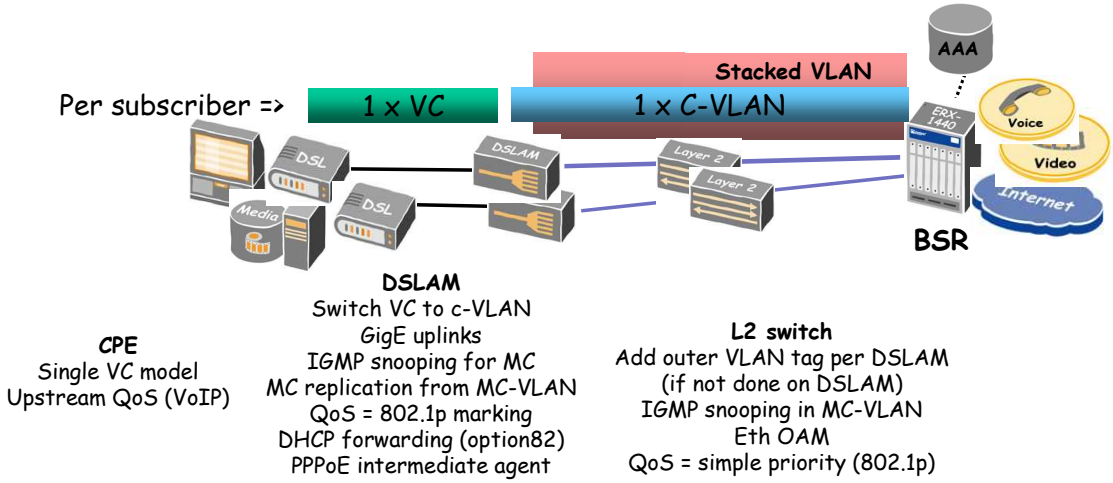


Рис. 7 Пример реализации модели C-VLAN

Обсуждению данного вопроса посвящен большой раздел в рамках dsl-

Copyright © 2005, Juniper Networks, Inc.

форума, последние редакции[3] которого, по совокупности различных факторов констатировали преимущество C-VLAN-модели. Сравнение проводилось по степени эффективности и сложности управления полосою пропускания и сетью в целом, процесса подписки на сервисы и по величине операционных расходов.

На следующем рисунке схематично проиллюстрированы отличия в двух подходах на уровне сервисной границы. Использование S-VLAN модели в принципе предполагает построение нескольких точек доступа к услугам, при этом C-VLAN модель выгодно отличается в части размера капитальных затрат и операционных расходов на поддержаний инфраструктуры.

Кроме того, C-VLAN модель по очевидным причинам лучше отвечает веяниям рынка терминальных устройств, когда будет появляться больше мультисервисных пользовательских терминалов. Типичной ситуацией будет являться использование ПК в качестве и IP/Video-телефона, и проигрывателя различного мультимедиа контента, и т.д.

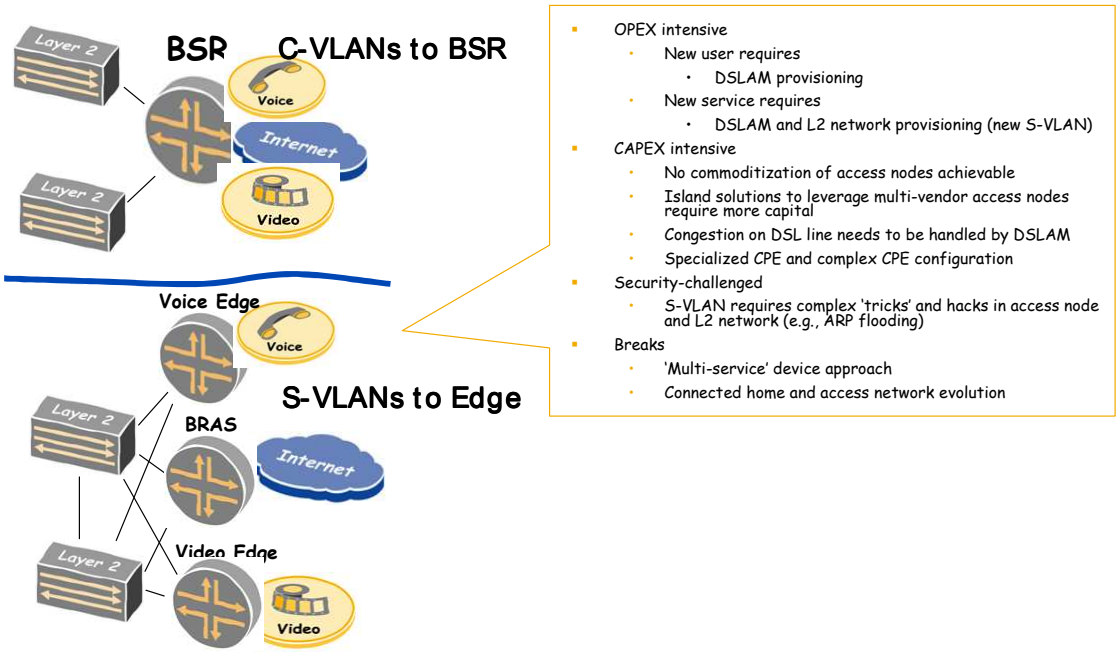


Рис. 8 C-VLAN против S-VLAN на сервисной границе

Эксплуатационные преимущества

[3] См. WT-101: *Migration to Ethernet Based DSL Aggregation* at www.dslforum.org.

Copyright © 2006, Juniper Networks, Inc.

Выбор модели C-VLAN позволит существенно упростить процесс провиженинга (настройки/авто-настройки сетевых параметров) при подключении новых пользователей, при подписке пользователей на услуги и организации на сети новых услуг. Данные утверждения связаны, прежде всего, с тем, что развертывание новых сервисов (на конкретном сегменте сети, который отвечает за определенную географическую зону) не требует установки новых маршрутизаторов, точкой доступа к новым сервисам будет по-прежнему являться центральный BSR. Использование лишь одного мультисервисного C-VLAN-а позволяет исключить DSLAM из процесса провиженинга, сконфигурировав все необходимые параметры на DSLAM (включая номера соответствующих C-VLAN-ов) в процессе их установки.

В конечном итоге в модели C-VLAN более просто могут быть выстроены процессы отладки неисправностей, отслеживания трафика конкретного пользователя и организация сервисов предусмотренных COPM.

Преемственность старой модели предоставления услуг

Не редкой сегодня является ситуация, когда оператор уже имеет в своем распоряжении широкополосную инфраструктуру для предоставления высокоскоростного доступа в Интернет (HSI),

Продвигаемое решение, нацеленное на предоставление услуг 3-Play, построенное с использованием консолидированной сервисной модели позволит оператору связи сохранить существующую модель предоставления сервиса и обеспечит постепенную миграцию пользователей (использующих PPPoE или DHCP) на новую инфраструктуру максимально удобным образом.

Напротив, в случае распределенной модели или модели использующей отдельные VLAN/VC для отдельного сервиса, процесс миграции представляется крайне сложным и потребует большой работы по перенастройке DSLAM-ов на протяжении всего времени миграции пользователей и включения их в систему провиженинга.

Гибкость по отношению к методу аутентификации

На BSR должны поддерживаться различные методы аутентификации и конфигурирования сетевых настроек для каждого типа устройства. При необходимости DHCP-запрос может бать перенаправлен к внешнему серверу, отвечающему за авторизацию и контроль доступа. В тоже время PPP сессия может быть локально терминирована или, например, перенаправлена в сторону BRAS субоператора. В случае локальной

Copyright © 2005, Juniper Networks, Inc.

терминации BSR посылает запрос на RADIUS или SDX сервер, последний может выступать в роли своеобразного сервера, переправляя запросы на старый радиус сервер, обеспечивая, таким образом, поддержку старой базы пользователей на новой инфраструктуре.

Планирование персонифицированного SLA при помощи ИЕРАРХИЧЕСКОГО QoS

Одно из центральных требований – это наличие иерархического механизма QoS, который оказывает существенно влияния на степень эффективности предоставления сервисов и распределение сетевых ресурсов. Иерархически записанные правила позволяют выстраивать конструкции, с помощью которых можно независимо приоритезировать потоки данных от разных приложений на уровне пользователя и в тоже время потоки данных, генерируемые разными типами подписчиков (домашние, корпоративные или премиум класса).

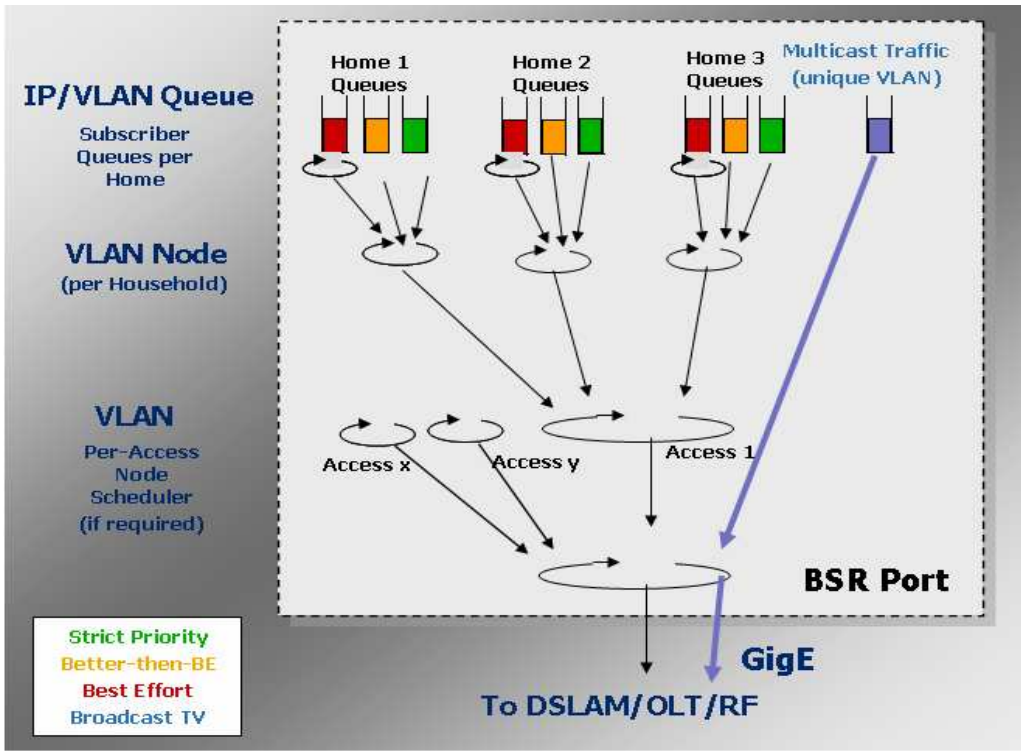


Рис. 9 Построение иерархических правил управления очередями на BSR

Это становится возможным благодаря присвоению так называемого веса для каждого типа трафика внутри отдельной пользовательской сессии и вместе с тем присвоению еще одного приоритета/веса в зависимости от типа

Copyright © 2006, Juniper Networks, Inc.

пользователя на физическом порту. Для трафика чувствительного к задержкам может быть определена очередь с безусловным приоритетом, попав в эту очередь, трафик сразу направляется на физический порт, минуя всю иерархическую последовательность правил, что позволяет гарантированно поддерживать уровень сервиса (свой для каждого типа приложений), который предусмотрен контрактом (SLA).

Возвращаясь к вопросу о выборе модели доставки трафика – C-VLAN/S-VLAN, необходимо отметить, что проблема приоритезации трафика одинаково остро стоит в обеих моделях. Выбрав подход, в котором отдельный VC/VLAN выделяется для отдельного сервиса (S-VLAN), мы сталкиваемся с необходимостью приоритезировать трафик между множеством VC/VLAN, при этом число приоритетов/весов, с которым придется оперировать на уровне порта, в разы превысит аналогичный параметр в случае C-VLAN. Действительно, если мы определим не сети 5 различных сервисов (каждый «живет» в отдельном VC) для 5 различных типов подписчиков, то каждому VC/VLAN, терминированному на BSR, необходимо будет на уровне порта присвоить одно из 25-ти значений приоритета. Каждое значение приоритета будет соответствовать отдельной комбинации типов пользователя и трафика, что отвечает «плоской» модели QoS.

Суммируя все выше сказанное - для того чтобы предоставлять множество сервисов BSR на аппаратном уровне (в направлении к абоненту!!!) должен поддерживать механизмы QoS и обладать следующими возможностями:

- Приоритезация IP трафика в рамках отдельной DHCP/PPPoE сессии.
- Приоритезация множества DHCP/PPPoE сессий друг относительно друга в рамках одного виртуального канала/домена (VC/VLAN) второго уровня
- Приоритезация трафика, принадлежащего разным VLAN/VC, в рамках одного физического порта.

Вопросы Масштабирования

Существуют определенные ограничения в классическом подходе построения L2 Ethernet сетей (802.3), которые связаны с тем, что один L2 сегмент не может поддерживать более 4000 VLAN-ов. Учитывая необходимость выделения одного (в случае C-VLAN) или нескольких (S-VLAN) каждому подписчику значение 4000 VLAN-ов может легко исчерпано. На помощь приходит технология, так называемого, стекирования тегов/меток VLAN-ов, в некотором смысле аналогичная

Copyright © 2005, Juniper Networks, Inc.

подходу, который применен в ATM, где для формирования виртуального канала используется пара индексов VP/VC. В случае Ethernet-кадра в его заголовок могут быть записаны два тэга – внешний и внутренний.

При таком подходе L2 домен (ниже BSR) может быть разбит на несколько секторов, каждому из которых будет поставлен в соответствие внешний тэг, при этом нижний тэг будет соответствовать номеру C-VLAN. Данная технология практически полностью позволяет решить вопрос масштабирования, увеличив число VLAN с 4000 до 16 000 000 (4000 x 4000).

Общие рекомендации по выбору модели доступа

С технической точки зрения, BSR должен поддерживать все описанные способы доставки услуг подписчику. Не смотря на то, что подход, связанный с организацией единой сервисной границы и единой точки доступа к сервисам, с нашей точки зрения, наиболее перспективен, иногда физически невозможно использовать чисто централизованный подход. Например, так случится, если различные приложения находятся за физически (ATM и Ethernet) различными сетями агрегации или магистрали.

В общем случае смешанной сети – ATM и Ethernet – наиболее эффективным (с точки зрения стоимости), обеспечивающим различные гарантированные уровни качества обслуживания для разных приложений, будет решение, основанное на модели C-VLAN, которая:

- обеспечивает выделение отдельного VLAN-а каждому подписчику;
- поддерживает стекированные VLAN-ы, и обеспечивает выделение отдельной внешней метки для каждого устройства доступа (DSLAM/L2 Ethernet switch);
- для подписчиков ATM сети, обеспечивает работу и доставку всех сервисов по одному VC.

Такое решение действительно может быть реализовано на оборудовании Juniper Networks и уже хорошо зарекомендовало себя, как наиболее эффективное, масштабируемое и управляемое решение для сетей широкополосного доступа.

Copyright © 2006, Juniper Networks, Inc.

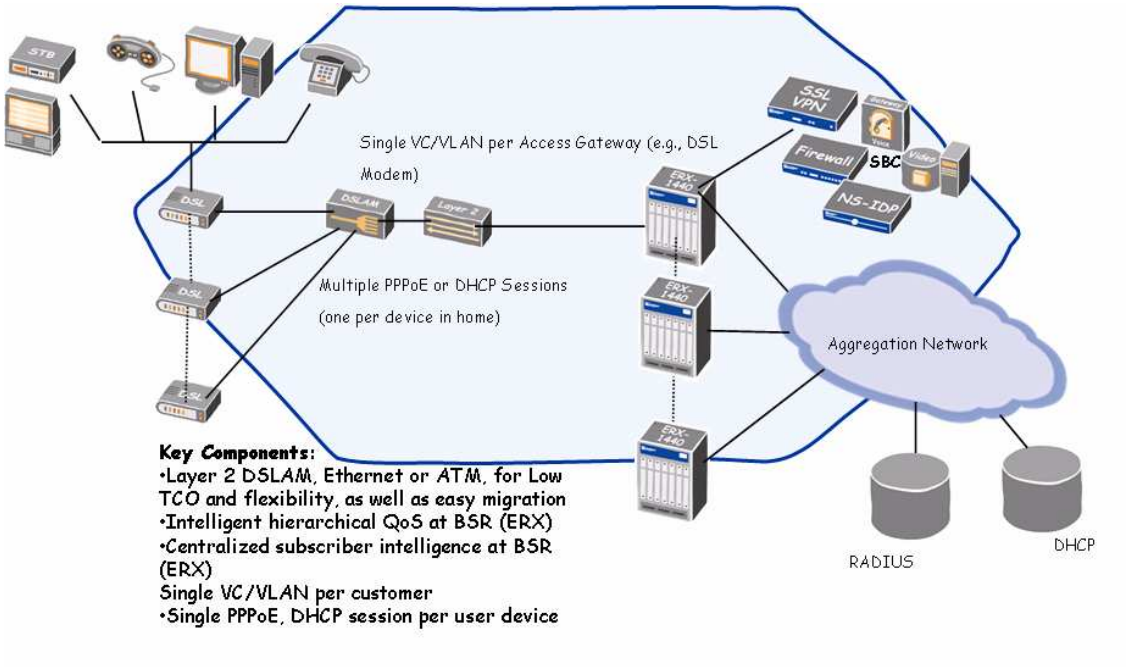


Рис. 10 Рекомендованный вид архитектуры для сети широкополосного доступа

КЛАССИЧЕСКАЯ BSR-МОДЕЛЬ И ДУАЛИСТИЧЕСКИЙ ПОДХОД BSA/BSR

Прежде чем перейти к непосредственному сравнению двух сетевых моделей, попробуем разобраться в основных положения, недостатках и достоинствах каждой модели в отдельности, после чего отличая двух подходов станут очевидны. Итак, как функциональность BRAS обеспечивается централизованной моделью BSR и эмулируется в распределенной архитектуре на основе нескольких устройств BSA/BSR?

Единая BSR-платформа управления правилами обслуживания и IP-маршрутизации

Создание единой платформы для выполнения функций агрегации, IP-маршрутизации, управления правилами обслуживания и подпиской на сервисы для сети широкополосного доступа, означает создание специализированной аппаратной платформы и программного обеспечения для нее. Таковой, например, является платформа E-серии, производимая компанией Juniper (см. Рис. 11).

Copyright © 2005, Juniper Networks, Inc.

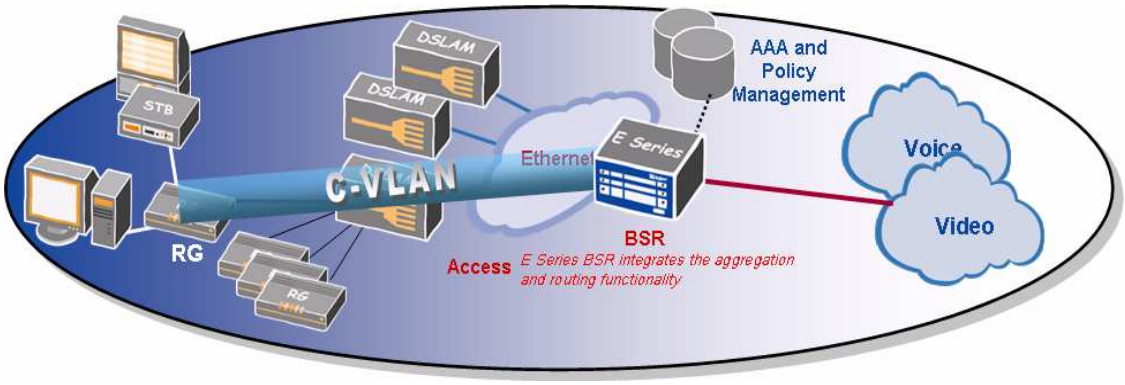


Рис. 11 Пример использования платформы E-серии для центрального BSR.

На Рис. 12 схематично представлены существенные для нашего рассмотрения процессы. Каждый C-VLAN терминируется внутри BSR и «прикрепляется» к уникальному IP-интерфейсу. Для каждого такого IP-интерфейса поддерживаются средства защиты от несанкционированной подмены IP-адреса (IP-spoofing) подписчика, как для DHCP, так и для PPPoE сессий. IP-маршрут в сторону конечного CPE устройства помещается в таблицу маршрутизации только после прохождения процедуры идентификации и авторизации (AAA).

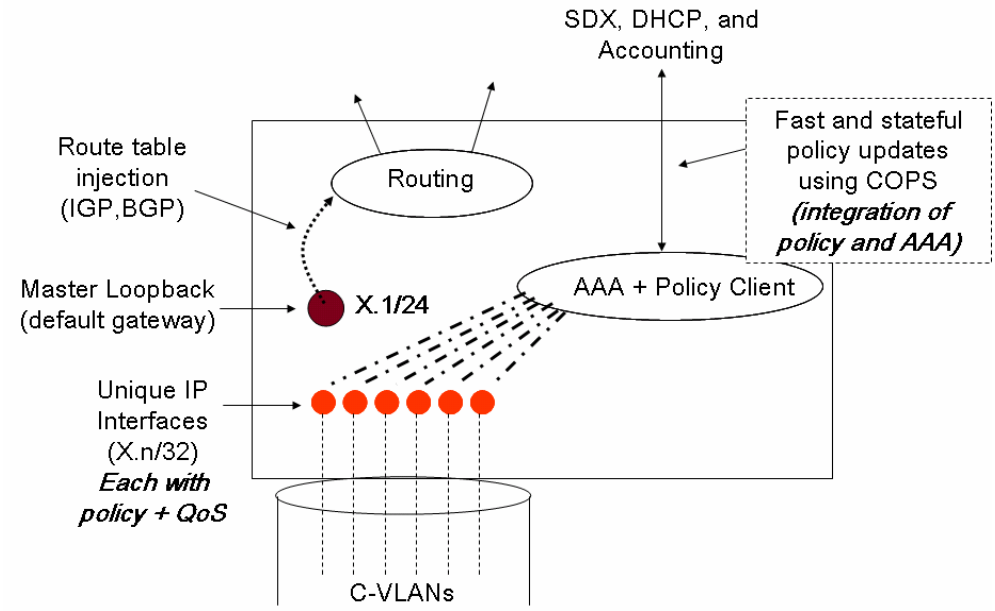


Рис. 12 Процессы маршрутизации и QoS в модели BSR

Copyright © 2006, Juniper Networks, Inc.

Адреса IP-интерфейсам присваиваются из единого пула адресов, который соответствует внутреннему логическому unnumbered-интерфейсу. Маршрут для соответствующей IP-подсети помещается в таблицу маршрутизации и распространяется в сети в соответствии с базовыми принципами IP-маршрутизации посредством маршрутизирующего IGP протокола.

Так как BSR является точкой наложения всех политик и правил обслуживания то для эффективного управления ими BSR должен иметь не только интерфейс в сторону системы управления сетевыми элементами и AAA, но иметь открытый интерфейс для взаимодействия с сервером управления подписчиками и услугами (активации сервисов). В случае маршрутизаторов E-серии в качестве такого интерфейса применен открытый стандарт Common Open Policy Service (COPS). Это позволяет BSR взаимодействовать с сервером управление подписчиками и услугами (SDX), управляя правилами QoS, списками доступа и т.д. в режиме реального времени, что крайне важно для новых приложений, таких как IP TV, VoD. По мере необходимости SDX формирует новые правила и отправляет их на BSR. Маршрутизатор в свою очередь формирует в ответ подтверждение о том, что правила применены, обеспечивая тем самым целостность базы текущих сервисов и статистических/биллинговых данных. Использование простых SNMP запросов на обновление конфигурационных файлов не годится именно из-за невозможности установить обратную связь с системой активации услуг.

Система управления пользователями и услугами является ключевым элементом для эффективного управления процессом предоставления услуг и в общем случае содержит информацию о login-ID, IP-адресе, перечень услуг, на которые подписан абонент, их текущий статус, описание уровня сервиса и т.д. и является промежуточным элементом между сетью и системой BSS/Биллинга.

Эмуляция BSR: Распределенная модель BSA/BSR

Классические IP маршрутизаторы и коммутаторы не приспособлены для идентификации пользователей и управления подпиской на сервисы в широкополосной сети. Основным недостатком является отсутствие способности быстро подстраивать таблицу IP-маршрутизации в условиях динамически меняющегося огромного (десятки и сотни тысяч) количества IP-хостов. Вместе с тем, процессоры, отвечающие за работу с политиками и правилами обслуживания, так же не рассчитаны на частые динамические изменение, характерные для современной широкополосной сети, и больше подходят для работы под управлением традиционной EMS. Эти сложности заставляют некоторых производителей прибегнуть к распределенной модели, которая позволяет использовать традиционные IP-платформы в

Copyright © 2005, Juniper Networks, Inc.

решениях для широкополосных сетей.

По существу, распределенная модель пытается эмулировать централизованную BSR-модель (см. Рис. 13) и необходима лишь для того, чтобы вынести часть функциональности (идентификацию подписчиков и точку оказания сервиса) с центрального BSR на некоторое число распределенных элементов – Broadband Service Agrigators (BSA).

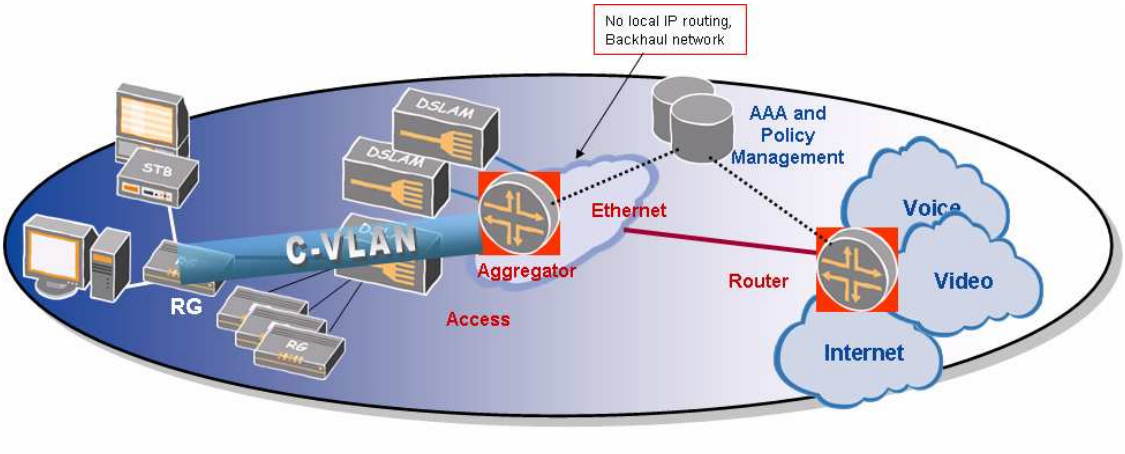


Рис. 13 Распределенная архитектура BSA/BSR

BSA – по сути своей является мультисервисным L3 Ethernet коммутатором операторского класса. BSA отвечает за наложения персональных правил обслуживания трафика (QoS) для каждого подписчика, терминацию абонентского C-VLAN-а и дальнейшую коммутацию трафика в направлении BSR. При этом вся коммутация происходит на втором уровне. BSR обеспечивает необходимую IP-маршрутизацию и приоритезацию трафика на основе его принадлежности к какому-либо из приложений, и безотносительно принадлежности к подписчику. Таким образом, это приводит к распределению зоны управления услугами на множестве устройств, что в общем случае сказывается на увеличении операционных затрат на обслуживание сети.

Copyright © 2006, Juniper Networks, Inc.

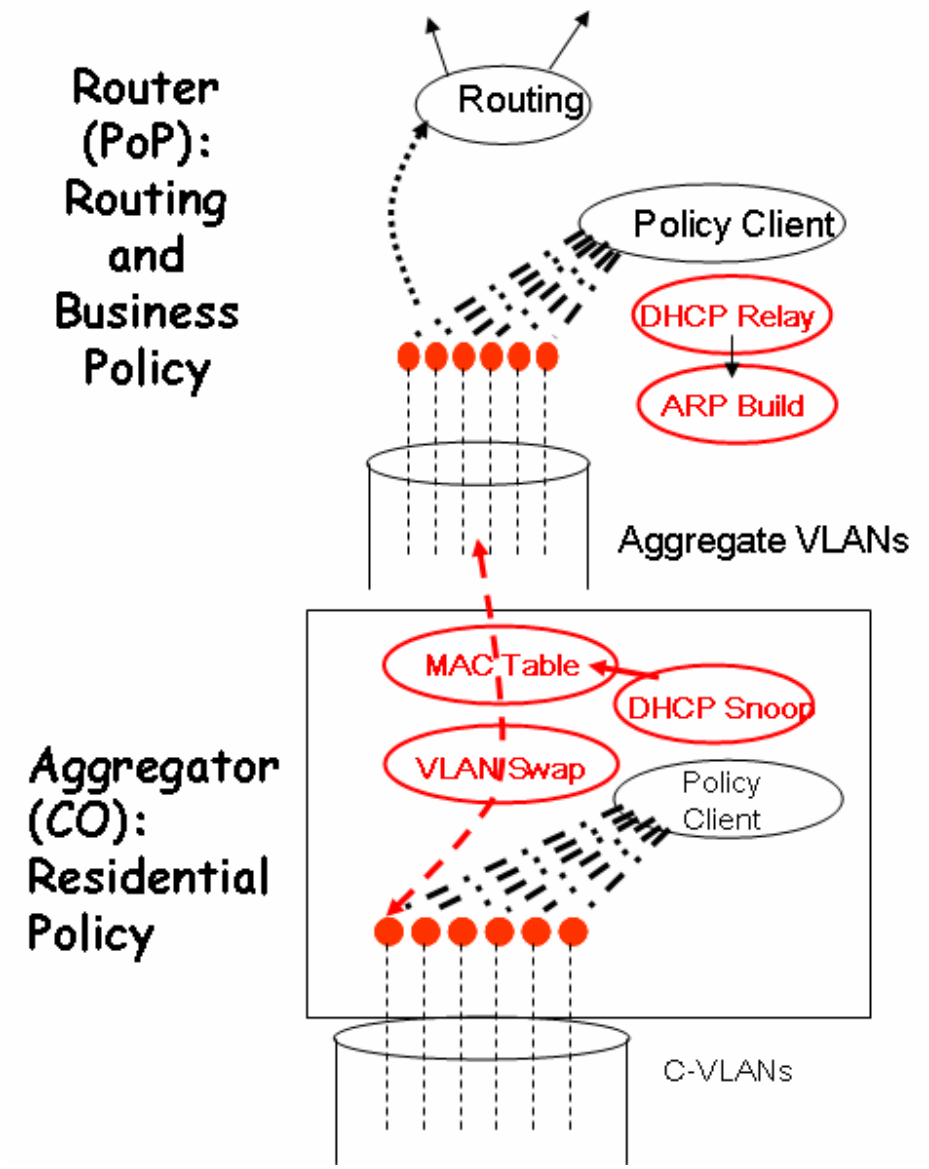


Рис. 14 Процессы маршрутизации и QoS в модели BSR/BSA

Данный подход связан с рядом дополнительных недостатков. Разделение функций маршрутизации (L3) и управления QoS (L2), приводит к необходимости поддерживать согласованным образом информацию о состоянии конкретного подписчика сразу на нескольких устройствах BSA и BSR.

Как правило, BSA осуществляет коммутацию на основе информации об arp-запросах и известных MAC-адресах, соответствующие таблицы пополняются на основе данных, которые BSA извлекает из DHCP запросов подписчиков. (Такой механизм предусмотрен в частности для того, чтобы

Copyright © 2005, Juniper Networks, Inc.

обезопасить сеть и подписчиков от сетевых атак, связанных с подменой IP/MAC адресов и несанкционированного доступа). Очень важно, чтобы эта информация оставалась согласованной между BSA/BSR даже в случае выхода из строя основного и переключения на резервный BSR.

Следующее неудобство связано с тем, что коммутация на основе IP может быть выполнена лишь на BSR, а вся статистическая информация об использовании того или иного сервиса подписчиками собирается на BSA. Представим себе ситуацию (типовую для любой современной широкополосной сети), когда за BSR находится несколько ресурсов или приложений, которые, по сути, являются различными сервисами, доступ к которым разделен и относится к разным тарифным планам. Самый простой пример это выход в Интернет через разных ISP. В таком случае BSA должен идентифицировать трафик, относящийся к данному IP-сервису поместить его в нужную L2 подсеть и сделать об этом соответствующую запись. Однако, единственным идентификатором на основе, которого можно дифференцировать один сервис от другого является IP-адрес сервисного ресурса, поэтому BSA в принципе не сможет этого сделать. Данная проблема связана именно с архитектурой распределенной модели BSA/BSR и накладывает серьезное ограничение на применимость подобных решений.

В заключение раздела отметим, что данная модель, по-видимому, будет развиваться и дальше, ярким сторонником распределенной архитектуры является компания Алкатель. Однако на данный момент решение не отработано в достаточной степени и имеет множество подводных камней, некоторые из которых мы описали выше:

- распределение функций BSR на множестве устройств потенциально ведет к более затратному и сложному процессу эксплуатации;
- отделение управления подпиской на сервисы и политиками QoS на втором уровне от IP-маршрутизации приводит к необходимости следить за целостностью L2/L3 состояний подписчиков сразу не нескольких устройствах;
- отделение управления подпиской на сервисы и политиками QoS на втором уровне от IP-маршрутизации приводит к невозможности, в общем случае, дифференцировать услуги на основе IP-адресов соответствующих сетевых ресурсов;
- модель обусловлена необходимостью конфигурировать на сети достаточно сложный набор дополнительных функций: extensive packet snooping, proxies, policy forwarding, vpls и т.д., которые необходимы для того, чтобы преодолеть отсутствие в модели централизованного IP-BSR.

Copyright © 2006, Juniper Networks, Inc.

ТРЕБОВАНИЯ К СОВРЕМЕННЫМ СЕТЯМ ШИРОКОПОЛОСНОГО ДОСТУПА

Выше приведенные аргументы заставляют по иному посмотреть на проблемы построения и принципы организации современных сетей широкополосной связи. Здесь мы сделаем некоторые предположения и определим несколько типовых ситуаций характерных для проектов построения сетей доступа операторов связи, предоставляющих услуги сети широкополосного доступа на территории РФ. Мы сформулируем основные требования, которым должны удовлетворять сети доступа в условиях складывающейся конъюнктуры рынка услуг фиксированной связи в секторе частных и корпоративных пользователей и покажем в последующих главах, как можно удовлетворить этим требованиям на примере решений продвигаемых компанией Juniper и ее партнерами на территории Российской Федерации.

Исходные данные. Предположения

При подготовке типовых решений мы будем исходить из следующих предположений:

	Тип 1	Тип 2	Тип 3
Население города	4 млн.	1млн	0.5 млн.
Число телефонных линий	1.6 млн.	300 тыс.	150 тыс.
Проникновение услуги высокоскоростного доступа в Интернет (HIS)	15%	15%	15%
Проникновение услуги IP TV	2%	2%	1%
Проникновение услуги VoD	0.2%	0.2%	-

Сеть так же предназначена для предоставления голосовых услуг связи посредством голосовых терминалов (IP/SIP-телефонов), которые находятся под управлением программного коммутатора (Softswitch) оператора связи. Сеть должна гарантировать необходимый уровень параметров QoS для голосового трафика, однако суммарное количество трафика, генерируемое данным типом приложения от «широкополосных» пользователей, незначительно по сравнению с трафиком Интернет, IP TV и VoD.

Сеть предназначена для предоставления доступа к услугам следующих категорий пользователей:

Домашние пользователи

Copyright © 2005, Juniper Networks, Inc.

Корпоративные клиенты (малый и средний бизнес)

Крупные корпоративные клиенты

Общие требования к архитектуре сети

Среди традиционных требований, предъявляемых к сетям операторского класса: масштабируемость, управляемость, доступность, надежность и отказоустойчивость, безопасность и т.д. отметим лишь наиболее специфичные для рассматриваемого класса сетей.

Архитектура сети доступа должна быть основана на модели централизованного BSR с единой точкой доступа к услугам и единой сервисной границей и должна быть рассчитана на предоставление IP-сервисов (!!!) конечным подписчикам (не включая крупных корпоративных заказчиков).

На сети должна быть реализована модель C-VLAN в качестве основного способа доставки сервисов абоненту сети.

Архитектура сети должна при необходимости сколь угодно долго поддерживать модель доступа с S-VLAN.

На уровне архитектуры сети должны быть предусмотрены механизмы защиты от подмены адресов с целью предотвращения неавторизованного доступа к услугам.

На уровне архитектуры должен быть реализован принцип независимости от технологии, используемой на уровне доступа.

На уровне архитектуры должен быть реализован принцип преемственности старых услуг на новой архитектуре, а так же важнейших аспектов ATM-DSL архитектуры в Ethernet-DSL подходе:

- Изоляция трафика различных пользователей на уровне доступа и на границе с сети агрегации, что является необходимым условием для обеспечения необходимого уровня безопасности, управляемости сети и облегчения процесса локализации сбоев.
- Возможность массовой преднастройки портов DSLAM-ов.
- Иерархическая структура организации виртуальных подключений в ATM (Virtual Path/Virtual Circuit (VP/VC)), позволяющая эффективно управлять полосою пропускания и параметрами QoS на участке CPE-BRAS.

При этом необходимо сохранить традиционные преимущества привносимые Ethernet.

Copyright © 2006, Juniper Networks, Inc.

- Лучшее в индустрии отношение цена/bit-rate.
- Гибкость в разделении трафика на основе VLAN-ов и классификация трафика на основе 802.1p-меток.

В сети должна быть предусмотрена централизованная система распределения адресного пространства среди подписчиков сети и сетевого провиженинга, рассчитанного на массовое предоставление услуг сети широкополосного доступа.

Архитектура сети должна соответствовать основным рекомендациям DSL-форума: TR-059 и WT-101.

Требования к BSR в централизованной модели доступа

Как уже отмечалось основной задачей, которую призван решить BSR – это организация на сети централизованной идентификации пользователя и единой точки доступа к сервисам.

Должны поддерживаться следующие типы сервисов: передача данных (доступ в Интернет), голоса, данных по верх IP-сети, организация различных типов защищенных сетей (на основе протоколов MPLS, SSL и IPsec), предоставление услуг системы детектирование сетевых атак и брандмауэра для домашних пользователей.

На BSR должен поддерживаться полный набор функциональности IP/MPLS по отношению к организуемым типам сервисов для их трансляции через IP/MPLS магистраль:

- организация виртуального соединения на втором уровне модели OSI (VLL);
- организация виртуальной частной сети (Virtual Private LAN Service (VPLS)) на втором уровне модели OSI;
- организация закрытых виртуальных частных сетей третьего уровня - является на сегодня основным механизмом для предоставления одной из наиболее востребованных услуг по организации виртуальных частных сетей (ВЧС/L3 VPN) для корпоративных заказчиков и используется для изоляции на третьем уровне сервисов приложений принадлежащим различным провайдерам (ASP).

По отношению к идентификации подписчиков и управления доступом BSR должен обладать следующим набором функций:

- поддержка протоколов для идентификации подписчиков – RADIUS

Copyright © 2005, Juniper Networks, Inc.

протокола для взаимодействия с AAA-северами (в случае PPPoE) и DHCP-протокола;

- управление процессом делегирования IP-адресов с поддержкой семейств протоколов IPv4 и IPv6;
- возможность настройки параметров QoS, сетевой безопасности, персонально для каждого подписчика (VLAN-а) и потока данных;
- поддержка механизмов авто-конфигурирования для совместного использования с внешней системой управления пользователя, услугами и самоподписки на услуги.
- поддержка протоколов IP over PPPoE и IP over Ethernet для организации доступа домашних пользователей;
- поддержка ряда дополнительных протоколов сбора статистики для L2 и L3 VPN-ов, и протоколов туннелирования (L2TP) для организации взаимодействия и предоставления услуг суб-провайдерам.
- Развитые механизмы работы с метками (тегами) VLAN-ов, поддержка вложенных меток (VLAN-stacking).

В соответствии с рекомендацией dsl-форума BSR, являясь центральной системой контроля и распределения ресурсов сети между подписчиками и потоками данных, должен поддерживать механизм иерархического QoS в направлениях, как к подписчику, так и в сторону магистрали.

На BSR должна быть реализована поддержка COPM за счет механизма зеркалирования трафика на основе идентификатора подписчика или линии доступа.

На BSR должны поддерживаться основные механизмы обеспечения сетевой безопасности: списки доступа, средства предотвращения атак DoS-типа, многоуровневые фильтры.

Уровень надежности BSR должен соответствовать высочайшему уровню доступности услуг (голос, TV), к которому привык конечный пользователь. Отказоустойчивость BSR должна быть обеспечена за счет разнесения функций управления и коммутации трафика на разных аппаратных элементах, а также за счет резервирования каждого управляющего элемента, контроллера ввода вывода, матрицы коммутации. При этом должен поддерживаться режим «горячей» замены и автоматического переключения между основным и резервным модулем без потери пользовательских сессий и с сохранением целостности информации о них.

Для поддержки сессий реального времени и мобильности некоторых

Copyright © 2006, Juniper Networks, Inc.

современных мультимедиа терминалов (предусмотренных для приложений VoIP, IMS, VoD), BSR должен обладать определенным интеллектом на уровне приложений, чтобы правильно идентифицировать сессии пользователей и применить к ним соответствующие правила обслуживания с точки зрения QoS, безопасности, сбора статистической информации. В частности BSR должен уметь разбирать сообщения SIP (Session Initiation Protocol) и RSTP (Real Time Session Protocol).

Требования к уровню сети доступа

DSLAMs

Устройства доступа по должны обладать следующими свойствами:

- IP DHCP Relay;
- IGMP Snooping, IGMP proxy;
- репликация трафика Multicast;
- поддержка стекирования меток VLAN.

Весь функционал, связанный с управлением IP QoS, правилами маршрутизации, контролем доступности сетевых ресурсов (Connection Admission Control), выделением IP-адресов выносится на BSR, таким образом, что BSR выступает в роли единой точки предоставления услуг.

L2/L1 Backhauling

Основные требования к данному уровню сводятся к агрегации Ethernet трафика и его высоконадежной доставки от устройств доступа (DSLAM) к BSR. Решением должны быть обеспечиваться уровень доступности не менее 0,99999 и защита от сбоя каналов и устройств на уровне не 50mc.

Требования к уровню CPE.

Основные свойства CPE-устройств обусловлены выбором модели доступа с централизованной единой точкой доступа и предоставления универсального C-VLAN каждому пользователю для всех сервисов, на которые он подписан.

CPE-должно поддерживать протоколы PPPoE или DHCP для установления сессии на втором уровне, автоматической настройки сетевых параметров и аутентификации/авторизации CPE в сети.

CPE-устройство должно поддерживать функцию маршрутизации (L3

Copyright © 2005, Juniper Networks, Inc.

CPE), протоколы трансляции адресов (NAT/PAT), DHCP Relay/Proxy. Таким образом, с точки зрения сети доступа/агрегации CPE является единым мультисервисным L3-устройством, так что реальное количество терминальных устройств домашней сети скрыто от оператора. Данный факт позволяет оператору связи упростить процесс эксплуатации сети и снизить операционные издержки. Дополнительным преимуществом, которое имеет такой подход, является предотвращение попадания в сеть доступа трафика обмена данных между устройствами домашней сети.

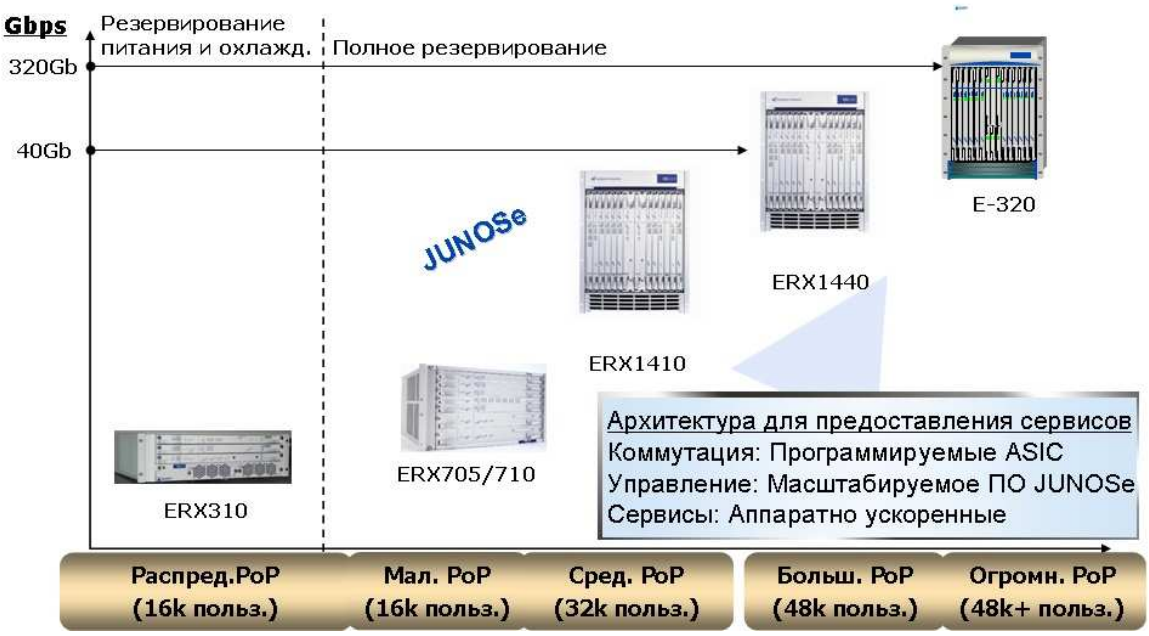
CPE-устройство должно поддерживать механизмы QoS-приоритезации трафика и управления очередями в направлении сети по отношению к трафику приложений реального (голосовой, видео телефонии).

Copyright © 2006, Juniper Networks, Inc.

BSR НА БАЗЕ МАРШРУТИЗАТОРОВ JUNIPER E-СЕРИИ

Juniper Networks имеет на сегодня наиболее полную линейку оборудований для построения сети широкополосного доступа на основе модели с консолидированным центром доступа к услугам, основным элементом, которой является BSR – Broadband Service Router.

Рис. 15 Линейка маршрутизаторов Juniper с функциональность BSR.



Соответствующая линейка оборудования представлена маршрутизаторами E-серии: наиболее мощным устройством является маршрутизатор E-320, далее в порядке уменьшение производительности следуют ERX-1440, ERX-1410, ERX705/710 и компактная модель ERX-310. Маршрутизаторы E-серии использовались в качестве центрального элемента для разных целей в широкополосных сетях многих ведущих операторов по всему миру.

Чтобы добиться эффективного управления сервисами в широкополосной сети, маршрутизаторы E-серии тесно проинтегрированы с другими продуктами Juniper, такими как IDP, firewall, SSL, SBC. На стороне магистральной сети решение может быть дополнено маршрутизаторами M-серии, что обеспечит наличие идеальной инфраструктуры для доставки

Copyright © 2005, Juniper Networks, Inc.

трафика IP TV через MPLS магистраль.[4]

При помощи устройств E-серии на основе единой платформы обеспечивается маршрутизация трафика групповой (multicast) рассылки, лучший в классе механизм QoS, управление подпиской на услуги, правилами обслуживания и безопасностью.

ОПЫТ ПОСТРОЕНИЕ СЕТЕЙ ДОСТУПА

В настоящее время уже имеется положительный опыт построения сетей широкополосного доступа на территории РФ на основе изложенных подходов с использованием оборудования Juniper.

Все решения основываются на иерархическом принципе где, можно выделить уровень магистрали, уровень агрегации и уровень доступа. Ниже мы приводим типовые схемы построения сетей доступа для городов разного масштаба, исходные данные, для которых были сформулированы в разделе «Исходные данные. Предположения».

Схема построения для каждого из трех городов предполагает полное резервирование на уровне устройств и топологии. Уровень магистрали выполнен на маршрутизаторах M320 или M120 Juniper Networks, которые устанавливаются в два магистральных узла.

Для 4-х миллионного города агрегация выполняется на самых производительных в линейке E-серии маршрутизаторах – E320, которые позволяют терминировать до 50000 одновременных широкополосных сессий (Рис. 16). Они расположены на центральных узлах присутствия и подключены к магистральным маршрутизаторам посредством каналом STM-16. Предусмотрена так же пара выделенных маршрутизаторов M10i, которые предлагается использовать для агрегации соединений сети доступа и предоставления услуг IP/VPN и L2 VPN для не большого количества корпоративных заказчиков. Маршрутизаторы M10i подключаются к каждому магистральному маршрутизатору M320 каналом Gigabit Ethernet.

[4] См. раздел: See *Video Transit on an MPLS Backbone* на www.juniper.net/solutions.

Copyright © 2006, Juniper Networks, Inc.

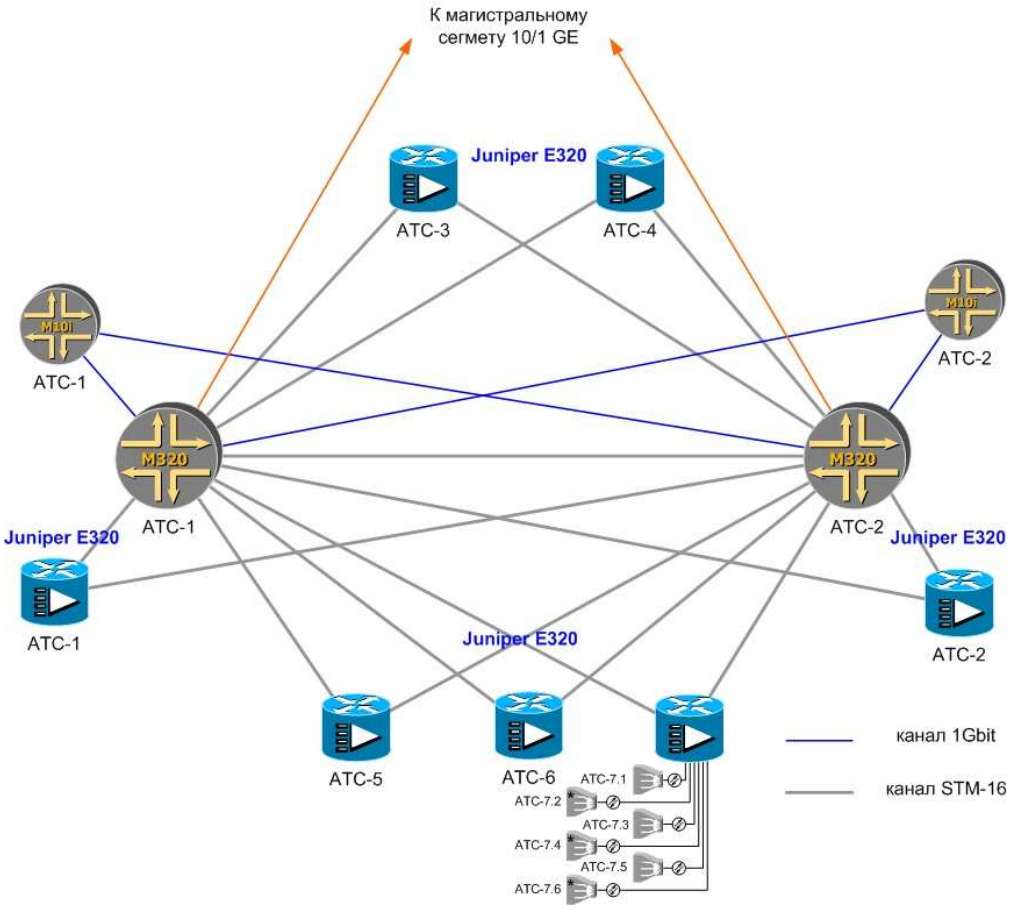


Рис. 16 Пример сети широкополосного города с населением 4 млн.

Для одно и полумиллионного города используются сходные топологии сети, в которых агрегирующие BSR располагаются на паре центральных узлов. В качества BSR используются маршрутизаторы ERX-1440 и ERX-310, предназначенные для массового предоставления услуг доступа в Интернет для абонентов сети.

BSR подключаются к каждому магистральному маршрутизатору каналом Gigabit Ethernet. На роль последних выбраны маршрутизаторы M120 и M40 соответственно.

На уровне доступа для связи ATC/POP используется технология CWDM, позволяющая создать логическую топологию «звезда» на физической топологии каналов «кольцо». Каждая ATC подключается к каждому из центральных узлов каналами Gigabit Ethernet, при этом на каждом из направлений используется два параллельных канала – один для трафика сети NGN/Voice и IP/VPN L2VPN (для агрегации на M-серии маршрутизаторов) и один для трафика 3Play (для агрегации на маршрутизаторах E-серии).

Copyright © 2005, Juniper Networks, Inc.

Между центральными узлами связи используется в общей сложности 10 каналов, 2 из них для связи магистральных узлов M120/M40, две пары других для обеспечения двойного подключения маршрутизаторов M10i и E-серии к устройствам магистрали, и две пары для связи сетей доступа, подключаемых непосредственно к узлам агрегации. Все 10 каналов предлагается передать через канал системы волнового мультиплексирования между центральными узлами, задействовав 5 лямбд.

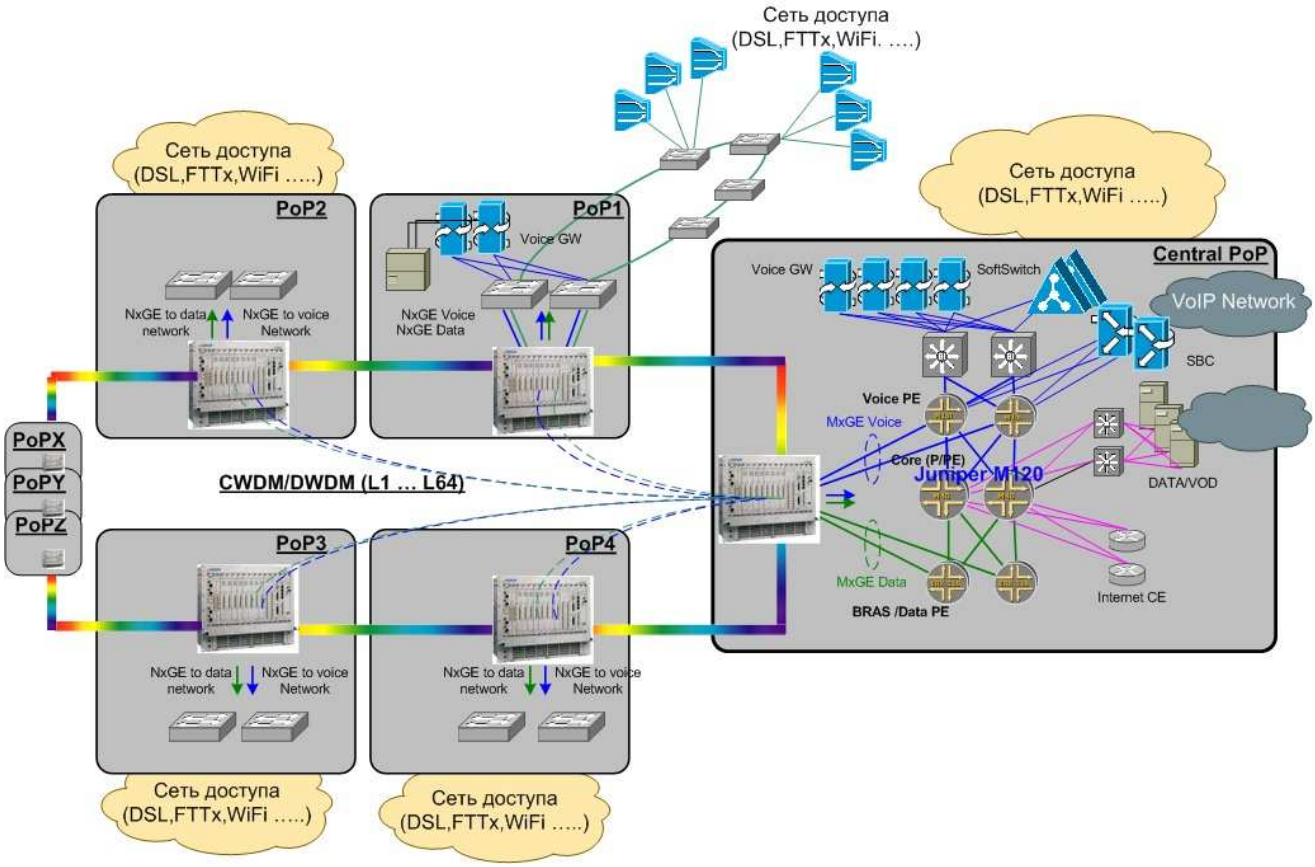


Рис. 17 Пример сети широкополосного города с населением 1 млн.

В качестве CWDM-мультиплексоров используются устройства Adva Optical FSP 2000, способные обеспечить 8 лямбд в одном кольце, передавая при этом по два потока Gigabit Ethernet на каждую лямбду (используются транспондеры с функцией мультиплексирования). В данной конфигурации используются 5 лямбд из 8.

Copyright © 2006, Juniper Networks, Inc.

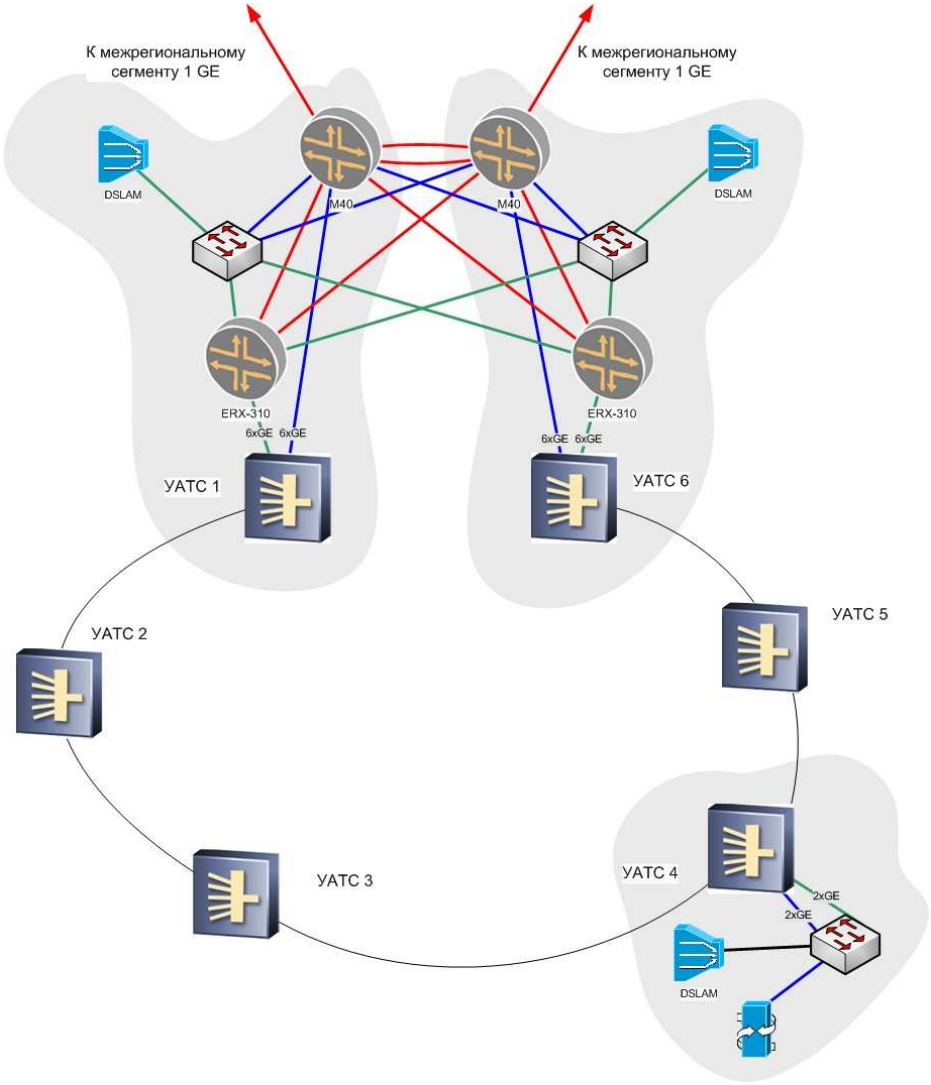


Рис. 18 Пример сети широкополосного города с населением 500 тыс.

ЗАКЛЮЧЕНИЕ

Новые широкополосные сервисы, такие как VoIP и Видео, услуги расширенной сетевой безопасности, VPN-услуги приводят к новым характеристикам и требованиям в сетях доступа. Миграция к новой инфраструктуре всегда связана с определенными технологическими препятствиями и финансовыми рисками. Чтобы снизить эти риски оператору необходимо обратить внимание на то, как уменьшить свои операционные и капитальные затраты и в тоже время получить в свое

Copyright © 2005, Juniper Networks, Inc.

распоряжение масштабируемую защищенную сеть. Простая архитектура, коей является централизованный подход, всегда оказывается более эффективной с точки зрения сохранения инвестиций.

Централизованный контроль подписки на сервисы и использование единой централизованной точки доступа к услугам совместно с моделью C-VLAN позволяет одновременно добиться простоты и эффективности за счет устранения из решения большого числа IP-устройств, которыми бы пришлось управлять в реальном времени в условиях частных изменений характерных для 3-Play сетей.

Платформа E-серии в роли BSR, снабженная механизмом иерархического QoS, дополненная необходимым функционалом на DSLAM-е по отношению к обработке трафика групповой рассылки (multicast), гарантирует эффективное управление полосою пропускания и независимую приоритезацию трафика на уровне пользователей и на уровне сервисов.

ПРИЛОЖЕНИЕ 1: ДОПОЛНИТЕЛЬНЫЕ МАТЕРИАЛЫ

Дополнительные материалы по теме можно найти на сайте компании www.juniper.net:

- *Video Transit on an MPLS Backbone:*
- *Network Based VPN/Firewall Services:*
- http://www.dslforum.org/:
  - TR-058: Multi-Service Architecture and Framework Requirements
  - TR-059: DSL Evolution – Architecture Requirements for the Support of QoS Enabled IP Services
  - WT-099: Architecture with a Layer 3 IP Aggregation Network between the DSLAM and Service Edge
  - WT-101: Migration to Ethernet Based DSL Aggregation

Copyright © 2006, Juniper Networks, Inc. All rights reserved. Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.