



ОПТИМИЗАЦИЯ ПЕРЕДАЧИ ВИДЕО ПО СЕТИ IP TRIPLE PLAY

Сервис-провайдеры, которые конкурируют на рынке развлечений и коммуникационных услуг, должны выйти за пределы «пакетного» обслуживания и предложить персонализированную среду и интерактивные услуги IPTV (IP-телевидения), включая развлечения, коммуникации и Интернет. При развертывании новых услуг IPTV инфраструктуры существующих сетей выйдут на предельные уровни своих возможностей. Для того чтобы поддерживать услуги IPTV, сети должны иметь возможность масштабироваться до миллионов пользователей, иметь достаточный ресурс полосы пропускания и обеспечивать качество обслуживания (QoS) и безопасность на всей цепочке технологического цикла. По этим и другим причинам особую важность при развертывании передачи видео по широкополосной сети приобретает интеллектуальность сети. Вот почему многие из наиболее успешных мировых провайдеров услуги Triple Play, включая Comcast, Fastweb, Hong Kong Broadband, Neuf Telecom и Surewest, построили свои сети следующего поколения (NGN) с использованием решений IP NGN от Cisco Systems®. На сегодняшний день более 10 миллионов абонентов во всем мире получают инновационные видеослужбы по интеллектуальным сетям Cisco® IP NGN.

Услуги видео в будущем будут доставляться по IP-сетям следующего поколения (IP NGN). Требования таких услуг серьезно отличаются от требований услуг высокоскоростного доступа в Интернет. В данном документе анализируются требования по оптимизированной передаче видео в сети IP Triple Play и показывается, как архитектура сети Cisco® IP NGN адресует требования видео сегодняшнего и завтрашнего дня.

ОСНОВНЫЕ ПОЛОЖЕНИЯ

Сервис-провайдеры, предлагающие высокоскоростной доступ в Интернет, обычно определяют услугу по скорости пропускания исходящего и входящего потока, и поэтому соглашение об уровне обслуживания (Service Level Agreement, SLA) определяется непосредственно параметрами передачи информации. В случае же IPTV-услуг сервис-провайдер оценивает услугу по количеству предоставляемых каналов, качеству видео, размеру библиотеки «видео по запросу», пользовательскому интерфейсу, возможностям видеозаписи и интерактивным свойствам, предоставляемым службой IPTV. Соглашение об уровне обслуживания в этом случае определяется не транспортными параметрами сети, а качеством работы, которую сеть просто должна поддерживать. Из-за этих явных различий Cisco разработала свою архитектуру IP NGN, чтобы дать возможность организовать оптимальную передачу данных для каждого конкретного типа обслуживания. При таком подходе каждая отдельная услуга может быть защищена независимым механизмом и соглашения SLA могут обеспечиваться по-разному. Например, высокоскоростной Интернет обрабатывается, как транспортная служба, и различный трафик Интернет пропускается через широкополосный сервер удаленного доступа (BRAS), который обеспечивает качество обслуживания и аутентификацию каждого отдельного абонента. В противоположность этому, видеотрафик обрабатывается, как услуга управляемого оператором приложения. Он изначально идет по IP-сети от кодировщика к ТВ-приставке (STB) и не проходит через BRAS. В этом случае качественное обслуживание предоставляется по каждой услуге, а аутентификацией и полномочиями абонента управляет прикладной уровень. Такой подход с разделением на услуги делает возможным для сервис-провайдера учитывать основные требования для видеотрафика по IP. Эти требования включают:

- оптимизированную модель многоадресной IP-рассылки, использующую все преимущества архитектуры IP, так как видеотрафик подается от источника на ТВ-приставку (STB);
- качество обслуживания, учитывающее возможности абонента;
- защиту сети, которая выходит за пределы восстановления просто от отказа связи и предоставляет эффективные механизмы устранения отказов для борьбы с простоями;
- механизмы управления доступом, защищающие сервис-провайдера от превышения лимита подписки на видео, которое может привести к ухудшению одновременного обслуживания большого числа абонентов.

ТРАНСПОРТНЫЕ УСЛУГИ В СРАВНЕНИИ С УПРАВЛЯЕМЫМИ ПРИКЛАДНЫМИ УСЛУГАМИ

При выборе средства транспортировки с учетом услуг управляемых приложений требования абонентов сильно различаются. Ширина полосы пропускания и ее доступность являются единственным критерием, которым обычно руководствуются абоненты при выборе высокоскоростного доступа в Интернет. Но будущие абоненты IPTV-сети оценивают видеослужбы самыми различными способами. Абоненты хотят получить широкий выбор каналов, богатую библиотеку «видео по запросу», простое в использовании электронное средство управления программами и большой объем высококачественного видеоконтента. При просмотре такого контента абонентов интересует устойчивое высокое качество телевизионного изображения и приемлемое время переключения каналов. Каждое из этих требований абонентов следует учитывать (с помощью различных соглашений об уровне обслуживания, которые используют различные инструменты и реализуют различные правила) для успешной доставки видео по широкополосной сети. Каждому провайдеру, обеспечивающему передачу видео по широкополосной сети точно так же, как это он делает, предоставляя услуги по высокоскоростному доступу в Интернет, придется приложить много усилий для отбора услуг, которые могли бы привлечь и удержать абонентов. Сеть Cisco IP NGN отвечает всем требованиям для самых различных типов услуг по передаче голоса, видео и данных (см. таблицу 1.).

Таблица 1. Сравнение требований транспортных и прикладных услуг

Тип услуги	Транспортная услуга	Управляемая прикладная услуга
Уровень обслуживания (SLA)	Транспортные характеристики <ul style="list-style-type: none"> • Ширина полосы пропускания, максимальная потеря пакетов, максимальная задержка и т. п. 	Соглашение об уровне обслуживания видеоприложений <ul style="list-style-type: none"> • Количество ТВ-приставок (STB) • Соотношение между базовым и премиальным уровнем
Аутентификация/идентификация абонента	Сетевой уровень <ul style="list-style-type: none"> • PPPoE, 802.1X • VLAN для каждого абонента, опция DHCP 82 	Прикладной уровень <ul style="list-style-type: none"> • Видеопортал (Middleware) • STB может быть аутентифицирован сетью при первом подключении
Выполнение SLA	Сетевой уровень <ul style="list-style-type: none"> • Формирование/контроль трафика для каждого абонента (shaping/policing) 	Прикладной уровень <ul style="list-style-type: none"> • На основе управления приложением
Качество обслуживания (QoS)	Для каждого абонента <ul style="list-style-type: none"> • «Золотой», «серебряный», «бронзовый» • Классификация для каждого абонента, организация очередей 	Агрегирование <ul style="list-style-type: none"> • Единая очередь для видео

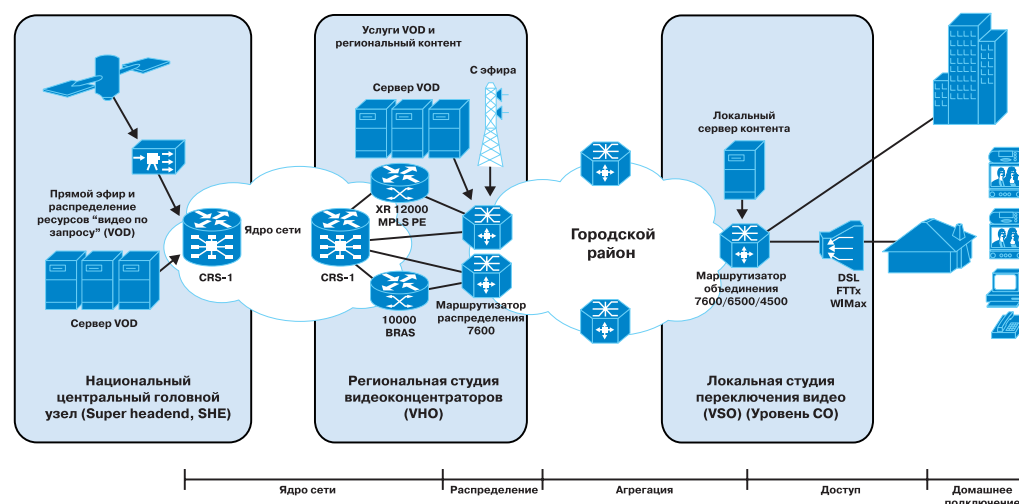
ОБЩИЕ СВЕДЕНИЯ ПО КОМПОНЕНТАМ IPTV-СЕТИ

Основные компоненты архитектуры IPTV-сети включают:

- **Центральная головная станция (SHE).** Передачи в прямом эфире и кодирование в реальном времени видеопередач, идущих из узла SHE, как это делают системы распределения ресурсов в услугах по запросу. Узел SHE также может включать такие внутренние системы, как, например, база данных абонентов. У операторов видео обычно есть один или два узла SHE, которые находятся в ядре транспортной сети.
- **Узлы концентрации видео (VHO).** VHO зачастую содержат кодировщики реального времени для местных телевещательных станций и серверов «видео по запросу» (VoD), а также маршрутизаторы сети, которые соединяют распределенную сеть с ядром сети. Многие VHO содержат серверы контента для услуг «видео по запросу». Многие операторы поддерживают несколько десятков региональных VHO, преимущественно в зонах больших городов. Эти VHO обычно обслуживают от 100 000 до 500 000 домов.
- **Узлы связи и узлы коммутации видео (VSO).** Агрегирующие маршрутизаторы центральной головной станции SHE и узлы VSO, объединяющие трафик от домов абонентов. Для провайдеров DSL центральный узел обычно обрабатывает трафик от мультиплексов доступа местных цифровых линий абонентов (DSLAM).

Сеть Cisco IP NGN может охватывать всю полосу пропускания и соответствовать всем требованиям услуг для IPTV, поскольку она отличается повышенной масштабируемостью и интеллектуальностью, в особенности на уровнях распределения и объединения (см. рис. 1.).

Рис. 1. Базовая архитектура IP-видеосети



ТРЕБОВАНИЯ ВИДЕОУСЛУГ

При оценке архитектуры IPTV полезно понимать общие требования, предъявляемые видеослужбами к сети.

- Широкая полоса пропускания.** Дом с подпиской на IPTV-услуги требует гораздо более широкой полосы пропускания, чем дом, имеющий лишь услуги высокоскоростного доступа в Интернет. Трафик растет так потому, что видео доставляется на ТВ-приставку (STB) абонента непрерывными, устойчивыми потоками. Качество изображения контролируется сервис-провайдером, который определяет режим кодирования. Например, стандарт сжатия MPEG2 требует около 3,75 Мбит/с. Более новый стандарт сжатия MPEG4¹ требует лишь 2 Мбит/с при аналогичном качестве изображения. ТВ высокой четкости (HDTV) требует от 6 Мбит/с до 15 Мбит/с, в зависимости от степени сжатия при кодировании. Другим важным вопросом при оценке архитектуры IPTV являются требования широкоэмитального ТВ в сравнении с «видео по запросу». Каналы широкоэмитального ТВ доставляются с помощью многоадресной IP-рассылки (IP Multicast), при которой используемая полоса пропускания зависит только от количества предлагаемых каналов и степени сжатия при кодировании. Например, 200 каналов программ в формате MPEG2 со стандартным разрешением используют полосу пропускания около 750 Мбит/с. Услуга «видео по запросу», однако, предоставляется индивидуальным транспортным потоком для каждого пользователя. Одна тысяча абонентов «видео по запросу» со стандартным разрешением потребует полосу около 3,75 Гбит/с. Это усложняет управление полосой пропускания VoD.
- QoS.** Качество обслуживания (QoS) исключительно важно при оценивании архитектуры IPTV, так как передача видео по IP очень чувствительна к потере пакетов. И хотя потеря одного или нескольких последовательных пакетов незначительно скажется на восприятии зрителем ТВ, если потеря длится более секунды, это заметно снизит качество изображения. ТВ-приставки имеют ограниченную функциональность для борьбы с потерями видеокадров. Многие из ТВ-приставок (STB), например, позволяют избежать видимых артефактов из-за перерыва в сети с помощью схем прямого исправления ошибок², которые скрывают отсутствующую информацию, или путем повторной передачи недостающей информации. Оба этих метода технически достаточно сложны³. Джиттер также является важным параметром, который следует учитывать, поскольку у ТВ-приставок (STB) ограничена емкость для компенсации джиттера (обычно порядка 150 мс). И хотя абсолютная задержка не столь важна при передаче видео (если она постоянна во времени), помощь в обеспечении контроля задержек от начала до конца является основным атрибутом для проекта передачи видео через IP-сеть. Наконец, также важно учесть совместное существование видео с передачей речи через IP (VoIP) и другого трафика реального времени. При передаче по одной и той же сети нескольких услуг появляются различные требования к организации очередности. Надежное планирование и механизмы исключения перегрузок, а также настраиваемые размеры очереди должны стать частью сетевого решения.
- Авторизация вызова (Admission Control).** Успешные видеослужбы ведут к быстрому увеличению числа абонентов, которые хотят получить доступ к видеоресурсам в сети. Недавние развертывания VoD, например, привели к десятикратному увеличению количества зрителей лишь за несколько лет. Нельзя проектировать сеть таким образом, чтобы превысить возможности подписки на видеотрафик, так как превышение подписки приведет к произвольному выпадению пакетов, что

¹ H.264. Часть 10.

² Как Pro-MPEG. Код технологии № 3.

³ Подходы с использованием таких способов в данный момент находятся в промышленной разработке.

скажется на работе всех услуг абонентов с нисходящим потоком. Для того чтобы избежать превышения возможностей подписки, сеть должна иметь механизмы, которые бы взаимодействовали с источниками видео и давали разрешение новым видеопотокам, только если они не вызовут перегрузку сети.

- **Время переключения широковещательного канала.** Хоты абоненты и не станут принимать решение о покупке услуги ТВ лишь по времени переключения каналов, оно все же влияет на удовлетворенность абонента услугой. Поэтому важно, чтобы сетевое решение было оптимизировано для минимизации задержки переключения каналов.
- **Доступность полной услуги.** «Видео по запросу» и широковещательное ТВ имеют радикально различные требования по доступности. Широковещательное ТВ состоит из многоадресных видеопотоков. Если в сети потеряется один источник многоадресной рассылки, это может сказаться на сотнях тысяч пользователей. Сеть должна быть оптимизирована для многоадресной IP-рассылки и предоставлять способы для «прозрачного» восстановления потери источника многоадресной рассылки. Внедрение географически распределенных избыточных источников многоадресной IP-рассылки является хорошим способом увеличения доступности, поскольку позволяет сети выбрать наиболее эффективный источник и предоставляет быстрое переключение при отказах от одного источника к другому. Напротив, «видео по запросу» является индивидуальной услугой для пользователя, так что потеря одного потока не столь катастрофична. Однако ненадлежащее управление потоками «видео по запросу» или недостаток должного определения очередности могут вызвать серьезные проблемы с превышением предела подписки. Например, если в сети произойдет отказ и при этом резервный путь приведет к сокращению полосы пропускания, произвольные выпадения пакетов от всех видеоисточников приведут к деградации качества для всех потребителей сервиса. Поэтому важно при рассмотрении доступности услуги использовать различные схемы QoS для «видео по запросу» и для широковещательного ТВ.
- **Жизненный цикл услуги:** При внедрении такой новой услуги, как видео, степень принятия видео будет меняться в зависимости от плотности заселения обслуживаемой территории, количества времени, в течение которого услуга уже предоставляется, целевых маркетинговых кампаний, промо-акций и т. п. Другими словами, база пользователей не является постоянным компонентом услуги. Сеть должна иметь возможность легко приспособиться к этим изменениям жизненного цикла услуги без значительных доработок. Она также должна легко масштабироваться, чтобы охватить нетронутых абонентов. И из-за того, что услуга сама может изменяться со временем, сеть должна быть достаточно гибкой для того, чтобы следовать изменениям с минимальным влиянием на подготовку. Так, например, при изменении интересов и привычек зрителей с течением времени можно легко удалять и вводить новые каналы. И когда услуги становятся более популярны по причине сезонного спроса, можно легко предоставить дополнительную полосу пропускания на несколько месяцев.

АРХИТЕКТУРА ПЕРЕДАЧИ ВИДЕО

Существует несколько разновидностей архитектур передачи IPTV, и каждая касается четырех логических сегментов сети – ядра сети, агрегирования, агрегирования и доступа – по-разному приводя к решению. В типовой модели на рис.1 устройства распределения подключены прямо к маршрутизаторам ядра сети, а устройства агрегирования являются первыми устройствами, пропускающими исходящий поток абонента, имеющего избыточные исходящие линки. В этой модели DSLAM является устройством доступа и платформы агрегирования непосредственно объединяют DSLAM-ы.

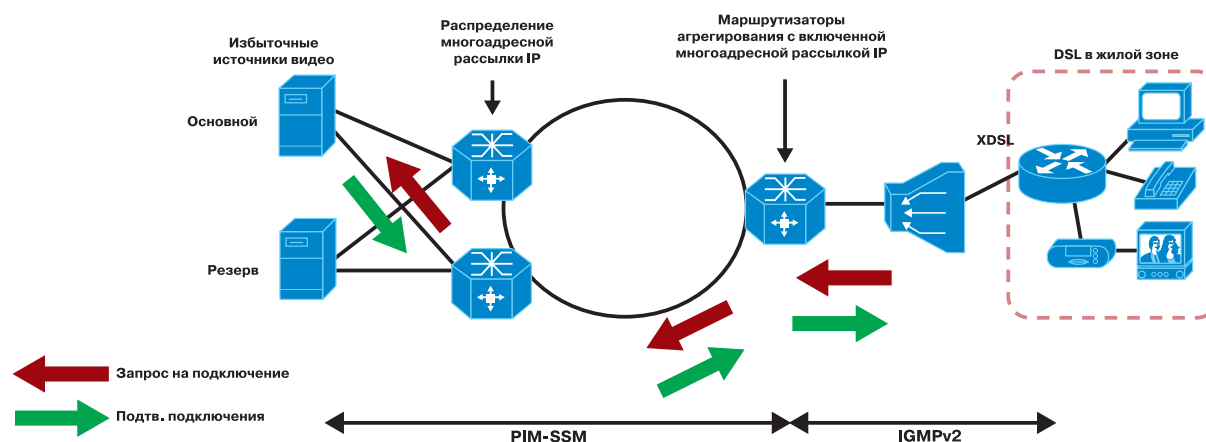
Термин «ядро сети» в данном контексте относится к сети, используемой для передачи видео от нескольких центральных узлов (SHE) к различным районам (VHO). Видео по IP может передаваться по большому разнообразию транспортных технологий, и архитектура Cisco IP NGN может адаптироваться к широкому спектру технологий передач. Например, ядро сети Cisco IP NGN может быть построено на MPLS, VPLS или просто на IP. Cisco предлагает несколько решений для многоадресной передачи через MPLS. Здесь следует отметить, что крупнейшие сети, предоставляющие широковещательное видео через IP, используют в ядре сети многоадресную рассылку IP для распределения каналов в зоны районов, где предоставляется услуга. Причина этого в том, что широковещание IPTV является приложением IP с многоадресной рассылкой. QoS может быть не лучше, чем качество реализации многоадресной рассылки IP, передающей ее.

Сегменты сети распределения и агрегирования предъявляют уникальные требования. На эти требования можно реагировать различными способами, которые характеризуют важный выбор, такие как, где находится граница уровня L3 (IP), у которого желательна поддержка предотвращения отказов, и как оптимизируется полоса пропускания. Главное архитектурное решение лежит в положении границы уровня L3, и здесь есть несколько возможностей, в том числе:

- **Размещение уровня L3 на распределительных маршрутизаторах.** Распределительный маршрутизатор может объединять 150 000 и более пользователей. Размещение границы уровня L3 близко к ядру сети затрудняет масштабирование MAC-адресов и ARP кэша в распределительных маршрутизаторах. Также это не позволяет создать эффективную защиту от отказов источников.

- **Размещение уровня L3 на DSLAM.** Хотя это позволяет избежать вышеуказанных проблем, развертывание DSLAM с IP приведет к повышению стоимости DSLAM и более сложному управлению пулом IP-адресов.
- **Размещение уровня L3 на маршрутизаторах агрегирования.** Существуют неоспоримые причины для установки места уровня L3 на уровне агрегирования между сетью провайдера и ТВ-приставкой (STB) абонента. На рис. 2 показан пример сети с многоадресной рассылкой IP, включенной в маршрутизаторы агрегирования.

Рис. 2. Простая многоадресная рассылка IP в агрегированной сети

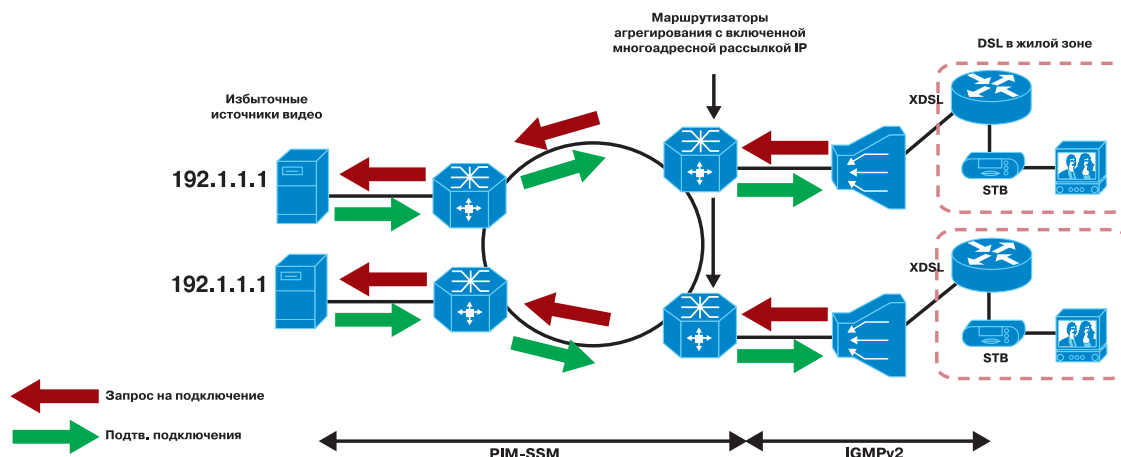


Оптимальный проект (с уровнем L3 на маршрутизаторах агрегирования) помещает способности многоадресной рассылки IP на уровень агрегирования, что предоставляет большие преимущества сервис-провайдерам, включая следующее:

- **Вставка местного контента.** Развертывание возможностей многоадресной рассылки Cisco IP на уровнях агрегирования и распределения дает провайдерам больший контроль, так что они могут определять источник видео, от которого ТВ-приставка (STB) получает потоки. Многоадресная рассылка IP также облегчает добавление и удаление источников видео без изменения настроек ТВ-приставки (STB). Например, сервис-провайдер может развернуть местную рекламу, нацеленную на конкретного потребителя. Вставка местной рекламы является одним из лучших способов получения дополнительного дохода от услуги IPTV. Однако местная вставка рекламы также ведет к увеличению числа каналов многоадресной рассылки IP: например, один канал с 10 разными рекламными зонами внезапно становится 10 каналами многоадресной рассылки.
- **Авторизация вызова (Admission Control).** Маршрутизатор агрегирования с IP может поддерживать встроенное управление доступом, чтобы предотвратить доступ новым видеопотокам, которые вызвали бы перегрузку сети, и возможную потерю пакетов видеопотоков. Иначе это привело бы к неприемлемому ухудшению качества изображения для пользователей.
- **Оптимальное распределение полосы пропускания.** В этой части сети полоса пропускания очень важна. Многоадресные видеопотоки IP в уровне L3 лишь отправляются к VSO и DSLAM, которые должны получать потоки. В сети агрегирования на уровне L2 все многоадресные рассылки – независимо от места назначения – повторяются через сеть агрегирования. Это в особенности проблемно в случае местной вставки рекламы, которая приведет к вставке нескольких видеопотоков для каждого канала, и они будут повторяться через сеть агрегирования (для предыдущего примера: все 10 каналов будут скопированы через сеть агрегирования уровня L2 даже несмотря на то, что они предназначаются конкретным районам). Такое копирование приводит потенциально к гигабитам потерянной полосы пропускания.
- **Асимметричное построение сети.** Другим преимуществом наличия устройства уровня L3 для агрегирования DSLAM-ов является способность использования однонаправленных компонентов. По сути трафик IPTV является практически однонаправленным. С учетом этого Cisco разработала однонаправленные оптические компоненты, которые позволяют сервис-провайдерам развернуть асимметричную сеть, обеспечивающую значительную экономию на транспортном оборудовании. Для обратного канала Cisco использует общую инкапсуляцию маршрутизации (GRE), технику инкапсуляции уровня L3, которая имеет такую способность на маршрутизаторе агрегирования.
- **Эффективный выбор источника видео и защита.** В сети Cisco IP NGN ТВ-приставки (STB) сами имеют возможность выбирать источник, от которого они хотели бы получать видеопоток. Такое более эффективное использование полосы пропускания достигается при помощи метода Anycast, который позволяет источникам многоадресной рассылки предоставлять один и тот же контент и разделять тот же IP-адрес. Избыточность источников и быстрый обход отказа источника – дополнительные преимущества использования Anycast. В случае отказа источника многоадресной

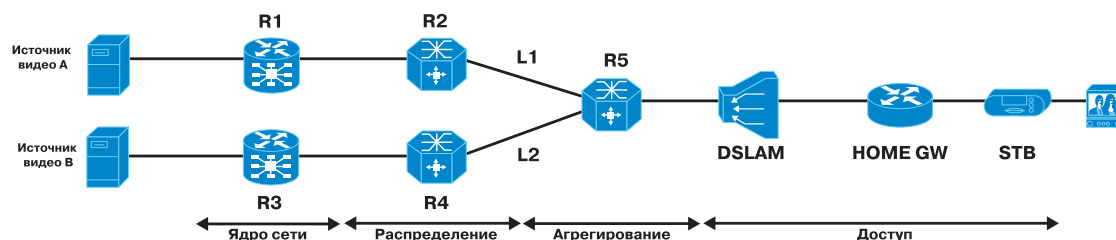
рассылки Cisco IP NGN автоматически и эффективно выбирает следующий ближайший доступный источник (см. рис. 3).

Рис. 3. Anycast и выбор ближайшего источника.



Наличие сети, которая быстро восстанавливается при возникновении отказа, является важной частью услуги передачи видео через широкополосный канал. Конечно же бывает много различных типов отказов. Часто встречающееся заблуждение состоит в том, что если элементы сети могут защитить сеть от сбоя связи за время менее 50 мс, абоненту гарантируется хорошее качество услуги. Например, рассмотрим типичный проект на рис. 4.

Рис. 4. Типичный проект



Пусть каждая связь в данной сети защищена механизмом с временем восстановления при отказе менее 50 мс. Если не установить других механизмов защиты, абонент будет страдать в течение секунд простоя из-за любого из следующих отказов оборудования:

- источник видео, от которого ТВ-приставка получает поток;
- маршрутизаторы, используемые видеоисточником для того, чтобы подключить STB (от R1 до R5);
- однонаправленное соединение⁴;
- DSLAM или домовый шлюз.

Для того чтобы предотвратить перерыв в обслуживании, сеть должна быть оптимизирована так, чтобы позволить быстрое переключение от сервера или кодировщика к другому серверу или кодировщику. Механизмы многоадресной IP-рассылки, такие как Anycast, делают возможным такую избыточность видеокomпонентов. Также доступны уровни приложения, осуществляемые в серверах. Кроме того, некоторые поставщики потокового видео через IP реализовали избыточные выходные интерфейсы Ethernet. Архитектура Cisco IP NGN была испытана и оптимизирована для того, чтобы помочь обеспечить то, что любой тип отказа не приводит к простоям длительностью более 1 секунды при любом развитии событий. А простоя в 1 секунду не заставит абонента звонить в центр поддержки и жаловаться на недостатки.

Cisco делает возможной избыточность сети с помощью широкого набора механизмов, защищающих ее от различных отказов (см. табл. 2).

⁴ Поведение при восстановлении зависит от используемой технологии защиты.

Табл. 2. Защитные механизмы избыточности сети

Уровень	Механизм	Соединение	Узел	Путь
Уровень L3	Улучшения Cisco OSPF ⁵	X	X	X
	Улучшения Cisco IS-IS	X	X	X
	Улучшения Cisco PIM	X	X	X
	Обнаружения двунаправленной коммутации (BFD)	X	X	
MPLS	Быстрая перемаршрутизация (связь по обходу) (FRR)	X	X	X
	Избыточность PW	X	X	X
Ethernet (уровень L2)	Быстрый протокол Spanning Tree (связующее дерево)	X	X	
	Resilient Packet Ring (RPR)	X	X	
	802.3ad LACP	X		
	Flexlink	X	X	
Уровень L1	DWDM и SONET	X	X	

МНОГОАДРЕСНАЯ РАССЫЛКА И СМЕНА КАНАЛА

Существует заблуждение в том, что широковещательная IP-рассылка приводит к медленной смене канала. Хотя несомненно, что остановка приема канала многоадресной рассылки и начало приема другого канала не являются мгновенными, многоадресная операция обычно занимает около 50 мс. Причина того, что эта задержка такая низкая, в том, что маршрутизатор агрегирования обычно обслуживает тысячи абонентов одновременно. Поскольку это число превышает число предлагаемых широковещательных каналов, вероятность запроса на подключение к многоадресной рассылке, идущего через весь путь к источнику видео (как показано в табл.1), близка к нулю. Кроме того, многоадресная рассылка не является главной составляющей в запаздывании смены канала. Видеопоток – это последовательность изображений, которые ТВ-приставка (STB) должна отображать. Изображения последовательно отправляются на ТВ-приставку и затем объединяются в группы изображений (GoP), которые содержат переменное количество изображений (обычно 15). Первое изображение в группе называется I-фреймом. Основа GoP в том, что все изображения после него (I-фреймы) вычисляются с помощью информации об изменении изображения при кодировании видео. Если GoP состоит из 15 изображений, то I-фрейм идет каждые 0,5 секунд. Когда пользователь переключает канал, ТВ-приставка (STB) посылает запрос в сеть на изменение канала. Как мы позже увидим, многоадресная рассылка IP представляет собой менее 10% всего времени переключения канала. Существует много других факторов, кроме многоадресной рассылки IP, которые вносят свой вклад в длительность смены канала, и сетевая архитектура многоадресной рассылки Cisco оптимизирована для минимизации вклада сети в длительность смены канала.

Табл. 3. Задержка смены канала

Факторы, влияющие на задержку при смене канала	Типичная задержка
Остановка приема старого канала	50 мс
Задержка для остановки многоадресного потока	150 мс ⁷
Подключение к многоадресной рассылке нового канала	50 мс
Заполнение буфера для защиты от джиттера	150–200 мс
Задержка на доступ по подписке ⁸	0 мс – 2 с
Задержка I-фрейма	500 мс

⁵ Собственные улучшения Cisco.

⁶ Значения, полученные на Cisco 7600 с 100 подключениями в секунду.

⁷ Зависит от DSLAM.

⁸ Задержка на доступ с подпиской применима к широковещательным каналам, зашифрованным с помощью системы доступа по подписке, которая периодически изменяет ключи расшифровки и передает обновленные ключи в видеопотоке. ТВ-приставка должна дождаться последнего набора ключей дешифрования в потоке видео перед тем, как он сможет начать выполнять декодирование. Количество времени, связанное с этими задержками, зависит от того, как часто система доступа присылает обновления информации для декодирования в видеопотоке.

СПЕЦИФИЧНАЯ К ИСТОЧНИКУ МНОГОАДРЕСНАЯ РАССЫЛКА В РАСПРЕДЕЛИТЕЛЬНОЙ СЕТИ (PIM SSM)

Все маршрутизаторы Cisco и коммутаторы уровня L3 поддерживают многоадресные рассылки IP и многоадресные рассылки, не зависящие от протокола (PIM), по умолчанию. PIM – это протокол маршрутизации, который делает возможным организацию многоадресного дерева распределения, которое распространяет широкоэвещательные каналы ТВ от их источников по всей сети. Cisco предлагает многоадресную рассылку, специфичную к источнику PIM (PIM-Source Specific Multicast, SSM), которая является улучшением стандартной многоадресной рассылки Интернет (Internet Standard Multicast, ISM). Она позволяет приемнику (ТВ-приставке) указывать, от какого источника он хочет получать канал. PIM-SSM предоставляет многие преимущества, в том числе:

- **Оптимальное дерево распределения.** Поскольку сеть имеет дерево распределения многоадресной рассылки, которое «растет» прямо от видеоисточника, видеопоток идет к ТВ-приставке по кратчайшему пути. Это особенно важно для сервис-провайдеров, имеющих большие требования к полосе пропускания видео.
- **Более совершенная система защиты.** Сеть более безопасна, поскольку она не позволяет хулиганам передавать свой контент любой группе и выполняет атаку «отказ в обслуживании» (DoS) по отношению к текущим зрителям данного канала. ТВ-приставки могут взять IP-адрес источника каналов из электронного руководства программ (EPG) и передать его при подсоединении к многоадресной группе. Если ТВ-приставки не поддерживают такую возможность из-за отсутствия поддержки IGMPv3, то маршрутизаторы Cisco, такие как серия маршрутизаторов Cisco 7600, способны собирать информацию об источниках с DNS-сервера от имени ТВ-приставки (STB). Это позволяет традиционным ТВ-приставкам получать преимущества PIM-SSM, не задумываясь о том, от какого источника должен идти канал.
- **Легкая установка и управление.** Поскольку сети не нужно следить за активными источниками, добавление и удаление видеосерверов происходит очень легко. Такая способность полезна для растущих сетей, которые должны приспособливаться к быстрому добавлению и удалению широкоэвещательных каналов. Еще одна выгода в том, что видеосерверы или кодировщики можно легко обслуживать, удалять или заменять.

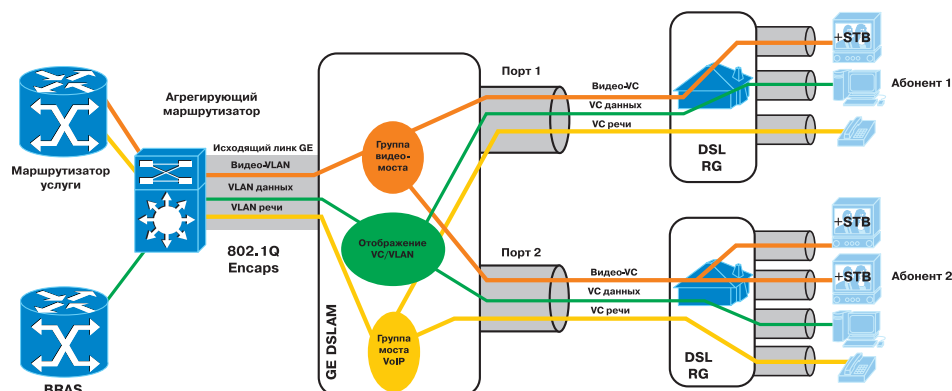
АГРЕГИРОВАНИЕ И УРОВЕНЬ ДОСТУПА

Существует множество способов конфигурирования уровня доступа. Опции конфигурации включают в себя:

- одно виртуальное соединение (VC) в сравнении с многими VC на линии DSL;
- виртуальную видео-ЛВС (VLAN) на услугу или на пользователя;
- высокоскоростной Интернет VLAN на услугу или на пользователя;
- домашний шлюз DSL уровня L2 в сравнении с уровнем L3;
- использование битов приоритета VLAN или уровня L2 для QoS.

Не существует однозначно лучшего решения, и каждая комбинация вышеуказанных опций будет иметь преимущества и недостатки. Богатое способностями оборудование Cisco может приспособиться практически к любому типу проекта, который выберет провайдер. Однако в компании Cisco обнаружили, что внедрение модели, показанной на рис. 5, предоставляет множество преимуществ, исходя из масштабирования, легкости управления и безопасности. В этой прямой конфигурации на каждую услугу используется по одной VLAN. Такой подход улучшает масштабируемость, поскольку каждая VLAN может быть приспособлена к такому количеству абонентов, которое позволяет полоса пропускания. Каждая независима от числа пользователей, подписанных на услугу. Поэтому DSLAM и ее присоединенные абоненты получают три VLAN.

Рис. 5. Пример агрегации и предоставления доступа



В этой модели домашней шлюз разделяет трафик и отображает каждую VLAN на собственный порт внутри дома. Можно настроить маршрутизатор агрегирования одним набором услуг VLAN или использовать уникальный набор VLAN услуг для каждого DSLAM, в этом случае обеспечивается более высокая безопасность. Для всех абонентов, подключенных ко всем DSLAM, объединяемым на этом маршрутизаторе, может быть использован один пул IP-адресов. Например, к маршрутизатору агрегирования обычно можно подключить около 10 000 пользователей. С использованием нумерованных виртуальных интерфейсов коммутатора IP (switch virtual interfaces, SVI) всех пользователей можно поместить в одну подсеть, что сделает управление IP-адресами масштабируемым.

Абонент аутентифицируется на уровне приложения вместе с видео. Однако сервис-провайдеру может потребоваться идентифицировать ТВ-приставку (STB). Форум DSL указывает несколько способов сделать это в спецификации WT101, которая использует метку одноранговой связи (PPP) или опцию 82 протокола Dynamic Host Configuration Protocol (DHCP). Опция 82 протокола DHCP работает следующим образом: когда ТВ-приставка (STB) подключается к сети, она отправляет запрос DHCP к DSLAM. DSLAM проверяет запрос DHCP и вставляет строку идентификатора, по которому запрос был принят в текстовое поле, называемое опция 82. Эта информация помещается в запрос DHCP и передается DHCP-серверу, который может сопоставить ТВ-приставку (STB) с его строкой идентификатора.

РАЗДЕЛЕНИЕ УСЛУГ

Важным аспектом сети передачи видео для архитектуры Triple Play является то, насколько полно сеть обеспечивает поддержку различной производительности и функций, требуемых для каждого типа услуг. Как минимум сеть должна быть способна отвечать требованиям по задержкам и потере пакетов для каждого типа услуг при разделении одной физической среды. Такая способность является неотъемлемой частью архитектуры QoS решения Cisco. Вдобавок Cisco IP NGN можно настроить так, чтобы для каждого типа услуг предоставлялись отдельные домены коммутации/маршрутизации. Такой уровень разделения весьма полезен, когда сервис-провайдер хочет управлять адресным пространством, топологией и инфраструктурой IP, связанной с каждой услугой по отдельности. Такая архитектура транспорта позволяет трафику, связанному с разными типами услуг, быть объединенным и/или завершаться в разных местах с использованием разных компонентов инфраструктуры. Эта архитектура также позволяет агрегацию трафика, связанного с доступом в Интернет, на широкополосном сервере удаленного доступа, в то время как трафик, связанный с видеослужбами, терминируется с помощью компонентов видеоинфраструктуры.

QOS

Видео по широкополосному каналу основывается на IP. Поэтому DSCP биты в заголовке IP-пакета являются ключевыми при определении политик QoS. В этой архитектуре наиболее масштабируемым способом обработки QoS является сегментное обслуживание (PHB) на основании битов IP DSCP.

Голос, видео, высокоскоростной Интернет и сигнализация для голоса/видео помещаются соответственно в собственную очередь. Это позволяет получить детерминистическое поведение от начала до конца по джиттеру/задержкам/потерям. В табл. 4 показан пример настроек, которые может выбрать пользователь для узлов доступа и агрегации.

Табл. 4. Настройка QoS для доступа и агрегации

Класс трафика	DiffServ PHB	Значение DiffServ DCSP	Метод постановки в очередь	Удельный вес очереди
Широковещательное видео	Гарантированная коммутация (AF)	AF 41	Взвешенный (1)	80% к клиенту ⁹ 20% от клиента ¹⁰
Видео по запросу		AF 42		
Речь + видео		CS3		Недоступно
Речь	Срочная коммутация (EF)	EF	Приоритет	20% к клиенту 80% от клиента
Доступ в Интернет	По умолчанию	0	Взвешенный (2)	

⁹ Удельный вес нисходящего видеопотока (downstream) является рекомендацией, учитывая, что весь видеотрафик будет потреблять не более 70% физической пропускной способности. Если предполагаемая доля видеотрафика в общей полосе пропускания значительно меньше, то можно использовать более низкое весовое значение очереди.

¹⁰ Вес очереди восходящего (upstream) видеопотока принимает во внимание лишь сигнализацию «речь + видео», поскольку трафик широковещательного видео и «видео по запросу» является однонаправленным. Действительное значение, используемое для удельного веса в очереди, может изменяться в зависимости от предполагаемого соотношения сигнального трафика в сравнении с полной полосой пропускания линка.

Когда такой элемент сети, как DSLAM, не способен проверять биты IP DSCP, маршрутизатор агрегирования настраивается так, чтобы отображать эти настройки в битах уровня 2 Ethernet 802.1p. DSLAM может помещать видеокадры в нужную ATM VC, и функция SAR будет правильно обслуживать пакеты с учетом различных приоритетов.

УПРАВЛЕНИЕ ДОСТУПОМ

Комбинация трафика, генерируемого «видео по запросу» и ширококестельным видео, с легкостью может превысить максимальную пропускную способность любого соединения в сети, особенно при отказах. Если такое произойдет, пакеты из очереди видео начнут произвольно выпадать. Это отрицательно скажется на просмотре всеми абонентами, находящимися ниже по каналу связи от места возникновения проблемы. Провайдеры должны иметь способы предотвращения возникновения таких катастрофических ситуаций. Некоторые провайдеры планируют ресурсы сети с избытком, так чтобы она могла обслужить трафик VoD со всех возможных путей распространения. Однако на основании расчетов пиковой нагрузки, полоса, потребляемая всеми абонентами, получающими потоки «видео по запросу», делает затраты на такой подход неприемлемыми. Cisco предлагает разнообразные инструменты управления доступом, которые помогают обеспечить хорошее качество для пользователей, даже когда сеть достигает максимума своей пропускной способности. Так провайдеры могут найти баланс между качеством предоставляемых услуг и оптимальными затратами.

• Управление доступом к ширококестельному видео (Broadcast Video Admission Control).

Обычно сервис-провайдеры планируют предлагать 200 или более ширококестельных каналов. На часто используемых исходящих соединениях Gigabit Ethernet DSLAM это может означать, что ширококестельные видеоканалы сами по себе потребляют 75% доступной полосы пропускания¹¹. Остающаяся полоса может оказаться недостаточной для предоставления высокодоходных услуг VoD. В таком случае провайдер может выбрать уменьшение полосы пропускания, потребляемой многоадресной рассылкой (без ухудшения для пользователя), используя механизмы контроля полосы (admission control) на каналах передачи для услуги ширококестельного видео. Поскольку маршрутизатор агрегирования выполняет многоадресную рассылку IP, у него имеется способность ограничения количества каналов, одновременно посылаемых в DSLAM. Критерием для выполнения этого может быть общая популярность или полоса пропускания, используемая конкретным видеоканалом (например, каналы высокой четкости в сравнении со стандартным разрешением). Это также могло бы гарантировать, что основные каналы никогда не заблокируются.

• **Управление доступом VoD (VoD Admission Control).** «Видео по запросу» может оказаться еще более требовательным. Если услуга VoD становится популярнее, чем прогнозировалось, то канал передачи между абонентами и комплексом серверов VoD может оказаться перегруженным. Например, возьмем пиковую нагрузку, когда 20% всех ТВ-приставок (STB) одновременно просматривают видео по требованию. В этом случае центральный узел, поддерживающий 10 тыс. абонентов, потребует пиково 2 тыс. потоков, или грубо от 4 до 7 Гбит/сек. (в зависимости от используемого кодека) для поддержки стандартного разрешения. Добавим контент по запросу с высоким разрешением и получим, что потребуется еще больше полосы. Что же произойдет, когда трафик превысит расчетный ресурс, заложенный при проектировании пропускной способности сети и/или услуги VoD? Если конкретный комплекс серверов VoD не может обслужить конкретный запрос, то он может быть повторно перемаршрутизирован к другому комплексу серверов VoD, у которого имеется доступный ресурс вещания. Если достигается максимальная пропускная способность сети на группе соединений, то разрешение слишком большого количества сессий VoD может стать причиной высокого уровня потери пакетов для всех видеопотоков. Это известно как проблема 1001-го потока: разрешение еще одного потока приводит к тому, что большое количество абонентов испытывает ухудшение видео- и аудиосигналов. Более того, в случае отказа сети, происходящего одновременно с окном пиковой нагрузки, возможно, что у всех пользователей получится простой. Одним из способов избежать широко распространенного простоя является использование встроенного управления доступом (Integrated Admission Control). Если видеосессия не может быть обслужена по причине превышения подписки где-нибудь в сети или на серверах обеспечения услуги, то встроенный контроль включения возвращал бы на запрашивающую ТВ-приставку (STB) сигнал «в данный момент услуга недоступна» («занято»). Хотя никто не любит сигнал занятости, опасность всеобщего ухудшения услуги VoD гораздо хуже. Легко представить, что приложению известно о существовании потоков, которые скоро завершатся, и оно могло бы предоставлять более информационные сообщения о занятости. Это дало бы абоненту больше выбора для запуска потока VoD с задержкой, предложения альтернативных видеослужб, коммерческих возможностей и т. п. В случае отказа система контроля доступа может быть настроена на сброс сначала всех бесплатных потоков VoD и лишь затем оплаченных потоков VoD, если это необходимо.

¹¹ Принимая во внимание 200 каналов MPEG2, кодированных при 3,75 Мбит/с.

- **Встроенные системы управления доступом On-Path и Off-Path (Integrated On-Path and Off-Path Admission Control).** Решение управления доступом VoD должно быть способно учитывать сложные топологии сети. Сюда должны включаться топологии, имеющие избыточные и разделяющие нагрузку пути в транспортной сети, а также каналы доступа и/или бизнес-политики, которые могут приводить в силу другие типы ограничений на услугу абонента. Для реализации данного метода маршрутизаторы сети совместно с менеджерами политик (Policy Manager) и серверами/менеджерами по запросу, должны коллективно использовать функционал управления доступом, который называется встроенным управлением доступом VoD (Integrated VoD Admission Control). Cisco разработала метод In-Path для выполнения управления доступом в сетях со сложной топологией магистральных и распределительных сетей, встречающихся в проектах сетей NGN. Он использует RSVP для маршрутной (In Path) сигнализации, отправляемой сервером VoD или его компонентами до начала сессии VoD. Сообщение RSVP проходит точно такой же путь, который будет использоваться сессией VoD, таким образом отслеживая по пути – в реальном времени – любые изменения в сложных топологиях в ядре сети и уровнях распределения. Вдоль пути маршрутизаторы IP Cisco выполняют функцию управления полосой пропускания, либо разрешая, либо запрещая поток VoD, если для него нет доступной полосы пропускания. Такое управление доступом возможно благодаря наличию маршрутизации на уровне L3 или IP, присутствующей на каждом элементе сети от комплекса серверов «видео по запросу» до маршрутизатора агрегации в центральном офисе. В отличие от предыдущего использования RSVP в голосовых сетях, количество видеопотоков в районе будет, вероятно, в пределах тысяч, так что масштабирование не является проблемой.

Для предотвращения отправки видеопотока на ТВ-приставку (если канал доступа к абоненту не имеет достаточной пропускной способности для передачи потока) сервер VoD или сетевой компонент в процессе авторизации маршрута отправит запрос к компоненте off-path. Это может быть сервер политик, который следит за состоянием сети доступа через подсчет полос пропускания. Сервер политик может проверить, есть ли у канала доступа достаточно неиспользованной полосы пропускания или есть ли бизнес-политики, которые могли бы разрешить или запретить поток VoD. Сервер политики затем разрешит сессию или в этот момент откажет в ней. Комбинация управления доступом «на пути» (in path) с сервером политик «вне пути» (off path) на границе является наиболее надежным и эффективным способом для решения управления доступом, чтобы решить, разрешить или нет новому потоку VoD достичь конкретного абонента. Потоки получают отказ, если будут запущены бизнес-правила по одному из подходов.

Авторизация вызовов для VoD и соответствующие механизмы учета полосы пропускания, добавленные в DiffServ QoS, позволяют обеспечить требуемую степень потери пакетов в пределах 10^{*-6} . Объединение различных технологий управления доступом с DiffServ QoS позволяет Cisco предложить упрощенную стратегию обслуживания и получить разделение всего видеотрафика в одной очереди, избегая таким образом сложных и затратных иерархических стратегий обработки очередей.

ЗАКЛЮЧЕНИЕ

Видеоуслуги завтрашнего дня будут доставляться по IP. Лидерство IP Cisco и инновации IP NGN поднимают качество работы всей системы IP-видео и Triple Play путем оптимизации транспортировки видео посредством уникальных свойств, разработанных Cisco. Cisco предлагает первое в промышленности решение IPTV, которое использует разделение услуг для оптимизации QoS и коммутации на основе типа услуги.

Разделение услуг использует различные подходы для транспортных услуг в сравнении с услугами, управляемыми приложением, такими как видео. Эта архитектура вводит интеллектуальность уровня 3 в объединяющую сеть и предоставляет некоторые ключевые преимущества:

- **Оптимальный выбор источника и эффективная доставка полосы пропускания услуг IPTV.** Специфическая к источнику многоадресная рассылка (SSM) в маршрутизаторах уровня агрегирования Cisco позволяет оптимально выбирать источник и эффективно доставлять полосу пропускания услуг IPTV при обеспечении уровня простоты и неотъемлемой безопасности, которая выше, чем предоставляемая маршрутизацией многоадресной рассылки в сетях агрегирования на уровне L2.
- **Опыт высококачественного просмотра.** Предоставлением встроенного управления доступом и агрегацией, наряду с преимуществами решений «на пути» и «вне пути», Cisco предоставляет управление, требуемое для предотвращения переподписки на видео. Это помогает обеспечить целостный опыт высококачественного просмотра видео.
- **Эффективная защита сети.** Продвинутое механизмы отказоустойчивости (такие, как Anycast) с переклещением критических источников широкоэмительного сигнала предоставляют улучшенное время восстановления при любых типах отказов, включая линки, узлы, видеосерверы и кодировщики.

При таких инновационных интеллектуальных способностях сети, как эти, неудивительно, что более 10 миллионов абонентов лишь в Северной Америке теперь получают свои услуги через инфраструктуру Cisco IP NGN.

ССЫЛКИ

1. Концепции многоадресных виртуальных частных сетей (Multicast VPN)
http://www.cisco.com/en/US/tech/tk828/technologies_white_paper09186a00800a3db6.shtml
2. Интернет-протокол многоадресной рассылки (IPMulticast)
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ipmulti.htm

Подготовил: Илгар Гасымов,
 системный инженер-консультант,
 igasymov@cisco.com



Cisco
 Россия, 115054, Москва,
 бизнес-центр
 «Риверсайд Тауерс»
 Космодамианская наб.,
 52, стр. 1, этаж 4
 Тел.: +7 (495) 961 14 10
 Факс: +7 (495) 961 14 60
www.cisco.ru
www.cisco.com

Cisco
 Россия, 191186,
 Санкт-Петербург,
 бизнес-центр «Регус»
 Невский проспект, 25,
 этаж 2, офис 30
 Тел.: +7 (812) 346 77 17
 Факс: +7 (812) 346 78 00
www.cisco.ru
www.cisco.com

Cisco
 Казахстан, 480099,
 Алматы,
 бизнес-центр «Самал 2»
 Ул. О. Жолдасбекова, 97,
 блок А2, этаж 14
 Тел.: +7 (3272) 58 46 58
 Факс: +7 (3272) 58 46 60
www.cisco.ru
www.cisco.com

Cisco
 Украина, 252004, Киев,
 бизнес-центр
 «Горайзон Парк»
 Ул. Николая Гринченко, 4В
 Киев, 03038, Украина
 Тел.: +7 (38044) 490 36 00
 Факс: +7 (38044) 490 36 66
www.cisco.ua
www.cisco.com

Cisco
 Азербайджан,
 AZ 1065, Баку,
 бизнес-центр «Карат»
 Ул. М. Мухтарова, 201,
 этаж 2
 Тел.: +7 (99412) 437 48 20
 Факс: +7 (99412) 437 48 21
www.cisco.ru
www.cisco.com

Cisco
 Узбекистан, 100000,
 Ташкент, бизнес-центр
 «ИНКОНЕЛЬ»
 Ул. Пушкина, 75, офис 605,
 этаж 6
 Тел.: +7 (99871) 140 44 60
 Факс: +7 (99871) 133 44 64
www.cisco.ru
www.cisco.com

Cisco has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the
Cisco Website at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong • SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe