УДК УДК 681.32; 621.39; 621.316.5

Костик Б. Я., д.т.н.; **Чайка Г. Е.,** д.ф.-м.н. *(ГУИКТ)*;
Биденко О. А. *(ООО «Дипломат Комфорт Сервис»)*

ЭФФЕКТИВНОСТЬ ИСПОЛЬЗОВАНИЯ ПОЛОСЫ ПРОПУСКАНИЯ ТРАНСПОРТНЫХ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

Костік Б. Я., Чайка Г. Є., Біденко О. А. Ефективність використання смуги пропускання транспортних мереж передачі даних. Розглянуті механізми збільшення ефективності використання смуги пропускання транспортних мереж передачі даних при використанні методів пакетної комутації із застосуванням протоколу RPR згідно рекомендації IEEE G802.17.

Ключові слова: ТРАНСПОРТНА МЕРЕЖА, ПАКЕТНА КОМУТАЦІЯ, СМУГА ПРОПУСКАННЯ, RPR, TRIPLE PLAY, IEEE G802.17

Костик Б. Я., Чайка Г. Е., Биденко О. А. Эффективность использования полосы пропускания транспортных сетей передачи данных. Рассмотрены механизмы увеличения эффективности использования полосы пропускания транспортных сетей передачи данных при использовании методов пакетной коммутации с применением протокола RPR согласно рекомендации IEEE G802.17.

Ключевые слова: ТРАНСПОРТНАЯ СЕТЬ, ПАКЕТНАЯ КОММУТАЦИЯ, ПОЛОСА ПРОПУСКАНИЯ, RPR, TRIPLE PLAY, IEEE G802.17

Kostik B. Ya., Chaika G. Ye., Bidenko O. A. Efficiency of the use of bandwidth of transport network communication of data. Ehe mechanisms of increase of efficiency of the use of bandwidth of transport network communication of data are In-process considered, at the use of methods of package commutation, and with the use of protocol of RPR, in obedience to recommendation of IEEE G802.17.

Keywords: TRANSPORT NETWORK, PACKAGE COMMUTATION, BANDWIDTH, RPR, TRIPLE PLAY, IEEE G802.17

Развитие телекоммуникационных технологий привело к созданию сетей абсолютно нового типа. Это диктуется необходимостью предоставления потребителю большого спектра услуг Triple Play. Они включают в себя помимо традиционных телефонных услуг и низкоскоростной передачи данных новые сервисы, такие как видео по запросу (video ondemand – VOD), видео через IP сети (video over IP – VideooIP), IP телефония (voice over IP – VoIP), предоставление высокоскоростных каналов для корпоративных сетей. Кроме того расширение спектра услуг сопровождается ростом требований к повышению качества предоставляемых услуг. Сети способные предоставлять конвергентные услуги связи получили название NGN (Next Generation Network). Транспортные конвергентные мультисервисные сети NGN должны удовлетворять следующим требованиям:

– *Транспорт для различных сетевых служб.* Появление новых и обеспечение традиционных услуг не должно ограничиваться возможностями транспортной сети NGN.

– *Дифференциация/изоляция сетевых служб.* Транспортная сеть NGN должна обеспечивать возможность передачи каждого типа услуг в отдельности не оказывая влияние на все остальные типы передаваемых услуг.

– *Обеспечение QoS для различных типов трафика и служб.* Обеспечение качественной передачи любого типа данных в соответствии с требованиями предъявляемыми к этим данным.

– *Масштабируемость*.

– *Наличие механизмов быстрого самовосстановления сети.* Обеспечение сетевой защиты для для различных сетевых служб с обеспечением всех качественных характеристик.

– *Эффективное использование сетевых ресурсов.* Наличие механизмов для автоматического управления сетевыми ресурсами сети и управления полосой пропускания.

– *Наличие средств OAM* для диагностики, мониторинга и измерения уровней потерь, задержек и джиттеров.

Существует несколько подходов к решению этой задачи.

Первый подход реализован на развитии существующих технологий с добавлением устройств конвертации данных и интерфейсов. Так например, хорошо зарекомендовавшие себя сети SDH [1, 2, 3] дополняются конверторами Ethernet over TDM и это решение получило

название SDH MSPP или SDH NGN. Но это решение, при всех своих достоинствах, имеет очень существенный недостаток, низкий коэффициент использования полосы пропускания. Коэффициент использования таких сетей колеблется от 20% до 50% в зависимости от метода построения защиты.

Второй подход, когда сети Ethernet дополняются конверторами TDM over Ethernet. Основными недостатками такого подхода можно назвать асинхронность сети, сложность построения защиты и не нормированность задержек и джитера.

Третий подход заключается в построении сетей на основе принципиально новой технологии пакетной коммутации PTS (Пакетные Транспортные Системы). Эта технология объединяет в себе достоинства предыдущих и компенсирует их недостатки. Именно поэтому в 2000 г. ряд ведущих телекоммуникационных компаний: Cisco, Corrigent, Nortel, HuaWei приступили к созданию нового протокола для PTS, который получил название Адаптивное Пакетное Кольцо - RPR (Resilient Packet Ring). В п.1.3. стандарта IEEE 802.17 [4] определены следующие свойства протокола RPR:

1) *Адресация.* Поддержка передачи данных unicast, multicast и broadcast трафиков.

2) *Услуги.* Поддержка качества мультисервисных услуг. Протоколы Per-service-quality и flow-control для регулирования трафика клиентов.

3) *Эффективность.* Стратегия увеличения эффективности пропускной способности для unicast, multicast и broadcast трафиков.

4) *Честность.* Справедливое разделение полосы пропускания трафика.

5) *Автоматическая установка.* Автоматическое распознание топологии и свойств каждого узла без ручного вмешательства.

6) *Защита от ошибок.*

7) *Средства OAM* для диагностики, мониторинга и измерений.

В свою очередь соответствующий комитет IEEE 802.17 регламентировал основные механизмы для создания оборудования мультисервисных конвергентных сетей нового поколения NGN.

Рассмотрим действие этих механизмов с точки зрения эффективности использования полосы пропускания сетевой структуры.

Адресация. Стандарт IEEE 802.17 определяет уровень доступа к среде передачи посредством MAC адреса (media access control). Каждая станция в кольце имеет уникальный 48-битный MAC адрес. Кольцевая топология обеспечивает построение сетей с защитой передаваемых данных и не только. Протокол RPR реализует механизм повышения эффективности использования полосы пропускания. В кольце RPR используются три основные операции по обработке пакетов:

1) вставка (insert) пакетов в кольцо;

2) копирование (copy) входящего пакета для передачи на вышестоящий уровень обработки или передачи на подуровень управления;

3) удаление (delete) пакета из кольца.

Механизм копирования позволяет не только снизить время передачи пакета по сети, запараллеливая процессы обработки и транзитирования информации, но и улучшить утилизацию на уровне магистрали. Так например для передачи широковещательных пакетов (IPTV) используется один пакет в не зависимости от количества потребителей. Этот пакет будет тиражироваться на каждом из узлов до тех пор, пока информация не достигнет последнего узла назначения. Количество переприемов задается в поле TTL (время жизни). Это также защищает сеть от зацикливания пакетов в сети.

Таким образом, в заголовке пакета есть вся необходимая информация для первичной обработки пакетов: DA (адрес получателя) и TTL (время жизни пакета). Это позволяет быстро отсортировать транзитные пакеты, которые копируются из буфера одного агрегата в другой практически без задержек.

Для обеспечения работоспособности RPR сети и обеспечения функций “автоматического распознания топологии” используется три типа фреймов: защита топологии (topology protection -TP), топологическая контрольная сумма (topology checksum - TC), распознавание атрибутов (attribute discovery - ATD).

1) В TP передается информация о конфигурации и статусе станций. Станции в кольце RPR рассылают широковещательные сообщения с информацией о своей конфигурации и статусе, а также обновляют свою топологическую базу данных SAS DB после приёма TP фреймов от других станций. В конечном счёте, все станции в кольце синхронизируют между собой топологическую базу данных SAS DB.

2) TC фреймы передают информацию о контрольной сумме топологической базы данных SAS DB. Так достигается стабильность сети RPR.

3) ATD фреймы переносят атрибуты локальных станций: MAC-адрес и название станции. Эти атрибуты также будут включены в топологическую базу данных SAS DB.

Эффективное использование сетевых ресурсов. Под определением топологии RPR кольца понимаются сети со статической коммутацией на уровне сети. Таким образом, при создании любого виртуального соединения происходит заполнение таблиц баз данных SAS DB. Эта база содержит состав узлов кольца, их расположение, состояние элементов, оптических линков и свойств соединения. Это обеспечивает создание сети, подготовленной для передачи любого типа трафика. Эффективность систем передачи зависит от вероятности конфликтных ситуаций, т.е. интенсивности столкновений. В RPR интенсивность столкновений практически стремится к 0, так как передача осуществляется по подготовленному каналу для каждого виртуального соединения. Характеристики такого соединения устанавливаются в момент его создания и контролируются всеми сетевыми элементами в течение всего времени его существования.

Очевидно, что при стремлении интенсивности столкновений к 0 время обслуживания трафика в сети (t) зависит от длины кадра MTU (D), межкадрового интервала $t=D/V+l+(N\cdot T)$, скорости передачи информации (V), количества элементов в сети (N) и времени нормированной задержки обработки пакета каждым узлом (T).

Повышение эффективности использования сетевых ресурсов осуществляется путем применения механизмов “справедливости” распределения полосы и “дросселирования” трафика. Ввиду того, что каждый сетевой элемент знает о состоянии всех остальных контрагентов сети и их готовности принять трафик, то вероятность передачи достоверной информации стремится к 1. Это относится не только к готовности принять трафик, но и к готовности принять трафик с определенными качественными и количественными характеристиками. Так в случае возникновения в сети скачкообразного трафика (всплесков), которые могут привести к перегрузке в каком либо сетевом элементе N, сетевой элемент N отсылает сообщение предыдущему элементу N-1 с рекомендацией дросселировать исходящий трафик для определенного соединения с определенным классом сервиса CoS до уровня пропускной способности сетевого элемента N. По мере освобождения полосы пропускания, элемент N снимает ограничения на пропуск трафика. Таким образом, обеспечивается эффективное использование полосы пропускания в час наибольшей нагрузки ЧНН. Этот механизм применяется только для типов трафика с низкими приоритетами, которые не критичны к задержкам. Трафик с высоким приоритетом (online) всегда имеет гарантированную полосу пропускания, задержку и джиттер.

Передача аварийных сигналов о состоянии агрегатных интерфейсов передается также и в заголовке SDH (LOS, AIS и другие).

В протоколе RPR также заложен механизм приоритезации. Существует четыре класса сервиса: A, B(G1), B(G2) и C. Свойства различных классов сервиса и их приоритезация показаны в табл. 1. Как видно из таблицы, класс A имеет наивысший приоритет и может иметь два подкласса: A0 и A1. Подкласс A0 – полная имитация SDH-соединения для

передачи TDM трафика с минимальными задержками и нормированным джиттером (дрожанием) задержки. Этот тип трафика всегда имеет 100 % резервирование по защитному пути.

Классы сервиса для трафика в RPR Табл. 1

Класс сервиса в RPR			Качество обслуживания (QoS)			
Имя	Использование	Подкласс	Гарантированная пропускная способность	Задержка / Jitter	Тип пропускной способности	Подтип пропускной способности
classA	Real-time HP	subclassA0	Да	Низкая	распределенный	Резервированная
		subclassA1				
classB	Guaranteed G1/G2	classB-CIR	Да	Ограниченна	распределенный	Переменная CIR/PIR
		classB-EIR	Нет	Не ограничена	авантюрный	
classC	Best-effort BE	BE				

Трафик подкласса A1 также имеет наивысший приоритет, но резервирование на защитном пути может меняться от 0 до 100%, а неиспользованная полоса может быть использована для передачи низкоприоритетного трафика. Класс B также имеет два подкласса: B(G1) с минимально гарантированной полосой пропускания (CIR) и B(G2) без гарантированной полосы. Класс C (best-effort – лучшее, что осталось) – это трафик с минимальным приоритетом. Однако это не значит, что при передаче этого трафика допускаются потери. Трафики классов G2 и C некритичны к задержкам.

Защита. Важным свойством PTS NGN является защита трафика. Наиболее защищенными являются SDH сети с кольцевой топологией [5], где весь трафик может полностью резервироваться, но при этом приходится жертвовать минимум 50 % суммарной пропускной способностью сети. Защита сети с использованием протокола RPR построена аналогично сетям SDH с той разницей, что полоса защитного пути может быть использована для передачи коммерческого трафика и трафика управления, а в случае повреждения основного пути задействуется механизм «справедливого» распределения полосы и “дросселирования”.

В RPR различают два вида защиты: заворот (wrapping) и перенаправление (steering).

1) В режиме заворота (wrapping) после повреждения оптического линка или станции, в точке повреждения защищаемый трафик направляется в противоположное полукольцо Ringlet. Два полукольца, таким образом, формируют сомкнутое одиночное кольцо вокруг точки повреждения.

Как показано на рис.1, после того, как повреждается интервал между станциями A и B в полукольце Ringlet 0, трафик, который обычно проходит от станции A к станции B

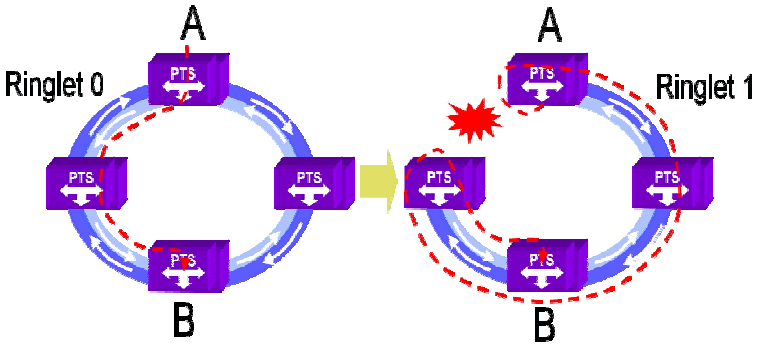

Рис. 1. Режим заворота (wrapping)

по полукольцу Ringlet 0, перенаправляется в полукольцо Ringlet 1 для достижения станции B. Поскольку режим заворота позволяет быстро переключиться, потеря фреймов данных минимизируется. Это, однако, приводит к снижению пропускной способности в два раза.

2) В отличие от режима заворота, в режиме перенаправления (steering) две станции по обеим сторонам от точки повреждения сначала обновляют свои топологические базы данных; затем эти станции посылают TP фреймы с быстрыми интервалами на другие станции в кольце. Таким образом, трафик заворачивается в узле источника трафика. После того, как новая топология стабилизируется, станция-источник перенаправляет защищённые фреймы в полукольцо Ringlet 0, как показано на рис. 2.

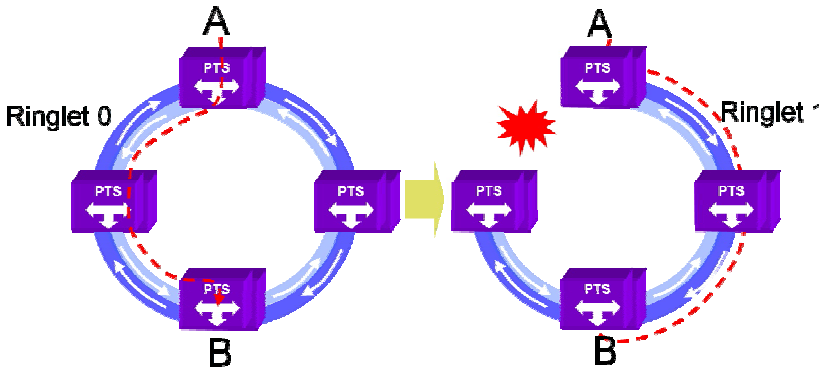

Рис. 2. Режим перенаправление (steering)

Как видно, время переключения в режиме заворота минимальное, следовательно этот метод защиты наиболее эффективно применять для трафика A0 (real time). Но при этом режиме менее эффективное использование полосы пропускания защитного пути.

Заключение. Подводя итоги, можно сделать вывод, что поступательное движение разработчиков сетевых протоколов пришло к пониманию необходимости создания транспортного протокола, позволяющего передавать информацию различных сетевых служб с высоким качеством и защитой от возможных аварийных ситуаций с минимальными затратами. Попытки создания такого сетевого протокола велись на протяжении последних лет. Результатом стало появление таких протоколов как FDDI, Token Ring и стпндарт IEEE 802.17. Протокол RPR IEEE 802.17 взял все лучшее от протоколов SDH и TCP/IP. В этой статье описаны далеко не все возможности этого протокола. Возможно, в дальнейшем появятся протоколы еще с более высокой агрегацией трафика, но на сегодняшний день RPR наиболее эффективный протокол для построения транспортных сетей MAN NGN с высокой степенью конвергенции трафика и хорошей масштабируемостью сети.

Литература

1. Стефано Брени. Синхронизация цифровых сетей / Стефано Брени. – М.: Мир, 2003. – 456 с

2. Бирюков Н. В. Транспортные сети и системы электросвязи Системы мультиплексирования / Н. В. Бирюков, В. К. Стеклов, Б. Я. Костик. – К.: Техніка, 2003. – 352 с.

3. Хмелев К. Основы SDH / К. Хмелев. – К.: Політехніка, 2003. – 584 с.

4. RESILIENT PACKET RINGS // Стандарт IEEE 802.17.

5. Слепов Н. Н. Синхронные цифровые сети SDH / Н. Н. Слепов. – М.: ЭКО-ТРЕНДЗ, 1998. – 148 с.