А.М. Голиков

Транспортные и мультисервисные системы и сети связи

Учебное пособие

Томск

Голиков А.М. Транспортные и мультисервисные системы и сети связи: Учебное пособие. Часть1. – Томск: Томск. гос. ун-т систем управления и радиоэлектроники, 2015. – 102 с.

Учебное пособие содержит лекционный материал по транспортным системам и сетям связи (Часть 1) по курсу «Транспортные и мультисервисные системы и сети связи» специальности 210601-2.65 – Радиоэлектронные системы и комплексы передачи информации. Представлены описания аппаратно-программных комплексов и методики построения систем.

Оглавление

1. Общая характеристика мультимедийного трафика

Знание характеристик трафика, создаваемого пользователями (абонентами), является непременным условием для грамотного проектирования сетей электросвязи. Значение трафика непосредственно определяет как капитальные затраты на оборудование сети, так и возможные доходы за счет его эксплуатации.

1.1. Классификация мультимедийного трафика

Мультимедийный трафик. Под мультимедийным трафиком понимается цифровой поток данных, который содержит различные виды сообщений, воспринимаемых органами чувств человека (обычно звуковая и/или видеоинформация). Мультимедийные потоки данных передаются по телекоммуникационным сетям с целью предоставления удаленных интерактивных услуг. Наиболее распространенными на сегодняшний день мультимедийными услугами, предоставляемыми пользователям сети, являются: видеотелефония, высокоскоростная передача мультимедийных данных, 1Р-телефония, цифровое телевизионное вещание, мобильная видеосвязь и цифровое видео по запросу.

В зависимости от типа предоставляемого сервиса выделяются две основные категории мультимедийного трафика.

1. Трафик реального времени, предоставляющий мультимедийные услуги для передачи информации между пользователями в реальном масштабе времени.

2. Трафик обычных данных, который образуется традиционными распределенными услугами современной телекоммуникационной сети, таких, как электронная почта, передача файлов, виртуальный терминал, удаленный доступ к базам данных и др.

В качестве примеров услуг, генерирующих трафик реального времени, можно привести следующие: 1Р-телефония, высококачественный звук, видеотелефония, видеоконференцсвязь, дистанционное (удаленное) медицинское обслуживание (диагностика, мониторинг, консультация), видеомониторинг, широковещательное видео, цифровое телевидение, вещание радио- и телевизионных программ.

1Р-телефония. Данный сервис осуществляет передачу голосового трафика (речи) между двумя абонентами сети, в которой, в качестве сетевого, используется протокол IP (Internet Protocol). Для организации сервиса «IP-телефония» могут быть использованы локальные, корпоративные, глобальные сети, а также сеть Интернет. С помощью специальных шлюзов, используемых в телефонной сети общего пользования, обеспечивается IP-телефонная связь между абонентами телефонных сетей и абонентами сетей передачи данных.

Высококачественный звук. Под «высококачественным звуком» понимается такой сервис, который осуществляет передачу и вещание высококачественного звука, например, музыки, концертных выступлений и т.д.

Видеотелефония. Данный сервис осуществляет передачу человеческой речи вместе с его изображением невысокого качества между двумя абонентами. Клиенты данного сервиса, через соответствующую коммутационную аппаратуру, могут слушать и видеть друг друга в режиме реального времени.

Видеоконференция. Данный сервис осуществляет передачу голосового и видеотрафика между группой абонентов, причем звуковые и видеосигналы передаются по сети независимо один от другого (по разным транспортным соединениям), их синхронизация на приеме обеспечивается соответствующим протоколом транспортного уровня.

Дистанционное медицинское обслуживание. Данный сервис обеспечивает проведение дистанционного медицинского обследования, диагностики и консультации больных. Трафик данного сервиса включает голосовые и видеоданные, результаты обследования, переданные в реальном масштабе времени, и др.

Видеомониторинг. Данный сервис осуществляет видеонаблюдение помещений, применяется для охраны территорий различного назначения, оперативной сигнализации о различных нештатных ситуациях, постоянного (в режиме реального времени) мониторинга в местах скопления людей.

Вещание радио и телевизионных программ. Данный сервис осуществляет вещание обычных радио- и телевизионных каналов по цифровой телекоммуникационной сети.

Цифровое телевидение. Данный сервис осуществляет вещание высококачественного цифрового телевидения (художественных фильмов, музыкальных видеоклипов, спортивных трансляцией) по запросу клиентов данного сервиса.

Основной тенденцией в развитии современных телекоммуникационных сетей является поддержка различных видов сервиса, в том числе мультимедийного. Требования различных типов мультимедийного трафика к сетевым ресурсам могут отличаться весьма существенно. Например, обычный трафик, как правило, не налагает особых ограничений на время его доставки до получателя. Все что требуется такому трафику, - это выделение ему минимальной пропускной способности.

Другим примером может быть трафик для проведения видеоконференций в реальном масштабе времени. Он требует не только значительной пропускной способности, но также и минимизации времени доставки видеокадров до получателя. Кроме того, качество проведения сеанса видеоконференции не будет удовлетворительным, если задержки пакетов информации имеют слишком нерегулярный характер. В данном случае к ресурсам

сети предъявляются жесткие требования по многим параметрам. Эти параметры подробно будут рассмотрены ниже.

Описание и анализ мультимедийного трафика в современных телекоммуникационных сетях является сложной и трудной задачей. Основными причинами этих трудностей являются:

- широкий диапазон скоростей передачи - от нескольких кбит/с, как в случае передачи телефонного трафика, до сотен Мбит/с, при передаче видепотоков;

- разнообразные статистические свойства передаваемых мультимедийных информационных потоков (трафик реального времени налагает жесткие требовании к ресурсам сети);

- большое разнообразие сетевых конфигураций, множество технологий и протоколов передачи (Gigabit Ethernet, ATM, MPLS и др.);

- многоуровневая обработка передаваемых сообщений, вследствие чего качество обслуживания оказывается зависящим от нескольких уровней обработки.

1.2. Общий подход к параметризации мультимедийного трафика

Имеется множество моделей описания трафика в различных телекоммуникационных сетях.

В общем случае мультимедийный трафик некоторой услуги представляется в виде случайного процесса. Пусть мгновенное значение трафика - есть число блоков информации, которые генерирует соответствующий сервис в единицу времени. Тогда в наиболее общем случае случайный процесс $B(t)$ описывается семейством функции распределения $F_{B(t)}(x)$, где

$$F_{B(t)}(x)=Bep\{B(t)\ \Phi\ x\}$$

Практическое использование такого метода описания затруднительно [не создан математический аппарат, обеспечивающий оценку параметров качества такой нестационарной нагрузки общего вида, сложность в адекватном оценивании семейства функции распределения $F_{B(t)}(x)$].

Для параметризации мультимедийного трафика, как правило, используется ряд характеристик, которые определены рекомендациями ITU-T. Эти характеристики описывают интегральные параметры случайного процесса $B(t)$, пример реализации которого приведен на рис. 1.1.

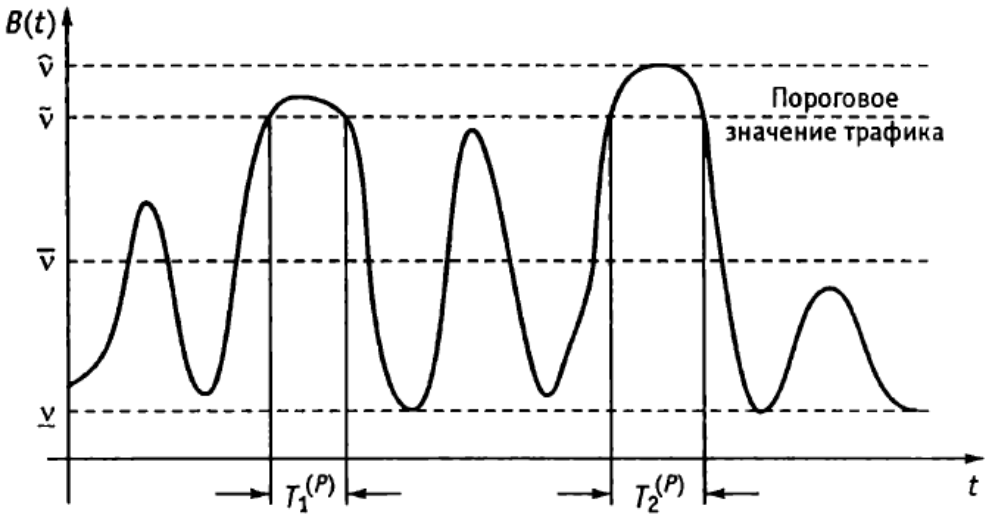


Рис. 1.1. - Основные параметры мультимедийного трафика

К характеристикам трафика, который генерируется различными мультимедийными услугами, относятся следующие:

- значения трафика (мгновенное, максимальное, пиковое, среднее и минимальное), бит/с;
- коэффициент пачечности трафика (пульсация);
- средняя длительность пикового трафика;
- средняя длительность сеанса связи;
- форматы элементов трафика;
- максимальный, средний, минимальный размеры пакета;
- интенсивность трафика запросов.

Максимальное значение трафика $\hat{v}$. Максимальное число блоков информации, которое соответствующий сервис генерирует в единицу времени, определяется как:

$$\hat{v} = maxB(t)$$

Пиковое значение трафика. Трафик соответствующего сервиса, который превышает установленный для него пиковый порог $\tilde{v}$.

Среднее значение трафика $\bar{v}$. Среднее число блоков информа ции, которое соответствующий сервис генерирует в единицу времени, определяется как

$$\bar{v} = \frac{1}{T^{(s)}} \int_0^{T^{(s)}} B(t)dt$$

где $T^{(s)}$ – длительность сеанса связи.

Минимальное значение трафика $\underline{v}$. Минимальное число блоков информации, которое соответствующий сервис генерирует в единицу времени, определяется как

$$\underline{v} = minB(t)$$

t

Коэффициент пачечности трафика К. Определяется как отношение между максимальным и средним трафиком соответствующего сервиса. Коэффициент пачечности вычисляется по формуле:

$$K = \frac{\hat{v}}{\bar{v}}$$

Средняя длительность пика $\bar{T}^{(p)}$. Средняя длительность интервала времени, в течение которого, соответствующий сервис генерирует пиковый трафик, вычисляется по формуле:

$$\bar{T}^{(p)} = \frac{1}{N^{(p)}} \sum_{i=1}^{N^{(p)}} T_i^{(p)}$$

где $N^{(p)}$ – число пиков в течение сеанса связи; $T_i^{(p)}$ - длительность *i*-пика процесса *B(t)*, $i = \overline{1, N^{(p)}}$, а длительность *i*-пика определяется выражением

$$T_i^{(p)} = t_i^{(e)} - t_i^{(s)}$$

где $t_i^{(e)}$, $t_i^{(s)}$ - моменты начала и окончания i-пика, которые определяются следующими выражениями:

$$t_i^{(s)} = \min_{\substack{B(t)>\bar{v} \\ t>t_{i-1}^{(s)}}} t, \quad t_i^{(e)} = \min_{\substack{B(t)>\bar{v} \\ t>t_i^{(s)}}} t, \quad \text{где } t_0^{(s)}, t_0^{(e)} = 0.$$

Перечисленные выше параметры используются для описания трафика соответствующего сервиса в течение одного сеанса связи с абонентом сервиса.

Интенсивность запросов λ на получение обслуживания абонентами сети у соответствующего сервиса определяется как среднее число поступивших запросов на обслуживание в единицу времени.

Средняя длительность сеанса связи $\bar{T}^{s}$ – средняя продолжительность интервала времени, в течение которого соответствующий сервис обслуживает поступивший запрос.

Максимальный размер пакета $\hat{s}$ – максимальный размер элемента трафика в битах (элемент трафика передается адресату как единое целое).

Таблица 1.1. Параметры трафика мультимедийных услуг (типичные значения)

Тип ультимедийного сервиса	Параметры мультимедийных трафиков					
	$\hat{v}$, Мбит/с	$\bar{v}$, Мбит/с	K	$T_i^{(p)}$, с	$T_i^{(s)}$, с	λ, Сеанс/сут
IP-телефония	0,064	0,064	1	100	100	5
Высококачественный звук	1	1	1	53	53	3
Видеотелефония	10	2	5	1	100	6

Видеоконференция	10	2	5	1	1000	6
Дистанционное медицинское обслуживание	10	2	5	1	1000	3
Видеомониторинг	10	2	5	-	-	6
Вещание радио и телевизионных программ	34	34	1	-	-	6
Цифровое телевидение	34	34	1	-	5400	6

Средний размер пакета $\bar{s}$ – средний размер элемента трафика в битах.

Минимальный размер пакета $\underline{s}$- минимальный размер элемента трафика в битах.

Некоторые типичные параметры трафика, генерируемого соответствующими источниками, приведены в табл. 1.1.

1.3. Параметры качества обслуживания мультимедийного трафика в сетях

При передаче разного вида трафика, каждому пользователю должно быть представлено телекоммуникационное (транспортное) соединение, которое обеспечивает соответствующее этому трафику качество обслуживания в соответствии с международными рекомендациями и стандартами.

Выделяются следующие основные параметры качества соединения: 1) время установления соединения; 2) вероятность установления соединения; 3) вероятность разрыва соединения; 4) задержка; 5) вероятность потери; 6) джиттер.

Время установления соединения $t^{(cn)}$ – определяется как интервал времени от момента выдачи абонентом запроса на предоставление соответствующего мультимедийного сервиса до момента начала предоставления этого сервиса.

Вероятность установления соединения $P^{(cn)}$ – отношение числа запросов, которым уже предоставлен соответствующий сервис, к общему числу запросов на предоставление этого сервиса.

Вероятность разрыва соединения $P^{(rj)}$ – определяется как отношение числа запросов, которым соответствующий сервис не был предоставлен полностью, к общему числу обслуженных запросов.

Задержки τ_i – определяется как интервал времени между моментом начала передачи отправителям i-блока данных трафика соответствующего сервиса и моментом окончания приема этого же блока его получателем. Задержка τ_i, складывается из времен пакетизации, передачи и распространения передаваемых блоков данных по каналам связи между

узлами телекоммуникационной сети, а также из времени ожидания этих блоков в очередях промежуточных коммутаторов и маршрутизаторов сети.

В асинхронной телекоммуникационной сети задержка блоков данных может быть различной для каждого блока и представляет собой случайную величину, которая выражается следующим образом:

$$\tau_i = \tau_i^p + \sum_{k=1}^{M} \tau_{ik}^{pr} + \sum_{j=1}^{N} \left(\tau_{ij}^{sr} + \tau_{ij}^{wt} \right),$$

где τ_i^p – случайная величина времени пакетизации *i*-блока данных трафика; M – общее число каналов связи между двумя абонентами сервиса; N – общее число коммутационных устройств, расположенных между двумя абонентами сервиса; τ_{ik}^{pr} – случайная величина времени распространения *i*-блока данных трафика по k-каналу связи; τ_{ij}^{sr} – случайная величина времени обслуживания *i*-блока данных трафика в *j*-коммутационном устройстве; τ_{ij}^{wt} – случайная величина времени ожидания в очереди *i*-блока данных трафика в j-коммутационном устройстве.

Средняя задержка $\bar{\tau}$ определяется как среднее значение всех задержек передаваемых блоков данных,

$$\bar{\tau} = \frac{1}{N^{(b)}} \sum_{i}^{N^{(b)}} \tau_i ,$$

где $N^{(b)}$ – общее число доставленных блоков данных.

Вероятность потери $P^{(rs)}$ определяется отношением числа не доставленных адресату блоков данных к общему числу переданных.

Джиттер $\sigma^{(\tau)}$ – определяется как разница между $\tau^{(max)}$ и $\tau^{(min)}$ задержкой передачи блоков данных трафика соответствующего сервиса

$$\sigma^{(\tau)} = \tau^{(max)} - \tau^{(min)},$$

где

$$\tau^{(min)} = \bar{\tau} - \sqrt{D[\tau]}, \quad \tau^{(max)} = \bar{\tau} + \sqrt{D[\tau]},$$

а дисперсия

$$D[\tau] = \frac{1}{N^{(b)}} \sum_{i=1}^{N^{(b)}} \left(\tau_i - \bar{\tau} \right)^2 .$$

Влияние параметров транспортного соединения на качество представляемого абонентам сервиса представлено в табл. 1.2.

Значения времени доставки и джиттера доставки являются важными сетевыми характеристиками для услуг, осуществляемых в реальном масштабе времени.

Допустимые значения задержки, джиттера, вероятности потери пакета, вероятности установления соединения, времени установления соединения и вероятности разрыва соединения, определенные для основных типов мультимедийных услуг, полученные в результате исследований Европейского исследовательского центра в области телекоммуникаций (RACE - Research on Advanced Communication in Europe), приводятся в табл. 1.3.

Таблица 1.2. Влияние параметров транспортного соединения на качество предоставления сервиса

Параметры качества	Тип сервиса			
	телефонный	видеоконференции	видео по запросу	передача данных
Задержка	Значительное	Значительное	Умеренное	незначительное
Время установления соединения	Значительное	Значительное	Умеренное	Умеренное
Джиттер	Значительное	Значительное	Значительное	Незначительное
Вероятность потери	Умеренное	Умеренное	Умеренное	Значительное
Вероятность установления соединения	Значительное	Значительное	Значительное	Значительное
Вероятность разрыва соединения	Значительное	Значительное	Значительное	Незначительное

Примечание. Термины значительное, умеренное, незначительное означают: значительное - сильное влияние параметра телекоммуникационного соединения на качество предоставления сервиса. Большое значение этого параметра неприемлемо; умеренное - среднее влияние параметра телекоммуникационного соединения на качество предоставления сервиса. Небольшое значение этого параметра допустимо; незначительное - слабое влияние параметра телекоммуникационного соединения на качество предоставления сервиса. Большое значение этого параметра допустимо.

Таблица 1.3. Допустимые значения параметров качества обслуживания при передаче мультимедийного трафика

Тип сервиса	Параметры качества обслуживания				
	$t^{(cn)}$, с	$P^{(\eta)}$	τ, мс	$P^{(rs)}$	σ_τ, с
IP-телефония	0,5…1	10^{-3}	25…500	10^{-3}	100…150
Видеоконференция	0,5…1	10^{-3}	30	10^{-3}	30…100
Цифровое видео по запросу	0,5…1	10^{-3}	30	10^{-3}	30…100
Передача обычных данных	0,5…1	10^{-6}	50…1000	10^{-6}	–
Телевизионное вещание	0,5…1	10^{-8}	1000	10^{-8}	–

1.4. Характеристика трафика в сетях связи Российской Федерации. Прогнозирование трафика.

Потребности абонентов (пользователей) в обмене информацией в настоящее время удовлетворяются тремя доступными средствами - стационарной сетью, сотовой сетью подвижной (мобильной) связи, Интернет.

Таблица 1.4. Прогноз трафика для РФ

Трафик/год	2002	2007	2015
ТфОП	22,9	29,5	40,7
Сотовые сети	1,1	4,9	11,0
Интернет	1,0	6,2	120

Среднее значение удельного абонентского трафика для стационарной сети ТфОП составляет 0,1 Эрл. Распределение абонентского трафика в час наибольшей нагрузки (ЧНН) подчиняется нормальному закону.

Удельный абонентский трафик для сотовой сети подвижной связи по результатам измерений составляет 0,009 Эрл, а плотность распределения трафика подчиняется нормальному закону.

Удельный абонентский трафик пользователей Интернет составляет около 0,1 Эрл. Распределение абонентского трафика подчиняется логарифмически нормальному закону со среднеквадратичным отклонением σ = 0,45 Эрл.

Входящий и исходящий трафики для абонентов ТфОП и сетей подвижной связи считаются равными. Вместе с тем для пользователей Интернет практически весь трафик может быть отнесен к входящему. Для трехмерного вектора входящего трафика пользователя в мультисервисных сетях $Y_0 = \{Y_ф, Y_с, Y_и\}$ ($Y_ф$, $Y_с$, $Y_и$, соответственно, трафик ТфОП, сотовой сети подвижной связи, Интернет) имеют место следующие количественные характеристики нагрузки:

$$Y_Ф = 0{,}05 \text{ Эрл}, \quad \sigma(Y_Ф) = 0{,}225 \text{ Эрл};$$
$$Y_С = 0{,}0045 \text{ Эрл}, \quad \sigma(Y_С) = 0{,}067 \text{ Эрл};$$
$$Y_И = 0{,}1 \text{ Эрл}, \quad \sigma(Y_И) = 0{,}45 \text{ Эрл}.$$

С точки зрения оператора сети связи, наиболее интересными являются значения трафика за определенный период времени и на перспективу. Эти значения для сетей связи Российской Федерации в миллиардах минуто-занятий в месяц приведены в табл. 1.4.

Быстрыми темпами растет трафик сотовых сетей. Число сотовых телефонов уже сравнялось с числом стационарных. В соответствии с прогнозами, предельное число сотовых телефонов в Российской Федерации с учетом существующего народонаселения в 144,8 млн. или в форме телефонной плотности 122,4%. В то же время предельное значение телефонной плотности в условиях ускоренного роста сотовой связи составит около 40%. Сегодня и на ближайшую перспективу основная доля доходов операторов связи будет приходиться на голосовые услуги. Однако, учитывая бурный рост трафика передачи данных, операторы связи должны уже сейчас проектировать сети как мультисервисные.

Таблица 1.5. Распределение трафика по видам услуг

Категории услуг	Общий суточный трафик для крупных городов, Тбит	Общий трафик в ЧНН
Мультимедийные сообщения (MMS)	9,92	1,02
Голосовые услуги с расширенными возможностями (Rich Voice)	28,66	4,73
Информационные услуги	42,04	2,95
Мобильный Интернет	18,87	1,13
Мобильный доступ к локальным сетям Intranet/Extranet	78,14	6,70
Услуги определения местоположения (Location-Based Services)	1,30	0,09
Голосовые услуги	71,28	4,26
Всего:	249,21	20,88

Рассмотрим более подробно тенденции изменения трафика в сетях подвижной связи третьего поколения (UMTS), которые с полным основанием можно отнести к мультисервисным. В качестве примера возьмем страны Западной Европы и основные характеристики трафика, прогнозируемого на период до 2012 г.

В проведенных UMTS-Forum исследованиях трафика в сетях UMTS была использована модель, учитывающая:

– профили зон обслуживания (ячейка, город, страна, регион, в мировом масштабе);
– профили абонентов (демографические данные - возраст, денежный доход, область деятельности и род занятий);
– сегмент рынка услуг (корпоративные клиенты, массовый рынок);
– тип соединения (машина-машина, человек-человек, человек-машина, точка-точка, точка-много точек);
– тип мультимедийного трафика (с высокой и низкой скоростями передачи данных);

– качество услуг (по таким параметрам, как время задержки пакетов, скорость передачи данных, приоритет предоставления услуги);
– тип терминального оборудования (ноутбук, карманный компьютер, мобильный телефон) и др.

Исследование строилось на анализе ранее полученных данных о состоянии рынка (Previous Analysis from Market Study) и текущем его изучении и прогнозировании (Current Study).

Данные исследований, приведенные в табл. 1.5, характеризуют распределение общего трафика (Тбит = 10^{12} бит) в крупных городах по видам услуг. Большая его доля приходится на мобильный доступ к Интернет и локальным сетям, обычные голосовые услуги и информационные услуги. Однако приведенные в таблице услуги имеют характерное отличие по трафику в час наибольшей нагрузки (ЧНН). Так, наиболее выраженный пиковый характер трафика принадлежит мобильному доступу к Интернет (доступу к сетям Intranet/Extranet), обычным голосовым услугам и голосовым услугам с расширенными возможностями (Rich Voice). Суточное распределение трафика для некоторых услуг передачи данных показано на рис. 1.2-1.5.

Рассмотрим более подробно данные исследований по характеристике трафика для отдельных видов услуг передачи данных.

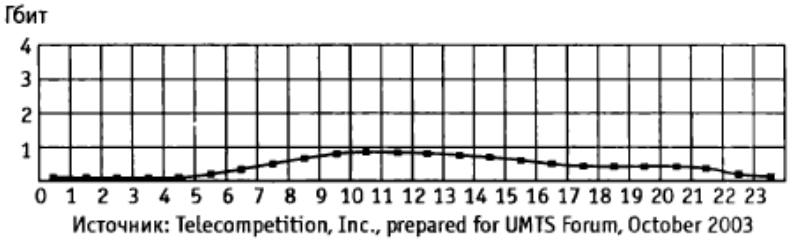


Рис. 1.2. Суточное распределение трафика MMS

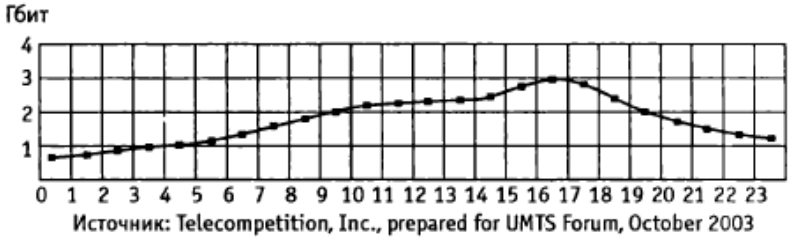


Рис. 1.3. Суточное распределение трафика информационных услуг

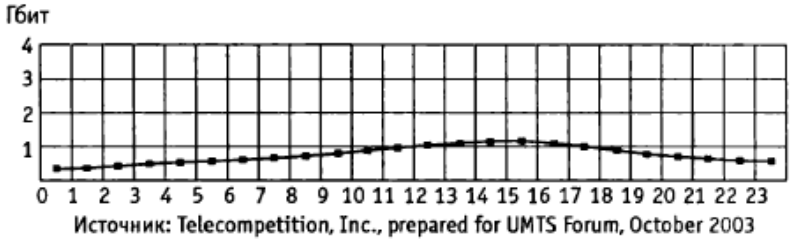


Рис. 1.4. Суточное распределение трафика мобильного Интернета

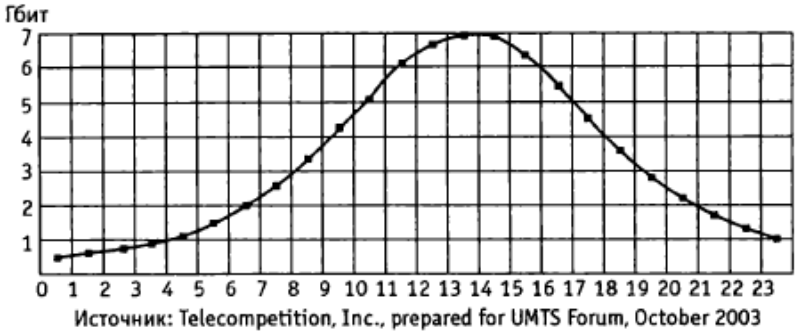


Рис. 1.5. Суточное распределение трафика мобильного доступа к Intranet/Extranet

Мобильный доступ к Интернет. Исследованы услуги для взрослых пользователей:

– электронная почта;

– «скачивание» видео- и аудио-файлов;

– мобильная торговля в Интернет;

для молодежи:

– электронная почта;

– «скачивание» мультимедийных файлов;

– мобильные игры.

В табл. 1.6 приведены данные о средних размерах файлов, передаваемых от пользователя и к пользователю при мобильном доступе в Интернет, а также асимметрии трафика в этих направлениях.

Услуги на основе определения местоположения абонента (LBS). Исследованы пять видов услуг LBS:

– информационные услуги по месту нахождения абонента (реклама, путеводитель);

– бизнес-приложения;

– навигация для автомобилистов;

– слежение за передвижением грузов;

– слежение за детьми, пожилыми людьми, животными.

Данные о средних размерах файлов, передаваемых от пользователя (UP) и (DL) к пользователю, приведены в табл. 1.7.

Услуги мультимедиа (MMS). Исследованы следующие виды услуг MMS:

Таблица 1.6. **Размеры файлов и асимметрия трафика**

Категория услуг	Линия «вверх» (UL), кбит	Линия «вниз» (DL), кбит	Асимметрия трафика (UL:DL)
E-mail	436	1746	1:4
Скачивание видео/ аудио	189	4725	1:25
Web Browsing	454	3175	1:7
MMS	189	4725	1:25
Мобильные игры	288	7200	1:25

Таблица 1.7. **Средние размеры файлов, передаваемых от пользователя к пользователю**

Категория услуг	Линия «вверх» (UL), кбит	Линия «вниз» (DL), кбит	Асимметрия трафика (UL:DL)
Реклама по месту абонента	0	100	0:1
Навигация (путеводитель)	83	100	1:1,2
Персональное отслеживание	0,01	0,02	1:1
Слежение за передвижением грузов	0,01	0,01	1:1
Телематические услуги	83	166	1:2

Таблица 1.8. **Средние размеры файлов при передаче MMS**

Типы терминалов	Категории сообщений	Длина сообщения, кбит
Обычные терминалы	Текст и графика с низким разрешением	10
	Фото	30
	Видео	100
Сложные терминалы	Текст и графика с низким разрешением	30
	Фото	100
	Видео	150

человек-человек:

– передача коротких видеоклипов;

– передача фото;

– передача текста с графическими вставками с невысоким разрешением;

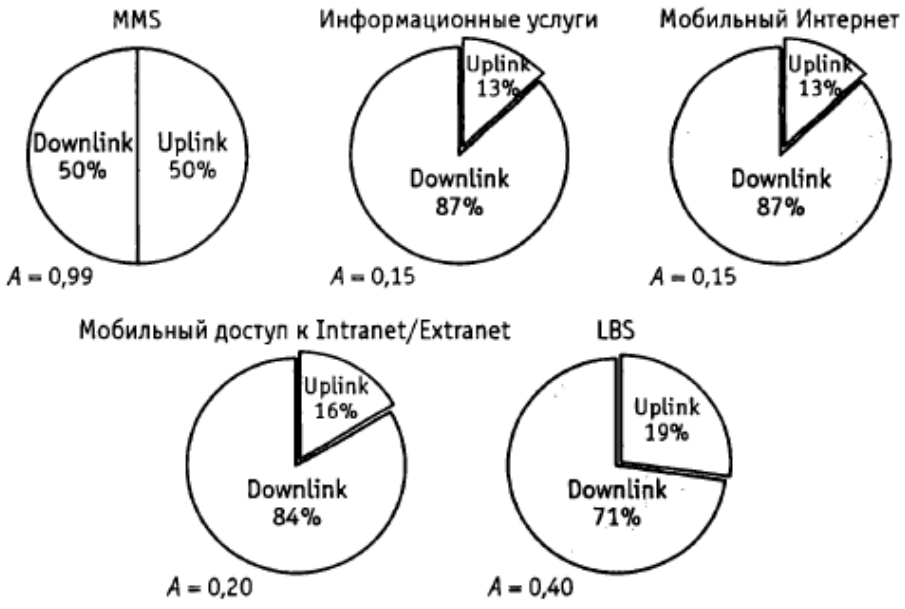
машина-машина (телематические услуги):

– просмотр объектов;

– передача информационно-развлекательных программ (к примеру, между различными серверами).

Данные о средних размерах файлов при передаче ММБ для различных типов терминалов приведены в табл. 1.8.

Часы набольшей нагрузки (трафика ММЭ) для корпоративных пользователей и массового рынка имеют ярко выраженное отличие: для корпоративных пользователей - это дневное время (10.00–13.00), для массового рынка - 19.00-21.00. При этом доля корпоративных ММ8-клиентов составляет 19%, доля массового рынка ММЭ – 12% от общего числа пользователей услугами Зв. Число передаваемых ими ММ8-сообщений в день составляет 5 и 11 соответственно. По типам ММЭ-сообщения распределяются следующим образом: 66% – текстовые сообщения с элементами графики невысокого разрешения, 24% – фото, 10% – сообщения с видеокомпонентами. По взаимодействию сетей: 32% – мобильная-мобильная, 40% - мобильная фиксированная, 28% – фиксированная-мобильная.



Источник: Telecompetition, Inc., prepared for UMTS Forum, October 2003

Рис. 1.6. Асимметричность трафика для различных видов услуг

Практически для всех видов услуг в сетях UMTS трафик имеет яр ко выраженный характер асимметричности. На рис. 1.6 показана асимметрия (А) трафика для различных услуг в каналах UP и DL в час наибольшей нагрузки.

Приведенные характеристики трафика в сетях UMTS позволяют сформировать представление о развитии рынка услуг 3G в Европе и в то же время ярко свидетельствуют о сложном его характере, который необходимо учитывать при проектировании и планировании сетей UMTS в России.

2. Технологические аспекты построения мультисервисных сетей

На сетях связи межрегиональных компаний (МРК) сегодня используются различные технологии. Как видно из материалов ЛОНИИС, представленных в табл. 3.1, большинство операторов избрали подход, ориентированный на использование в качестве базовой технологии группы технологий IP-MPLS-ATM. Для переноса IP-трафика большинство операторов склоняются к двум вариантам IP over SDH и MPOA (Multiprotocol over ATM).

Таблица 3.1. **Технологии на сетях МРК**

Межрегиональная компания	Базовая технология мультисервисной сети	Метод переноса IP-трафика		
		IP over SDH	MPOA	MPLS
ОАО «МГТС»	IP-MPLS-ATM	–	–	+
Центральный регион	ATM	+	–	+
Северо-Западный регион	IP-MPLS-ATM	+	+	–
Приволжский регион	IP-MPLS-ATM	+	+	–
Южный регион	ATM	+	+	–
Уральский регион	IP-MPLS-ATM	+	+	–
Сибирский регион	ATM	+	–	–
Дальневосточный регион	ATM	+	+	–

2.1. Физический уровень. Волновое уплотнение (WDM, DWDM, CWDM)

В настоящее время на сетях России используются преимущественно оптические волокна, соответствующие рекомендации G.652 и синхронные мультиплексоры уровня STM-16 (2,5 Гбит/с) без оптических усилителей с длиной участка регенерации до 100... 120 км. В то же время, волоконно-оптические линии обладают существенно более высокой пропускной способностью.

Действительно, теоретический предел пропускной способности оптического волокна (ОВ) в третьем окне прозрачности, т.е. на частоте порядка 193 ГГц, составляет примерно 3-109 ОЦК. В то же время для STM-16 число ОЦК 3-105, что составляет 0,01% от пропускной способности ОВ. Повысить коэффициент использования оптического волокна и, следовательно, решить проблему нехватки оптического волокна, можно за счет волнового уплотнения (Wave length-Division Multiplexing, WDM). В литературе, применительно к WDM, также встречается термин «спектральное мультиплексирование по волнам» и «волновое мультиплексирование».

В зависимости от числа волн, размещаемых в одном ОВ, различают технологии WWDM, CWDM, DWDM и HWDM. Так, если в ОВ организовано всего два канала с использованием окон прозрачности 1300 и 1500 нм, то это технология с разнесенным

спектральным мультиплексированием (Wide Band Wave Length Division Multiplexing, WWDM).

Системы грубого волнового мультиплексирования (Coarse WDM) работают в спектральном диапазоне 1300... 1650 нм, используя 16 оптических несущих, интервалы между которыми 20 нм. В DWDM используется до 160 оптических несущих с выделением для каждого из каналов полосы 25...50 ГГц.

Главное достоинство технологий WDM заключается в том, что они позволяют преодолеть ограничения на пропускную способность канала и существенно увеличить скорость передачи данных. Причем используются уже проложенный волоконно-оптический кабель и стандартная аппаратура временного мультиплексирования. Благодаря WDM удается организовать двустороннюю многоканальную передачу трафика по одному волокну (в обычных линиях используется пара волокон - для передачи в прямом и обратном направлениях).

Существенно и то, что в сетях SDH появилась возможность выбирать для отдельного канала значение скорости (уровень иерархии), не зависящее от скорости других каналов, и затем использовать разные методы передачи. Наконец, распространению WDM способствуют последние технологические достижения: создание узкополосных полупроводниковых лазеров, имеющих ширину спектра излучения менее 0,1 нм, широкополосных оптических усилителей и оптических фильтров для разделения близких каналов.

Может сложиться представление, что технологии WDM являются универсальным решением проблемы увеличения пропускной способности, некой панацеей от всех бед, с которыми сталкиваются пользователи глобальных сетей. Между тем применение WDM тормозится рядом факторов как экономического, так и чисто технического характера.

Если говорить об экономической стороне дела, то внедрение WDM в местных сетях сдерживается высокой стоимостью соответствующей аппаратуры, особенно передающих устройств, и сложностью коммутации трафика. Вместе с тем исследования показывают, что решения на базе WDM могут оказаться экономически эффективными и в сетях меньшего масштаба. Для этого, в частности, в них должны применяться недорогие мультиплексоры ввода/вывода, устанавливаемые в местах сопряжения местных и опорных сетей.

Фактор высокой стоимости аппаратуры оказывается еще более существенным для реализации технологии DWDM. При использовании близких частот требуются узкополосные полупроводниковые лазеры с высокой стабильностью длины волны генерируемого излучения, которые являются наиболее дорогим элементом DWDM-

систем, сдерживающим распространение последних. Тем не менее основными преимуществами технологий DWDM остаются:

- высокие скорости передачи, и как следствие, высокий коэффициент использования ОВ;
- возможность обеспечения 100%-ной защиты на основе кольцевой топологии и простого наращивания каналов в оптической магистрали.

В настоящее время сети DWDM применяются для построения высокоскоростных транспортных сетей операторов национального масштаба, на основе топологий «точка-точка» или «кольцо» и мощных городских транспортных магистралей, которые могут использоваться большим количеством пользователей с потребностями в высоких скоростях передачи и использующих различные протоколы.

Специалисты по организации оптических сетей связи отмечают, что при использовании WDM отсутствуют многие ограничения и технологические трудности, свойственные TDM. Для лучшего использования пропускной способности ОВ вместо увеличения скорости передачи в едином составном канале, как это реализовано в TDM, в технологии WDM увеличивают число каналов (длин волн), применяемых в системах передачи.

Повышение скорости передачи при использовании технологии WDM осуществляется без дорогостоящей замены оптического кабеля. Применение технологий WDM позволяет сдавать в аренду не только оптические кабели или волокна, но и отдельные длины волн, т.е. реализовать концепцию «виртуального волокна». По одному волокну на разных длинах волн можно одновременно передавать самые разные приложения - кабельное телевидение, телефонию, трафик Интернета, «видео по требованию» и т.д. Как следствие, часть волокон в оптическом кабеле можно использовать для резерва.

Применение технологий WDM позволяет исключить дополнительную прокладку оптических кабелей в существующей сети. Даже если в будущем стоимость волокна уменьшится за счет использования новых технологий, волоконно-оптическая инфраструктура (проложенное волокно и установленное оборудование) всегда будет стоить достаточно дорого. Для ее эффективного использования необходимо иметь возможность в течение долгого времени увеличивать пропускную способность сети и менять набор предоставляемых услуг без замены оптического кабеля. Технологии WDM предоставляют такую возможность.

Технологии WDM используются пока в основном на линиях связи большой протяженности, где требуется большая полоса пропускания. Сети городского и регионального масштаба и системы кабельного телевидения потенциально также являются широким рынком для технологий WDM.

В то же время применение технологий DWDM предъявляет существенно более высокие требования к оборудованию и компонентам линии и, соответственно, к точности расчета их параметров. Чтобы возможности ВОЛС соответствовали запросам рынка, важно правильно спланировать их развитие. Это позволит распределить затраты на строительство ВОЛС во времени и наращивать их емкость с учетом запросов потребителей.

2.2. Технологии канального, сетевого и транспортного уровней

2.2.1. Технология IP-сетей

Структура стека протоколов TCP/IP. Архитектура протоколов Интернета четырехуровневая. Появившуюся намного позже семиуровневую архитектуру протоколов эталонной модели ISO можно рассматривать как дальнейшее развитие TCP/IP - декомпозицию двух уровней TCP/IP. Действительно, отличие двух архитектур состоит в том, что три высших уровня (прикладной, представления данных, сеансовый) модели OSI в архитектуре TCP/IP объединены в один - прикладной (рис. 3.20). Уровень сетевых интерфейсов TCP/IP соответствует двум уровням OSI - канальному и сетевому.

Прикладной уровень TCP/IP поддерживает традиционные услуги:

– электронная почта и обмен новостями, которые реализуются с помощью простого протокола передачи электронной почты SMNP (Simple Mail Transfer Protocol); почтовых протоколов IMAP (Internet Message Access Protocol), POP (Post Office Protocol) и X.400; сетевого протокола обмена новостями NNTP (Network News Transfer Protocol);

– виртуальный терминал реализуется с помощью протокола Telnet;

– передача файлов осуществляется с помощью протоколов FTP (Fail Transfer Protocol), TFTP (Trivial File Transfer Protocol) и NFS (Network File Systems);

– справочные службы реализуются с помощью системы доменных имен DNS (Domain Name System) и X.500;

– вспомогательные протоколы: получения собственных идентификаторов – BOOTP, времени – NTP (Network Time Protocol), диагностики – Echo и информации о системе – Finger.

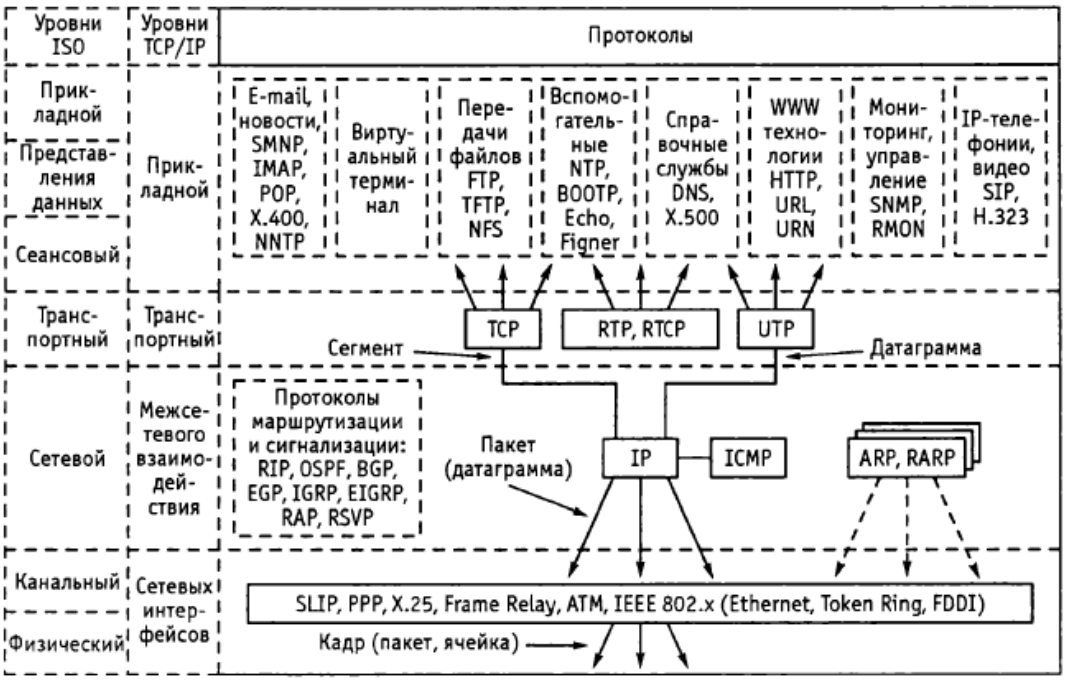


Рис. 3.20. Структура стека протоколов TCP/IP

В середине 1990-х годов активно внедрялись услуги, базирующиеся на технологии WWW (World Wide Web), основанной на протоколе передачи гипертекста (Hypertext Transfer Protocol, HTTP) с использованием URL (Universal Resource Locator) и URN (Universal Resource Names).

Сегодня популярны услуги пакетной IP-телефонии на базе протоколов SIP (Session Initiation Protocol), RTP (Real-time Transport Protocol), RTCP (Real-rime Transport Control Protocol), рекомендаций H.323 и др.

Особое место в стеке занимают протоколы мониторинга и управления:

– SNMP (Simple Network Management Protocol);

– RMON (Remote Monitoring).

С помощью этих протоколов отслеживают состояние сети и проводят ее администрирование.

Для сетевого взаимодействия большинство приложений пользуются услугами протоколов транспортного уровня TCP и UDP. Протокол TCP гарантирует надежную полнодуплексную передачу сегментов данных с предварительным установлением логического соединения.

Протокол датаграмм пользователя UDP (User Datagram Protocol) обеспечивает передачу датаграмм без установления соединения, что не гарантирует их доставку.

Передачу пакетов между сетями различной архитектуры обеспечивает основной протокол стека - IP. Датаграммный протокол IP не гарантирует надежной передачи

пакетов, что, однако, увеличивает пропускную способность при передаче данных через множество сетей.

На сетевом уровне также используются:

– диагностический протокол ICMP (Internet Control Message Protocol), который передает сообщения узлам сети об ошибках и сбоях в передаче;

– протоколы разрешения проблемы адресов: ARP (Address Resolution Protocol) трансформирует IP адрес в физический адрес узла сети (MAC - адрес станции); RARP (Reverse Address Resolution Protocol) выполняет обратную функцию, т. е. с помощью MAC адреса определяет IP адрес.

Работу сетевого уровня поддерживают ряд протоколов маршрутизации и сигнализации: RIP (Routing Internet Protocol), OSPF (Open Shortest Path First), IGRP (Interior Gateway Routing Protocol), EIGRP (Enhanced IGRP), BGP (Border Gateway Protocol), RAP (Routing Access Protocol), RSVP (Resource Reservation Protocol) и др.

Стек протоколов TCP/IP взаимодействует на канальном уровне с большим количеством протоколов и сетевых технологий, которые инкапсулируют пакеты IP протокола. На сегодня вопросам взаимодействия Интернета с другими сетями посвящено более 290 документов RFC.

Чтобы выяснить, как выполняется передача данных с помощью любой технологии, необходимо рассмотреть следующее:

1) как формируется и распределяется адресное пространство сети;

2) логические характеристики (назначение полей пакетов) основных протоколов IP-технологии;

3) основные процедурные характеристики протоколов, которые обеспечивают нормальное функционирование процесса передачи информации;

4) каким образом решается вопрос определения путей передачи данных от отправителя к получателю, т. е. как маршрутизируются пакеты.

Опуская рассмотрение вопросов 1-3, перейдем к пункту 4.

Методы маршрутизации. Протоколы маршрутизации (см. рис. 3.20) представляют собой наиболее сложную группу протоколов Интернет, которая динамично развивается. Под маршрутизацией понимают решение задачи поиска оптимального пути от отправителя информации к ее получателю. Оборудование, которое решает эту задачу, называют маршрутизаторами (router). В IP-сетях (Интернет и др.) главным параметром маршрутизации является адрес в IP-протоколе. Сеть Интернет организована как совокупность взаимосвязанных между собою автономных систем или доменов (domains). Автономная система включает в себя IP-сети, которые имеют единое административное

управление и общую политику (стратегию) маршрутизации (policy routing). В пределах домена используются протоколы внутренней (Interior Gateway Protocol, IGP), а между ними протоколы внешней маршрутизации (Exterior Gateway Protocol, EGP).

При рассмотрении маршрутизации выделяют две проблемы:

– определение и распространение сведений о маршрутах в сети (домене), которые связаны с реализацией политики маршрутизации и регламентируются алгоритмами «вектор-расстояние» (distance vector) и «состояния каналов» (link state);

– продвижение по установленным маршрутам пакетов от отправителя к получателю, которое определяется алгоритмами поэтапной маршрутизации (hop-by-hop routing) и маршрутизацией от источника (source specified routing).

Алгоритм «вектор-расстояние» базируется на том, что каждый объект (маршрутизатор), который принимает участие в маршрутизации, сохраняет в своей базе информацию обо всех адресах сети и метрику - расстояние до получателя информации. Объекты обмениваются между собой маршрутными базами. При принятии решения о маршруте передачи пакета оценивается каждый путь к объекту и выбирается наилучший. Этот алгоритм реализован в протоколах маршрутизации RIP и IGRP.

Алгоритм состояния каналов. Здесь на первом этапе каждый объект формирует топологическую базу (link state database) и строит граф связей сети, который описывает ее топологию с учетом того, что каждая связь (канал) характеризуется своей метрикой. Объекты, обмениваясь базами, обновляют сведения о сетях. На втором этапе объект решает проблему определения оптимального пути к каждой известной ему сети. Этот алгоритм реализован в протоколах OSPF и EIGRP.

Поэтапная маршрутизация. В этом методе каждый маршрутизатор принимает независимое решение о продвижении пакета на основании адреса получателя и информации, которая находится в маршрутной базе.

Маршрутизация от источника. Маршрут формируется отправителем пакета и записывается в каждый пакет, который отправляется в сеть.

Протокол RIP. Протокол RIP - это протокол внутренней маршрутизации, предназначенный для небольших доменов. Первая версия протокола RIP стандартизирована RFC 1058, а вторая - RFC 1722 и др. RIP для передачи сообщений использует протокол UDP (порт 520). Сообщения RIP состоят из IP-адреса сети и числа шагов (маршрутизаторов) к ней. Максимальное количество шагов - 15. В одном сообщении RIP может быть информация о 25 сетях. Маршрутизатор, на котором работает RIP, получая сообщения RIP от других маршрутизаторов, строит свою таблицу маршрутизации, в которой прописаны пути к другим сетям. Обмениваясь RIP

сообщениями, маршрутизаторы каждые 30 секунд обновляют свои таблицы маршрутизации и с их помощью выполняют продвижение пакетов по сети.

Недостатки протокола:

– не всегда выбирается самый эффективный маршрут;

– из-за медленной сходимости образуются логические петли и медленно возобновляются таблицы после сбоя в работе маршрутизатора;

– используются широковещательные рассылки большого количества служебной информации (таблицы маршрутизации), которые загружают сеть;

– ограничен размер домена маршрутизации (15 переходов);

– не работает с адресами подсетей и не различает автономных систем.

Протокол OSPF стандартизирован в RFC 1370, 1578, 1793, 1850, 2328. Применяется для внутренней и внешней маршрутизации, используя алгоритм состояния каналов. Может обслуживать автономную систему, которая состоит из нескольких зон. Протокол OSPF значительно эффективнее протокола RIP. Маршрутизатор, на котором работает OSPF, решает проблему оптимизации маршрутов, анализируя граф сети с метрикой, характеризующей качество обслуживания.

Основными параметрами метрики являются: пропускная способность, задержка, надежность, а дополнительными - загрузка канала, безопасность. Маршрутизаторы обмениваются сообщениями только при изменении топологии сети. OSPF быстрее, чем RIP, перестраивает маршрутную таблицу.

К основным преимуществам OSPF относятся:

– применение групповой передачи коротких сообщений при изменении топологии сети, что снижает непроизводительную загрузку сети;

– поддержка распределения информации по параллельным каналам в зависимости от их пропускной способности, что улучшает работу сети в целом (более подробно OSPF дано в приложении).

Протоколы IGRP и EIGRP. Эти протоколы разработаны фирмой Cisco Systems и используются для внутренней маршрутизации. IGRP использует алгоритм «вектор-расстояние», имеет значительно лучшие характеристики, чем протокол RIP, в частности:

– надежно работает в сетях сложной топологии;

– обладает лучшей, чем RIP, сходимостью;

– значительно снижает объем передачи служебной информации;

– распределяет информацию между каналами с одинаковыми метриками.

В метрику протокола входят следующие параметры канала: пропускная способность, задержка, нагрузка, надежность. Эти параметры могут меняться в широких пределах. Например, пропускная способность может изменяться от 1200 бит/с до 10 Гбит/с.

EIGRP - это протокол, который объединяет все преимущества алгоритмов «вектор-расстояние» и «состояния каналов». Протокол реализован на базе алгоритма распределенного обновления - (Distributed Update Algorithm, DUAL), который позволяет маршрутизатору быстро возобновлять работу после изменения сетевой топологии. Протокол имеет:

– возможность находить соседа;

– алгоритм DUAL;

– усовершенствованный механизм инкапсуляции сообщений в IP.

В первую очередь маршрутизатор определяет достижимость своего «соседа» – маршрутизатора, который напрямую взаимодействует с ним. Для этого он периодически посылает пакет Hello. Затем алгоритм DUAL по полученной от «соседей» информации о маршрутах определяет оптимальный маршрут передачи нагрузки, который не является частью петли маршрутизации.

Протоколы EGP и BGP принадлежат к протоколам внешней маршрутизации сети Интернет. С помощью EGP взаимодействуют выделенные маршрутизаторы разных автономных систем, которые собирают информацию о системе с помощью внутренних протоколов маршрутизации.

К недостаткам EGP можно отнести следующее: не используется метрика, т.е. не выполняется интеллектуальная маршрутизация; не отслеживается появление петель маршрутов; служебные сообщения имеют большой размер.

В последнее время вместо EGP используют более совершенный протокол BGP, который, в свою очередь, для передачи служебных сообщений использует протокол TCP. Это повышает надежность при взаимодействии между автономными системами, поскольку TCP гарантирует доставку маршрутной информации. BGP полностью исключает недостатки протокола EGP. В качестве метрики используется скорость передачи в канале, его надежность и т.п. На сегодня BGP (третья версия) - это основной протокол сети Интернет, который определяет маршруты к удаленным автономным системам.

2.2.2. Технология ATM

Технология ATM считается наиболее «мультисервисной». Она позволяет достаточно эффективно решать задачи объединения сетей, построенных с использованием различных

технологий передачи данных, обеспечения необходимого качества обслуживания и др. Все операторы МРК используют эту технологию (см. табл. 3.1) и основная конкуренция при создании МСС ожидается между технологиями ATM и MPLS. Большинство специалистов предрекают победу MPLS.

Напомним, что в ATM используются пакеты небольшой длины фиксированного размера (53 байта), называемые ячейками, и очень простые функции в транзитных узлах. Обнаружение и исправление ошибок осуществляется только в заголовке. Для содержимого информационных ячеек никакой проверки и восстановления не применяется, и используется передача информации, ориентированная на соединение. Реализация ATM обычно осуществляется аппаратным обеспечением. Все это в сочетании с статистическим мультиплексированием уменьшает время задержек, что особенно важно при передаче трафика реального времени.

Технология ATM предоставляет методы управления трафиком и механизмы качества обслуживания. Это означает, что в сетях ATM могут быть зарезервированы ресурсы, гарантирующие требуемые значения пропускной способности, задержки передачи и уровня потерь ячеек. Стек протоколов ATM. В стеке протоколов ATM (рис. 3.21) различают следующие уровни: адаптации, ATM и физический. Уровень адаптации ATM (ATM Adaptation layer, AAL) делится на два подуровня конвергенции (Convergence Sub-layer, CS) и сегментации и восстановления (Segmentation And Reassebly, SAR). Уровень адаптации ATM по сути является интерфейсом между приложениями пользователя и уровнем ATM и обеспечивает поддержку четырех различных групп (классов) приложений.

Рис. 3.21. Стек протоколов ATM

Все приложения используют один и тот же подуровень SAR, но каждый тип приложений реализует свой собственный специфический подуровень CS.

После краткого рассмотрения подуровней AAL перейдем к их более полному описанию.

Подуровень конвергенции (CS) отвечает за получение протокольного модуля данных (Protocol Data Unit, PDU) от вышележащих уровней и их адаптацию, обычно за счет добавления служебной информации для дальнейшего представления уровню SAR. Так как

каждый тип трафика требует специфической обработки, различают четыре типа уровней адаптации AAL.

Задачей подуровня SAR является формирование модулей длиной 48 октетов, которые становятся полезной нагрузкой ячеек ATM. Правило функционирования подуровня SAR заключается в том, что ничто не покидает подуровень, если его длина не равняется 48 октетам. В некоторых случаях в подуровне SAR могут добавляться свои собственные данные к модулю PDU подуровня CS, в других - он просто «нарезает» модули PDU подуровня CS в модули по 48 октетов и передает их вниз на уровень ATM.

Уровень ATM соответствует нижней части канального уровня модели OSI. Его основной задачей является коммутация ячеек способом, подходящим для осуществления их передачи между отправителем и получателем. Основным модулем на уровне ATM является ячейка. Как упоминалось выше, длина ячейки составляет 53 октета, из которых 48 предназначены для переноса полезной нагрузки, оставшиеся 5 октетов - для служебной информации уровня ATM, т. е. заголовка ячейки ATM.

Сети ATM на физическом уровне обычно используются SDH.

На рис. 3.22 представлена обобщенная структура операций, осуществляемых на различных уровнях ATM. Здесь H - означает заголовок (Head), T - концевик (Trailer).

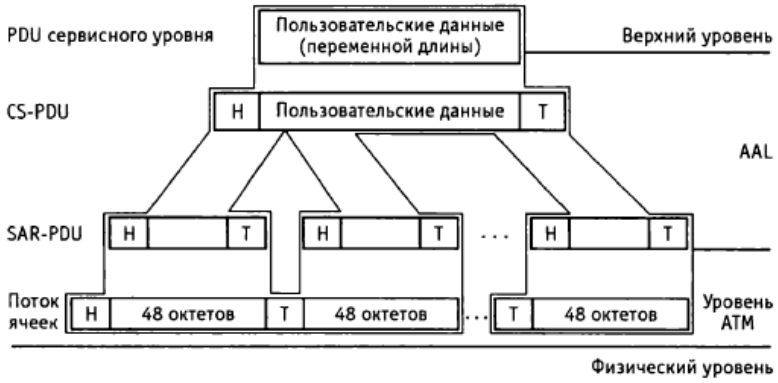


Рис. 3.22. Операции протокола ATM

Модуль PDU протокола вышележащего уровня (например, IP-пакет) поступает на подуровень CS уровня адаптации. Там путем добавления служебной информации к модулю PDU вышележащего уровня формируется модуль CS-PDU. Каждый тип AAL имеет свой специфический подход к формированию этой служебной информации. После того как модуль CS-PDU сформирован, он передается подуровню SAR. Основная задача подуровня SAR заключается в сегментации модуля CS-PDU на блоки длиной 48 октетов. На уровне ATM к ним добавляется 5 октетов заголовка ячейки. Затем ячейки преобразуются в формат соответствующего протокола физического уровня. На принимающей стороне процесс, показанный на рис. 3.22, происходит в обратном порядке.

Классы обслуживания AAL (рис. 3.23). Различают четыре класса обслуживания, охватывающие определенные типы трафика, которые, по мнению создателей ATM, встречаются в настоящее время или могут появиться в будущем. Услуга класса A является сервисом с установлением соединения. Он поддерживает трафик с постоянной скоростью битов, который требует сквозной синхронизации. Этот класс услуг обычно используется для передачи потоковых речевых и видеосигналов без сжатия.

Трафик (класс услуги)	Звук (A)	Видео со сжатием (B)	Данные, FR, ... (C)	LAN (D)
Синхронизация	Требуется		Не требуется	
Скорость	Постоянная	Переменная	Переменная доступная	Переменная неопределенная
Соединение	Установление соединения, виртуальные каналы			Без соединения
Тип AAL	AAL1	AAL2	AAL3/4	
			AAL5	
Временной параметр	Реальное	Реальное/ нереальное	Нереальное	

Рис. 3.23. Классы обслуживания AAL

Услуга класса B является сервисом с установлением соединения и отличается от сервиса класса A только поддержкой сигналов с переменной скоростью передачи битов. Для трафика, который использует сервис класса B, также требуется синхронизация. Сигналы, которым необходима услуга класса B, включают сжатые и разбитые на пакеты речевые и видеоданные.

Услуга класса C является услугой с установлением соединений и предназначена для поддержки трафика с переменной скоростью передачи данных, не требующих поддержки синхронизации. Трафик, который использует услугу класса C, может включать, но не ограничен данными, предполагающими установление соединений, такими как кадры Frame Relay.

Услуга класса D поддерживает трафик данных, ориентированный на отсутствие соединений. Такой трафик характеризуется изменчивостью скорости передачи битов и отсутствием требований к сквозной синхронизации. Примером такого трафика являются пакеты протокола IP.

Четырем типам класса обслуживания первоначально соответствовали четыре типа протоколов адаптации ATM. Впоследствии протоколы AAL3 и AAL4 были заменены протоколом AAL3/4, который оказался неэффективным. Это привело к разработке нового протокола, получившего название SEAL (Simple Efficient Adaptation Layer – простой эффективный протокол адаптации). ATM-форум после принятия этого протокола дал ему название AAL5. Будущее, по-видимому, принадлежит AAL5.

2.2.3. Технология Ethernet

Сегодня более 85% локальных сетей выполнены по технологии канального уровня Ethernet. Отличительной особенностью канального уровня Ethernet является его разбиение на два подуровня: управления доступом к среде (Media Access Control, MAC) и управления логическим каналом (Logical Link Control, LLC). Подуровень MAC определяет алгоритм доступа к среде, адресацию рабочих станций в сети, а также поддерживает функции совместного использования физической среды. Подуровень LLC поддерживает следующие службы:

– обслуживания без установления соединения и без подтверждения;

– обслуживания, ориентированного на соединение;

– обслуживания с подтверждением без установления соединения.

Главным недостатком технологии является конкурентный доступ к среде. В то же время это является и достоинством, позволяющим существенно уменьшить стоимость оборудования. При этом ограничения по дальности, традиционно относящие Ethernet к технологии локальных сетей, в случае использования ОВ снимаются: Ethernet становится технологией городских и глобальных сетей.

В своем развитии технология Ethernet прошла ряд эволюционных этапов (рис. 3.24) и из простой шинной архитектуры (10 Мбит/с Ethernet) превратилась в технологию реализации сегментов с увеличением скорости до 10 Гбит/с и более. При этом следует заметить, что пропускная способность Ethernet каждые 5-7 лет увеличивается в 10 раз. В настоящее время десятигигабитный Ethernet (Gigabit Ethernet, GE) использует технологию DWDM на физическом уровне.

В настоящее время GE прочно вошел в перечень базовых сетевых технологий для современных цифровых сетей. Технология GE прошла этап первичной стандартизации и представлена на рынке новейшей аппаратурой - маршрутизаторами/коммутаторами GE, выпускаемыми ведущими производителями ЦСП, и уже находит применение при построении современных высокоскоростных сетей передачи данных.

Интерфейс маршрутизаторов/коммутаторов GE 1000Base-X основывается на стандарте физического уровня Fibre Channel (FC) – технологии взаимодействия рабочих станций, суперкомпьютеров, устройств хранения и периферийных узлов, имеющей 4-уровневую архитектуру. Два нижних уровня FC-0 (интерфейсы и среда) и FC-1 (кодирование/декодирование) перенесены в GE, что значительно сократило время на разработку оригинального стандарта Gigabit Ethernet. В модели ВОС/OSI стандарту GE соответствуют канальный и физический уровни.

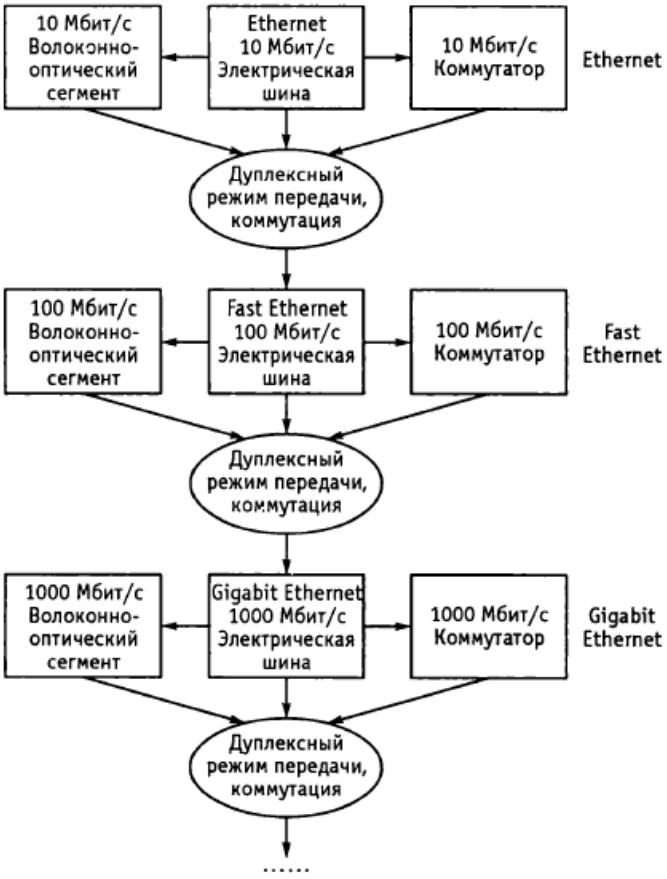


Рис. 3.24. Эволюция технологии Ethernet

Оборудование Ethernet всех поколений совместимо друг с другом и использует открытые стандарты. Поверх Ethernet возможна передача голоса, данных, видео. Технология многоадресной рассылки позволяет доводить до каждого пользователя неограниченное количество телевизионных и телефонных каналов, а скорость среды передачи данных дает возможность обеспечивать доступ пользователей к услугам на скоростях в сотни мегабит и гигабит в секунду уже сегодня.

Как отмечалось выше, большинство традиционных операторов используют в своих транспортных сетях технологию SDH. Отсюда вытекает вывод о целесообразности разворачивания мультисервисных сетей поверх существующих сетей SDH. Идея демонтировать SDH и перейти напрямую на ОВ с использованием WDM вряд ли кому то придет в голову, хотя бы из экономических соображений. Однако по своей идеологии мультисервисная сеть отличается от сети SDH, в первую очередь, по набору ориентированных на область применения функциональных свойств.

В данном случае наиболее проблемным является участок доступа. Развитие транспортной сети на этом участке обеспечивает задел для развития сети в будущем.

Операторам телематических служб, которые предоставляют в основном услуги широкополосной передачи данных и только начинают строить собственные транспортные сети, следует обратить внимание на технологии GE/10GE. В отличие от традиционных

операторов, компании, реализующие телематические услуги, обычно не имеют собственной инфраструктуры SDH, но располагают хорошо развитым участком доступа.

Рассмотрим далее отдельные вопросы, представление о которых необходимо иметь при выборе оборудования Ethernet поверх SDH (Ethernet over SDH).

Инкапсуляция Ethernet. Основная проблема инкапсуляции трафика Ethernet заключается в том, что блоки данных (контейнеры) SDH передаются безостановочно, независимо от наличия или отсутствия полезной нагрузки, в то время как кадры Ethernet передаются только при наличии нагрузки. Существует несколько процедур инкапсуляции трафика Ethernet в контейнеры SDH.

Стандартизованы процедуры GFP (Generic Framing Procedure – общая процедура кадрирования) и X.86 (известна как LAPS – протокол доступа к каналу SDH). Какая из них лучше? Обе инкапсулируют трафик Ethernet в контейнеры SDH, но по-разному. Процедура GFP выполняет инкапсуляцию более эффективно и, в отличие от LAPS, является детерминированной. Данные процедуры подробно описаны в стандартах ITU-T X.86 (LAPS) и ITU-T G.7041 (GFP). Отметим, что некоторые производители до сих пор используют свои собственные разработки.

Сцепка виртуальных контейнеров. Основной проблемой при передаче трафика Ethernet в сетях SDH является несогласованность скорости передачи кадров Ethernet с размерами контейнеров SDH.

Решить эту проблему помогает сцепка (concatenation) виртуальных контейнеров. Различают два вида сцепок: смежные (contiguous) и виртуальные (virtual). Виртуальная сцепка позволяет увеличивать пропускную способность сцепки виртуальных контейнеров с шагом VC-12 (2,176 Мбит/с), в то время как смежная сцепка может быть применена только начиная с уровня VC-4 (149,76 Мбит/с). Типы смежных и виртуальных сцепок представлены в табл. 3.8.

Нужно отметить, что при использовании виртуальных сцепок нет необходимости проводить какие-либо изменения в транзитных узлах существующей сети SDH, в то время как применение смежных сцепок требует замены оборудования всех транзитных узлов. Виртуальные сцепки имеют и другие достоинства, которые станут ясны, когда мы рассмотрим вопросы защиты трафика SDH. Все это позволяет утверждать, что следует использовать виртуальные сцепки контейнеров SDH. Процедура виртуальной сцепки описана в ITU-T H.707.

Регулирование емкости соединения. Функция автоматической защиты каналов SDH, описанная в документе ITU-T G.841, определяет три типа каналов:

– рабочий канал (если рабочее соединение по каким-либо причинам будет разорвано, трафик будет переключен на защитный канал в течение 50 мс);

– защитный канал - переносит трафик в случае отказа основного рабочего канала: данное соединение «простаивает», когда основной рабочий канал функционирует нормально, однако документ G.841 описывает использование защитного канала для передачи дополнительного трафика и в том случае, когда основной канал функционирует нормально;

– незащищенный канал.

Таблица 3.8. **Типы смежных и виртуальных сцепок**

SDH-контейнеры	Тип	Полезная нагрузка, Мбит/с
VC-12	Low Order	2,176
VC-3	High Order	48,384
VC-4	High Order	149,76
Contiguous Concatenation (смежная сцепка)		
VC-4-4c	High Order	599,04
VC-4-8c	High Order	1198,08
VC-4-16c	High Order	2396,16
VC-4-64c	High Order	9584,64
Virtual Concatenation (виртуальная сцепка)		
VC-12-Xv	Low Order	X·2,176 (X = 1...63)
VC-3-Xv	Low Order	X·48,384 (X = 1...255)
VC-4-Xv	High Order	X·149,76 (X = 1...255)

Потеря хотя бы одного незащищенного виртуального контейнера VC-12, входящего в виртуальную группу, приводит к потере всей группы. Для того чтобы этого не происходило, используется протокол LCAS (Link Capacity Adjustment Scheme - схема регулирования емкости соединения). Протокол LCAS выполняет функцию защиты трафика Ethernet, передаваемого по сетям SDH, и позволяет более гибко работать с этим трафиком.

Рассмотрим ситуацию, когда трафик передается с использованием нескольких каналов, объединенных в единую группу (рис. 3.25). При отказе незащищенного канала 1 трафик всей виртуальной группы будет потерян, но механизм LCAS отследит потерю соединения. Затем процедура GEP мгновенно изменит скорость и восстановит соединение с использованием оставшихся контейнеров, входящих в виртуальную группу. Это позволит задействовать каналы 2, 3 и 4 для передачи трафика без снижения отказоустойчивости сети. Время реакции LCAS для контейнеров VC-4 не превышает 64 мс, а для контейнеров VC-12 - 128 мс.

Как видно из данного примера, использование LCAS позволяет динамически распределять трафик между рабочими каналами, а также задействовать каналы защиты для передачи дополнительного трафика. Протокол LCAS описан в ITU-T G.7042.

Дополнительная функциональность Ethernet. Описанные выше возможности позволяют создать соединения Ethernet «точка-точка» E-line (рис. 3.26). Но это всего лишь выделенные каналы Ethernet, и не более того, сеть SDH является чистым транспортом для трафика Ethernet.

Строя сеть таким образом, оператор должен обеспечить число Ethernet-портов, равное числу соединений, а также использовать дополнительное оборудование для коммутации пакетов Ethernet. Кроме того, рано или поздно оператор столкнется с нехваткой ресурсов транспортной сети, хотя среднестатистическая загруженность каждого из каналов будет при этом мала. Следовательно, необходимо обеспечить возможность обработки пакетов Ethernet в соответствии с действующими стандартами (IEEE 802.1 D, 802.1 P и др.), что позволит более гибко работать с трафиком Ethernet и разделять его не только на уровне портов, как это делается сейчас многими операторами, но и на уровне Ethernet.

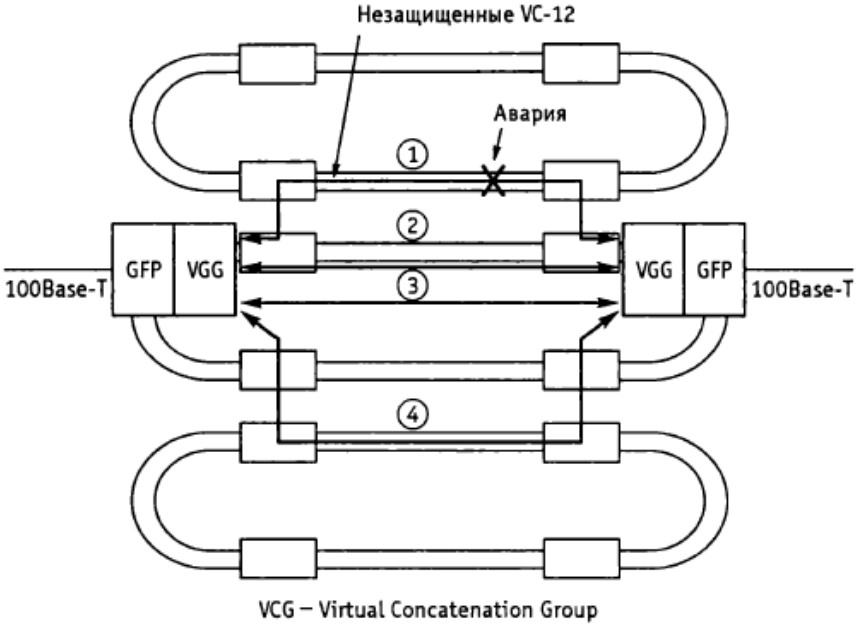


Рис. 3.25. Пример организации защиты трафика Ethernet с использованием технологии LCAS

Технология Ethernet позволяет разделять трафик абонентов или услуг в общем канале виртуальных локальных сетей (Virtual Local Area Network, VLAN). Большинство абонентов уже широко используют все достоинства данного метода, для реализации которого необходимо обеспечить беспрепятственную передачу идентификаторов VLAN через транспортную сеть. Механизмы создания собственных VLAN, а также приоритизации трафика Ethernet должны соответствовать существующим стандартам.

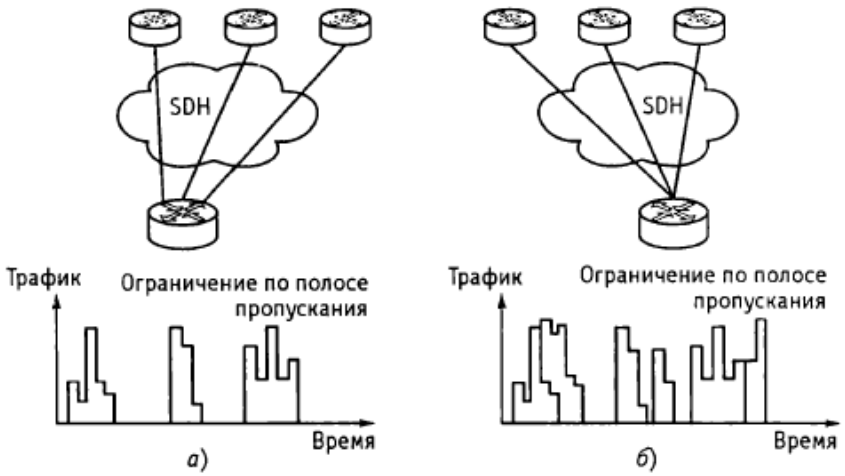


Рис. 3.26. Организация соединений:
а) «точка–точка»; *б*) «точка–много точек»

Все это позволяет строить сложные структуры «точка-много точек» и «много точек-много точек», известные как E-LAN (см. рис. 3.26), а также осуществлять концентрацию клиентского трафика и рационально использовать транспортную инфраструктуру.

Таким образом, следует обеспечить возможность полноценной работы с трафиком Ethernet в соответствии с рекомендациями IEEE 802.1 D (Bridge Protocol and Spanning Tree), IEEE 802.1 Q (VLAN) и IEEE 802.1 P (Priority).

Качество обслуживания. При увеличении числа обслуживаемых абонентов оператор сталкивается с проблемой обеспечения определенного качества обслуживания. Опыт зарубежных операторов показывает, что в ближайшее время функций Ethernet по обеспечению заданного в SLA (Service Level Agreement - договор об уровнях обслуживания) уровня обслуживания будет достаточно. Но в дальнейшем нужно будет дополнительно использовать возможности технологии MPLS (см. гл. 4).

Стек протоколов. Стек протоколов формируется следующим образом (рис. 3.27): абонент передает кадры Ethernet (с использованием или без использования собственных VLAN), которые инкапсулируются в кадры GFP, а они затем инкапсулируются в виртуальные сцепки контейнеров. Механизм LCAS обеспечивает защиту трафика Ethernet на случай возможных отказов путем динамического изменения пропускной способности соединения. SDH реализует взаимодействие на физическом уровне с существующими сетями.

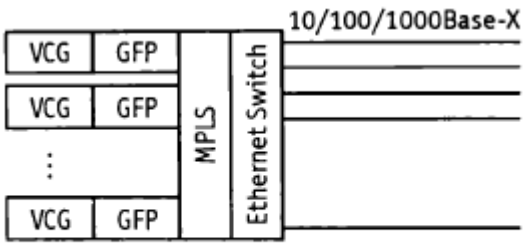


Рис. 3.27. Стек протоколов Ethernet-over-SDH с использованием технологии MPLS

3. Многопротокольная коммутация по меткам

3.1. Основы MPLS

Одним из перспективных направлений построения современной сетевой инфраструктуры является использование оптических технологий для организации высокоскоростной магистральной сети и единой системы сигнализации, позволяющей объединять различные типы сред и систем передачи информации. В качестве такой объединяющей технологии в настоящий момент рассматривается технология многопротокольной коммутации по меткам (Multiprotocol Label Switching, MPLS). Данная технология представляет собой попытку ускорить продвижение IP-пакетов и сохранить гибкость, характерную для IP-сетей, с помощью механизмов управления трафиком и поддержания качества обслуживания, применяющихся в сетях ATM. Внедрение технологии MPLS позволяет сохранить все лучшее, что присуще архитектуре IP-over-ATM (эффективное мультиплексирование и гибкость трафика, высокая производительность), и при этом она еще больше повышает масштабируемость сетей, упрощает их построение и эксплуатацию. Важно и то, что MPLS может использоваться не только с ATM, но и с любой другой технологией канального уровня. MPLS использует и развивает концепцию виртуальных каналов, используемых в сетях X.25, Frame Relay, объединяя ее с техникой выбора путей на основе информации о топологии и текущей загрузке сети, получаемой с помощью протоколов маршрутизации сетей IP. Это упрощает переход к следующему поколению волоконно-оптических магистралей Интернет на основе технологий SDH/WDM или IP/WDM.

MPLS - это технология быстрой коммутации пакетов в многопротокольных сетях, основанная на использовании меток. MPLS сочетает в себе управление трафиком, характерное для технологий канального уровня, масштабируемость и гибкость протоколов сетевого уровня. «Многопротокольность» в названии технологии означает, что MPLS - инкапсулирующий протокол и может транспортировать множество других протоколов (рис. 4.1).

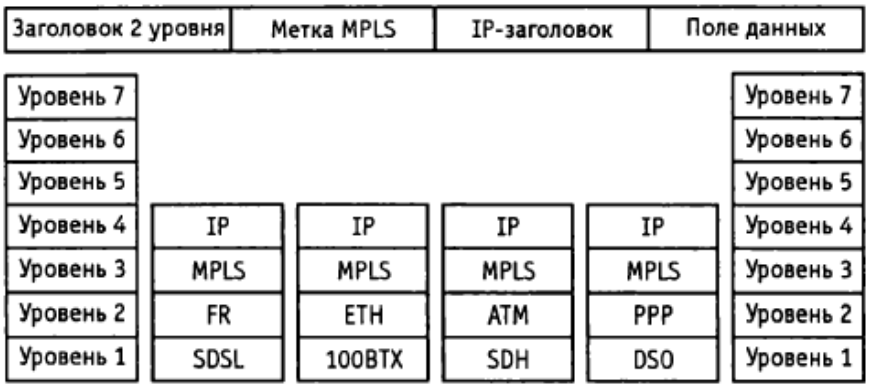


Рис. 4.1. Технология MPLS в IP-сетях и модель OSI/ISO

Сети ряда Интернет-провайдеров построены сегодня на основе многоуровневой модели, подразумевающей, что логическая маршрутизируемая IP-сеть функционирует поверх коммутируемой топологии второго уровня (ATM либо Frame Relay) и независимо от нее. Коммутаторы второго уровня обеспечивают высокоскоростные соединения, в то время как IP-маршрутизаторы на периферии сети, связанные друг с другом сетью виртуальных каналов второго уровня, осуществляют интеллектуальную пересылку IP-пакетов.

Таким образом, MPLS - это один из шагов на пути эволюционного развития сети Интернет в сторону упрощения ее инфраструктуры путем интеграции функций второго (коммутация) и третьего (маршрутизация) уровней.

В спецификации технологии MPLS заложен принцип разделения функций транспортировки потоков и управления ими (рис. 4.2). Отделение управляющей компоненты от пересылающей позволяет разрабатывать и модифицировать каждую из них независимо. Естественное обязательное требование состоит в том, чтобы управляющая компонента могла передавать информацию пересылающей компоненте через таблицу пересылки пакетов. Управляющая компонента задействует стандартные протоколы маршрутизации (OSPF, IS-IS, BGP-4) для обмена информацией с другими маршрутизаторами. На основе этой информации формируется и модифицируется сначала таблица маршрутизации, а затем, с учетом информации о смежных системах на каждом интерфейсе - таблица пересылки пакетов. Когда система получает новый пакет, пересылающая компонента анализирует информацию, содержащуюся в его заголовке, ищет соответствующую запись в таблице пересылки и направляет пакет на выходной интерфейс. Пересылающая компонента практически всех систем многоуровневой коммутации, включая и MPLS, основана на использовании последовательных меток пакетов. Метка - это короткое поле фиксированной длины в заголовке пакета.

С помощью MPLS можно решать следующие задачи:

- интеграцию ATM и Frame Relay с IP;

- ускоренное продвижение пакетов внутри сети оператора вдоль кратчайших традиционных маршрутов;

- создание виртуальных частных сетей (VPN);

- выбор и установление путей с учетом загрузки ресурсов (Traffic Engineering, TE).

Рис. 4.2. Функциональные компоненты маршрутизации

В книге не рассматриваются детально все возможности технологии MPLS. Желающие могут ознакомиться с ними сами. Мы ограничимся одним из наиболее важных применений технологии MPLS, а именно, службой VPN.

3.2. Элементы сети MPLS

В сетях, многопротокольной коммутации по меткам (MPLS-сетях), используются два вида сетевых узлов. Расположенные на границе сети MPLS маршрутизаторы должны распознавать и анализировать поступающие IP-потоки и направлять их по подходящим маршрутам. Эти устройства называются пограничными маршрутизаторами с коммутацией меток (Label Edge Router,LER). Различают входной и выходной LER.

Входной LER анализирует, как и обычный маршрутизатор, IP-заголовок и устанавливает, к какому классу эквивалентного обслуживания (Forwarding Equivalency Class, FEC) при выборе адреса следующей передачи пакета он принадлежит. FEC - класс пакетов сетевого уровня, которые получают от сети одинаковое обслуживание как при выборе пути продвижения пакета, так и с точки зрения доступа к ресурсам.

Абстрагирование отдельных пакетов в класс эквивалентности (или класс эквивалентного обслуживания, что одно и то же) FEC позволяет объединять большое количество потоков трафика, требующих одинаковой обработки. Объединенные в класс эквивалентности FEC потоки трафика идентифицируются одной и той же MPLS-меткой.

Возможность объединения потоков трафика независимо от адреса сетей назначения значительно увеличивает возможность MPLS к масштабированию за счет уменьшения объема информации о маршрутах, хранимой и обрабатываемой маршрутизаторами коммутации меток (LSR-маршрутизаторами).

IP-дейтаграмма заключается в модуль данных протокола (Protocol Data Unit, PDU) технологии MPLS, а заголовок MPLS прикрепляется к дейтаграмме. Если заголовок объединен с операцией QoS (например, DiffServ), то входной LER будет рассматривать трафик в соответствии с правилами DiffServ. Далее LER принимает решение о выборе пути для данного пакета, посылая его к соответствующему транзитному маршрутизатору с коммутацией меток (Label Switch Routers, LSR). LSR получает PDU и использует заголовок MPLS для принятия решений пересылки. Он также производит замену меток. Данный LSR не занимается обработкой заголовка третьего уровня (IP-заголовка), а принимает решение о пересылке на основе метки пакета, а не на основе таблицы маршрутизации, и пересылает пакет дальше.

Далее, проходя, в общем случае, через несколько LSR, пакет попадает к выходному LER, который производит операцию разборки PDU, удаляет из пакета метку, анализирует заголовок пакета и направляет его к адресату, находящемуся вне MPLS-сети (рис. 4.3).

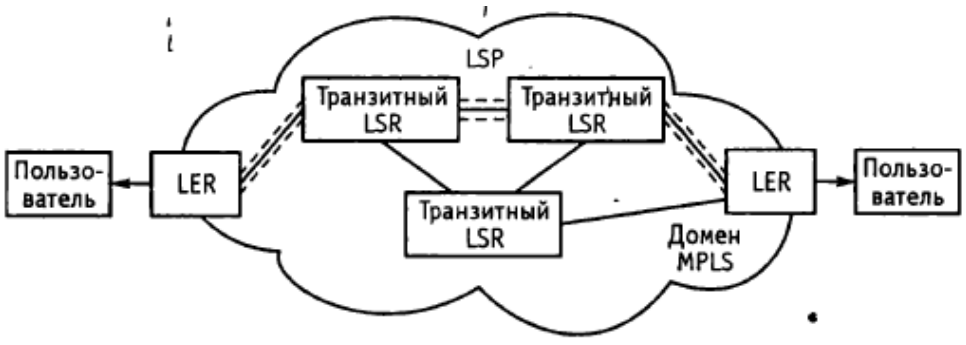


Рис. 4.3. Элементы сети MPLS

Пакеты, принадлежащие одному классу FEC, проходят путь от входного LER до выходного LER через множество транзитных LSR, образуя виртуальный коммутируемый по меткам тракт или путь (Label Switched Path, LSP). Установленное соединение является симплексным. Для организации полудуплексного соединения должны быть установлены два LSP. LSP всегда начинается на крае сети, заканчивается на противоположном конце, проходя через несколько транзитных маршрутизаторов.

3.3. Некоторые особенности технологии MPLS

3.3.1. Метки и способы маркировки

Метка - короткий идентификатор фиксированной длины, используемый на локальном участке сети, предназначен для определения класса эквивалентного обслуживания пакета при его пересылке по сети. На сегодняшний день стандартом определен формат 32-битной метки, располагаемой между заголовками второго уровня (Layer 2) и третьего уровня (Layer 3). Для примера рассмотрим включение метки в IP-пакет заголовка Ethernet (рис. 4.4).

- Поле «Метка» - состоит из 20 бит и содержит собственное значение метки, используемое для определения маршрутизатора следующего шага, т. е. для продвижения пакетов.

- CoS (Class of Service) - поле необходимо для предоставления дифференциальных услуг в MPLS-сети. Для сквозного обеспечения QoS на границе MPLS-сети можно скопировать поле IP-приоритета в поле CoS. Поле состоит из 3 бит. Таким образом, в нем может передаваться только 3-битовое поле IP-приоритета, а 6-битового поля дифференцированной услуги (Differentiated Services Code Point, DSCP) - нет. При необходимости CoS может передаваться в виде одной из меток MPLS-стека. Поле метки способно вместить как поле IP-приоритета, так и поле DSCP.

- S - поле стека предназначено для поддержки иерархического стека меток. Бит S устанавливается в единицу для последней метки в стеке и в ноль для всех остальных меток стека. Это позволяет привязать префикс к нескольким меткам, другими словами - к стеку меток. Каждая метка стека имеет свои собственные значения поля CoS, S-бита и поле TTL.

- Время жизни (Time To Live , TTL) - 8 бит, используемых для кодирования количества ретрансляционных участков.

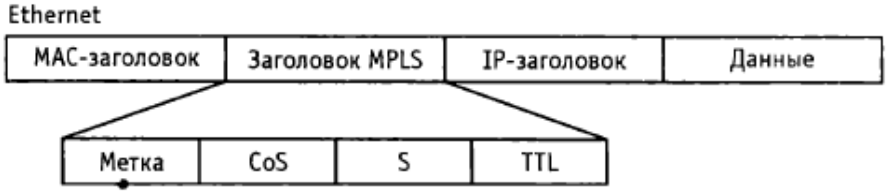


Рис. 4.4. Формат метки MPLS

Поле «Время жизни» является ключевым полем в заголовке IP-пакета. Обычно в объединенной IP-сети это поле уменьшается на единицу на каждом участке маршрута, и когда значение счетчика достигает нуля, пакет отбрасывается. Это делается для того, чтобы избежать зацикливания пакета или слишком долгого пребывания пакета в

объединенной сети из-за неверной маршрутизации. Поскольку LSR не исследует IP-заголовок, поле времени жизни включается в метку, что позволяет сохранить функциональность этого поля.

Правила обработки поля времени жизни в метке:

1. Когда IP-пакет прибывает на входной пограничный маршрутизатор MPLS-домена (домен - это MPLS-сеть), в стек пакета помещается одна метка. Значение поля времени жизни этой метки устанавливается равным значению поля времени жизни IP-заголовка.

2. Когда MPLS-пакет прибывает на очередной транзитный маршрутизатор MPLS-домена, значение поля времени жизни в метке, находящейся на вершине стека, уменьшается на единицу.

- Если получившееся значение времени жизни нулевое, MPLS-пакет дальше не передается. В зависимости от значения метки в стеке, пакет либо просто отбрасывается, либо передается соответствующему «обычному» сетевому уровню для обработки ошибок (например, для формирования сообщения об ошибке с использованием протокола межсетевых управляющих сообщений – Internet Control Message Protocol, ICMP).

- Если получившееся значение времени жизни положительное, оно помещается в поле времени жизни в верхней записи стека для исходящего MPLS-пакета, после чего сам MPLS-пакет перенаправляется дальше. Исходящее значение поля времени жизни является функцией только входящего значения поля времени жизни и не зависит от того, были ли помещены в стек или извлечены из стека какие-либо метки до того, как переправить пакет дальше. Значения полей вре'мени жизни в записях, не находящихся на вершине стека, на ход обработки не влияют.

3. Когда MPLS-пакет прибывает на выходной пограничный маршрутизатор MPLS-домена, значение поля времени жизни, единственной находящейся в стеке записи, уменьшается на единицу, после чего метка извлекается из стека и стек меток становится пустым. В этом случае пакет выдается пользователю либо на сетевой уровень для обработки ошибок.

- Если получившееся значение положительное, оно помещается в поле времени жизни IP-заголовка, после чего IP-пакет перенаправляется дальше путем обычной маршрутизации. До того как переправить пакет дальше, должна быть пересчитана заново контрольная сумма IP-заголовка. Эта процедура необходима, чтобы убедиться, что повреждения заголовка не произошло при пересылке сообщения.

Использование меток значительно упрощает процедуру пересылки пакетов, так как маршрутизатор обрабатывает не весь заголовок IP-пакета, а только метку. Что занимает значительно меньше времени.

3.3.2. Стек меток

В рамках архитектуры MPLS вместе с пакетом разрешено передавать не одну метку, а несколько. При этом различают верхние и нижние метки:

- нижняя метка - будет обрабатываться самой последней по пути следования пакета;

- верхняя метка - обрабатывается самой первой по пути следования пакета.

Операции добавления/изъятия метки определены как операции на стеке. Результат коммутации задает лишь верхняя метка стека, нижние же передаются прозрачно до операции изъятия верхней.

Такой подход позволяет создавать иерархию потоков в сети MPLS и организовать туннельные передачи. Стек состоит из произвольного числа заголовков. Если стек меток имеет глубину т, то считается, что самая нижняя метка размещена на уровне 1, метка над ней имеет уровень 2 и т.д., а метка наверху стека имеет уровень т. Верхняя метка в стеке находится ближе к заголовку сетевого уровня, а нижняя метка располагается ближе к заголовку канального уровня;

- CoS в стеках не используются.

Метка может принимать любое значение, кроме нескольких зарезервированных.

Пакет сетевого уровня следует сразу за записью стека с установленным в единицу битом S.

Записи стека меток располагаются после заголовка уровня передачи данных (канального уровня), но до заголовков сетевого уровня. В кадре протокола передачи данных (рис. 4.5, а), например протокола PPP (Point-to-Point Protocol - протокол точка-точка), стек меток располагается между IP-заголовком и заголовком уровня передачи данных.

В кадре сети стандарта IEEE 802 (рис. 4.5, б) стек меток располагается между IP-заголовком и заголовком уровня LLC (Logical Link Control - управление логическим соединением).

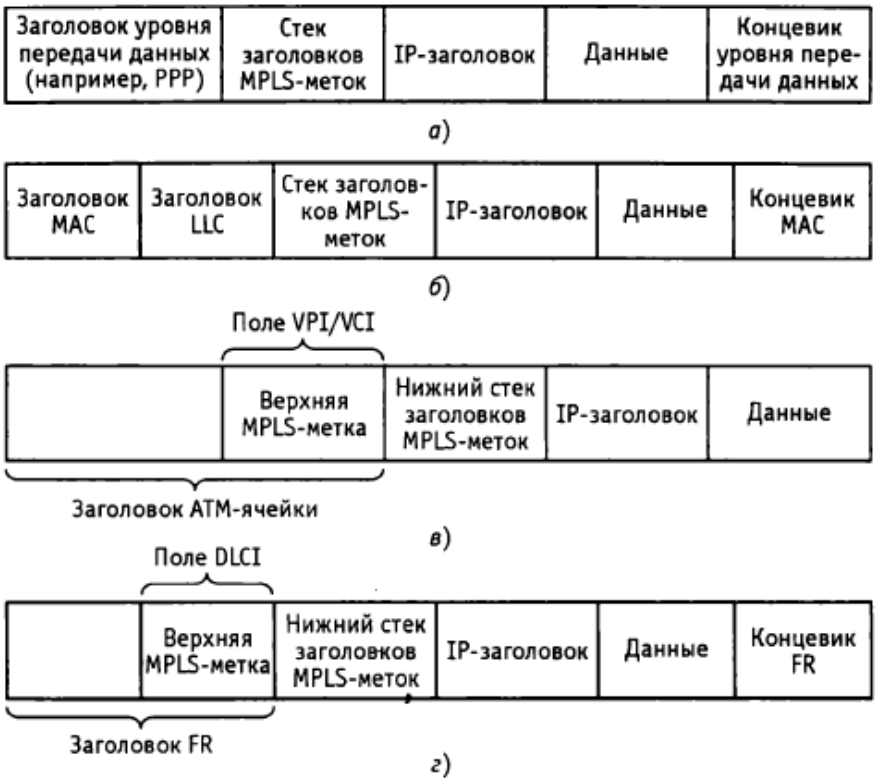


Рис. 4.5. *а*) Стеки заголовков меток MPLS в протоколе PPP; *б*) стек заголовков меток в кадре сети стандарта 802.x; *в*) стек заголовков меток MPLS в поле VPI/VCI; *г*) стек заголовков меток MPLS в поле DLCI

Если архитектура MPLS используется поверх ориентированной на соединение сетевой службы, может применяться другой подход, который иллюстрируют рис.4.5, в и г.

В ячейках ATM верхняя метка помещается в поле VPI/VCI в заголовке ячейки ATM. Верхняя метка остается на вершине стека, вставляемого между заголовком ячейки и IP-заголовком. Помещение значения метки в заголовок ATM-ячейки упрощает работу ATM-коммутатора, которому по-прежнему достаточно просмотреть только заголовок ячейки.

Подобным же образом значение самой верхней метки может быть помещено в поле DLCI или в заголовке кадра FR (рис . 4.5, г). Необходимо обратить внимание, что в обоих случаях поле времени жизни остается невидимым для коммутатора и уменьшается на единицу по мере следования через транзитные узлы до станции назначения.

3.3.3. Классы эквивалентного обслуживания (FEC)

Классом эквивалентного обслуживания (Forwarding Equivalency Class,FEC) - называется группа пакетов третьего уровня, например IP-пакетов, которые одинаково обслуживаются и пересылаются. Термин FEC применяют для операций коммутации меткой. При использовании технологии MPLS соответствие между пакетом и «классом эквивалентного обслуживания» FEC устанавливается один раз, на входе в сеть MPLS. К одному FEC относятся пакеты всех потоков, пути следования которых через сеть (или

часть сети) совпадают. С точки зрения выбора ближайшего маршрутизатора, к которому их надо переслать, все пакеты одного FEC неразличимы.

FEC используется для описания пакетов с адресом назначения, обычно адресом конечного получателя трафика, например хост-машины.

Использование FEC позволяет:

- Объединять пакеты в классы. При таком объединении значение FEC в пакете может использоваться для установки приоритетов. При обработке пакетов предоставляется более высокий приоритет одним пакетам по отношению к другим.

- Обеспечить поддержание эффективных операций QoS. Например, FEC могут быть связаны с высокоприоритетным голосовым трафиком в реальном времени, низкоприоритетным трафиком Интернет-конференций и т. д.

FEC-класс пакета может определяться по одному или по нескольким параметрам, указанным сетевым администратором. Среди возможных параметров можно назвать:

- IP-адрес отправителя и/или получателя или IP-адреса сетей;

- номера портов отправителя и/или получателя;

- идентификатор IP-протокола;

- код дифференцированной службы;

- метку потока IPv6.

Для различных классов обслуживания используются различные FEC и связанные с ними метки.

В сети MPLS возможны два подхода к пересылке пакетов с учетом класса обслуживания.

Таблица 4.1. **Пример связи адресов и FEC**

Адрес	FEC ID
120.166.4.8/4	A
177.200.7.8/3	B
202.240.76.9/1	C
387	D
474	E

Первый - предусматривает обработку пакетов в выходных очередях маршрутизаторов с учетом значений приоритета, указанного в заголовке MPLS.

Второй - базируется на том, что для каждой пары, состоящей из входного и выходного маршрутизаторов, определяется несколько путей коммутации меток (Label Switched Path, LSP) с различными характеристиками производительности, полосы пропускания, времени задержки и других параметров. После этого входной граничный маршрутизатор направляет один тип трафика по одному пути, другой – по другому, третий - по третьему и т.д.

В маршрутизаторах хранится таблица связи меток (Incoming Label Mapping, ILM). Для ее создания используется таблица переадресации помеченных пакетов (Next Hop Label Forwarding Entry, NHLFE). Производится обмен старой метки на новую, после чего пакет

пересылается с новой меткой дальше. Эта процедура называется обменом меток. Одна входная метка может меняться на несколько исходящих меток. FEC является одним из основных компонентов MPLS, который определяет во многом работу всей сети. Все целевые адреса принадлежат к классам обслуживания FEC. FEC обычно ассоциируется напрямую с одним или несколькими адресами назначения. Эти данные записываются в таблицу маршрутизации. Если требуется направить поток данных к нескольким сетевым адресам одним и тем же путем, то для этих адресов выбирается один класс обслуживания. В простейшем случае записи не должны быть очень точными. Все пакеты с одной определенной сетью назначения ассоциируются с одним и тем же FEC. Также возможно один и тот же префикс относить к различным классам FEC. Назначение определенного FEC-класса должно выполнятся либо путем ручной настройки, либо с помощью сигнального протокола, либо на основе анализа пакетов, поступающих на входные маршрутизаторы.

Трафик одного FEC-класса пересекает MPLS-домен по LSP-пути.

Для определения топологии и текущего состояния домена требуется протокол маршрутизации, позволяющий каждому FEC-классу назначать конкретный LSP-путь. Протокол маршрутизации должен быть способен собирать и использовать информацию для поддержания требований к качеству обслуживания данного FEC-класса. Отдельные маршрутизаторы должны знать о LSP-пути данного FEC-класса, должны назначать LSP-путь входящей метке, а также должны обмениваться этой меткой со всеми остальными маршрутизаторами, которые могут послать им пакеты данного FEC-класса. LSP-пути классифицируются следующим образом:

- Между двумя граничными LER MPLS-домена проходит один маршрут.

- Один выходной LER, несколько входных маршрутизаторов. Назначенный одному FEC-классу трафик может поступать от разных источников через разные входные LER. Примером такой ситуации является корпоративная Интернет-сеть, расположенная в одном регионе, но с доступом к MPLS-домену через несколько входных LER. В такой ситуации через MPLS-домен проходит несколько маршрутов, возможно, с общими конечными ретрансляционными участками.

- Несколько выходных маршрутизаторов для трафика целевой рассылки. В рекомендации RFC 3031 утверждается, что чаще всего пакету присваивается FEC-класс на основе (частично или целиком) адреса получателя сетевого уровня. В противном случае, возможно, для FEC-класса потребуются маршруты к нескольким различным выходным маршрутизаторам. Однако, скорее всего, существует несколько сетей, в которые трафик может быть доставлен через один выходной LSR-маршрутизатор.

- В RFC 3031 групповая рассылка упоминается как предмет дальнейших исследований.

При создании сети нужно обратить внимание, чтобы число классов обслуживания было оптимальным для реализации всех важных приложений и требуемых параметров качества.

3.3.4. Таблицы

Для связи полученных меток с выходными метками используются различные таблицы и карты. Они предназначены для последующего управления стеками меток.

1. Таблица переадресации помеченных пакетов (Next Hop Label Forwarding Entry, NHLFE) - или строка пересылки следующего транзитного участка - используется, когда происходит пересылка пакета с меткой (табл. 4.2). Записи в таблице NHLFE содержат адрес следующего маршрутизатора и операции, которые необходимо совершить с данным пакетом:

- обмен внешней метки из стека;

- извлечение внешней метки из стека;

- обмен метки (т.е. каждый LSR после получения пакета изменяет значение метки прежде, чем послать пакет следующему LSR);

- вставка новой метки в стек.

Таблица 4.2. **Пример таблицы NHLFE**

NHLFE	Следующий LSR	Операция с меткой	Выходная метка	Исходящий порт
126	LSR C	Вставка	888	3821
546	LSR D	Обмен	777	7653
338	LSR F	Извлечение	–	–

Таблица 4.3. **FEC-to-NHLFE**

FEC	NHLFE
A	126
C	546
K	777

Таблица 4.4. **Пример таблицы Incoming Label Map (ILM)**

Label	NHLFE
888	126
777	546
555	757

Таблица также может содержать информацию о последовательности сборки пакета на канальном уровне и кодировании MPLS-заголовка стека.

Возможно, что принявший пакет маршрутизатор является последним на маркированном маршруте LSP. Тогда метка из пакета извлекается и пакет посылается дальше на основании решения третьего уровня эталонной модели ВОС (OSI).

2. Таблица связи (FEC-to-NHLFE, FTN) используется, если был принят пакет, не имевший до этого метки, но к которому была добавлена метка перед отправкой. В табл. 4.3. записано соответствие между каждым FEC и набором NHLFE. То есть карта FEC-to-NHLFE соотносит каждый класс FEC к множеству NHLFE, содержащих больше чем одну метку, но, прежде чем пакет будет послан, должна быть выбрана ровно одна метка множества.

3. Существует также карта входной метки (Incoming Label Map, ILM) - табл. 4.4. В ней находится связка к таблице NHLFE для пакетов, уже содержащих метку, т. е. протокол распределения меток (Label Distribution Protocol, LDP) записывает каждую входную метку в NHLFE. Если ILM вносит конкретную метку во множество NHLFE, то, прежде чем пакет будет отправлен, из стека должна быть выбрана ровно одна метка из множества. Метка в начале стека используется как индекс в ILM. Если ILM вносит метку во множество, содержащее больше чем один NHLFE, то это может быть полезно, если, например, она применяется для распределения нагрузки между различными каналами.

3.3.5. Правила назначения меток

На рис. 4.6 узлы A, B, G и H являются пользовательскими машинами и они не работают с MPLS. Узел C является входным LER, узлы D и E - транзитные LSR, а узел F - выходной LER. Информация передается пользователю узла G. Адрес этого узла может быть IP-адресом или некоторым другим адресом, например, IPX- или телефонным номером.

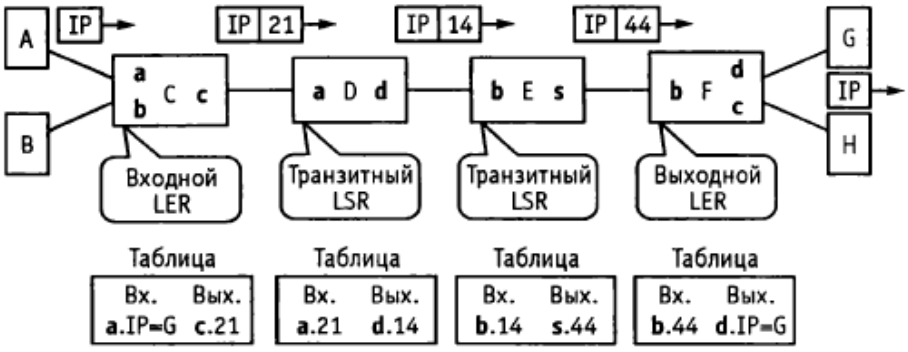


Рис. 4.6. Замена меток и пересылка

LER C получает IP-дейтаграмму, предназначенную для узла G, от узла A по интерфейсу a. LER C анализирует поля FEC, связывает FEC с меткой 21, вставляет дейтаграмму IP после заголовка метки и посылает пакет по выходному интерфейсу c. С учетом выходной строки в таблице NHLFE, LER C помещает метку 21 в заголовок метки в пакете. Производимая операция в LER C называется вводом метки.

Теперь LSR D и E обрабатывают только заголовок метки. Их таблицы замены меток используются (в LSR D) для замены метки 21 на метку 14, и для замены метки 14 на метку 44 (LSR E). Заметим, что данные таблицы используют входные и выходные интерфейсы на каждом LSR для связи меток с входными и выходными линиями передачи. Выходной LER F настроен так, что он распознает метку 44 по интерфейсу b как свою собственную метку. Далее выходная строка в таблице F указывает LER F послать дейтаграмму к G по интерфейсу d, что предполагает удаление метки из пакета.

Такое удаление метки является частью операции под названием вывод (выталкивание) метки.

3.4. Виртуальные частные сети MPLS (VPN MPLS)

VPN служит для организации прямого, безопасного соединения через общедоступный Интернет между клиентами (обычно конечным пользователем и корпоративным офисом) или между двумя ЛВС. Благодаря VPN удаленные пользователи могут обращаться к серверам предприятия и связываться с различными офисами своей компании. VPN может применяться как базовая архитектура обеспечения безопасности для экстрасети.

Для VPN не нужны выделенные линии, поэтому пользоваться ею может каждый, кто располагает доступом к Интернету. После того как соединение установлено, сотрудникам может предоставляться доступ ко всем ресурсам сети - так, словно они присутствуют в офисе. Самое большое достоинство технологии заключается в том, что, несмотря на общедоступную инфраструктуру, прямое соединение VPN, иногда именуемое «туннелем», защищено столь надежно, что украсть данные или получить несанкционированный доступ к территориально-распределенной сети становится очень трудно.

Сети VPN обладают рядом экономических преимуществ перед другими методами дистанционного доступа. Пользователи VPN могут обращаться к корпоративной сети, не устанавливая коммутируемое соединение, что позволяет сократить численность модемов или вообще отказаться от них. Можно обойтись и без выделенных линий, соединяющих удаленные офисы. Кроме того, повышается производительность труда, так как сотрудники могут пользоваться самыми быстрыми линиями связи, имеющимися в их распоряжении, вместо того чтобы тратить время на установление коммутируемого соединения через банк модемов.

Компоненты MPLS VPN. Сеть MPLS VPN делится на две области: сети IP клиентов и внутренняя (магистральная) сеть MPLS провайдера, которая необходима для объединения сетей клиентов (рис. 4.7).

В общем случае у каждого клиента может быть несколько территориально обособленных сетей IP, каждая из которых в свою очередь может включать несколько подсетей, связанных маршрутизаторами. Такие территориально изолированные сетевые «островки» корпоративной сети принято называть сайтами. Принадлежащие одному клиенту сайты обмениваются IP-пакетами через сеть провайдера и образуют виртуальную частную сеть этого клиента. Для обмена маршрутной информацией в пределах сайта узлы пользуются одним из протоколов IGP, OSPF или IS-IS, область действия которого ограничена автономной системой (набор сетей, которые находятся под единым управлением и совместно используют общую стратегию маршрутизации).

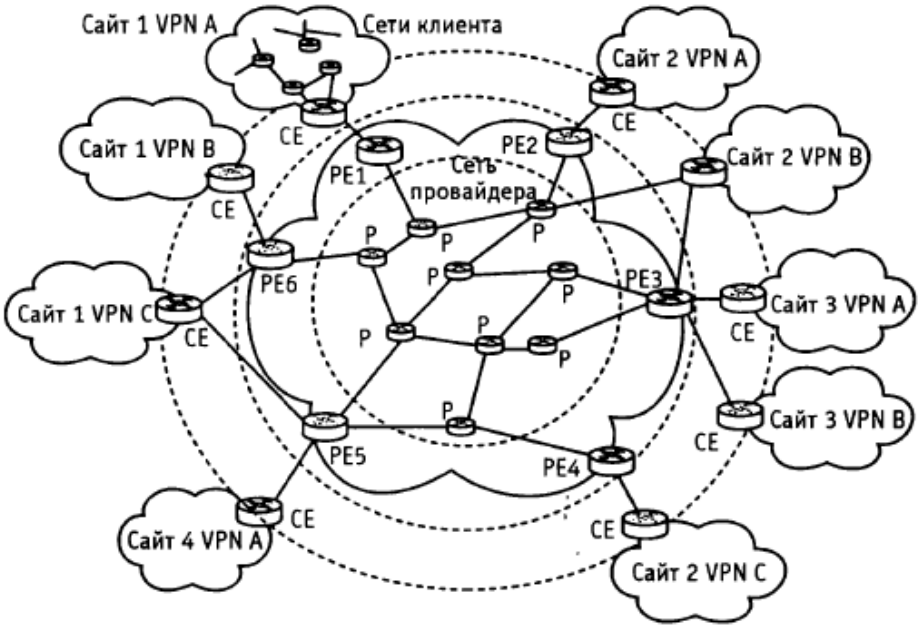


Рис. 4.7. Компоненты MPLS VPN

Маршрутизатор, с помощью которого сайт клиента подключается к магистрали провайдера, называется пограничным маршрутизатором клиента (Customer Edge router, CE). Будучи компонентом сети клиента, CE не имеет сведений о существовании VPN. Он может быть соединен с магистральной сетью провайдера несколькими каналами.

Магистральная сеть провайдера является сетью с технологией IP/MPLS, где пакеты IP продвигаются на основе не IP-адресов, а локальных меток. Сеть IP/MPLS состоит из маршрутизаторов с коммутацией меток (LSR), которые направляют трафик по предварительно проложенным путям с коммутацией меток (LSP) в соответствии со значениями меток. Устройство LSR - это своеобразный гибрид маршрутизатора IP и коммутатора, при этом от маршрутизатора IP берется способность определять топологию сети с помощью протоколов маршрутизации и выбирать рациональные пути следования трафика, а от коммутатора - техника продвижения пакетов с использованием меток и локальных таблиц коммутации. Устройства LSR для краткости часто называют просто маршрутизаторами, и в этом есть свой резон - они с таким же успехом способны продвигать пакеты на основе IP-адреса, если поддержка MPLS отключена.

В сети провайдера среди устройств LSR выделяют пограничные маршрутизаторы провайдера (Provider Edge router, PE). Для их обозначения также используется аббревиатура LER (Label Edge Router).

К PE через маршрутизаторы CE подключаются сайты клиентов и внутренние маршрутизаторы магистральной сети провайдера (Provider router, P). Маршрутизаторы CE и PE обычно связаны непосредственно физическим каналом, на котором работает какой-либо протокол канального уровня - например, PPP, FR, ATM или Ethernet. Общение

между CE и PE идет на основе стандартных протоколов стека TCP/IP, поддержка MPLS нужна только для внутренних интерфейсов PE (и всех интерфейсов P). Иногда полезно различать входной PE и выходной (удаленный) PE для определения направления продвижения трафика.

В магистральной сети провайдера только пограничные маршрутизаторы PE должны быть сконфигурированы для поддержки виртуальных частных сетей, поэтому только они «знают» о существующих VPN. Если рассматривать сеть с позиций VPN, то маршрутизаторы провайдера P непосредственно не взаимодействуют с маршрутизаторами заказчика CE, а просто располагаются вдоль туннеля между входным и выходным маршрутизаторами PE.

Маршрутизаторы PE являются функционально более сложными, чем P. На них возлагаются главные задачи по поддержке VPN, а именно, разграничение маршрутов и потоков данных, поступающих от разных клиентов. Маршрутизаторы PE служат также оконечными точками путей LSP между сайтами заказчиков, и именно PE назначает метку IP-пакету для его транзита через внутреннюю сеть маршрутизаторов P.

Таблица маршрутизации (VPN Routing and Forwarding, VRF).

Пути LSP могут быть проложены двумя способами: либо с применением технологии ускоренной маршрутизации (ЮР) с помощью протоколов LDP, либо на основе технологии трафик-инжиниринга (TE) с помощью протоколов RSVP. Прокладка LSP означает создание таблиц коммутации меток на всех маршрутизаторах PE и P, образующих данный LSP.

В совокупности эти таблицы задают множество путей для разных видов трафика клиентов. В VPN применяется различная топология связей: полносвязная, «звезда» (часто называемая в англоязычной литературе hub-and-spoke) или ячеистая (mesh).

Для корректной работы VPN требуется, чтобы информация о маршрутах через магистральную сеть провайдера не распространялась за ее пределы, а сведения о маршрутах в клиентских сайтах не становились известными за границами определенных VPN.

Барьеры на пути распространения маршрутных объявлений могут устанавливаться соответствующим конфигурированием маршрутизаторов. Протокол маршрутизации должен быть оповещен о том, с каких интерфейсов и от кого он имеет право принимать объявления определенного сорта и на какие интерфейсы и кому их распространять.

Роль таких барьеров в сети MPLS VPN играют пограничные маршрутизаторы PE или LER. Можно представить, что через маршрутизатор PE проходит невидимая граница между зоной клиентских сайтов и зоной ядра сети провайдера. По одну сторону

располагаются интерфейсы, через которые PE взаимодействует с маршрутизаторами P, а по другую - интерфейсы, к которым подключаются сайты клиентов. С одной стороны, на PE поступают объявления о маршрутах магистральной сети, с другой стороны - объявления о маршрутах в сетях клиентов.

На рис. 4.8 показан маршрутизатор PE, на котором установлено несколько протоколов класса IGP. Один из них сконфигурирован для приема и распространения маршрутных объявлений только с тех трех внутренних интерфейсов, которые связывают этот PE с маршрутизаторами P. Два других протокола IGP обрабатывают маршрутную информацию от сайтов клиентов.

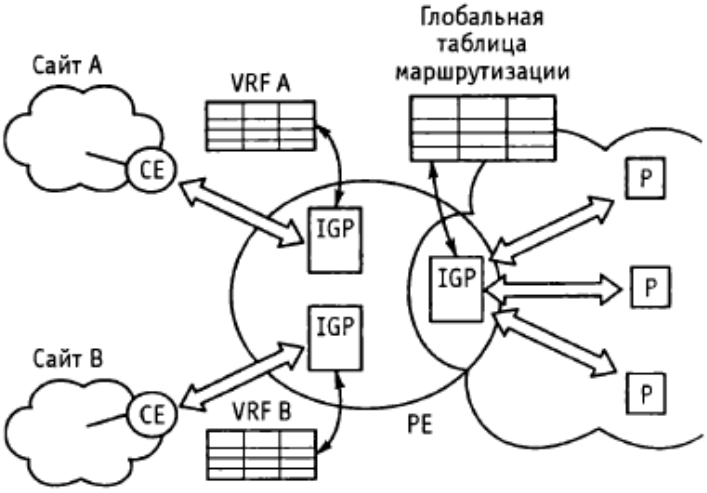


Рис. 4.8. Протоколы маршрутизации PE

Аналогичным образом настроены и остальные PE. Маршрутизаторы P принимают и обрабатывают маршрутную информацию IGP, поступающую со всех интерфейсов. В результате на всех маршрутизаторах PE и P создается по таблице маршрутизации, где содержатся все маршруты в пределах внутренней сети провайдера. Подчеркнем, что никакой информации о маршрутах в сетях клиентов в этих таблицах нет. Вместе с тем, и сети клиентов ничего не «знают» о маршрутах в сети провайдера. Таблица маршрутизации, создаваемая на пограничных маршрутизаторах PE на основе объявлений из магистральной сети, имеет специальное название «глобальная таблица маршрутизации». В отличие от нее таблицы, которые PE формирует на основе объявлений, поступающих из сайтов клиентов, получили название таблиц VRF (VPN Routing and Forwarding). В VRF хранятся данные о маршрутах, информация о которых получена от клиентских маршрутизаторов.

Сайты клиентов представляют собой обычные сети IP, маршрутная информация в которых может передаваться и обрабатываться с помощью любого протокола маршрутизации класса IGP. Очевидно, что этот процесс никак не регламентируется провайдером. Маршрутные объявления свободно распространяются между узлами в пределах каждого сайта до тех пор, пока они не доходят до пограничных маршрутизаторов PE, служащих преградой для их дальнейшего распространения.

Разграничение маршрутов разных клиентов обеспечивает установка на маршрутизаторах PE отдельного протокола маршрутизации на каждый интерфейс, к

которому подключен сайт клиента. Этот протокол принимает и передает клиентские маршрутные объявления только с одного, определенного для него интерфейса, не пересылая их ни на внутренние интерфейсы, через которые PE связан с маршрутизаторами P, ни на интерфейсы, к которым подключены сайты других клиентов. В результате на маршрутизаторе PE создается несколько таблиц маршрутизации VRF.

Несколько упрощая, можно считать, что на каждом PE создается столько таблиц VRF, сколько сайтов к нему подключено. Фактически на маршрутизаторе PE организуется несколько виртуальных маршрутизаторов, каждый из которых работает со своей таблицей VRF. Возможно и другое соотношение между сайтами и таблицами VRF. Например, если к некоторому PE подключено несколько сайтов одной и той же VPN, то для них может быть создана общая таблица VRF.

Объединение сайтов. Чтобы связать территориально разнесенные сайты заказчика в единую сеть, необходимо, во-первых, создать для них общее пространство распространения маршрутной информации, и, во-вторых, проложить во внутренней сети пути, по которым принадлежащие разным сайтам узлы одной и той же VPN могли вести обмен данными защищенным образом.

Механизмом, с помощью которого сайты одной VPN обмениваются маршрутной информацией, является многопротокольное расширение для BGP (Multiprotocol extensions for BGP-4, MP-BGP). С помощью этого протокола пограничные маршрутизаторы PE организуют взаимные сеансы и в рамках этих сеансов обмениваются маршрутной информацией из своих таблиц VRF.

Особенность протокола BGP и его расширений заключается в том, что он получает и передает свои маршрутные объявления не всем непосредственно связанным с ним маршрутизаторам, как протоколы IGP, а только тем, которые указаны в конфигурационных параметрах в качестве соседей. Маршрутизаторы PE сконфигурированы так, что все получаемые от клиентских сайтов маршрутные объявления они адресно пересылают с помощью MP-BGP определенным пограничным маршрутизаторам PE. Вопрос о том, кому отправлять маршрутные объявления, а кому нет, целиком зависит от топологии виртуальных частных сетей, поддерживаемых данным провайдером. Так, на рис. 4.7 маршрутизатор PE1 передает маршруты из таблицы VRF сайта 1 в VPN A на маршрутизаторы PE2, PE3, PE5, к которым подключены остальные сайты 2, 3 и 4 той же VPN A. Полученный маршрут заносится в таблицу VRF соответствующего сайта.

Таким образом, кроме маршрутов, поступающих от непосредственно подсоединенных к PE сайтов, каждая таблица VRF дополняется маршрутами, получаемыми от других

сайтов данной VPN по протоколу MP-BGP. Целенаправленное распространение маршрутов между маршрутизаторами PE обеспечивается надлежащим выбором атрибутов протокола MP-BGP.

Независимость адресных пространств. Если некоторое множество узлов никогда, ни при каких условиях, не получает маршрутную информацию от другого множества узлов, то адресация узлов в пределах каждого из этих множеств может выполняться независимым образом.

Ограничение области распространения маршрутной информации пределами отдельных VPN изолирует адресные пространства каждой VPN, позволяя применять в ее пределах как адреса Internet общего пользования, так и частные (private) адреса, зарезервированные в соответствии с RFC 1819.

Почему же в таком случае не сделать выбор адресов в пределах VPN совершенно произвольным и ограниченным только общими правилами адресации стека TCP/IP? Дело в том, что во многих случаях клиенты не хотят полной изоляции VPN: в частности, они нуждаются в выходе в Интернет. Независимое же, не согласованное с регламентирующими органами Интернет, назначение адресов узлам VPN может привести к совпадению внутренних адресов сайтов с уже выделенными адресами общего пользования, в результате чего связь с Интернет общего пользования станет невозможной. При использовании зарезервированных частных адресов проблема связи клиентов VPN с внешним миром решается с помощью стандартной техники трансляции адресов (Network Address Translator, NAT), описанной в RFC 3022. В любом случае должно соблюдаться требование уникальности адресов в пределах VPN.

Использование в разных VPN одного и того же адресного пространства создает проблему для маршрутизаторов PE. Протокол BGP изначально был разработан в предположении, что все адреса, которыми он манипулирует, во-первых, относятся к семейству адресов IPv4 и, во-вторых, однозначно идентифицируют узлы сети, т.е. являются глобально уникальными в пределах всей составной сети. Ориентация на глобальную уникальность адресов выражается в том, что, получив очередное маршрутное объявление, протокол BGP анализирует его, не обращая внимания на то, какой VPN принадлежит этот маршрут. Если на вход BGP поступают описания маршрутов к узлам разных VPN, но с совпадающими адресами IPv4, то BGP считает, что все они ведут к одному и тому же узлу, а, следовательно, как и полагается в таком случае, он помещает в соответствующую таблицу VRF только один кратчайший маршрут.

Проблема решается за счет применения вместо потенциально неоднозначных адресов IPv4 расширенных и однозначных адресов нового типа, а именно, адресов VPN-IPv4,

получаемых в результате преобразования исходных адресов IPv4. Преобразование заключается в том, что ко всем адресам IPv4, составляющим адресное пространство той или иной VPN, добавляется префикс, называемый различителем маршрутов (Route Distinguisher, RD), который уникально идентифицирует эту VPN. В результате на маршрутизаторе PE все адреса, относящиеся к разным VPN, обязательно будут отличаться друг от друга, даже если они имеют совпадающую часть - адрес IPv4.

Именно здесь оказалась полезной способность расширенного протокола MP-BGP переносить в маршрутных объявлениях адреса разных типов, в том числе IPv6, IPX, а, главное, VPN-IPv4. Адреса VPNIPv4 используются только для маршрутов, которыми маршрутизаторы PE обмениваются по протоколу BGP. Прежде чем передать своему напарнику некоторый маршрут, входной маршрутизатор PE добавляет к его адресу назначения IPv4 префикс RD для данной VPN, тем самым преобразуя его в маршрут VPN-IPv4.

Как уже было сказано, различители маршрута должны гарантированно уникально идентифицировать VPN, чтобы избежать дублирования адресов. Упростить выбор RD, не создавая для этих целей дополнительных централизованных процедур (например, распределения RD органами Интернет подобно распределению адресов IPv4), предлагается за счет использования в качестве основы для RD заведомо уникальных чисел - либо номеров автономных систем, либо глобальных адресов интерфейсов PE с магистральной сетью провайдера (в сети провайдера всегда необходимы глобальные адреса для взаимодействия с сетями других провайдеров).

Различитель маршрутов RD имеет длину 8 байтов и состоит из трех полей. Первое поле Type длиной 2 байта определяет тип и разрядность второго поля, которое называется Administrator и однозначно идентифицирует провайдера. Значение 0 поля Type говорит о том, что в поле Administrator указывается IP-адрес интерфейса маршрутизатора PE, и длина данного поля составляет, естественно, 4 байта. Если же значение Type равно 1, то в качестве идентификатора провайдера выбрано значение номера его автономной системы, так что длина поля Administrator составит уже 2 байта. Третье поле носит название Assigned Number, его назначение - обеспечить уникальность адресов VPN в пределах сети провайдера. Значения поля Assigned Number выбирает сам провайдер, при этом использование в качестве поля Administrator IP-адресов интерфейса PE более удобно, так как ограничивает требование уникальности значений Assigned Number пределами отдельного PE.

Документ RFC 2547bis не требует, чтобы все маршруты внутри одной VPN индексировались одним и тем же значением RD. Более того, один и тот же сайт,

подключенный к разным интерфейсам одного PE или к разным PE, может иметь различающиеся RD. Благодаря этому путь к одному и тому же узлу может описываться разными маршрутами, что дает возможность выбора того или иного маршрута для различных пакетов. Однако принципиально важно, чтобы RD разных VPN не совпадали.

Пересылка пакета по сети MPLS VPN. Пусть, например, из сайта 1 в VPN A узел с адресом 10.2.1.1/16 (16 - класс эквивалентности при доставке FEC) отправляет пакет узлу сайта 2 этой же VPN, имеющему адрес 10.1.0.3/16 (рис. 4.9). Стандартными транспортными средствами IP-пакет доставляется на пограничный маршрутизатор сайта CE1A, в таблице которого для номера сети 10.1.0.0 в качестве следующего маршрутизатора указан PE1. На маршрутизатор PE1 пакет поступает с интерфейса int2, поэтому для выбора дальнейшего продвижения пакета он обращается к таблице VRF 1A, связанной с данным интерфейсом.

В таблице VRF 1A адресу 10.1.0.0 соответствует запись протокола BGP, которая указывает, 4to очередным маршрутизатором для пакета определен PE2. Следующее поле записи содержит значение метки Lvpn = 7, определяющей интерфейс выходного маршрутизатора PE, которое должно быть присвоено пакету для того, чтобы он попал в нужную VPN. Здесь также указывается, что запись была сделана протоколом BGP, а не IGP. На этом основании маршрутизатор PE «понимает», что очередной маршрутизатор не является непосредственным соседом, и путь к нему надо искать в глобальной таблице маршрутизации.

В глобальной таблице для адреса PE2 указывается начальное значение метки L пути LSP, равное 3. Способ его прокладки между маршрутизаторами PE1 и PE2 не имеет в данном случае принципиального значения - главное, чтобы такой путь существовал.

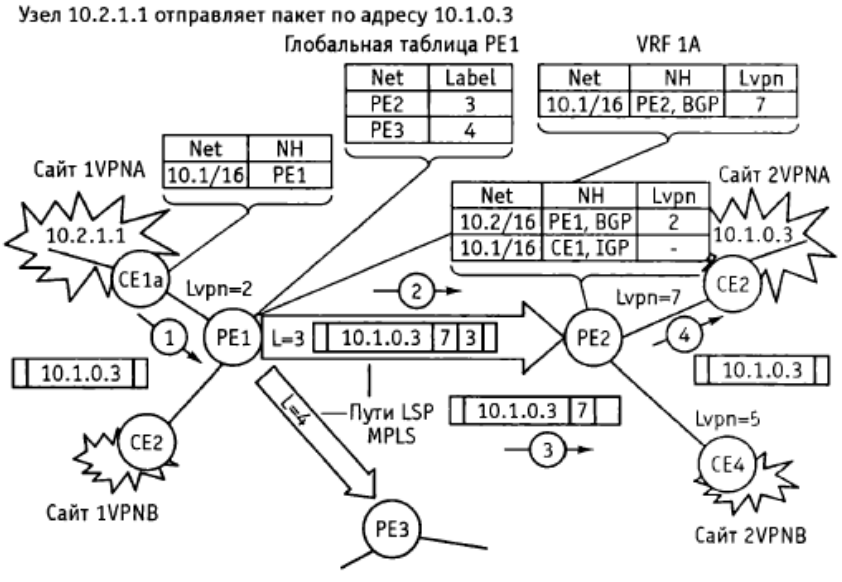


Рис. 4.9. Путешествие пакета между сайтами VPN

Технология MPLS VPN использует иерархические свойства путей MPLS, за счет чего пакет может быть снабжен несколькими метками, помещаемыми в стек. На входе во внутреннюю сеть провайдера, образуемую маршрутизаторами P (LSR), пакет будет снабжен двумя

метками - внутренней Lvpn = 7 и внешней L = 3. Метка Lvpn интерпретируется как метка нижнего уровня - оставаясь на дне стека, она не используется, пока пакет путешествует по туннелю PE1-PE2. Продвижение пакета происходит на основании метки верхнего уровня, роль которой отводится метке L. Каждый раз, когда пакет проходит очередной маршрутизатор P вдоль туннеля, метка L анализируется и заменяется новым значением. И только после достижения конечной точки туннеля маршрутизатора PE2 из стека извлекается метка Lvpn. В зависимости от ее значения пакет направляется на тот или иной выходной интерфейс маршрутизатора PE2.

Из таблицы VRF 2A, связанной с данным интерфейсом и содержащей маршруты VPNA, извлекается запись о маршруте к узлу назначения, указывающая на CE2 в качестве следующего маршрутизатора. Заметим, что она была помещена в таблицу VRF 2A протоколом IGP. Последний отрезок путешествия пакета от CE2 до узла 10.1.0.3 осуществляется традиционными средствами IP.

Несмотря на достаточно громоздкое описание механизмов MPLS VPN, процесс конфигурирования новой VPN или модификации существующей достаточно прост, поэтому он хорошо формализуется и автоматизируется. Для исключения возможных ошибок конфигурирования - например, приписывания сайту ошибочной политики импорта/экспорта маршрутных объявлений, что может привести к присоединению сайта к чужой VPN, - некоторые производители разработали автоматизированные программные системы конфигурирования MPLS. Примером может служить Cisco VPN Solution Center, который снабжает администратора средствами графического интерфейса для формирования состава каждой VPN, а затем переносит полученные конфигурационные данные в маршрутизаторы PE.

Повысить степень защищенности MPLS VPN можно с помощью традиционных средств: например, применяя средства аутентификации и шифрования IPSec, устанавливаемые в сетях клиентов или в сети провайдера. Услуга MPLS VPN может легко интегрироваться с другими услугами IP, например, с предоставлением доступа к Интернет для пользователей VPN с защитой их сети средствами межсетевого экрана, установленного в сети провайдера. Провайдер также может предоставлять пользователям MPLS VPN услуги, базирующиеся на других возможностях MPLS: в частности, услуги с предоставлением гарантированного качества обслуживания на основе методов MPLS TE. Что же касается сложностей ведения в маршрутизаторах провайдера таблиц маршрутизации пользователей, на которые указывают некоторые аналитики, то они несколько преувеличены, так как таблицы создаются автоматически, с помощью стандартных протоколов маршрутизации, и только на пограничных маршрутизаторах PE.

Механизм виртуального маршрутизатора полностью изолирует эти таблицы от глобальных таблиц маршрутизации провайдера, что обеспечивает необходимые уровни надежности и масштабируемости решений MPLS VPN.

3.5. Обобщенная многопротокольная коммутация по меткам (GMPLS)

Технология обобщенной (универсальной) многопротокольной коммутации по меткам (Generalized Multi-Protocol Label Switching, GMPLS) была разработана технической комиссией Интернет (Internet Engineering Task Force, IETF). В проекте стандарта GMPLS говорится:

«Сети будущего будут состоять из таких систем, как маршрутизаторы, DWDM системы, Add-Drop мультиплексоры (ADMS), фотонные (PXCs) или оптические коммутаторы (OXCs), которые будут использовать GMPLS».

В GMPLS используются концепции и протоколы, разработанные применительно к MPLS. В GMPLS принцип коммутации по меткам расширен применительно к оптическим сетям. Здесь, в отличие от MPLS, вместе с меткой необходимо передавать информацию о ее типе, поскольку в качестве меток могут быть выбраны различные компоненты - длина волны λ, номер оптического волокна в канале, номер SDH-контейнера и т.д. В настоящий момент предложены следующие базовые типы меток:

- Packet - метка, идентифицирующая Ethernet (GE, FE);
- PDH - метка, идентифицирующая кадры ETSI/ANSI POH (T1, E1, E3);
- SONET/SDH - метка, идентифицирующая контейнеры SONET/SDH (VT, VC, STS-n, STM-n);
- Digital Wrapper - метка OTN G.709 (2,5,10, 40 Гбит/с);
- λ - длина волны при использовании фотонных λ-коммутаторов OXC;
- Fiber - метка, идентифицирующая номер оптического волокна;
- Fiber Channel - метка, идентифицирующая оптический канал.

Перечисленные выше типы меток описывают тип устанавливаемого соединения LSP, а не транспортной технологии, через которую данный LSP устанавливается. Например, использование метки X означает, что устанавливаемое соединение LSP следует обеспечивать прозрачно без оптико-электрических преобразований. Тип метки Ethernet означает, что следует также обеспечить синхронизацию и, возможно, согласование скоростей на транзитных коммутаторах. В свою очередь, при запросе, например метки SONET/SDH, необходимо указывать тип и количество контейнеров.

GMPLS эволюционировала от MPLS (через MPA.S) путем расширения существующей парадигмы коммутации по меткам, от технологий коммутации пакетов/ячеек/фреймов к

технологиям, ориентированным на установление соединения. Хотя принцип коммутации по меткам был изначально внедрен для повышения скорости маршрутизации в IP-сетях (посредством исключения трудоемкого сравнения полных префиксов), акцент сместился в сторону увеличения стабильности, улучшению QoS и более гибким и эффективным механизмам управления (возможных благодаря улучшенному планированию трафика).

GMPLS охватывает всю сферу коммутационных возможностей: от коммутации пакетов до коммутации оптических волокон. GMPLS не только использует концепцию MPLS (например, планирование трафика MPLS и восстановление), но и базируется на тех же протоколах маршрутизации (например, OSPF-TE) и сигнализации (RSPV-TE).

Фундаментальная концепция GMPLS (интегрированная плоскость управления, (многоуровневое) восстановление, и распределенное управление) могут быть применены для устранения недостатков существующих технологий для многоуровневых сетей. Повышенная гибкость сети, обеспечиваемая GMPLS, может повысить доходы операторов, так как они могут предложить и твердо придерживаться более строгих (и более прибыльных) соглашений об уровне обслуживания (SLA). А благодаря оптимизированному распределению ресурсов восстановления и эффективным (многоуровневым) механизмам восстановления, можно снизить капитальные затраты (CAPEX). К тому же, автоматическое восстановление - с исключением необходимости в дорогостоящих и вносящих ошибки ручных вмешательствах – может снизить эксплуатационные расходы (OPEX).

Улучшенные возможности- QoS позволяют эффективно передавать через единую сеть сообщения с различными классами обслуживания (Class of Service, CoS), такие, как голос, видео, и данные с их специфическими требованиями в плане задержки, джиттера и доступности. Гибкое и эффективное сетевое управление, предоставленное унифицированной плоскостью управления GMPLS, позволяет быстрее и проще вводить (новые) услуги, что также приводит к увеличению прибылей (более ранней тарификации услуг) и снижению эксплуатационных затрат (OPEX) благодаря упрощенному сетевому управлению.

4. Объединение традиционной телефонной сети и пакетной сети на основе технологии Softswitch

Сеть сигнализации является основой для всех телекоммуникационных служб, находящихся в сетях разных типов. И хотя сигнальная архитектура интеллектуальных сетей будущего полностью не определена, некоторые ее важные черты ясны уже сегодня. Так, она будет поддерживать разнообразные протоколы, чтобы операторы смогли оказывать многочисленные новые услуги в интеллектуальных сетях, построенных с использованием унаследованной инфраструктуры. «Стандартный» набор возможностей, которыми обладает классическая сигнализация телефонных сетей общего пользования (ТфОП) - обнаружение неисправностей, разделение сигнальной нагрузки, распределенный интеллект, будет усилен за счет масштабируемости, быстродействия и экономичности пакетных сетей.

В сетях будущего важную роль сохранит сигнализация ОКС №7. Она будет отвечать за перенаправление вызова, запоминание данных о вызове и другие функции обработки вызовов, работу бизнес-приложений - расчет с абонентами (биллинг), индивидуальное обслуживание абонентов и т.д., а также за предоставление многих услуг нового поколения - уведомление абонента, работающего on-line, о поступлении вызова, оказание услуг по предоплате, навигацию в Интернет при подключении on-line по беспроводной сети и др. В то же время комбинация технологий IP и ОКС № 7 на уровне сигнальной сети позволит операторам воспользоваться преимуществами сетей обоих типов: сохранить инвестиции, вложенные в построение инфраструктуры интеллектуальных сетей (IN), и перейти к конвергированным сетям, использующим протоколы сигнализации для передачи голоса через IP. В конвергированных сетях IP-технологии помогут поддерживать сеансы мультимедиа, новые режимы доступа абонентов, новые услуги, более эффективно использовать полосу пропускания и, как результат, значительно снизить расходы операторов.

Стыковка сетей традиционной телефонии с сетями пакетной коммутации в современных конвергированных сетях осуществляется на основе общей сигнальной сети, обеспечивающей независимое управление передачей информации и соединяющей разнородные сети. Общая сигнальная сеть позволяет провайдерам оказывать услуги, присущие ТфОП, с гибкостью и эффективностью, которые свойственны пакетным сетям.

Современная инфраструктура сигнальных сетей развивается в направлении распределенной архитектуры, которая основана на использовании технологии Softswitch.

По мере того как интеллект сигнальной сети будет возрастать, сети сигнализации начнут приближаться к информационным системам, решающим задачи сетевого планирования, предотвращения мошенничества, расчетов с абонентами, гарантированного предоставления услуг и поддержки других бизнес-приложений, а операторы инфраструктуры станут широко применять методы искусственного интеллекта для анализа сигнальной информации.

4.1. Оборудование для сетей на основе Softswitch от компании ZTE

Компания ZTE считает целесообразным использовать оборудование Softswitch прежде всего для построения NGN классов 4 и 5. NGN класса 4 (тандемного типа) предоставляет абонентам услуги передачи голоса и данных: местные и междугородные соединения VoIP между абонентами ТфОП и услуги ПД по сети IP. В NGN класса 4 отсутствуют коммутаторы ТфОП с входящими интерфейсами соединительных линий, а подключение ТфОП к IP-сети осуществляется с помощью сигнального и транспортного шлюзов. NGN класса 5 будет предоставлять услуги VoIP, что позволяет избежать крупных инвестиций для построения телефонных узлов и ПД. Исключены любые коммутаторы ТфОП, а медные пары абонентов подключаются непосредственно к шлюзам NGN или устройствам интегрированного доступа.

NGN классов 4 и 5 предложат абонентам большой набор услуг, что делает технологию Softswitch весьма привлекательной для операторов и сервис-провайдеров.

Компания выделяет следующие технологические преимущества своего оборудования:

1. Полностью конвергированные услуги передачи голоса и данных в IP-сети, возможность подключения к ТфОП. Высокие показатели QoS голосовой связи.

2. Высокая производительность - поддержка более 2 млн соединений в ЧНН при использовании одного контроллера Softswitch и более 6 млн. соединений при каскадном соединении трех котроллеров.

3. Гибкие сетевые решения для построения NGN класса 4 (услуги междугородной связи) и класса 5 (услуги местной связи с помощью устройств интегрированного доступа IAD).

4. Возможность сохранения коммутаторов ТфОП путем подключения NGN к ТфОП с помощью сигнального и транспортного шлюзов.

5. Надежная система управления NGN.

6. Разумные цены и четкое обслуживание абонентов.

Таблица 5.1. **Проекты компании ZTE**

Операторы	Количество абонентов	Трафик, мин./день	Стоимость, долл./мин.
China Netcom	21 000	170 000	0,03…0,04
China Unicom	Коммерческое тестирование с 1000 абонентов		
China Railway	Коммерческое тестирование с 1000 абонентов		
China Telecom	> 6000 абонентских линий в 400 IP phone 150 000 1. ZTE, Huawei, Alcatel, Cisco и VocalTel приняли участие в первом этапе тендера по проекту TT&T NGN 2. ZTE и Huawei вышли на второй этап тендера. Softswitch от ZTE прошел все виды тестирования для TT&T. В настоящее время ZTE и TT&T ведут переговоры о дальнейшем сотрудничестве		
Thailand TT&T Project			
Hong Kong Wharf NGN	1. ZTE и Lucent и Nortel приняли участие в первом этапе тендера по проекту Hong Kong Wharf NGN 2. ZTE и Nortel вышли на второй этап тендера. Softswitch от ZTE прошел все тесты для Hong Kong Whart NGN project. В настоящее время ZTE и Hong Kong Wharf NGN ведут переговоры о дальнейшем сотрудничестве		
Philippine Digital NGN	1. ZTE, Huawei, Cisco, Alcatel, UT, Ericsson и Sandra приняли участие в первом этапе тендера по проекту Digital NGN 2. ZTE, Huawei и Cisco вышли на второй этап тендера		
Romania RPO NGN	ZTE – единственный победитель тендера по проекту Romania RPO NGN		

Компания имеет большой опыт реализации NGN проектов (табл. 5.1).

Достоинством оборудования Softswitch, производимого компанией ZTE, является его совместимость с оборудованием других вендоров (табл. 5.2).

Отметим также, что решения ZTE предусматривают интеграцию оборудования с интеллектуальными и мобильными платформами. Так, Softswitch ZTE может использоваться в качестве виртуального SSP (пункта коммутации услуг IN) с поддержкой INAP/TCAP. Пока Softswitch соединяется с мобильными платформами через ТфОП, однако в ближайшее время планируется выпуск проводно-беспроводного контроллера Softswitch, интегрированного с мобильными платформами и работающего в ядре сети 3С.

Таблица 5.2. **Совместимость оборудования**

Вендор	Оборудование	Протокол взаимодействия
Протестировано взаимодействие со следующими Softswitch		
Lucent Softswitch SIP-T		
SS8 SGS SIP-T		
Cisco SIP Proxy SIP		
Siemens Softswitch SIP-T		
Nortel Softswitch SIP-T		
Протестировано взаимодействие со следующими транспортными шлюзами		
Audiocodes MP108, MP100, MP200 MGCP		
InnoMedia MTA3328-4 MGCP		
TAINET VENUS2804 MGCP		
CodentNetworks CS2912 MGCP		
Протестировано взаимодействие со следующими терминалами		
3COM Sip phone SIP		
Pingtel Sip phone SIP		
Welltech Sip phone SIP		
Cisco Sip phone SIP		
Cisco ATA 186 SIP		
PhotonicBridges P103 MGCP		
ACT P103B H.248		
Leadtek BVP8770 (Video Phone) H.323		
INNOmedia MTA3368 (Video Phone) SIP		

В заключение заметим, что Softswitch производства ZTE отвечает требованиям COPM, а NGN ZTE включает в себя систему управления сетью (NMS) для авторизации всех устройств, находящихся под управлением контроллера Softswitch. Опорная сеть IP имеет и другие системы защиты от атак хакеров: брандмауэры, сообщения (traps) SNMP, системные журналы регистрации.

4.2. Примеры использования Softswitch компании ZTE на сетях NGN

4.2.1. Развертывание NGN класса 5 для China Netcom

В августе 2001 г. корпорация ZTE успешно завершила строительство сети NGN на основе Softswitch для компании China Netcom. Это была первая в мире NGN на основе Softswitch, и после ее расширения она стала одной из самых крупных в мире NGN класса 5 (рис. 5.18). На первом этапе производимые ZTE устройства управления Softswitch (ZXSS10 SS1), транковый шлюз TG (ZXSS10 M100) и шлюз сигнализации SG (ZXSG10) устанавливались и конфигурировались на центральной станции с терминалами нескольких типов, такими как интегрированное устройство доступа (IAD), MP100 от Audio Codes и SIP-телефон от PingTel.

SG и TG были подключены к PSTN через фронтальный процессор компании Netcom. На этом этапе были проведены всесторонние испытания системы Softswitch от ZTE с точки зрения рабочих характеристик вызовов.

На втором этапе в жилых домах, в некоторых жилых зонах и на некоторых предприятиях города Ниньбо, имеющих доступ к городской сети (Metropolitan Area

Network, MAN), были установлены оконечные устройства IAD. Развертывание этого оборудования позволило пользователям непосредственно на своем опыте проверить реализацию услуг речевой связи на основе VoIP, предоставляемых платформой Softswitch от ZTE.

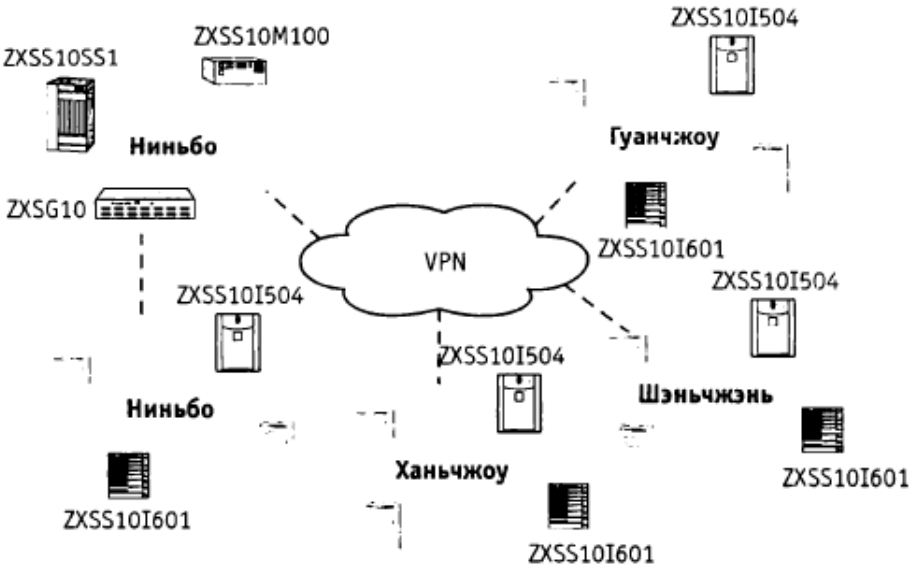


Рис. 5.18. Взаимодействие широкополосных речевых услуг, предоставляемых системой Softswitch от ZTE, в нескольких городских сетях

На третьем этапе устройства IAD были развернуты в других городах, таких как Ханьчжоу, Гуанчжоу и Шэньчжэнь. Все IAD во всех четырех городах функционируют под управлением системы Softswitch, установленной в Ниньбо, которая обеспечила возможность взаимодействия речевых услуг в пределах домена Softswitch через VoIP и взаимодействие между системой Softswitch и сетью PSTN.

Успешное развертывание сети NGN в Ниньбо подтвердило высокую надежность системы Softswitch от ZTE как системы операторского класса и как возможного решения для сети следующего поколения. Проект компании China Netcom в Ниньбо обеспечил предоставление речевых услуг, реализуемых на основе VoIP-услуги системы Softswitch от ZTE, для более чем 30 ООО абонентов.

Сетевая среда. Компания China Netcom, общая пропускная способность линий которой составляет около 40 Гбит/с, планирует создание общенациональной широкополосной телефонной сети на базе технологии Softswitch, которая позволит полностью использовать традиционные ресурсы городских сетей в каждом городе. Этот проект обеспечит обслуживание 100 ООО абонентов в 22 городах.

Для обеспечения заданного качества (QoS) речевых услуг компания China Netcom организовала VPN-сеть передачи речи, охватывающую весь Китай. VPN-сеть используется для объединения речи и данных, для того чтобы обеспечить приоритет речевой информации и облегчить управление сетью передачи речи. В речевой VPN

используются частные IP-адреса. Речевое взаимодействие в сети MAN реализуется посредством внутренней маршрутизации в MAN, а речевое взаимодействие между сетями MAN обеспечивается за счет MPLS VPN, развернутой между смежными сетями MAN. Взаимодействие на уровне передачи данных с другими MAN компании China Netcom или сетями общего пользования реализуется через NAT, подключенный к оборудованию на базовом уровне MAN посредством трансляции адресов и преобразования данных.

Организация сети. В соответствии с сетевой средой и проектными требованиями China Netcom корпорация ZTE предложила решение по локальному речевому доступу на базе Softswitch + TG + SG + IAD (включая два типа IAD с одним или несколькими интерфейсами), облегчающее реализацию пользовательского доступа и позволяющее полностью использовать сетевые ресурсы. Система состоит из базового устройства управления Softswitch, транкового шлюза, шлюза сигнализации, устройства IAD и полноценной системы управления сетью и биллинга (рис. 5.19).

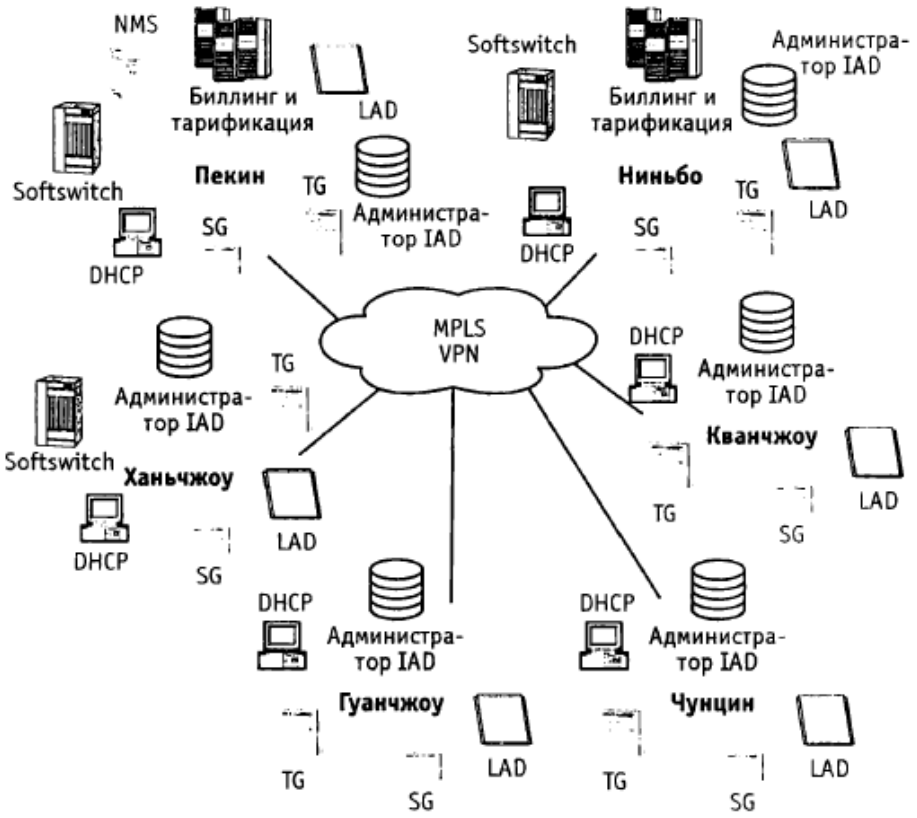


Рис. 5.19. Широкополосная телефонная сеть компании China Netcom, построенная на основе Softswitch от ZTE

На данный момент завершено строительство сети в 22 основных городах, таких как Пекин, Ханьчжоу, Ниньбо, Шанхай, Гуанчжоу и т.д., при этом базовое устройство управления ZXSS10 SS1 расположено в Пекине, и начальная проектная емкость составляет 100 000 абонентов.

4.2.2. Развертывание NGN класса 4 для China Telecom

В декабре 2001 г. корпорация ZTE со своей системой Softswitch выиграла тендер на участие в проекте построения сети следующего поколения компании China Telecom на основе Softswitch, став, таким образом, единственным национальным поставщиком подобного оборудования. В рамках этого проекта China Telecom предполагает провести испытания технологии Softswitch и приобрести дополнительный опыт по ее использованию, а также проверить преимущества системы Softswitch и возможность ее применения в сети следующего поколения. N1GN прошла испытания в сетях пакетной коммутации компании China Telecom, при этом в качестве базовой IP-сети использовалась сеть China Netcom, а в качестве базовой сети ATM – мультимедийная широкополосная сеть общего пользования. ZTE предлагает всеобъемлющее сквозное решение для системы NGN, позволяющее проверить различные варианты ее применения, включая создание крупномасштабной сети, восстановление в аварийных ситуациях, возможность взаимодействия сетей, доступ с использованием различных терминалов, передачу изображений/видеоинформации и т.д.

В соответствии с проектом системы в городе Шэньчжень было установлено два комплекта устройства управления Softswitch ZXSS10 SS1 и два комплекта шлюзов сигнализации ZXSS10 S200. Один комплект медиа-шлюза ZXSS10 M100 был установлен в Гуанчжоу, а другой - в Шэньчжене. В качестве пользовательских терминалов в этом проекте использовались устройства IAD, SIP-телефон и PC-телефон (рис. 5.20).

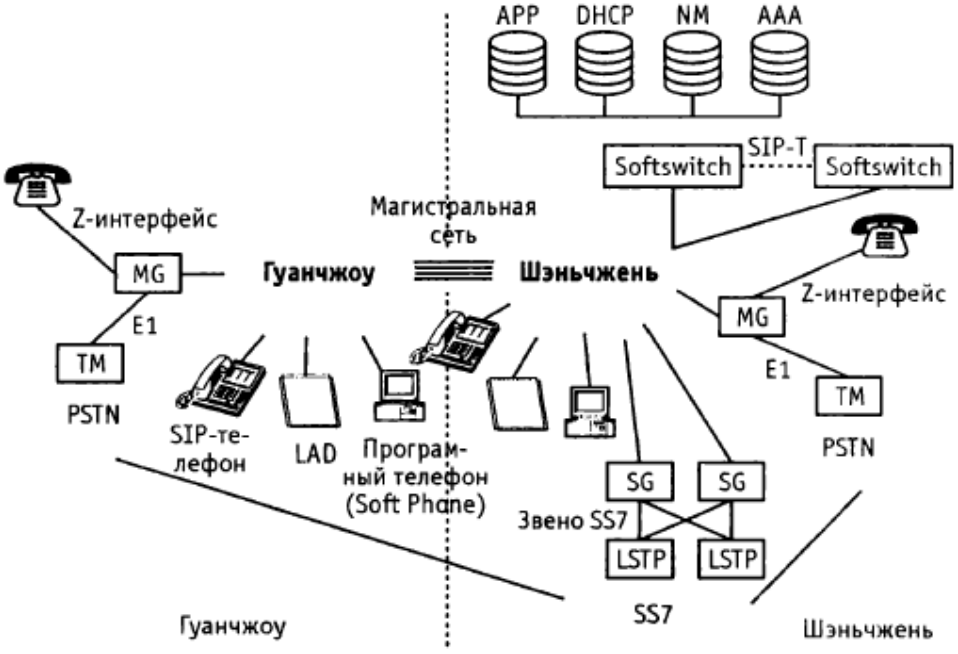


Рис. 5.20. Архитектура экспериментальной сети NGN компании China Telecom

5. Качество обслуживания в IP-сетях

Вопросы качества обслуживания (QoS) в IP-сетях в последнее время стали особенно актуальными, поскольку от их решения напрямую зависит архитектура перспективной сети связи XXI века.

За последние несколько лет в рамках организации IETF было предложено несколько архитектур и механизмов, призванных в той или иной степени обеспечить QoS. Наиболее известными и реализованными являются IntSerf, DiffSerf, MPLS (GMPLS), а также механизм принудительной маршрутизации.

5.1. Стандарты QoS ITU-T для IP-сетей

Для поддержки конвергенции IP-сетей и сетей ТфОП, IP-сети должны обеспечивать надежное дифференцированное QoS для разнообразных приложений пользователей, включая телефонию. Для обеспечения QoS из конца в конец, провайдерам IP-сетей необходимо согласовать общий набор параметров производительности передачи IP-пакетов и задачи QoS. Далее будут рассмотрены две новые рекомендации ITU-T, Y.1540 и Y.1541 по вопросам QoS.

5.1.1. Постановка вопроса

Существует широко распространенное мнение, что сегодняшние сети КК и КП постепенно объединятся в сети, основанные на IP-инфраструктуре, которая будет переносить как трафик ТфОП, так и традиционных приложений Internet. Такой сценарий конвергенции привлекателен тем, что. обеспечивает как снижение себестоимости через объединение технологий, так и развитие индустрии через создание новых услуг. Однако на практике конвергенция идет довольно медленно. С технической точки зрения главным камнем преткновения оказалась проблема качества обеспечения обслуживания (QoS). Традиционные IP-сети используют подход «наилучшей попытки» (best effort) к качеству, предоставляющий пользователям справедливую долю доступных сетевых ресурсов, но не гарантирующий выполнения никакого определенного уровня производительности. Принцип best effort был достаточно эффективен для поддержки приложений нереального масштаба времени (электронная почта, передача файлов) и был расширен для приложений, близких к реальному масштабу времени (аудио/видео вещание, просмотр Web). Основанная на текущем избытке пропускной способности многих маршрутов, парадигма наилучшей попытки сталкивается с сегодняшними потребностями многих пользователей в интерактивной голосовой телефонии и в других приложениях реального времени.

Однако маловероятно обеспечить качество, ожидаемое пользователями интерактивной голосовой телефонии и других приложений реального времени, когда ограничения пропускной способности приводят к существенному увеличению величины задержки или к потерям пакетов.

Для того чтобы реализовать полностью полезный эффект от конвергенции, будущие, основанные на IP-сети, нуждаются в использовании новых принципов разделения ресурсов, способных надежно обеспечить дифференцированное QoS для большого и многообразного набора пользовательских приложений, включающих, что особенно важно, голос поверх IP (VoIP).

Решения QoS из конца в конец для IP делают возможной успешную конвергенцию IP/ТфОП, которая может быть реализована, например, в три шага:

1. Выполнение сетевыми провайдерами соглашений относительно общего набора параметров производительности IP и требований QoS.

2. Развертывание сетевых механизмов, поддерживающих заданные требования QoS на участке терминал-терминал.

3. Внедрение требований QoS в протоколы сигнализации для возможности создания по запросу IP-потоков с гарантированным QoS.

13-я исследовательская группа Международного Союза Электросвязи (сектор стандартизации телекоммуникаций) - МСЭ-Т недавно выпустила два международных стандарта (рекомендации), которые выполняют первый из этих трех шагов. Первая рекомендация, Y.1540, определяет стандарты параметров производительности для передачи пакетов в IP-сетях. Вторая, Y.1541, специфицирует требования к стыку сетевой интерфейс-сетевой интерфейс (network-interface-tonetwork-interface, NI-NI) для параметров рекомендации Y.1540 и группирует эти численные требования по шести классам QoS для IP-сетей. Далее будет описываться развитие этих новых рекомендаций, выводы по их техническому содержанию, а также будет определено, что еще необходимо сделать для оптимизации их использования в будущих IP-сетях, гарантирующих QoS.

5.1.2. Рекомендация Y.154Q

Рекомендация Y.1540 определяет параметры, которые будут использоваться для спецификации и оценивания скорости, точности, надежности и готовности передачи IP-пакетов в международных сетях передачи данных. Параметры могут быть использованы для описания IP-потоков из конца в конец и отдельных частей сети, поддерживающих такие потоки. В соответствии с определениями Y.1540, транспорт без установления соединения является отличительной чертой IP. Y.1540 применяется к IP-потокам с

использованием IP протокола четвертой версии (IP Version 4, IPv4). Однако здесь следует отметить, что принципы и рекомендации для протокола IP шестой версии (IPv6) остаются теми же самыми.

Предполагаемые пользователи рекомендации Y.1540 - это провайдеры IP-сетей, производители оборудования и конечные пользователи. Провайдеры будут использовать Y.1540 при планировании, разработке и оценивании IP-сетей во взаимодействии с необходимой пользователям производительностью. Один крупный сетевой провайдер уже использует параметры рекомендации Y.1540 для мониторинга производительности передачи пакетов. Производители будут использовать Y.1540 при разработке и сбыте оборудования, согласующегося со спецификациями провайдера. Конечные пользователи будут применять рекомендацию для оценки производительности IP-сетей по фактическому взаимодействию между терминалами.

Процесс разработки параметров. На рис. 6.1 показан трехшаговый процесс, который традиционно использовался 13-й исследовательской группой ITU-T при разработке параметров работы цифровых сетей, и в данном же контексте установлены границы рассмотрения рекомендации Y.1540.

Первый шаг заключается в определении интерфейсов, для которых будут применяться параметры специфических событий, которые могут происходить на данных интерфейсах. Сеть моделируется как объединение сетевых сегментов, соединенных каналами передачи данных (звеньями обмена). Интерфейсы между ними, названные точками измерения (Measurement Point, MP), являются функциональными границами, на которых могут быть проведены наблюдения стандартизированных протоколов. Важные, с точки зрения работы, события, которые могут быть посчитаны, измерены во времени или сравнены в точках измерения (MP), будем называть опорными событиями (Reference Event, RE). Специфические опорные события определяются протоколом интерфейса.

Второй шаг заключается в определении набора первичных параметров, которые в совокупности характеризуют работу сети. Первичные параметры связаны с частными коммуникационными функциями и описаны в терминах опорных событий. Коммуникационная функция определяет ожидаемую реакцию сети (или сетевого сегмента) на специфическое внешнее воздействие; воздействия и реакции являются опорными событиями.

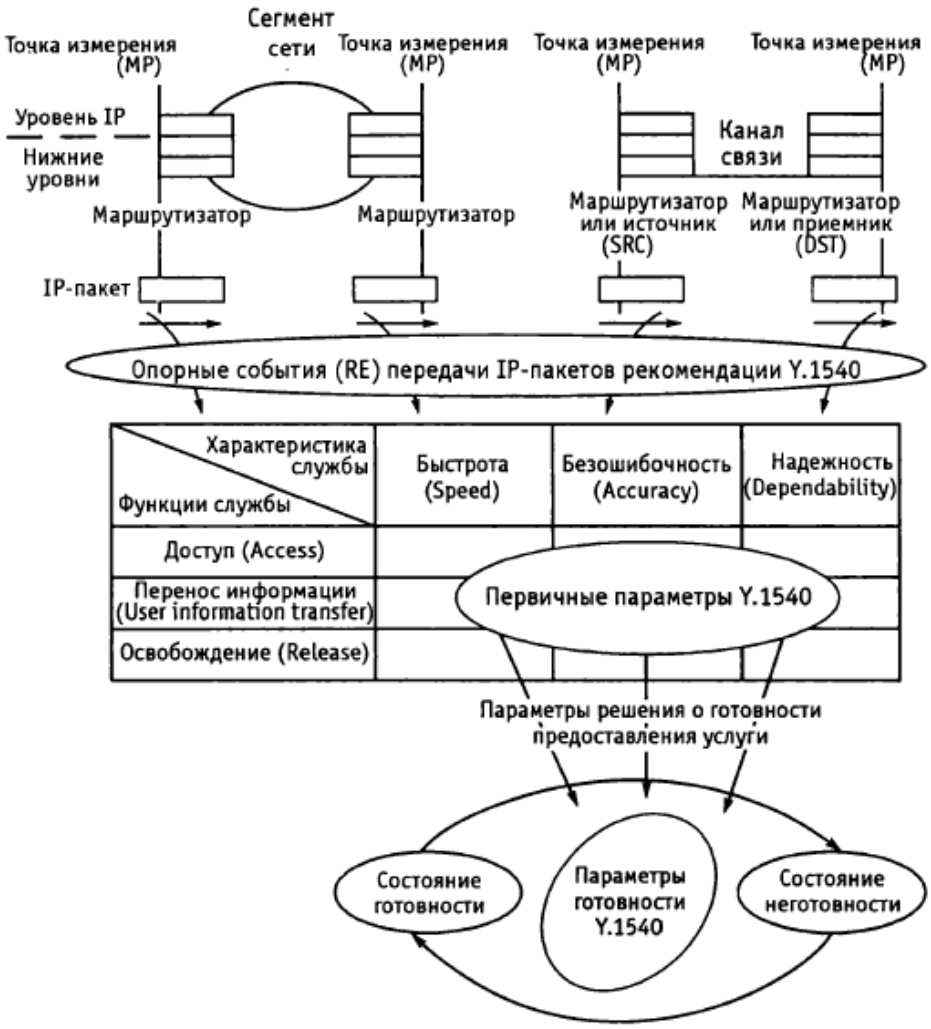


Рис. 6.1. Эталонная модель и область действия рекомендации Y.1540

При описании работы цифровой сети обычно используются три общих коммуникационных функции: доступ, передача пользовательской информации и освобождение.

Согласно статистике, параметры работы случайным образом изменяются на некотором пространстве выборок, которое различает возможные исходы, которые могут быть у функции работы. Для любой дискретной функции можно различить три общих типа исходов: успешная работа, неправильная работа и невыполнение. Соответствующие пользователю критерии работы - это: скорость, безошибочность и надежность. Они связаны с общими коммуникационными функциями в известной матрице размерностью 3x3. Для описания каждой комбинации функция/критерий в матрице определен один или несколько первичных параметров. Матричный подход помогает удостовериться, что не пропущен ни один существенный атрибут.

Третий шаг при разработке параметров заключается в определении набора параметров готовности для описания работы с более долговременной точки зрения. Параметры готовности определяются на основе наблюдаемых значений для подмножества первичных

параметров, параметров решения о готовности. Канал связи между парой (или больше) пользователей может находиться в одном из двух состояний: готовном или неготовном, что определяется функцией готовности, которая сравнивает наблюдаемые значения параметров принятия решения с соответствующими критическими порогами за последовательные периоды наблюдения. Параметры готовности характеризуют бинарный вероятностный процесс в статистических терминах.

При разработке Y.1540 13-я исследовательская группа согласилась, что точки измерений (MP) являются юридическими границами, которые разделяют независимо управляемые IP-сети (автономные системы) и пользовательские терминалы. Подходящим интерфейсным протоколом является IPv4, а подходящими информационными блоками - IP-пакеты.

Опорное событие передачи IP-пакета (IP Packet Transfer Reference Event, IPRE) для указанной пары источник/получатель (SRC/DST) происходит, когда IP-пакет с определенными IP-адресами SRC/DST (и правильной контрольной суммой заголовка) пересекает MP. Единственная коммуникационная функция, к которой обращается рекомендация Y.1540 - это передача IP-пакета (IP packet transfer), функции доступа и освобождения не рассматриваются. Это отражает тот факт, что сегодня IP-сети - это сети без установления соединения. ITU-T SG 13 и другие исследовательские группы разрабатывают параметры работы для IP-сетей, которые могли бы поддерживать такие функции в будущем (например, установление и разъединение ориентированных на соединение потоков).

Рекомендация Y.1540 определяет четыре индивидуальных результата передачи пакета, основанных на опорных событиях (RE) в точках измерений (MP), что в упрощенном виде показано на рис. 6.2. Приходящий в сегмент IP-пакет, на входящей MP может столкнуться со следующими исходами: успешная передача, ошибка или потеря.

IP-пакет, который появляется на входящей MP без соответствующей исходящей, будем называть ложным. События и результаты при передаче IP-пакета в рекомендации Y.1540 определены более формально, принимая во внимание общую информацию маршрутизации и возможность фрагментации пакетов. Различная маршрутизация объясняется определением в данное время и для данного IP-потока из конца в конец набора допустимых входящих и исходящих MP. Фрагментация пакетов объясняется определением результатов передачи пакетов когда RE на одной MP кончается несколькими соответствующими событиями на других MP. (Y.1540 также определяет результат потери мультипакетного блока и связанный с ним параметр - коэффициент потери блоков для определения и ограничения последовательных или сгруппированных

(пачечных) событий потери блоков). Рабочие параметры передачи IP-пакетов. Рекомендация Y.1540 определяет пять рабочих параметров передачи IP-пакетов на основе результатов, приведенных на рис. 6.2.

Задержка передачи IP-пакета (IP Packet Transfer Delay, IPTD) – это время ($t_2 – t_1$) между возникновением двух, связанных с передачей IP пакета, событий: входящее событие RE_1 в момент времени t_1 и исходящее событие RE_2 в момент времени t_2, где ($t_2 > t_1$) и ($t_2 – t_1$) ≤ T_{max}. IPTD определен для всех удачных и ошибочных результатов передачи пакетов. Если пакет фрагментирован, то t_2 - это время соответствующего последнего выходного события. Подразумевается, что задержка передачи IP-пакета, специфицированная в рекомендации Y.1541 - это среднее арифметическое задержек IP-пакетов.

Джиттер задержки IP-пакетов (IP Packet Delay Variation, IPDV) определяется на основе наблюдений соответствующих потоков IP-пакетов на входящих и исходящих MPs (например, MP_1 и MP_2 на рис. 6.13). Джиттер задержки пакетов (v_k) для IP-пакета к между MP_1 и MP_2 - это разность между абсолютной задержкой (x_k) передачи IP-пакета и определенной задержкой ($d_{1,2}$) передачи контрольного IP-пакета между этими самыми MPs: $v_k = x_k - d_{1,2}$. Задержка передачи контрольного IP-пакета $d_{1,2}$ между SRC и DST - это абсолютная задержка передачи IP-пакета, определяемая первым IP-пакетом между этими двумя MPs. (Положительные значения IPDV соответствуют большим задержкам пакета, чем определенные контрольным пакетом, а отрицательные значения - соответственно меньшим. Распределение !PDV идентично распределению абсолютных задержек передачи пакетов, сдвинутых на постоянную величину $d_{1,2}$).

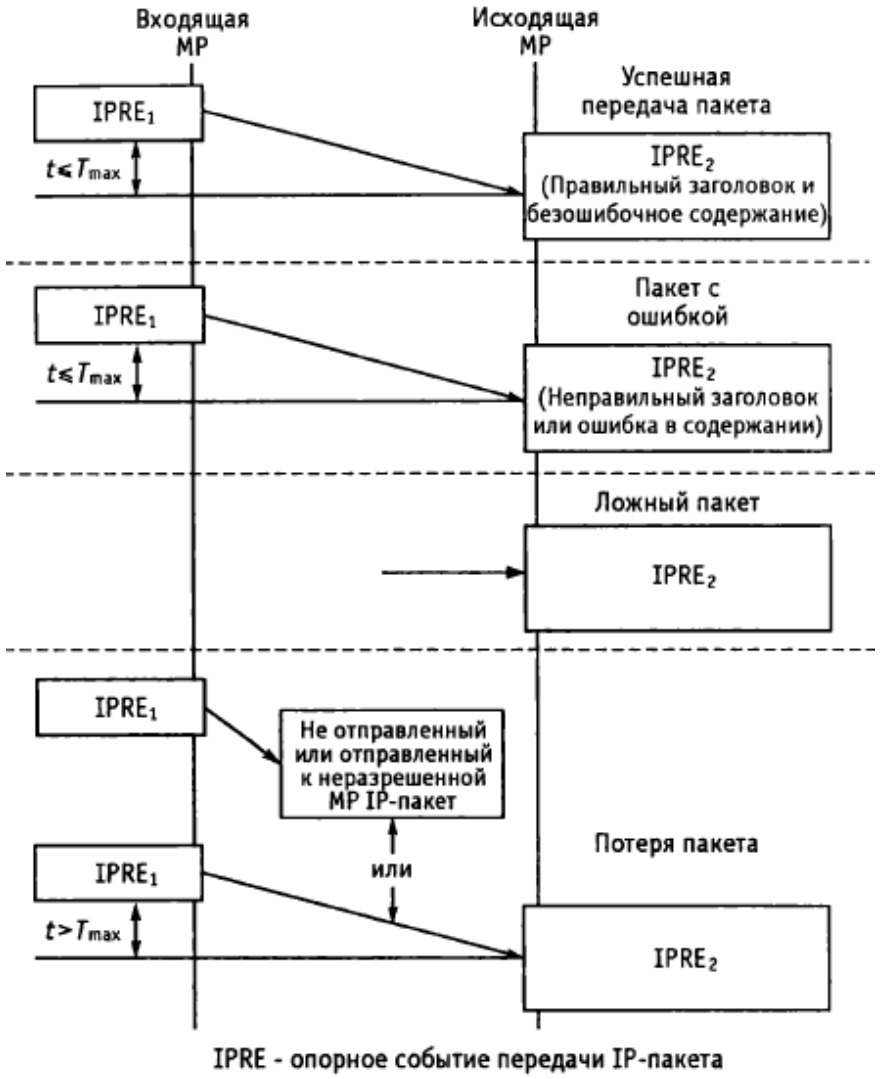


Рис. 6.2. Возможные исходы передачи IP-пакета

Коэффициент потери IP-пакетов (IP Packet Loss Ratio, IPLR) – это отношение общего числа потерянных пакетов к общему числу переданных пакетов в общей совокупности.

Уровень ложных пакетов (Spurious IP packet rate, SIPR) на исходящей MP - это общее число ложных пакетов, наблюдаемых на исходящей MP в течение определенного интервала времени, ограниченного длительностью этого интервала (например, число ложных пакетов в секунду). Этот параметр выражен как уровень за определенное время, а не как отношение, поскольку механизмы, причиной которых является появление ложных пакетов, имеют мало общего с числом переданных IP-пакетов.

Хотя и не исчерпывающе, эти параметры вместе описывают основные рабочие отношения пользователей IP сетей. Задержка передачи IP-пакета описывает среднее время, затрачиваемое сетью на передачу пакета между входящей и исходящей MP. Ограничения IPTD будут решающими для успешного развертывания VoIP, видеоконференцсвязи и приложений реального времени и будут оказывать сильное влияние на принятие клиентами других услуг. Изменение задержки пакетов характеризует

джиттер во времени опорных событий передачи пакета на исходящем интерфейсе по отношению к соответствующей модели входных событий. IPDV должен контролироваться для избежания недогрузки или перегрузки IP-маршрутизаторов или буферов терминалов. Коэффициент потери IP-пакетов выражает вероятность того, что пакет, вверенный сети на входном интерфейсе, не доставлен соответствующей выходной точке (точкам).

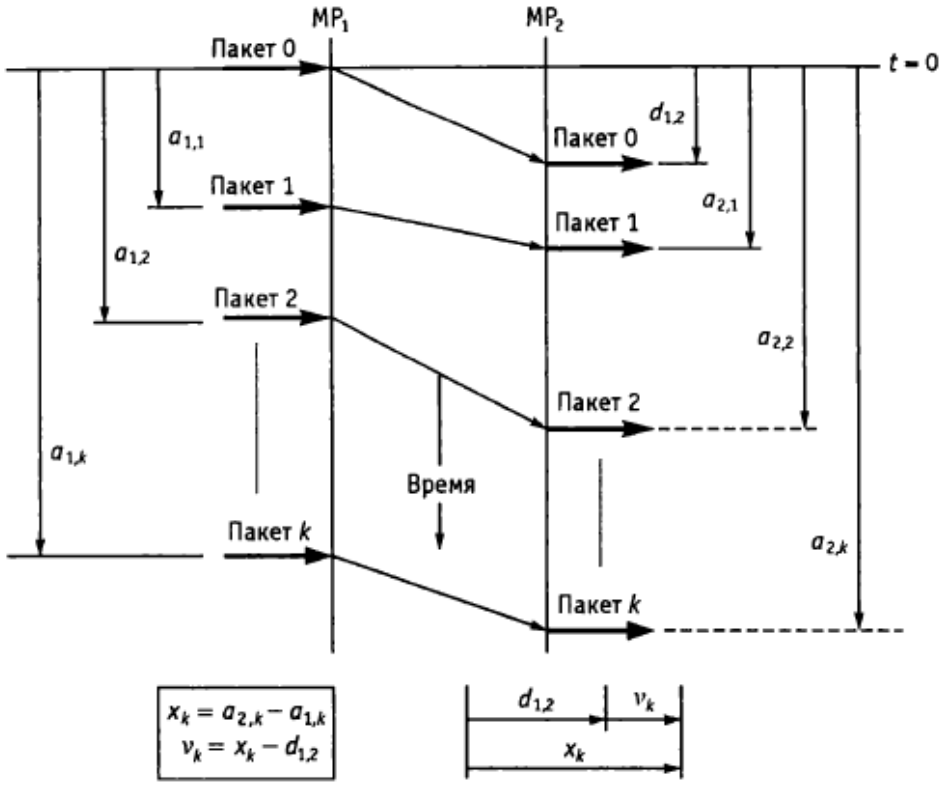


Рис. 6.3. Джиттер задержки IP-пакетов

Коэффициент IPLR должен ограничиваться для гарантирования разборчивости и приемлемого качества изображения для голосовых и видеоприложений реального времени, а также обеспечения приемлемого качества других приложений. (Учет последовательной потери пакетов представляет особый интерес для некоторых неэластичных приложений реального времени, таких как голос и видео. Коэффициент потери блоков - один из путей для характеристики таких событий). Коэффициент ошибок IP-пакетов и уровень ложных пакетов выражают вероятность, что данные пользователя на выходном интерфейсе отличаются от входных данных в результате искажения, дублирования или неправильной маршрутизации в сети.

В нормативном наборе рекомендаций Y.1540 отсутствуют любые параметры, которые описывают скорость передачи данных пользователя или пропускную способность, обеспечиваемую сегментом сети. Y.1541 обращает внимание на то, что производительность и другие связанные с потоками вопросы рассматриваются, используя дескриптор трафика IP-сети, определенный в сопутствующей рекомендации Y.1221. База

для возможной будущей работы по определению метрик большой пропускной способности представлена в RFC 3148.

Параметры готовности. Как определено в Y.1540, готовность относится к однонаправленному IP-потоку между определенной парой (или набором) MP. В Y.1540 функция готовности определяет IPLR как единственный параметр принятия решения о доступности. Для данного потока сетевой сегмент определяется как готовный на отрезке наблюдения, если наблюдаемое значение IPLR для потока ниже порога c_1. Иначе сегмент не готовен. Y.1540 определяет значение c_1 равное 0,75 и отмечает, что спецификации ожидаемого значения IPLR должны исключать все периоды неготовности (т. е. все интервалы времени, в течение которых наблюдаемое значение IPLR превышает Ст). Рекомендация определяет минимальный период наблюдения готовности в 5 мин. (Мониторинг низкоуровневой работы и ошибок сетевых элементов может разрешить идентификацию надвигающейся неготовности в более короткое время и направить корректирующее действие.) Определение готовности предназначено для использования в работе характеризуемой сети как для нормального трафика между источником и получателем, так и для синтетического трафика, генерируемого наборами тестов или другими устройствами измерения. Y.1540 отмечает, что испытательный трафик должен быть ограничен так, чтобы это не вызывало перегрузок, которые могут исказить результаты испытаний.

Рекомендация Y.1540 определяет два рабочих параметра готовности. Для данного сетевого сегмента и потока процент готовности – это доля от запланированного времени готовности, в течение которого сегмент фактически поддерживает поток в готовном состоянии. Процент неготовности - это дополнение предыдущего параметра, т. е. доля от запланированного времени готовности, в течение которого поток является неготовным.

При любом задании сумма двух значений равна 100 %. Базовый период для планирования времени готовности ограничен, чтобы исключить любые согласованные периоды неготовности (например, запланированное время простоя для профилактического техобслуживания).

5.1.3. Рекомендация Y.1541

Рекомендация ITU-T Y.1541 определяет числовые значения, которые должны быть достигнуты на международных отрезках IP-сетей между оконечными терминалами пользователей для каждого из ключевых параметров работы, определенных в рекомендации Y.1540. Указанные значения сгруппированы в некоторое число различных классов QoS для установления практической базы для связи между конечными

пользователями и провайдерами сетей, а также и среди провайдеров по качеству, которое будет поддерживаться из конца в конец на отрезках IP-сетей. С одной стороны, операторы сетей признают, что работа из конца в конец ограничивается самым плохо работающим сегментом сети, и требования пользовательских приложений могут быть удовлетворены только, если каждая из объединенных сетей разработана и функционирует с учетом этих требований. С другой стороны, операторы знают, что наличие рабочих спецификаций дает ощутимый толчок сетевой экономике, играя роль в дифференциации конкурентоспособного продукта и маркетинге, и если оператор берет на себя определенные обязательства, то пользователи ожидают их выполнения. То что эти переговоры регулярно следуют, позволяет, несмотря на технологическое разнообразие независимо управляемых сетей, сотрудничать в обеспечении надежной, высококачественной всемирной связи. При определении характеристик работы из конца в конец для конкретных пользовательских приложений и сетевых технологий, 13-я исследовательская группа ITU-T применила два исторически сложившихся, дополняющих друг друга и конкурирующих подхода для оценки работы. Первый «нисходящий» метод переводит требования приложения пользователя и ожидаемое качество в числовые значения стандартизированных ITU-T параметров, что наблюдается в интерфейсах пользователь/сеть. Такой нисходящий перевод сделан для каждой широкой категории пользовательских приложений и должен обеспечить изменчивость в функциональности терминала и работе. Второй «восходящий» метод переводит технические спецификации, определяющие возможности и ограничения отдельных сетевых элементов в числовые значения тех же самых, стандартизированных ITU-T параметров работы, наблюдаемых в тех же самых интерфейсах пользователь/сеть. Восходящий перевод основан на базовых конфигурациях, идентифицирующих типичные связи сетевых путей (линий) и узлов, и наихудших значенях ключевых переменных типа географических расстояний между сетевыми интерфейсами. В разделенных сетях также должны рассматриваться и другие переменные, такие как пропускная способность сети, предполагаемый трафик и механизмы управления ресурсами. В идеале, восходящий и нисходящий методы производят наложение диапазонов значений для стандартизированных параметров, из которых одна или более характеристика может быть специфицирована.

Процесс выбора числовых характеристик работы был особенно трудоемким в случае рекомендации У.1541. По нисходящей перспективе ключевой проблемой было охватить разнообразнейший набор пользовательских приложений и терминалов. Участники 13-й исследовательской группы были в состоянии ограничить и сегментировать пространство приложений, систематически рассматривая для каждого приложения функциональные

отношения между удовлетворением пользователя и значениями параметров рекомендации У.1541. Нисходящий анализ был значительно облегчен близкой связью с 12-й исследовательской группой, которая уже много лет специализировалась по вопросам воспринимаемости качества и принятия конечным пользователем определенных приложений и медиа (например, речь, изображение, текст) при ухудшении сетевой передачи, принимая во внимание работу телефонного, аудиовизуального и интерактивного голосового терминалов.

13-я исследовательская группа получила серьезную поддержку в виде информации относительно восходящего подхода от сетевых провайдеров по характеристикам возможностей работы, ограничениям доступных сетевых элементов и определению реалистичных базовых конфигураций.

Восходящий и нисходящий анализы быстро подтвердили, что не существует единственного набора уровней работы IP-сети, который мог бы экономно поддерживать все предполагаемые приложения для будущих, основанных на IP-инфраструктуре сетей; соответственно, 13-я исследовательская группа взяла на себя ответственность по определению нескольких наборов характеристик работы - классов OoS рекомендации Y.1541.

Выбор классов OoS, которые должны были быть включены в Y.1541, обсуждался на 4-й рабочей встрече 13-й исследовательской группы на протяжении нескольких заседаний. В ранних дискуссиях участники рассматривали подход, касающийся каждого параметра, который позволял бы пользователям определять значения для каждого параметра независимо. Однако все довольно быстро согласились, что разрешение подобной свободы выбора будет слишком сложно осуществить. Фактически имелось четкое согласие, что число различных классов QoS, специфицированных в Y.1541, должно быть строго ограничено, чтобы избежать чрезмерного усложнения рекомендации (и, что более важно, сетевых технологий, требуемых для реализации этого). Для обеспечения наибольшего охвата группа согласилась, что определенные классы должны все вместе охватить широкий набор приложений и высокий процент нужд пользователей на отсталых IP-сетях. В дополнение к традиционным приложениям Интернет сюда же включены телефония точка-точка, мультимедийные телеконференции и интерактивная передача данных (например, сигнализации). Группа заключила, что потребности некоторых, особо требовательных приложений (например, видео реального времени высокого разрешения, широкополосные TCP соединения) пока не будут отражены в стандартных классах. Было согласовано, что каждый класс QoS должен охватывать группу приложений с подобными требованиями работы, значительно отличающимися от требований других классов. И

здесь, с точки зрения ограничения сложности структуры классов, может быть задан вопрос, будут ли операторы управляемых IP-сетей для каждой пары предложенных классов делать какие-нибудь различия при их осуществлении. Классы QoS будут различаться только при утвердительном ответе на этот вопрос.

Эталонный маршрут рекомендации Y.1541. Характеристики работы IP из конца в конец, определенные в рекомендации Y.1541, применяются от NI до NI, как показано на рис. 6.4. Сетевой маршрут из конца в конец в IP-сети включает набор сетевых сегментов и каналов передачи, транспортирующих IP-пакеты от SRC до DST. Нижние протоколы, включающие уровень IP вместе с SRC и DST, могут также рассматриваться как часть IP-сети. Сетевые сегменты соответствуют областям операторов и могут содержать архитектуры доступа к IP-сети. Устройство клиента включает в себя все терминальное оборудование, такое как хосты, и любые оконечные маршрутизаторы или ЛВС.

Характеристики и классы QoS. Характеристики работы и классы QoS рекомендации Y.1541 представлены в табл. 6.1. Каждый класс QoS создает определенную комбинацию границ на подмножестве значений рабочих характеристик. Классы и связанные с ними характеристики работы применяются к потокам IP-пакетов между MP, которые разграничивают IP сеть из конца в конец (т.е. сетевые интерфейсы (СИ), показанные на рис. 6.4). Поток IP-пакетов - это трафик, ассоциированный с данным соединением или потоком без установления соединения, имеющим те же самые хост источника (SRC), хост назначения (DST), класс обслуживания и идентификацию сессии. Другие документы могут использовать термины «микропоток» и «подпоток» в отношении потоков трафика при такой степени классификации.

Классы 0 и 1 определяют верхние границы по задержке передачи пакетов и потерям пакетов. Они также ограничивают джиттер задержки. Классы 2 и 3 определяют верхние границы по задержке передачи пакетов и потерям пакетов, но не ограничивают джиттер задержки. Классы 0 и 2 отличаются от классов 1 и 3 по характеристикам передачи пакетов. Класс 4 ограничивает потери пакетов и обеспечивает довольно «мягкую» верхнюю границу задержки. Y.1541 также определяет неспецифицируемый класс (класс 5), не предоставляющий никаких определенных гарантий работы. Значение для характеристики потери одиночных пакетов было выбрано для того, чтобы гарантировать, что потеря пакета - доминирующая причина дефектов, представленных верхними уровнями. Характеристики QoS применимы, когда скорость каналов доступа соответствует скоростям T1 или E1 или выше. Характеристики IPTD классов 0 и 2 будут не всегда достижимы на длинных маршрутах. Y.1541 предполагает, что пользователь и провайдер сети должны согласовывать профиль трафика, который применяется к одному

или более потокам пакетов по классу QoS. В настоящее время соглашающиеся стороны могут использовать любые спецификации пропускной способности, которые они считают приемлемыми, до тех пор, пока они осуществимы и проверяемы. Например, пиковая скорость передачи в битах (включая издержки нижних уровней) может быть достаточной. Когда доступны протоколы и системы, поддерживающие динамические запросы, пользователи могут заключать соглашение о трафике, определяющее один или несколько параметров трафика в соответствии с рекомендацией Y. 1221.

Таблица 6.1. **Определение классов QoS и характеристик IP-сети**

Параметр работы сети	Суть рабочей характеристики	Классы QoS					
		класс 0	класс 1	класс 2	класс 3	класс 4	класс 5
IPTD	Предельное значение среднего значения IPTD, мс	100	400	100	400	1000	Н
IPDV	Предельное значение, мс	50	50	Н	Н	Н	Н
IPLR	Предельное значение вероятности потери пакета	$1 \cdot 10^{-3}$	$1 \cdot 10^{-3}$	$1 \cdot 10^{-3}$	$1 \cdot 10^{-3}$	$1 \cdot 10^{-3}$	Н
IPER	Предельное значение	$1 \cdot 10^{-4}$	$1 \cdot 10^{-4}$	$1 \cdot 10^{-4}$	$1 \cdot 10^{-4}$	$1 \cdot 10^{-4}$	Н

Н – неспецифицировано

Сети, предлагающие 1Р-коммуникации в соответствии с У.1541, как ожидается, будут поддерживать эти границы (пределы) из конца в конец для времени существования потока до тех пор, пока пользователи (и другие сети) не превысят согласованную пропускную способность. Рекомендация предусматривает, что сети, выполняющие Y.1541, не обязаны поддерживать согласованные значения QoS при превышении установленной пропускной способности. Сеть, испытывающая такой избыточный поток, может отбрасывать число пакетов, равное числу пакетов превышения. Такие отброшенные пакеты не учитываются как потерянные при оценке параметра IPLR работы сети.

Таблица 6.2. **Руководство по классам QoS для IP**

Класс QoS	Приложения (примеры)	Узловые механизмы	Сетевые технологии
0	Реального времени, чувствительные к джиттеру, с высокой интенсивностью обмена данными (VoIP, видео телеконференции)	Раздельные очереди с предпочтениями обслуживания, отвод трафика	Принудительная маршрутизация и размещение
1	Реального времени, чувствительные к джиттеру, интерактивные (VoIP, видео-телеконференции)		Менее принудительная маршрутизация и размещение
2	Транзакции, высокая интерактивность (например, сигнализации)	Раздельные очереди, приоритеты потерь	Принудительная маршрутизация и размещение
3	Транзакции, интерактивность		Менее принудительная маршрутизация и размещение
4	Только низкие потери (короткие транзакции, блоки данных, потоковое видеовещание)	Длинные очереди, приоритеты потерь	Любой маршрут/путь
5	Традиционные приложения существующих IP-сетей	Раздельные очереди (низший приоритет)	Любой маршрут/путь

В дополнение к характеристикам работы и классам QoS рекомендация Y.1541 определяет различные вспомогательные переменные (минимальные периоды наблюдения, длину тестовых пакетов, типовые размеры и т.д.) для облегчения оценки работы и сравнения. Например, минимальный интервал наблюдения в 10...20 секунд рекомендуется для оценки VoIP при типовой скорости передачи пакетов (50-100 пакетов в секунду). Рекомендуемый интервал наблюдения за потерями, задержками и IPDV равняется 1 мин, соблюдая баланс между статистической достоверностью и значимостью для работы пользователя. Табл. 6.2 представляет собой руководство по применению и разработке классов QoS. Y.1541 отмечает, что эти руководящие принципы являются полностью предоставленными на собственное усмотрение; провайдеры сетей могут использовать любые выбранные ими механизмы узлов, ограничения маршрутизации или другие технологии.

5.1.4. Заключение и направление будущих работ

Рекомендации ITU-T Y.1540 и Y.1541 совместно обеспечивают ключевое решение головоломки QoS в IP. Y.1540 определяет стандартные рабочие параметры передачи пакетов в IP-сетях. Y.1541 устанавливает характеристики NI-NI для параметров Y.1540 и группирует эти численные характеристики по шести отдельным классам QoS для IP-сети.

Весь набор классов охватывает главные категории IP-приложений пользователя. Рабочие значения специфицируемых параметров могут быть достигнуты в реальных сетях и могут быть проверены в подведомственных границах, оборудованных терминальным оборудованием или межсетевыми функциями. Эти рекомендации документируют важное

соглашение между сетевыми провайдерами, производителями оборудования и конечными пользователями по уровням качества, которые должны поддерживаться для широкого диапазона IP-приложений, включая телефонию. Они же могут использоваться как база для установления соглашений между сетями, а также для поддержания взаимодействия по QoS среди различных технологий.

Хотя Y. 1540/Y. 1541 представляют собой полезный шаг вперед, успешное развитие, основанных на IP сетей следующего поколения, обеспечивающих динамический набор определенных классов QoS, не поддерживается. Сегодня механизмы QoS еще не являются широко распространенными на IP-сетях.

Хотя соглашения о статичных классах QoS могут осуществляться и сегодня путем сопоставления маркировки пакета (например, поля TOS или DiffServ code points) с определенным классом QoS, все еще необходима работа по определению более гибкой архитектуры QoS и установлению того, как применять классы QoS рекомендации Y.1541 в протоколах сигнализации.

Провайдерам необходимо будет определять и, возможно, стандартизировать средства распределения рабочих характеристик среди нескольких независимых сетей, которые будут типично взаимодействовать в предоставлении IP-потоков с гарантированным QoS между конечными терминалами пользователей. Говоря короче, продолжающаяся конвергенция IP/ТфОП потребует слияния мысли и действия в отношении QoS IP-сетей. 13-я исследовательская группа ITU-T и другие организации по стандартизации работают над этой задачей.

5.2. Стратегии сосуществования IPv6 и IPv4 в сетях следующего поколения

Версия 6 протокола IP. IPv6, шестая версия межсетевого протокола IP, разрабатывается для того, чтобы преодолеть следующие ограничения версии IPv4 (четвертой, используемой ныне в Интернет):

- Пространства 32-битных адресов уже не хватает.
- IPv4 плохо управляет качеством предоставляемых услуг.
- IPv4 не имеет встроенных средств защиты.

В IPv6 предусмотрены 128-битные адреса, что представляется вполне достаточным.

Заголовок пакета IPv6 состоит из стандартного 40-байтного заголовка, за которым могут следовать дополнительные заголовки. Стандартный заголовок имеет следующий формат:

[Version | Priority | Flow | Tota I Length | Next Header | Hop Limit| SA | DA]

В поле Flow указывается ожидаемое качество обслуживания пакета и, возможно, характеристики соединения, которому принадлежит пакет. Маршрутизатор может использовать это поле для управления ресурсами данного соединения и назначения пакетов для передачи. Поле Hop Limit имеет то же значение, что и поле Time to live в IPv4. Поле Next Header указывает на протокол транспортного уровня (например, TCP или UDP), если больше нет дополнительных заголовков, или на следующий дополнительный заголовок. Было определено шесть дополнительных заголовков:

- Hop-by-Hop: используется маршрутизаторами для предоставления информации о доставке пакетов.

- Destination: определяет опции, согласованные с оконечной системой.

- Routing: задает предпочтительный путь в тех случаях, когда маршрутизация определяется отправителем.

- Fragmentation: для фрагментации больших дейтаграмм.

- Authentication: определяет правила аутентификации.

- Encryptedpayloach содержит шифрованную полезную информацию.

Каждый дополнительный заголовок содержит поле Next Header, указывающее на протокол транспортного уровня, если нет других дополнительных заголовков, или на следующий дополнительный заголовок.

Обычно фрагментирует пакеты в IPv6 сам компьютер-источник, а не промежуточные маршрутизаторы. Для осуществления фрагментации хост-отправитель должен определить максимальную длину блока на пути до получателя. Маршрутизаторы IPv6 реализуют алгоритм для вычисления пути МДБ. Хост-отправитель всегда может отправить сообщение через определенный маршрутизатор или через поставщика услуг P при помощи туннеля (осуществляющего инкапсуляцию в пакеты для P) или с помощью дополнительного заголовка Routing.

IPv6 использует для маршрутизации протокол IDRP (Interdomain Routing Protocol, междоменный протокол маршрутизации), основанный на алгоритме предпочтительного пути, более мощный, чем BGP; протокол IDRP может работать с несколькими семействами адресов, такими, например, как адреса IPv4 и IPv6.

IPv6 был разработан, помимо прочего, для расширения адресного пространства, чтобы удовлетворять будущие требования работы сетей. В данном разделе будут проанализированы и обсуждены важные аспекты сценариев развертывания IPv6 и предложена системная архитектура, совместимая и интегрируемая с сетями IPv4/MPLS, а также исследованы различные стратегии развертывания IPv6 с приведением примеров

проектирования сетей. Затем будет предложено развертывание IPv6 на оборудовании поставщиков услуг.

Непрерывный рост глобальной сети Интернет требует развития архитектуры сетей для приспособления к новым технологиям, что в свою очередь необходимо для поддержки растущего числа пользователей, приложений, устройств и услуг. IPv6 разработан для удовлетворения этих требований и позволяет возвратиться к глобальной сквозной среде, где сетевые правила адресации становятся прозрачными для приложений. Текущее адресное пространство IP не способно удовлетворить огромный рост числа пользователей или географические потребности расширения Интернет, не говоря уже о требованиях вновь появляющихся приложений, таких как персональный карманный компьютер (Personal Digital Assistant, PDA), домашние сети (Home Area Network, HAN), транспортировка с помощью Интернет-соединений, интегрированные телефонные услуги и распределенные игры. IPv6 увеличивает в 4 раза число битов сетевого адреса с 32 бит (в IPv4) до 128 бит, что дает более чем достаточное число уникальных глобальных IP-адресов для каждого сетевого устройства на планете. Использование уникальных глобальных IP-адресов упрощает механизмы, используемые для достижения доступности и сквозной безопасности сетевых устройств, функционально критичных для управления приложениями и услугами, зависящими от адресов. Срок службы IPv4 был продлен использованием методов, таких как повторное использование адресов с трансляцией и лимиты временного использования. Хотя эти методы, как может показаться, увеличивают адресное пространство и соответствуют традиционной схеме клиент/сервер, они не в состоянии удовлетворить требования новых приложений. Потребность в постоянно работающем оборудовании (например, резидентский домашний Интернет через широкополосный кабельный модем или Ethernet) препятствует методам преобразования, объединения и временного использования IP-адресов. Причем требуемый «plug-and-play» для устройств пользователей Internet еще больше увеличивают требования к адресу. Гибкость адресного пространства IPv6 обеспечивает поддержку частных адресов, но должна ограничить использование технологии трансляции сетевых адресов (Network Address Translation, NAT) по причине широкой доступности глобальных адресов. IPv6 повторно предоставляет сквозную безопасность, что не всегда возможно через основанные на NAT сети.

В данный момент мы находимся на ранней стадии внедрения IPv6 с малым числом приложений IPv6 по сравнению с IPv4 на рынке и малым числом сетевых продуктов, нуждающихся в обмене между доступными услугами IPv6. Хотя, в конечном счете, успех IPv6 будет зависеть от инновационных приложений, работающих по IPv6, ключевая часть

разработки IPv6 - это его способность интеграции и совместного использования с уже существующими IP-сетями. Предполагается, что хосты (узлы) IPv4 и IPv6 будут вынуждены сосуществовать довольно продолжительное время неуклонного перехода от IPv4 к IPv6, и как раз разработка переходных стратегий, инструментов и механизмов и была основной частью проекта IPv6 с самого начала. Выбор стратегии (или стратегий) внедрения будет зависеть от текущего состояния сетевой среды и таких факторов, как прогнозируемый объем трафика IPv6, доступность приложений IPv6 для конечных систем и стадии развертывания. Мы сделаем попытку подвести итог различным стратегиям интеграции/совместного использования IPv6 вместе с примерами проектов сетей, а также предложим системную архитектуру, интегрирующуюся и совместно используемую с сетями IPv4/MPLS. Будет кратко обсужден проект сети IPv6 для сетевой среды поставщика услуг со сравнением стратегий развертывания.

5.2.1. Стратегии интеграции и сосуществования IPv6 и IPv4

Успешное утверждение на рынке любой новой технологии зависит от простоты ее интеграции с существующей инфраструктурой без существенного разрушения услуг. В определении стратегий внедрения IPv6 принимали участие несколько рабочих групп IETF (Internet Engineering Task Force), например рабочие группы IPv6, v6ops. Ниже будут рассмотрены следующие сценарии развертывания:

- магистраль двойного стека;
- IPv6 по туннелям IPv4;
- механизмы трансляции протоколов;
- выделенные каналы данных;
- магистрали MPLS.

Далее будут кратко пересмотрены и сравнены первые три сценария развертывания, а также предложены и обсуждены сценарии IPv6 по выделенным каналам данных и магистрали MPLS.

Краткий обзор механизма перехода. Сосредотачиваясь на первичной цели обеспечения взаимодействия приложений IPv6 на хостах, многие сетевые разработчики рекомендуют сначала развертывать IPv6 на периферии, где находятся приложения и хосты, а затем постепенно двигаться к ядру сети, для того чтобы снизить издержки, неустойчивость работы и воздействие интеграции. К тому же, перемещение IPv6 на периферию (в расположение пользователя) является относительно более легким, поскольку основные операционные системы (например Microsoft, Linux) уже поддерживают IPv6.

Ключевые стратегии развертывания IPv6 на периферии сети включают перенос трафика IPv6 по инфраструктуре сети IPv4, позволяя изолированным доменам IPv6 связываться друг с другом до тех пор, пока не будет осуществлен полный переход к магистралям IPv6. Затем, когда настанет время планирования полной модернизации, будет возможно перемещать через сеть и IPv6 и IPv4 с любой периферии через ядро. Дополнительно может потребоваться механизм трансляции для работы устройств, поддерживающих только IPv6 или IPv4, для того чтобы хосты, поддерживающие только один протокол, могли прозрачно связываться с хостами, работающими по другому протоколу. Все методы предполагают модернизацию сетей и постепенное развертывание IPv6 без или с небольшим разрушением услуг IPv4.

Ниже рассмотрены четыре ключевых метода развертывания IPv6.

Внедрение на магистрали двойного стека. Этот метод позволяет приложениям IPv4 и IPv6 совместно работать на магистрали с двойной маршрутизацией IP-уровня. Все маршрутизаторы (например, оборудование доступа клиента, мультиплексирующие или магистральные маршрутизаторы) в сети должны быть модернизированы до двухстековых для соединений IPv4, используя стек IPv4, а для соединений IPV6 - соответственно стек IPv6. Протоколы маршрутизации для обеих версий IP должны быть выбраны и адекватно сконфигурированы. Внутренний протокол шлюза (Interior Gateway Protocol, IGP) - это выбор между решением «корабль в ночи» (например, OSPFv2 для IPv4 и 0SPFv3 для IPv6) и интегрированным решением (например, ISIS), обеспечивая выравнивание топологий IPv4 и IPv6.

Внедрение IPv6 по туннелям IPv4. Эти туннели инкапсулируют трафик IPv6 в пакеты IPv4, что применяется, прежде всего, для связи между изолированными областями IPv6 или для соединений с удаленными сетями IPv6 через магистраль IPv4. Технология предполагает использование вручную сконфигурированных туннелей, туннелей общей маршурутированной инкапсуляции (Generic Routing Encapsulation, GRE), полуавтоматических механизмов туннелирования, таких как услуги туннельного брокера, и полностью автоматических механизмов туннелирования, таких как 6в4 (6to4), для глобальной сети и протокола автоматической адресации туннелей внутренних областей (Intrasite Automatic Tunnel Addressing Protocol, ISATAP) для сетей кампусов. Это достаточно легкий сценарий для внедрения с технологии IPv6.

Внедрение IPv6 с использованием выделенных каналов передачи данных. Данная технология позволяет обеспечить связь между доменами IPv6 используя тот же самый второй уровень инфраструктуры, что используется для IPv4, но с использованием для IPv6 технологии Frame Relay или асинхронного режима передачи (Asynchronous Transfer Mode,

ATM), постоянных виртуальных каналов (Permanent Virtual Circuit, PVC), разделенных оптических линий или разных длин волн в технологии плотного мультиплексирования по длине волны (Dense Walelength Division Multiplexing, DWDM).

Внедрение IPv6 на магистралях MPLS. Данная технология позволяет доменам IPv6 взаимодействовать друг с другом поверх магистрали IPv4/MPLS без модификации структуры ядра. В различных точках сети доступны различные технологии, но каждая требует некоторых изменений магистральной инфраструктуры или изменения конфигурации маршрутизаторов ядра, потому что пересылка основа на на метках, а не на самих заголовках IP-пакетов.

После краткого описания стратегий развертывания IPv6 приведем более подробное.

Внедрение двойного стека IPv4/IPv6. Магистраль двойного стека является основной стратегией для маршрутизации обоих протоколов- IPv4 и IPv6. Приложения, не модернизированные для поддержки стека IPv6, могут совместно работать с модернизированными приложениями в одной и той же конечной системе. Для поддержки адресов IPv4 и IPv6 и запросов службы доменных имен (Domain Name Service, DNS) был определен новый прикладной программный интерфейс (Application Programming Interface, API). Приложения выбирают между использованием IPv4 или IPv6, основываясь на поиске имени; оба адреса и IPv4 и IPv6 могут быть возвращены DNS с требованием (или согласно системе, соответствующей правилам, определенным в документе IETF «Ошибка выбора адреса для IPv6») выбора правильного адреса на основании типа IP-трафика.

При развертывании магистрали двойного стека, все маршрутизаторы сети должны быть модернизированы до двухстековых. Сегодня, маршрутизация с использованием двойного стека протоколов – это вполне обоснованная стратегия для специфических сетевых инфраструктур со смешанным использованием IPv4 и IPv6 (например, на кампусе или агрегированной точке присутствия), требующих конфигурации обоих протоколов. Однако, кроме очевидной необходимости модернизации всех маршрутизаторов сети, менеджеры сети, выбирающие этот подход, должны знать, что все маршрутизаторы в данном случае потребуют определения двойной схемы адресации, потребуют двойного управления протоколами маршрутизации и должны будут быть сконфигурированы с достаточным объемом памяти для обеих маршрутных таблиц - для IPv4 и IPv6.

Внедрение IPv6 по туннелям IPv4. Туннелирование - это одна из ключевых стратегий развертывания как для поставщиков услуг, так и для предприятий на период совместного использования IPv4 и IPv6.

Для развертывания IPv6 доступны разнообразные механизмы. Эти механизмы включают вручную созданные туннели, такие как сконфигурированные туннели IPv6 и

IPv6 поверх IPv4 GRE туннелей, а также полуавтоматические механизмы туннелирования, такие как услуги туннельного брокера, и полностью автоматические механизмы туннелирования, такие как ISATAP и туннели 6в4 (6to4).

Все туннельные механизмы требуют работы конечных точек туннеля в двухстековом режиме. Двухстековые маршрутизаторы, работающие одновременно с обоими протоколами, IPv4 и IPv6, могут непосредственно взаимодействовать как с IPv4, так и с IPv6 конечными системами и маршрутизаторами.

Не все стратегии перехода могут быть применимы ко всем ситуациям и всем сетям. Поскольку ожидается, что, по крайней мере, первоначально, большинство клиентов могут заинтересоваться туннелированием IPv6 поверх их существующих сетей IPv4. Ниже будет представлено сравнение следующих технологий туннелирования IPv6 для использования поверх сетей IPv4:

- вручную сконфигурированный туннель;
- IPv6 поверх IPv4 GRE туннеля;
- автоматический, 1Ру4-совместимый туннель;
- автоматический туннель 6в4 (6to4);
- ISATAP туннель;
- туннель Тередо (Teredo tunnel).

В табл. 6.3 приведены особенности всех перечисленных выше механизмов туннелирования. Каждый механизм имеет свои «за» и «против». Однако, на основании изучения этой таблицы можно сделать важный вывод, который заключается в том, что даже без ручной конфигурации мы можем обеспечить работу оконечных станций и кампусов IPv6 поверх облака IPv4, используя вышеперечисленные механизмы. Для обеспечения безопасности конфигурации туннелей IPv6 поверх IPv4 менеджеры сети могут на конечных маршрутизаторах сконфигурировать IPsec либо для IPv4, либо для IPv6.

Механизмы трансляции IPv6/IPv4. Все эти стратегии интеграции обеспечивают IPv6 из конца в конец. Однако некоторые организации или частные лица могут не захотеть применять любую из этих стратегий трансляции IPv6, поскольку на своих узлах или сетях применяют только IPv6, и не могут применять двойной стек протоколов. Даже если на некоторых узлах или сетях и будет установлен двойной стек протоколов, они могут не иметь IPv4 адресов для использования с двухстековыми узлами. Исходя из этих обстоятельств, взаимодействие между узлами, одни из которых работают только по IPv4, а другие - только по IPv6, требует некоторого уровня трансляции между протоколами IPv6 и IPv4 на хостах или маршрутизаторах или на двухстековых хостах, с прикладным

уровнем, понимающим, какой из протоколов использовать. Например, сеть, работающая только по IPv6, все еще может хотеть иметь доступ к ресурсам сети, работающей только по IPv4, к таким как Web-серВера.

Таблица 6.3. **Сравнение различных механизмов туннелирования**

Механизм	Первичное использование	Полезный эффект	Ограничения	Требования
Вручную сконфигурированные туннели IPv6	Устойчивые и безопасные каналы регулярной связи. Соединение с Internet IPv6	Хорошо известная стандартная технология туннелирования. Конечные точки могут быть защищены использованием IPv4 IPsec	Туннель только между двумя точками. Большие издержки на управление	Зарегистрированный IPv6 адрес ISP. Двухстековые маршрутизаторы
IPv6 поверх IPv4 GRE туннеля	Устойчивые и безопасные каналы регулярной связи	Хорошо известная стандартная технология туннелирования. Конечные точки могут быть защищены использованием IPv4 IPsec	Туннель только между двумя точками. Издержки на управление. Реализация GRE туннеля редко доступна на хостах	Зарегистрированный IPv6 адрес ISP. Двухстековые маршрутизаторы. Требуется IS-IS для сконфигурированного по туннелю IPv6
Туннельный брокер	Автономные изолированные IPv6 оконечные системы	Устанавливаемый и управляемый ISP туннель	Косвенное обеспечение потенциальной безопасности	Услуга туннельного брокера должна знать, как создать и отправить скрипт для программного обеспечения
Автоматический IPv4-совместимый туннель	Отдельные хосты или небольшие области. Редкая связь	Автоматический туннель	Связь только с другими IPv4-совместимыми областями. Плохо масштабируем, поскольку предлагает тоже самое адресное пространство, что и IPv4, почти выступая против предпочтительного решения 6в4	Префикс IPv6 (0::/96). Двухстековые маршрутизаторы. Требуется IPv4 адрес для каждого хоста
Автоматический туннель 6в4	Соединение многочисленных удаленных IPv6 доменов. Частая связь	Простота развертывания без издержек на управление	При связи с IPv6 Internet не оптимизирован выбор пути возврата. Потенциальная проблема безопасности, если нет защиты по IPsec (для IPv4 или IPv6)	Префикс IPv6 (2002::/16). Двухстековые маршрутизаторы
ISATAP туннель	Области кампусов. Переход немаршрутизируемых областей	Простое развертывание IPv6 для немногочисленного числа хостов кампуса	Предложенные характеристики канала могут быть не самыми лучшими по сравнению с исходным коммутатором 3-го уровня. Не предлагает решения для широковещательного трафика IPv6	Реализация ISATAP на хостах и маршрутизаторах IPv6. Двухстековые маршрутизаторы
Туннели 6поверх4 (6over4)	Области кампусов. Переход немаршрутизируемых областей	Простое развертывание IPv6 для немногочисленного числа хостов кампуса	Неприемлем, заменен на ISATAP. Требование широковещательности IPv4	—

Различные механизмы трансляции IPv6/IPv4, находящиеся на рассмотрении рабочей группы v6Ops IETF, следующие:

- NAT-Protocol Translation (NAT-PT);
- TCP-UDP relay;
- Bump-in-the-stack (BIS);
- SOCKS-based gateway.

Данные механизмы трансляции протоколов становятся более значимыми, поскольку IPv6 становится все более распространенным и поскольку IPv6 становится протоколом выбора, позволяя традиционным IPv4 системам стать частью общей, всеобъемлющей IPv6 сети.

Механизмы трансляции можно разделить на две категории: те, которые не требуют никаких изменений в хостах IPv4 или IPv6, и те, которые требуют. Примером прежнего подхода является механизм ретрансляции TCP-UDP (TCP-UDP relay), который работает на выделенном сервере и создает отдельные соединения на транспортном уровне с IPv4 и IPv6 хостами, а затем просто передает информацию между ними. Примером более позднего подхода может служить механизм BIS, требующий добавления дополнительных протокольных уровней в протокольный стек IPv4. В механизме BIS между уровнем

приложений и сетевым уровнем протокольного стека IPv4 добавляются три дополнительных уровня (названные разрешения расширения, отображения адреса и трансляции). Всякий раз, когда приложению необходимо связаться с хостом, работающим только по IPv6, дополнительные уровни отображают IPv6 адрес в IPv4 адрес хоста IPv4.

В дополнение к стратегиям развертывания IPv6 в среде IPv4, необходим также механизм трансляции протоколов, такой как NAT-PT, для обеспечения связи между приложениями, одни из которых используют только IPv6, а другие - только IPv4 (например, чтобы браузер, работающий только по IPv6, мог связаться с Web-сервером, работающим только по IPv4, или двухстековым сервером). Но здесь есть один недостаток, хорошо известный пользователям NAT – это необходимость в выделенных шлюзах уровня приложения (Application Layered Gateways, ALGs), когда полезная нагрузка приложения включает IP-адрес. Суть механизма, основанного на SOCKS шлюза IPv4/IPv6 состоит в ретрансляции двух законченных IPv4 и IPv6 соединений на прикладном уровне. Данный механизм заключается в дополнительной функциональности обеих конечных систем (клиентов) и двухстекового маршрутизатора (шлюза), позволяющей связываться узлам IPv4 и IPv6. Механизм основан на протоколе SOCKSv5 и наследует все его особенности.

Механизмы трансляции могут быть полезны, так как развертывание IPv6 переходит от тестирования на стадию фактического использования и поскольку (что еще более важно) разработчики приложений решили, что продолжение поддержки IPv4 экономически не эффективно. В конечном счете, поскольку IPv6 становится протоколом выбора, эти механизмы позволят традиционным системам IPv4 стать частью всеохватывающей сети IPv6. Механизмы трансляции IPv4 и IPv6 на оконечных системах, выделенных серверах, маршрутизаторах сетей IPv6 и вместе на двухстековых хостах обеспечивают полный набор инструментов для возрастающего развертывания IPv6 без разрушения трафика IPv4. Сравнение механизмов трансляции приведено в табл. 6.4.

Развертывание IPv6 по выделенным каналам данных. Многие глобальные сети (WAN) и сети масштаба метрополиса (MAN) были построены с использованием технологий второго уровня, таких как frame relay, ATM, оптических технологий, а кое-где уже начинает использоваться DWDM. На рис. 6.5 представлена типовая конфигурация для IPv6 по выделенным каналам данных.

Маршрутизаторы, подключенные к глобальной сети или метросети поставщика услуг Интернет (ISP), могут быть сконфигурированы для использования той же самой инфраструктуры второго уровня, что и для IPv4, но для работы IPv6, например, поверх выделенной ATM или виртуальных частных каналов (PVC) frame relay, или на различных

длинах волны. Такая конфигурация дает дополнительный доход поставщику услуг, не подвергая опасности доходы и трафик IPv4 в связи с интеграцией с IPv6 даже при использовании инфраструктуры второго уровня.

Таблица 6.4. **Сравнение механизмов трансляции протоколов**

Механизм	Первичное использование	Полезный эффект	Ограничения	Требования
NAT-PT	Связь хостов, использующих только IPv6, с хостами, использующими только IPv4	Нет двойного стека	Не обеспечивается IPSec из конца в конец. Выделенный сервер – единственная точка отказа. Технология NAT-PT требует ALG для приложений, включающих IP-адрес	Выделенный сервер. DNS с поддержкой IPv6
TCP-UDP relay	Трансляция между сессиями TCP/UDPv6 и TCP/UDPv4	Свободно распространяемое программное обеспечение	Не обеспечивается IPSec из конца в конец. Выделенный сервер – единственная точка отказа	Выделенный сервер. DNS с поддержкой IPv6
BIS	Связь хостов, использующих только IPv6, с хостами, использующими только IPv4	Реализация в оконечных системах	Все стеки должны быть обновлены	Обновленный стек IPv4
SOCKS-based IPv6/IPv4 gateway	Связь хостов, использующих только IPv6, с хостами, использующими только IPv4	Свободно распространяемое программное обеспечение	Требует дополнительного программного обеспечения для шлюза	Программное обеспечение клиента и шлюза на хосте и маршрутизаторе

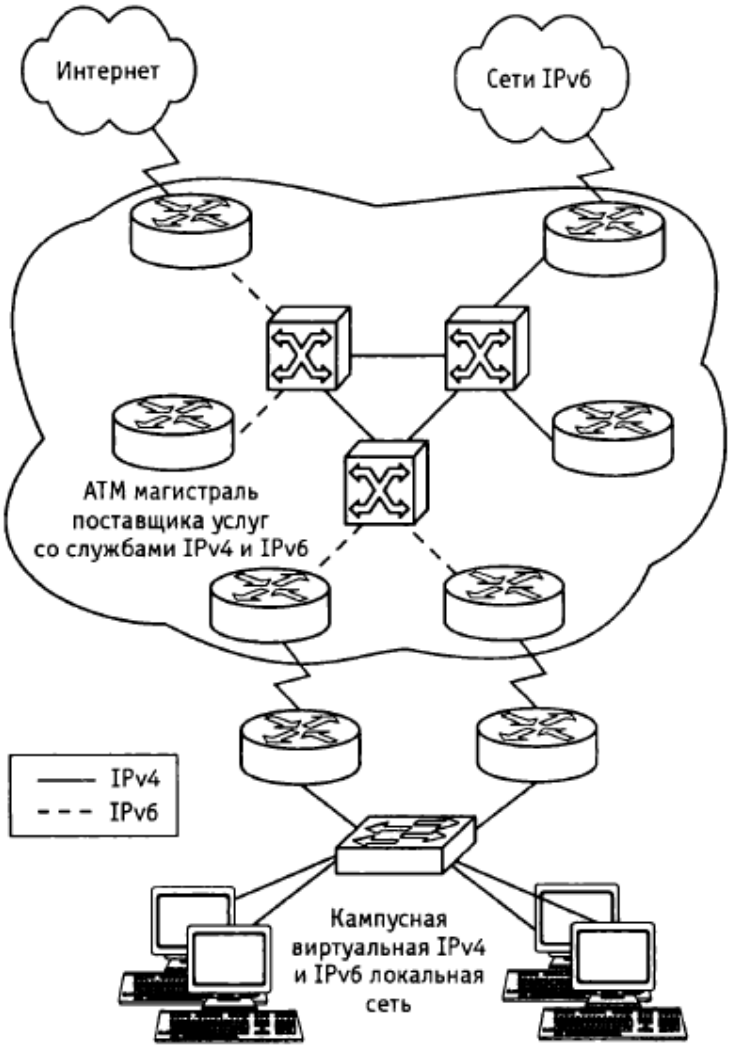


Рис. 6.5. Развертывание IPv6 по выделенным каналам данных

5.2.2. Развертывание IPv6 по магистрали MPLS

IPv6 поверх магистрали MPLS позволяет доменам IPv6 связываться друг с другом через ядро сети IPv4 MPLS. Такое внедрение требует небольшой модернизации инфраструктуры магистрали и не требует реконфигурации маршрутизаторов ядра, так как пересылка основана больше на метках, чем непосредственно на заголовках IP, обеспечивая высокорентабельную стратегию развертывания IPv6. В дополнение к этому, услуги, свойственные виртуальным частным сетям (Virtual Private Network, VPN) и инжинирингу трафика (Traffic Engineering, TE), доступные в среде MPLS, позволяют IPv6 сетям быть объединенными в виртуальные частные сети или экстрасети на инфраструктуре, поддерживающей IPv4 VPNs и MPLS-TE.

Ниже перечислены доступные или находящиеся в разработке стратегии развертывания:

- IPve-туннели на маршрутизаторах на стороне клиента (IPv6 tunnels on customer edge (CE) routers);

- транспорт канала второго уровня через MPLS (Layer 2 circuit transport over MPLS);

- IPv6 на маршрутизаторах на стороне провайдера (IPv6 on provider edge (PE) routers - 6PE);

- добавление IPv6 MPLS VPNs к 6PE (Adding IPv6 MPLS VPNs to 6PE - 6VPE);

- исходная, основанная на MPLS магистраль IPv6 (плоскость управления MPLS основана на IPv6).

Как показано на рис. 6.6, первая из этих стратегий не оказывает влияния и не требует изменений в ядре MPLS, состоящем из маршрутизаторов поставщика (P) и маршрутизаторов на стороне поставщика (PE). Это обеспечивается тем, что эта стратегия использует туннели IPv4 на двухстековых маршрутизаторах на стороне клиента (CE) для инкапсуляции трафика IPv6, который, таким образом, внутри сети MPLS появляется как трафик IPv4. Вторая стратегия не требует никаких изменений в базовых механизмах маршрутизации. Третья и четвертая стратегии требуют изменений в маршрутизаторах на стороне поставщика (PE) для поддержки двойного стека, но все функции ядра, т. е. маршрутизаторов поставщика (P) остаются на уровне IPv4. Последняя из стратегий предполагает работу собственного IPv6 MPLS ядра, но данная стратегия требует полной сетевой модернизации всех маршрутизаторов (как P, так и PE) с двойными плоскостями управления для IPv4 и для IPv6. В табл. 6.5 представлено сравнение этих стратегий для транспортировки IPv6 по магистрали MPLS. Ниже каждый из этих механизмов будет рассмотрен более подробно.

IPv6 по транспортному каналу второго уровня по MPLS. Использование любого канального транспорта для развертывания IPv6 по сетям MPLS не оказывает влияния на

работу и инфраструктуру MPLS. Такой метод не требует изменений ни в маршрутизаторах P ядра, ни в маршрутизаторах PE (для поддержки одного из механизмов канального транспорта второго уровня поверх MPLS), соединенных с пользователями. Связь между удаленными доменами IPv6 обеспечивают исходные протоколы IPv6 по выделенным каналам, где основные механизмы полностью прозрачны для IPv6. Трафик IPv6 туннелируется с использованием любого транспорта поверх MPLS (Any Transport Over MPLS - AToM) или Ethernet no MPLS (Ethernet over MPLS - EoMPLS) с помощью IPv6 маршрутизаторов, подключенных через ATM или Ethernet интерфейсы соответственно.

На рис. 6.7 приведен пример развертывания IPv6 по любому каналу транспорта по MPLS.

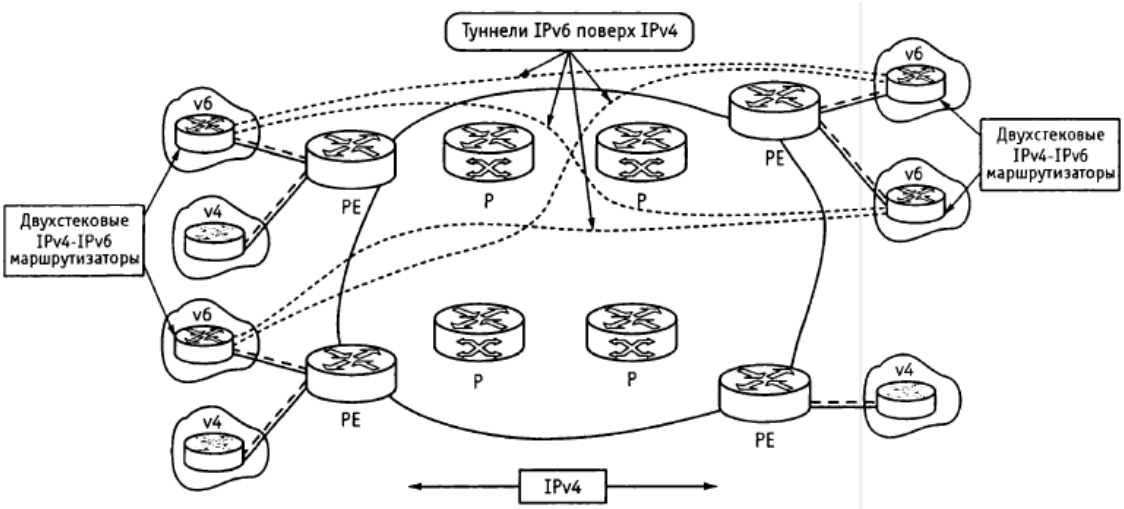


Рис. 6.6. Развертывание IPv6 с использованием туннелей на CE маршрутизаторах

Таблица 6.5. **Сравнение различных механизмов передачи IPv6 по магистрали MPLS**

Механизм	Первичное использование	Полезный эффект	Ограничения	Требования
Использование IPv6 туннелей на маршрутизаторах CE	Корпоративные клиенты, желающие использовать IPv6 поверх существующих услуг MPLS	Не оказывает влияния на инфраструктуру MPLS	Проблема масштабируемости при росте числа туннелей между CE	Двухстековые маршрутизаторы CE
Транспорт канала второго уровня через MPLS	Поставщик услуг с ATM или Ethernet каналами к маршрутизаторам CE	Полностью прозрачная IPv6 связь	Нет смешения IPv4 и IPv6 трафика	Необходим транспорт второго уровня по MPLS
IPv6 на маршрутизаторах на стороне провайдера (6PE) поверх MPLS	Поставщики услуг Интернет и поставщики мобильных услуг, желающие предлагать услуги IPv6	Дешевая и низкорисковая модернизация маршрутизаторов PE без воздействий на ядро MPLS	Применимо только к инфраструктуре MPLS	Модернизация программного обеспечения маршрутизаторов PE
IPv6 VPN на маршрутизаторах на стороне провайдера (6VPE) поверх MPLS	Поставщики услуг Интернет и поставщики мобильных услуг, желающие предлагать услуги IPv6 VPN	Дешевая и низкорисковая модернизация маршрутизаторов PE без воздействий на ядро MPLS	Применимо к инфраструктуре MPLS, хотя может быть исполнено и для других механизмов туннелирования. Утечка IPv6 адреса из глобальной маршрутной таблицы должна хорошо контролироваться	Поддержка VPN или VRF

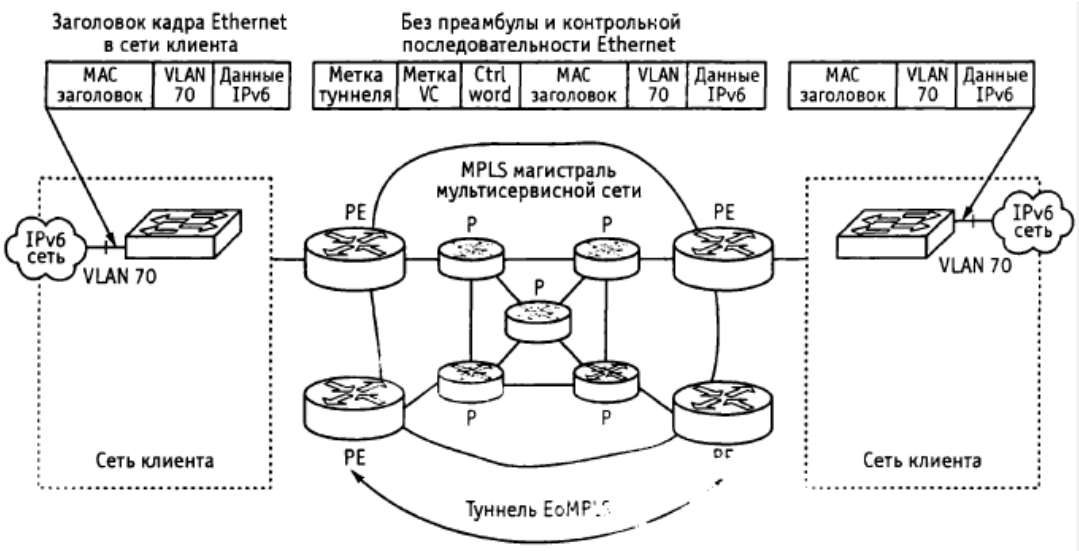


Рис. 6.7. IPv6 по «Ethernet по MPLS»

IPv6 на маршрутизаторах на стороне провайдера (PE). Другая стратегия развертывания заключается в конфигурировании IPv6 на MPLS PE маршрутизаторах. Данная стратегия имеет основное преимущество для поставщиков услуг, при которой нет необходимости в модернизации ни аппаратных, ни программных средств P маршрутизаторов в ядре MPLS сети, что, таким образом устраняет влияние на доход, генерируемый существующим IPv4 трафиком. Стратегия сохраняет выгоды от текущих особенностей IPv4 MPLS (например, MPLS-TE или VPN) наряду с появлением возможности предоставления исходных IPv6 услуг для корпоративных клиентов (используя поставляемые ISP IPv6 префиксы). Архитектура 6PE разрешает поддержку VPN для IPv6. На рис. 6.8 приведен пример развертывания IPv6 на маршрутизаторах PE.

Пересылка IPv6 данных выполняется благодаря коммутации по меткам, устраняя потребность как в туннелях IPv6 поверх IPv4, так и в дополнительной инкапсуляции 2-го уровня, разрешая появление исходных услуг IPv6, которые можно предлагать по всей сети и масштабировать, поскольку число пользователей IPv6 растет, в то время как технологии, такие как отражатели маршрутов, могут быть сконфигурированы позже.

Каждый маршрутизатор PE, который должен поддерживать IPv6 соединения, нуждается в модернизации до двухстекового (становится 6PE маршрутизатором) и конфигурируется для работы с MPLS на интерфейсах, соединяющих его с маршрутизаторами ядра P. В зависимости от требований области применения, каждый маршрутизатор может быть сконфигурирован для пересылки IPv6 или IPv6 и IPv4 трафика на интерфейсах к маршрутизаторам CE, таким образом, обеспечивая возможность предоставления либо только исходных услуг IPv6, либо одновременно услуг IPv4 и IPv6. Маршрутизатор 6PE обменивается как IPv4, так и IPv6 маршрутной информацией по

любому из поддерживаемых протоколов маршрутизации, в зависимости от соединения, и переключает IPv4 и IPv6 трафик по исходным IPv4 и IPv6 интерфейсам, не работающим по MPLS.

Маршрутизатор 6PE обменивается информацией о доступности с другими 6PE маршрутизаторами в домене MPLS, используя мультипротокольный граничный шлюзовой протокол (Border Gateway Protocol, BGP) и совместно использует с другими P или PE устройствами домена общий протокол маршрутизации IPv4, такой как открытый протокол «кратчайший путь выбирается первым» (Open Shortest Path First, OSPF) или интегрированный протокол «промежуточная система - промежуточная система» (Intermediate System to Intermediate System, IS-IS). Маршрутизаторы 6PE инкапсулируют трафик IPv6, используя два уровня меток MPLS. Высшая метка распределяется в соответствии с протоколом распределения меток (Label Distribunion Protocol, LDP) или протокола распределения тегов (Tag Distribution Protocol, TDP), используемых устройствами ядра для переноса пакетов к назначенному 6PE в соответствии с маршрутной информацией IPv4. Вторая или низшая метка связана с префиксом адреса IPv6 пункта назначения через мультипротокол BGP-4, обеспечивая выполнение баланса нагрузки.

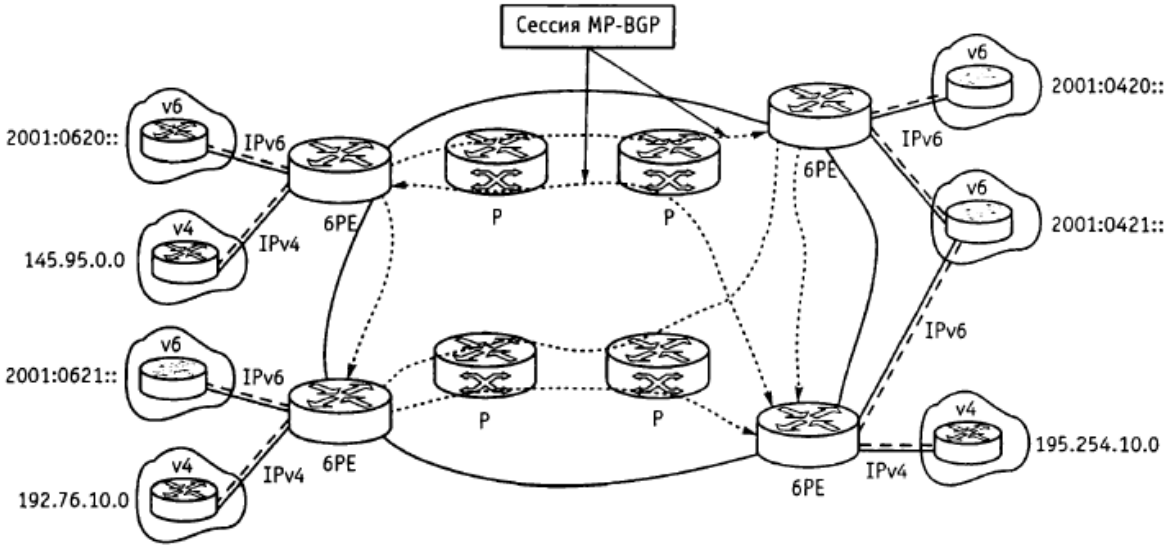


Рис. 6.8. IPv6 на маршрутизаторах на стороне провайдера (PE)

Маршрутизаторы IPv6 VPN на стороне провайдера по магистрали MPLS. Поставщики услуг, предлагающие своим клиентам услуги MPLS/VPN, могут ожидать добавления услуг IPv6/VPN к их портфелю услуг. Как ожидается, VPN станут IPv6/VPN, когда CE маршрутизаторы будут поддерживать исходный IPv6 на интерфейсах или подынтерфейсах к маршрутизаторам PE. Добавление IPv6/VPN способностей 6PE маршрутизатору, называемому в таком случае 6VPE для IPv6 VPN маршрутизатором на

стороне поставщика поверх MPLS, является альтернативой, позволяющей для ISP предоставлять подобные услуги и по IPv4. Подобно IPv4/VPN распределению маршрутов, BGP и его расширения используются для распределения маршрутов от областей IPv6/VPN ко всем другим 6VPE маршрутизаторам, соединенным с той же самой областью IPv6/VPN. PE используют таблицы VPN маршрутизации и форвардинга (VPN Routing and Forwarding - VRF) для раздельного обслуживания информации о доступности и информацию о пересылке данных для каждой IPv6 VPN, как показано на рис. 6.9.

Когда 6VPE1 получает IPV6 пакет от CE A, он ищет адрес пункта назначения пакета IPv6 в таблице VRF A. Это позволяет ему найти VPNIPv6 маршрут, который будет иметь соответствующую MPLS метку и соответствующее значение BGP next hop. Метка MPLS накладывается на IPv6 пакет. 6VPE1 непосредственно выдвигает другую метку, верхняя метка присваивается с помощью LDP/IGPv4 адресу IPv4 следующего «прыжка» BGP (BGP next hop) для достижения 6VPE2 через MPLS облако на стеке меток промаркированного пакета IPv6/VPN. Эта самая верхняя налагаемая метка соответствует траектории маркированного маршрута (Label Switched Path, LSP), начинающегося на 6VPE1 и заканчивающегося на 6VPE2. Как было упомянуто выше, нижняя метка связана с префиксом IPv6 VPN через BGP.

Все P маршрутизаторы в ядре сети коммутируют VPN пакеты, основываясь только на верхней метке стека, которая указывает на встречный маршрутизатор 6VPE2. Так как в соответствии с нормальными правилами перенаправления MPLS, P маршрутизаторы никогда не смотрят дальше первой метки, то, таким образом, полностью ничего не знают о второй метке или о переносимом через магистраль сети IPv6 VPN пакете.

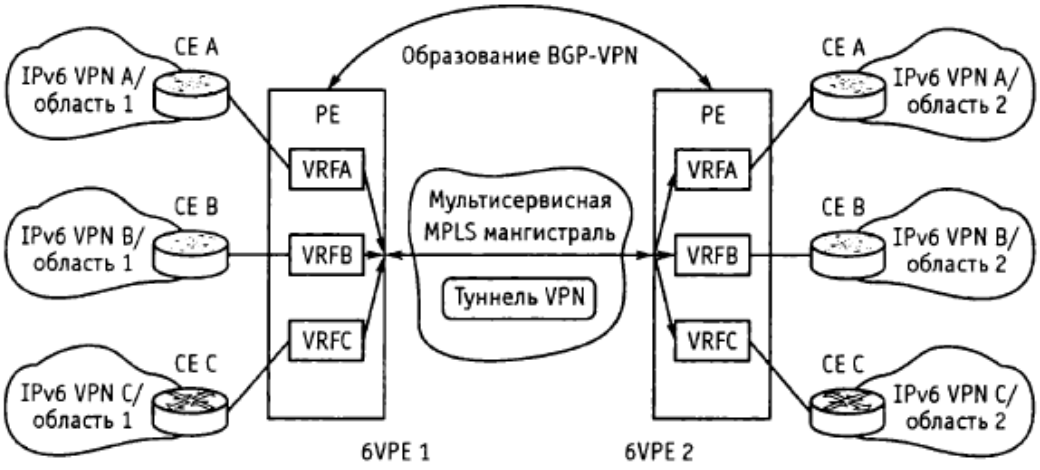


Рис. 6.9. Архитектура IPv6 MPLS VPN

Таблица 6.6 **Сравнение всех стратегий развертывания или механизмов перехода**

Стратегия развертывания	Ключевые пользователи и первичное использование	Полезный эффект	Ограничения	Требования
IPv6 по туннелям IPv4	Поставщики услуг, желающие предоставлять исходные услуги IPv6. Организации, желающие связать домены или каналы IPv6 с удаленными IPv6 сетями	Может продемонстрировать требования минимальных инвестиций. Простота осуществления поверх существующей инфраструктуры IPv4. Низкая стоимость и низкий риск	Комплексное управление и диагностика благодаря независимости туннельной и канальной топологий	Доступ к IPv4 через двухстековые маршрутизаторы с IPv4 и IPv6 адресами. Доступ к IPv6 DNS
IPv6 по выделенным каналам данных	Поставщики услуг глобальных или метросетей, развертывающие ATM, Frame Relay или DWDM	Может предоставлять IPv6 из конца в конец без воздействия на трафик и доходы IPv4	—	Доступ к WAN через двухстековые маршрутизаторы, с IPv4 и IPv6 адресами. Доступ к IPv6 DNS
IPv6 по магистралям MPLS	Поставщики мобильных услуг или существующие региональные поставщики услуг, развертывающие MPLS	Интегрирует IPv6 по MPLS так, что не требуется модернизации аппаратного или программного обеспечения ядра	Реализация требует работы MPLS. Высокие затраты на управление	Минимальные изменения маршрутизаторов клиентов (CE) и граничных маршрутизаторов поставщика (PE), зависящие от технологии
Двухстековые магистрали	Небольшие сети организаций. Инфраструктура поставщиков услуг. Инфраструктура корпоративной WAN. Инфраструктура кампуса	Простота применения для малых кампусных сетей со смешением IPv4 и IPv6 приложений. Возможность предоставлять одинаковые услуги (multicast, QoS) и для IPv4 и для IPv6	Комплексное управление протоколами маршрутизации. Огромный объем модернизации для больших сетей	Сетевые устройства должны быть совместимы с двойным стеком. Доступ к IPv6 DNS. Проект сети должен быть применим к обеим версиям IP с достаточной памятью таблиц маршрутизации

Выходной PE маршрутизатор, 6VPE2, получая маркированный IPv6 VPN пакет, отбрасывает первую метку и выполняет поиск по второй метке, которая уникально идентифицирует нужную VRF A, а иногда даже и исходящий интерфейс на 6VPE2. По выполнении поиска в необходимой VRF A, IPv6 пакет посылается к надлежащему CE маршрутизатору в домене или области IPv6.

5.2.3. Рассмотрение проектов IPv6 сетей

Развертывание IPv6, когда проектировщики сети одобряют стратегию интеграции IPv6, которая начинается с границ сети и движется к центру, позволяет контролировать затраты на развертывание и сосредоточиться на потребностях приложений, а не на выполнении полной модернизации до исходной IPv6 сети на данной стадии. Различные стратегии развертывания разрешают сейчас первые шаги перехода к IPv6 либо как испытание возможностей IPv6, или как ранние контролируемые стадии использования IPv6 как основной сети. В табл. 6.6 приведено сравнение различных стратегий развертывания.

5.2.4. Развертывание IPv6 в сетевой среде поставщика услуг

Поставщик услуг как администратор сети может захотеть оценить применение IPv6 сейчас, потому что текущее распределенное адресное пространство может быть не в состоянии удовлетворить потенциально огромное увеличение числа пользователей или запросы новых технологий от конечных клиентов, которые могут открыть новые возможности бизнеса для поставщика услуг. Использование уникальных глобальных IPv6 адресов предоставляет благоприятные возможности для создания новых бизнес-моделей,

добавляет доходы и увеличивает портфель услуг. Определенный для будущего Интернет, для наших следующих поколений, IPv6 может использоваться для достижимости и обеспечения безопасности из конца в конец для вновь появляющихся сетевых устройств, таких как карманные персональные компьютеры с возможностью подключения к Интернет, домашние компьютерные сети (HAN), подключенные к Интернет автомобили, интегрированные телефонные услуги и распределенные игры.

Нужно рассматривать развертывание IPv6 относительно трех нижеперечисленных стадий, сосредотачиваясь на бизнес модели, которая поможет управляющему звену увидеть дополнительное значение проекта. В данном контексте настоятельно рекомендуется, чтобы IPv6 была двухстековой IPv4/IPv6 услугой, когда операторы имеют достаточно опыта работы с двойным стеком.

Предоставление IPv6 сервиса (включая двухстековый сервис IPv4 и IPv6) на уровне доступа клиента. Начало развертывания IPv6 на уровне доступа клиента позволяет предоставлять IPv6 услуги уже сейчас без основной модернизации инфраструктуры ядра и без воздействия на текущие IPv4/MPLS услуги. Данный подход позволяет произвести оценку продуктов и услуг IPv6 до их окончательного развертывания на сети и оценить будущие требования для IPv6 без солидных инвестиций на этой ранней стадии.

Работа IPv6 (включая двухстековый сервис IPv4 и IPv6) непосредственно в инфраструктуре ядра. По завершении данной стадии, поскольку системы управления сетью полностью охвачены IPv6, сетевая инфраструктура может быть модернизирована для поддержки IPv6.

Взаимодействие с другими поставщиками услуг IPv6. Взаимодействие с другими поставщиками услуг IPv6 или 1Ру6-магистралью (бBone) позволяет дальнейшее оценивание и дает лучшее понимание требований к IPv6.

Выводы

Сегодня Интернет не воспринимается как достаточно надежная сеть для передачи трафика реального времени. Но это происходит не из-за недостатка перспективных механизмов, таких как потоковые слежение и ограничение (shaping/policing), а из-за сложности выбора метода обеспечения QoS сети и компромисса между простотой и большей управляемостью. Хороший проект сети, простота, высокая доступность и обеспечение защиты являются ключевыми аспектами обеспечения QoS на магистралях Интернет. Хороший проект сети плюс некоторая степень резервирования ресурсов не только делают сеть более отказоустойчивой, но также и предотвращают многие проблемы, связанные с QoS, и устраняют потребность в сложных механизмах, разработанных для их решения. Это делает сеть более простой и увеличивает ее доступность. Три класса трафика (Premium, Assured, и Best effort) достаточны для удовлетворения обозримых потребностей клиентов. Различные классы трафика будут обслуживаться по-разному, особенно при неблагоприятных сетевых условиях. Быстрая перемаршрутизация MPLS или другие механизмы защиты могут использоваться для защиты Premium-трафика при отказах маршрутизаторов или каналов. При возникновении неисправностей в одной части сети инжиниринг трафика должен использоваться для перемещения трафика в другую часть сети. DiffServ инжиниринг трафика может использоваться для предотвращения концентрации высокоприоритетного трафика на любом канале, так что высокопроизводительный трафик будет иметь низкую задержку и джиттер, и при необходимости может обрабатываться предпочтительно за счет трафика других классов. Схемы управления трафиком на магистрали, такие как Policing и Shaping, должны применяться для микроконтроля и использоваться, когда инжиниринг трафика становится недостаточным.

Список литературы

1. Пакетная сеть связи общего пользования. Кучерявый А.Е., Гильченок Л.З., Иванов А.Ю. - СПб.: НкТ, 2004.
2. Телекоммуникационные системы и сети: Учебное пособие. В 3 т. Том 1: Современные технологии / Б.И. Крук, В.Н. Попантонопуло, В.П. Шувалов; под ред. проф. В.П. Шувалова. - 3-е изд., испр. и доп. - М.: Горячая линия - Телеком, 2003. - 647 с.
3. Телекоммуникационные системы и сети_ Учебное пособие. В 3 т. Том 3 - Мультисервисные сети. В. В. Величко, Е. А. Субботин, В. П. Шувалов, А. Ф. Ярославцев. М.: Горячая линия – Телеком, 2005. – 592 с.