МСЭ-Т Y.1291

(05/2004)

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

СЕРИЯ Y: ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА, АСПЕКТЫ МЕЖСЕТЕВОГО ПРОТОКОЛА (IP) И СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ

Аспекты межсетевого протокола (IP) – Архитектура, доступ, возможности сетей и административное управление ресурсами

Архитектурная модель для поддержки качества услуги в сетях с пакетной передачей

Рекомендация МСЭ-Т Y.1291

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ Y

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА, АСПЕКТЫ МЕЖСЕТЕВОГО ПРОТОКОЛА (IP) И СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА	
Общие положения	Y.100–Y.199
Службы, приложения и промежуточные программные средства	Y.200–Y.299
Сетевые аспекты	Y.300–Y.399
Интерфейсы и протоколы	Y.400–Y.499
Нумерация, адресация и присваивание имен	Y.500–Y.599
Эксплуатация, управление и техническое обслуживание	Y.600–Y.699
Безопасность	Y.700–Y.799
Рабочие характеристики	Y.800–Y.899
АСПЕКТЫ МЕЖСЕТЕВОГО ПРОТОКОЛА (IP)	
Общие положения	Y.1000–Y.1099
Услуги и приложения	Y.1100–Y.1199
Архитектура, доступ, возможности сетей и административное управление ресурсами	**Y.1200–Y.1299**
Транспортирование	Y.1300–Y.1399
Взаимодействие	Y.1400–Y.1499
Качество обслуживания и сетевые показатели качества	Y.1500–Y.1599
Сигнализация	Y.1600–Y.1699
Эксплуатация, управление и техническое обслуживание	Y.1700–Y.1799
Начисление платы	Y.1800–Y.1899
СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ (NGN)	
Структура и функциональные модели архитектуры	Y.2000–Y.2099
Качество обслуживания и рабочие характеристики	Y.2100–Y.2199
Аспекты служб: Возможности служб и архитектура служб	Y.2200–Y.2249
Аспекты служб: Взаимодействие служб и сетей в NGN	Y.2250–Y.2299
Нумерация, присваивание имен и адресация	Y.2300–Y.2399
Управление сетью	Y.2400–Y.2499
Архитектура и протоколы сетевого управления	Y.2500–Y.2599
Безопасность	Y.2700–Y.2799
Обобщенная мобильность	Y.2800–Y.2899

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т Y.1291

Архитектурная модель для поддержки качества услуги в сетях с пакетной передачей

Резюме

В данной Рекомендации приводится архитектурная модель для поддержки качества услуги (QoS) в сетях с пакетной передачей. Главным для этой архитектурной модели является набор общих сетевых механизмов (или конструктивных блоков для QoS) для управления ответом сети на запрос услуги, который может быть специфическим для сетевого элемента, для сигнализации между сетевыми элементами или для управления трафиком и его администрирования при прохождении через сеть. Конструктивные блоки, распределенные по трем логическим плоскостям (а именно, плоскости управления, плоскости данных и плоскости административного управления), могут быть использованы в разных комбинациях, образуя различные способы получения удовлетворительного суммарного эффекта от меняющихся показателей качества услуг, которые необходимы для ряда приложений, таких как передача файлов и мультимедийная конференцсвязь.

Источник

Рекомендация МСЭ-Т Y.1291 утверждена 7 мая 2004 года 13-й Исследовательской комиссией МСЭ-Т (2001–2004 гг.) в соответствии с процедурой, изложенной в Рекомендации МСЭ-Т A.8.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи. Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

Всемирная ассамблея по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяет темы для изучения Исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации носит добровольный характер. Однако в Рекомендации могут содержаться определенные обязательные положения (например, для обеспечения возможности взаимодействия или применимости), и соответствие данной Рекомендации достигается в случае выполнения всех этих обязательных положений. Для выражения необходимости выполнения требований используется синтаксис долженствования и соответствующие слова (такие, как "должен" и т. п.), а также их отрицательные эквиваленты. Использование этих слов не предполагает, что соблюдение положений данной Рекомендации является обязательным для какой-либо из сторон.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на то, что практическое применение или реализация этой может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, обоснованности или применимости заявленных прав интеллектуальной собственности, независимо от того, отстаиваются ли они членами МСЭ или другими сторонами вне процесса подготовки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для реализации этой Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что это может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ.

СОДЕРЖАНИЕ

Стр.

Рекомендация МСЭ-Т Y.1291

Архитектурная модель для поддержки качества услуги в сетях с пакетной передачей

1 Область применения

В данной Рекомендации приводится архитектурная модель для поддержки качества услуги (QoS) в сетях с пакетной передачей. Главным для этой архитектурной модели является набор конструктивных блоков для QoS, распределенных по трем логическим плоскостям (а именно, плоскости управления, плоскости данных и плоскости административного управления), для управления характеристиками функционирования сети даже в режиме соперничества за получение ресурсов сети. В конечном счете, эти конструктивные блоки должны способствовать получению "суммарного эффекта для качества услуг, который определяет степень удовлетворения пользователя данной услуги".

2 Ссылки

Указанные ниже Рекомендации МСЭ-Т и другие источники содержат положения, которые путем ссылки на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие источники могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других источников, перечисленных ниже. Список действующих в настоящее время Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ в данной Рекомендации не придает ему как отдельному документу статус Рекомендации.

- ITU-T Recommendation E.360.1 (2002), *Framework for QoS routing and related traffic engineering methods for IP-, ATM- and TDM-based multiservice networks*.
- ITU-T Recommendation E.360.2 (2002), *QoS routing and related traffic engineering methods – Call routing and connection routing methods*.
- ITU-T Recommendation E.360.3 (2002), *QoS routing and related traffic engineering methods – QoS resource management methods*.
- ITU-T Recommendation E.360.4 (2002), *QoS routing and related traffic engineering methods – Routing table management methods and requirements*.
- ITU-T Recommendation E.360.5 (2002), *QoS routing and related traffic engineering methods – Transport routing methods*.
- ITU-T Recommendation E.360.6 (2002), *QoS routing and related traffic engineering methods – Capacity management methods*.
- ITU-T Recommendation E.360.7 (2002), *QoS routing and related traffic engineering methods – Traffic engineering operational requirements*.
- ITU-T Recommendation E.361 (2003), *QoS routing support for interworking of QoS service classes across routing technologies*.
- ITU-T Recommendation E.860 (2002), *Framework of a service level agreement*.
- ITU-T Recommendation G.114 (2003), *One-way transmission time*.
- ITU-T Recommendation G.1000 (2001), *Communications Quality of Service: A framework and definitions*.
- ITU-T Recommendation G.1010 (2001), *End-user multimedia QoS categories*.
- ITU-T Recommendation I.350 (1993), *General aspects of quality of service and network performance in digital networks, including ISDNs*.

– ITU-T Recommendation J.112 (1998), *Transmission systems for interactive cable television services*.

– ITU-T Recommendation J.162 (2004), *Network call signalling protocol for the delivery of time-critical services over cable television networks using cable modems*.

– ITU-T Recommendation J.163 (2004), *Dynamic quality of service for the provision of real-time services over cable television networks using cable modems*.

– ITU-T Recommendation J.170 (2002), *IPCablecom security specification*.

– ITU-T Recommendation J.174 (2002), *IPCablecom interdomain quality of service*.

– ITU-R Recommendation M.1079-2 (2003), *Performance and quality of service requirements for International Mobile Telecommunications-2000 (IMT-2000) access networks*.

– ITU-T Recommendation X.805 (2003), *Security architecture for systems providing end-to-end communications*.

– ITU-T Recommendation Y.1221 (2002), *Traffic control and congestion control in IP-based networks*.

– ITU-T Recommendation Y.1540 (2002), *Internet protocol data communication service – IP packet transfer and availability performance parameters*.

– ITU-T Recommendation Y.1541 (2002), *Network performance objectives for IP-based services*.

3 Определения

В данной Рекомендации отсутствуют определения новых терминов.

4 Сокращения и акронимы

В данной Рекомендации используются следующие сокращения:

DiffServ Дифференцированные услуги

DQoS Динамическое качество услуг (QoS)

IETF Комитет по инженерным проблемам Интернет

IntServ Интегрированные услуги

МСЭ-Т Международный союз электросвязи – Сектор стандартизации электросвязи

LSP Коммутируемый по меткам тракт

MPLS Многопротокольная коммутация с использованием меток

MTA Мультимедийный терминальный адаптер

QoS Качество услуги; качество обслуживания

RSVP Протокол резервирования ресурсов

SLA Соглашение об уровне обслуживания

5 Введение

Качество услуги (QoS) относится, в конечном счете, к поддержке характеристик и свойств конкретных приложений. Однако требования для различных приложений могут быть совершенно разными. Например, для телемедицины точность доставки информации более важна, чем суммарная задержка или отклонение задержки передачи пакетов (то есть разброс), в то время как для IP-телефонии значение и разброс задержки являются ключевыми параметрами и должны быть минимизированы. Качество услуги (QoS) рассматривается в ряде Рекомендаций МСЭ-Т. В Рекомендации МСЭ-Т E.800 качество услуги (QoS) определяется как "суммарный эффект показателей качества услуги, который определяет степень удовлетворенности пользователя услуги".

Такое определение качества услуги (QoS) является исчерпывающим, если учесть, что в Рекомендации МСЭ-Т E.800 рассматриваются вопросы поддержки, простоты использования, удобства обслуживания и безопасности для всех параметров услуги. В Рекомендации МСЭ-Т G.1000 при расширении понятия качества услуги согласно Рекомендации МСЭ-Т E.800 показатели качества услуги (или качество услуги) разбиваются на функциональные компоненты, которые ассоциативно связываются с рабочими характеристиками сети, определенными в Рекомендациях МСЭ-Т I.350, Y.1540 и Y.1541. В дополнение к Рекомендации МСЭ-Т G.1000, где дана структура этих функциональных компонент, в Рекомендации МСЭ-Т G.1010 содержатся основные требования приложений конечного пользователя, выраженные в терминах общих категорий (таких, как диалоговый режим, допуски по ошибкам). В отношении соответствующих стандартов, касающихся конкретных приложений или параметров качества, в Рекомендации МСЭ-Т M.1079-2 определяются требования к качеству сквозной передачи речи и данных и к рабочим характеристикам для сетей доступа IMT-2000, в то время как в Рекомендации МСЭ-Т G.114 определяются границы для времени передачи по соединениям цифровой сети.

Для получения требуемых рабочих характеристик сети в ней должны быть реализованы определенные механизмы управления и предоставления различных ответов на запросы сетевых услуг, даже при наличии режима соперничества за получение ресурса. В документе IETF RFC 2990 приведены возможные характеристики управляемого ответа на конкретный запрос услуги, а именно: *непротиворечивость и предсказуемость с уровнем, равным или выше гарантированного минимума или установленным заранее*. Например, при режиме соперничества за получение ресурсов сети или перегрузке для реализации ожидаемого ответа на запрос услуги требуются различные средства, функционирующие в разных масштабах времени, начиная с тех, которые используются для точного расчета сети на основе моделей трафика для большого периода времени, и кончая теми, которые используются для дифференциального выделения ресурсов и контроля доступа к ним на основе текущего состояния нагрузки сети. Эти и другие механизмы (например, способ сигнализации для индикации желаемого уровня показателей качества сети) лежат в основе архитектурной модели поддержки качества услуги. В частности, в данной Рекомендации определяется набор общих сетевых механизмов поддержки качества услуги и приводится их структура. В конечном счете, для получения удовлетворительного суммарного эффекта от меняющихся показателей качества услуг, требуемых для разнообразных приложений, должны использоваться комбинации сетевых механизмов. Независимый от приложения вид определенной архитектурной модели отличает его от специфичных для приложений архитектур QoS, таких, которые определены в Рекомендации МСЭ-Т H.360, что характерно для мультимедийных приложений.

6 Конструктивные блоки для качества услуги (QoS)

Основой архитектурной модели для качества услуги (QoS) является набор общих сетевых механизмов управления ответом сети на запрос услуги, который может быть специфическим для некоторого сетевого элемента, для сигнализации между сетевыми элементами или для управления и администрирования трафиком, при его прохождении через сеть. (Следует отметить, что конструктивные блоки не должны приниматься во внимание для сквозных соединений.) Как показано на рисунке 1, конструктивные блоки распределены по трем плоскостям:

– Плоскость управления, содержащая механизмы управления трактами, через которые проходит трафик пользователя. В состав этих механизмов входит управление допуском, маршрутизация для QoS и резервирование ресурсов.

– Плоскость данных, содержащая механизмы, работающие непосредственно с трафиком пользователя. В состав этих механизмов входит управление буферами, предотвращение перегрузки, маркировка пакетов, организация очередей и диспетчеризация, классификация трафика, правила обработки трафика и моделирование трафика.

– Плоскость административного управления, содержащая механизмы, относящиеся к эксплуатации, администрированию и административному управлению сетью. В состав этих механизмов входят: соглашение об уровне обслуживания (SLA), восстановление трафика, измерение и регистрация, а также заданные правила доставки информации.

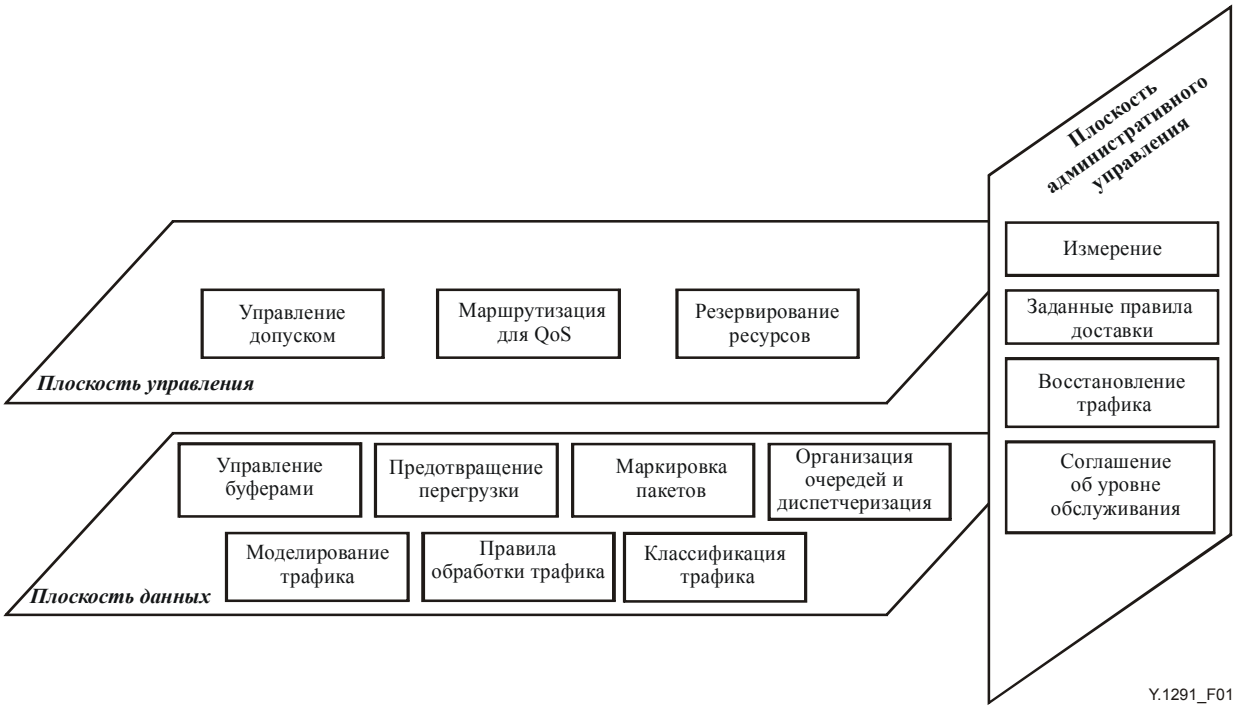


Рисунок 1/Y.1291 – Архитектурная модель для поддержки QoS

Конструктивный блок для QoS может быть специфическим для сетевого узла (что показывает управление буферами) или его можно применять к сегменту сети (что показывает маршрутизация для QoS). В последнем случае между узлами сети необходима сигнализация о том, являются ли они частью сегмента сети, который будет сквозным, от конца до границы, от границы до границы или от сети до сети. Сигнализация может существовать в любой из трех логических плоскостей. В плоскостях управления или административного управления сигнализация связана с использованием протокола сигнализации. Ввиду своих однозначно определяемых атрибутов сигнализация в данной Рекомендации интерпретируется как часть взаимодействия между конструктивными блоками для QoS и рассматривается в соответствующем разделе.

Важно отметить, что архитектурная модель для поддержки QoS носит логический характер и не налагает ограничений на способ реализации конструктивного блока. Реализация конструктивного блока, как таковая, может, например, быть распределенной или централизованной. В нижеследующих разделах приводится описание конструктивных блоков в соответствии с их распределением по плоскостям.

7 Механизмы плоскости управления

7.1 Управление допуском

Этот механизм управляет допуском трафика к сети. Обычно критерии допуска вытекают из заданных правил доставки [IETF RFC 2753]. Получит ли трафик допуск в сеть, зависит от априорного соглашения об уровне обслуживания. Кроме того, принятие решения может зависеть от того, доступны ли достаточные ресурсы сети, так чтобы вновь пропускаемый в сеть трафик не перегружал ее и не снижал качества услуг для текущего трафика. Для поставщика услуг должен быть допущен максимальный трафик, в то время как для существующего трафика сохраняется тот же уровень качества услуг (включая характеристики транзакций, а также ожидаемый уровень по надежности/доступности услуг).

Схемы допуска вызова, связанные с характеристиками транзакций, обычно основаны на контроле параметра или измерения. Схема на основе контроля параметра позволяет получить предельное значение в наихудшем случае для набора показателей (например, для потери пакетов, задержки и их разброса) из числа параметров трафика и соответствует предоставлению "жесткого" качества услуг для услуг с реальным масштабом времени. Такой подход обычно применяется при запросе на резервирование ресурсов, чтобы защитить необходимый ресурс от последующего потока трафика. В Добавлении I приводится пример схемы обеспечения QoS, использующей такой тип управления допуском.

В схеме на основе измерений, напротив, для принятия решения о допуске используются измерения существующего трафика. При таком подходе не гарантируется пропускная способность или жесткие предельные значения потери пакетов, задержки или их разброса, и этот подход соответствует предоставлению *гибкого* или относительного качества услуг (QoS). Вообще, этот подход обеспечивает более высокое использование ресурсов сети, чем при подходе на основе контроля параметров. В Добавлении II содержатся сводные данные об экспериментальном подходе к обеспечению качества услуг (QoS) на основе измерений. Следует заметить, что в принципе возможен "гибридный" подход, такой как использование измерений для обновления ресурсов, доступных при параметрическом подходе.

Управление допуском также может использоваться для соответствия требованиям по надежности/доступности в течение заданного периода времени для желаемых типов транзакций, в соответствии с условиями соглашения SLA. В частности, желаемые надежность/доступность услуги могут быть запрошены в виде уровня приоритета для управления допуском, который, в свою очередь, принимает решение об установлении "соединения" или тракта, такого как LSP. Правилами управления допуском отдается предпочтение потокам трафика (например, для экстренной связи), которые рассматриваются поставщиком услуг как критические в условиях перегрузки. Приоритет управления допуском – это способ предпочтения для допуска трактов LSP с более высоким приоритетом по сравнению с трактами LSP более низкого приоритета.

В Приложении A содержится продолжение описания уровней приоритетов для управления допуском.

7.2 Маршрутизация для качества услуг (QoS)

В узком смысле маршрутизация для QoS относится к выбору пути, удовлетворяющего требованиям потока по качеству услуг (QoS). Наиболее вероятно, что выбранный путь – это не традиционный кратчайший путь. В зависимости от специфических факторов и числа используемых показателей качества услуги, вычисления, необходимые для выбора пути, могут оказаться недопустимо дорогими по мере увеличения размера сети. Следовательно, в практических планах маршрутизации для QoS главным образом рассматриваются случаи с одним показателем качества услуги (например, с диапазоном передачи или задержкой) или с двумя показателями (например, стоимость – задержка, стоимость – диапазон передачи и диапазон передачи – задержка)[1]. Для дальнейшего снижения сложности вычисления пути существуют разные стратегии маршрутизации. В зависимости от того, как поддерживается информация о состояниях, и как выполняется поиск возможных путей, существуют такие стратегии, как маршрутизация по источнику, распределенная маршрутизация и иерархическая маршрутизация [Chen]. Кроме того, в зависимости от метода обработки множества показателей качества услуг, существуют такие стратегии, как упорядочение показателей и последовательная фильтрация, при которых уравновешиваются глобальная оптимальность и сниженная сложность вычислений [IETF RFC 2386].

Процесс выбора пути включает в себя наличие информации о требованиях по качеству услуг для потоков, о характеристиках и (часто меняющейся) информации о доступности сетевых ресурсов (выраженная в терминах стандартных показателей, таких как доступный диапазон передачи и задержка). Такого рода информацию можно получать и распределять с помощью протоколов сигнализации. Например, для передачи требований и характеристик потока и для расширений открытого протокола предпочтения кратчайшего пути (OSPF), как определено в документе IETF RFC 2676 для доступности ресурсов, может быть использован протокол резервирования ресурсов (RSVP) [IETF RFC 2205]. По сравнению с маршрутизацией по кратчайшему пути, когда оптимальные маршруты выбираются на основе относительно постоянного показателя (например, подсчета числа транзитов в сети или стоимости), маршрутизация для качества услуг (QoS) влечет за собой более частые и сложные вычисления пути и возрастание трафика сигнализации [Apostolopoulos].

Важно отметить, что маршрутизация для QoS предусматривает средства определения только того пути, который, вероятно, может обеспечить запрашиваемое качество. Чтобы гарантировать качество при передаче по выбранному пути, необходимо, чтобы маршрутизация для QoS использовалась в сочетании с резервированием ресурсов в целях резервирования необходимых сетевых ресурсов на всем протяжении пути.

Маршрутизация для QoS может также быть обобщена для применения к расчету трафика. (Что касается медленно меняющихся моделей трафика в течение длительного времени и разреженной гранулярности потоков трафика, то расчет трафика включает в себя управление трафиком, управление пропускной способностью, измерение и моделирование трафика, моделирование сети и

---

[1] Следует заметить, что некоторые из этих показателей носят аддитивный характер, а некоторые – ограничительный. Например, задержка и стоимость являются аддитивными, а диапазон передачи – ограничительным. Эти соображения важны при разработке реализуемых алгоритмов маршрутизации.

анализ качества.) С этой целью при выборе маршрутизации часто принимается во внимание множество ограничений, таких как атрибуты трафика, сетевые ограничения и ограничения в заданных правилах обработки [IETF RFC 3272]. Такая обобщенная маршрутизация для QoS называется также маршрутизацией на основе ограничений, которая может позволить выбрать путь с обходом перегруженных участков (или разделить нагрузку) и улучшить использование всей сети, а также автоматически выполнять правила расчета трафика.

В Рекомендациях МСЭ-Т серии E.360.x приводится описание, анализ и рекомендации методов по управлению ответом сети на требования трафика и другие воздействия, такие как отказы трактов или узлов. В частности, методы, упомянутые в Рекомендациях серии E.360.x, включают в себя маршрутизацию вызовов и соединений, управление ресурсами для качества услуг (QoS), управление таблицами маршрутизации, динамическую транспортную маршрутизацию, управление пропускной способностью и эксплуатационные требования. В Рекомендации МСЭ-Т E.361 содержится продолжение описания функции маршрутизации для QoS и связанных с ней параметров, таких как выделение и защита диапазона передачи, приоритет маршрутизации, приоритет обслуживания в очереди и идентификация класса обслуживания. Кроме того, Рекомендация МСЭ-Т E.361 предусматривает средства сигнализации для параметров маршрутизации для QoS через сети, использующие различные технологии маршрутизации.

7.3 Резервирование ресурсов

Этот механизм игнорирует требования к необходимым сетевым ресурсам, содержащиеся в запросе, для получения желаемых показателей качества сети. Будет ли удовлетворен запрос на резервирование, в значительной степени зависит от управления допуском, поэтому применяются все правила управления допуском. Но, вообще говоря, необходимым условием для удовлетворения запроса на резервирование является наличие достаточных ресурсов сети.

Точный характер резервирования ресурсов зависит от требований к показателям качества сети и конкретной сетевой технологии для удовлетворения этих требований. Например, при использовании технологии *IntServ* рассматриваются однонаправленные потоки, которые характеризуются в терминах параметров, описывающих блок маркеров, а инициируемое со стороны получателя резервирование ресурсов выполняется по запросу в соответствии с требованиями по пиковой скорости передачи, чтобы гарантировать пределы задержки. Несмотря на специфические факторы, важно, чтобы поставщики услуг могли платить за использование зарезервированных ресурсов, поэтому резервирование ресурсов требует поддержки аутентификации, проверки правомочности доступа, учета и взаиморасчетов между различными поставщиками услуг. Резервирование ресурсов обычно выполняется с использованием целевого протокола, такого как протокол RSVP [IETF RFC 2205].

Резервирование ресурсов может рассматриваться как функции, выполняемые распределенным или централизованным способом. Главным вопросом является несоответствие между фактической и предсказываемой доступностью ресурсов, поэтому необходимо проявлять осторожность при использовании самой последней информации о доступности узла, тракта и прочих ресурсов для обращения с запросом ресурсов.

8 Механизмы плоскости данных

8.1 Управление очередью (буферами)

Система управления очередью или буферами принимает решение о сохранении и отбрасывании пакетов, ожидающих передачи. Важной целью управления очередью является минимизация длины очереди в установившемся режиме, когда канал не используется, и устраняется монопольное использование, где одно соединение или поток монополизирует пространство очереди [IETF RFC 2309]. Схемы для управления очередью различаются, главным образом, по критериям отбрасывания пакетов и по тому, какие пакеты отбрасываются. Использование нескольких очередей вносит в эти схемы дальнейшие изменения, например, в способ распределения пакетов по очередям.

Общим критерием для отбрасывания пакетов является получение очереди максимальной длины. Пакеты отбрасываются, когда очередь заполняется полностью. От дисциплины отбрасывания зависит то, какие пакеты отбрасываются, например:

- При дисциплине "отбрасывание последнего пакета" отвергается вновь поступивший пакет. Это наиболее часто используемая стратегия.
- При дисциплине "отбрасывание первого пакета" вновь поступивший пакет сохраняется за счет пакета, стоящего первым в очереди.
- При дисциплине "отбрасывание случайного пакета" вновь поступивший пакет сохраняется за счет пакета, случайным образом выбранного из очереди. Такая схема может оказаться "дорогой", поскольку она требует перебора пакетов в очереди.

В схеме отбрасывания пакетов, только когда вся очередь заполнена, наблюдается тенденция сохранять очередь в таком заполненном состоянии в течение относительно большого периода времени, что может привести к катастрофическому результату в случае неравномерного трафика. Имеются схемы, использующие более динамичный критерий, не основанный на фиксированной максимальной длине очереди, и, таким образом, способные выполнять активное управление очередью. Такой известной схемой является схема раннего случайного обнаружения (RED) [Floyd], которая также помогает решать проблему заполненной очереди и избежать перегрузки. Согласно схеме RED, пакеты (входящие) отбрасываются с некоторой вероятностью на основе полученной оценки средней длины очереди. Вероятность отбрасывания пакетов возрастает с ростом оцениваемой средней длины очереди. Иными словами, если очередь в недавнем прошлом была главным образом пуста, то входящие пакеты будут иметь тенденцию к сохранению; если же недавно очередь главным образом была относительно заполнена, то, вероятно, входящие пакеты должны быть отброшены. Более конкретно, в схеме RED используются два порога для средней длины очереди. Один порог задает среднюю длину очереди, короче которой пакеты не отбрасываются; другой порог задает среднюю длину очереди, больше которой отбрасываются все пакеты. Что касается средней длины очереди между этими двумя порогами, то вероятность отбрасывания пакетов пропорциональна средней длине. Естественно, что эффективность схемы RED зависит от того, как установлены соответствующие параметры. Не существует одного набора параметров, действующих эффективно для всех типов трафика и сценариев перегрузки. Таким образом, появляются варианты схемы RED, например, такие:

– Потоковая схема RED (FRED) [Lin *et al*., 1997], когда в схему RED вводится дополнительное управление путем раздельного анализа отбрасываний пакетов для потоков на основе использования ими буферов. Если число пакетов из потока в очереди ниже характерного для потока порогового значения, то вновь поступивший пакет того же потока отброшен не будет. В противном случае он будет отброшен, и будут анализироваться потоки с меньшим числом пакетов в буфере. По сравнению со схемой RED схема FRED является более гибкой в отношении защиты потоков от использования более или менее справедливого разделения буферного пространства и диапазона передачи канала.

– Взвешенная схема RED, при которой в схему RED вводится дополнительное управление путем дифференцированного анализа отбрасывания пакетов на основе их приоритета. Чем выше приоритет пакета, тем ниже вероятность того, что он будет отброшен.

8.2 Предотвращение перегрузки

Перегрузка в сети возникает, когда трафик близок или превосходит тот объем, который может обработать сеть, из-за нехватки ресурсов, таких как диапазон передачи канала и буферное пространство. Признаком перегрузки является, например, тот факт, что очереди в маршрутизаторе (или устройстве коммутации) всегда заполнены, и маршрутизаторы начинают отбрасывать пакеты. Отбрасывание пакетов вызывает повторную передачу, что приводит к возрастанию объема трафика и усиливает перегрузку. В результате такой цепной реакции сеть может перестать работать, имея нулевую пропускную способность. Чтобы предотвратить перегрузку из-за уменьшения буферного пространства, интуиция подсказывает, что нужно использовать очень большие буферы. Однако Nagle [1987] показал, что имеет место противоположное явление. Задержка пакетов в длинных очередях из-за больших буферов приводит к повторной передаче пакетов, что затем создает перегрузку. Для предотвращения перегрузки необходимы более надежные средства для удержания нагрузки сети в пределах ее пропускной способности, чтобы сеть могла работать на приемлемом уровне качества, не испытывая последствий перегрузки.

Типичная схема предотвращения перегрузки действует посредством снижения объема трафика отправителя, поступающего в сеть, при индикации наличия перегрузки в сети (или при индикации состояния сети, близкого к перегрузке) [Jacobson, 1988]. Пока нет явной индикации, потеря пакетов или истечение тайм-аута в таймере обычно рассматриваются как неявная индикация сетевой перегрузки. От свойств транспортных протоколов зависит, как источник трафика возвратится к прежнему уровню трафика. В протоколе с передачей "окнами", например, таком как протокол TCP, это выполняется путем мультипликативного уменьшения размера окна.

В идеале источником снижения трафика является пользователь, приоритет управления допуском для которого не является критическим. Это может позволить трафику с более высоким приоритетом продолжать получать нормальное обслуживание.

Когда перегрузка снижается, отправитель затем постепенно наращивает трафик.

Чтобы предотвратить вероятность чрезмерных задержек из-за повторных передач после потерь пакетов, недавно были разработаны схемы явного уведомления о перегрузках (ECN). Схема ECN для IP-протокола и протокола TCP в числе прочих схем управления активным буфером описана в документе IETF RFC 3168. По этой схеме на начальную перегрузку сети указывает маркировка

пакетов, а не их отбрасывание. При приеме пакета, испытывающего перегрузку, хост-узел со схемой уведомления ECN реагирует, в сущности, таким же образом, как на отброшенный пакет.

8.3 Организация очередей и диспетчеризация

Принцип действия этого механизма заключается в управлении выбором пакетов для передачи по исходящему тракту. Входящий трафик удерживается в системе организации очередей, которая обычно состоит из нескольких очередей и планировщика. Управление системой организации очередей – это используемая дисциплина организации очередей и диспетчеризации. Существует несколько принципиальных дисциплин:

– Обслуживание очереди по принципу "первым вошел, первым вышел": пакеты помещаются в одну очередь и обслуживаются в том же порядке, в каком они поступают в очередь.
– Обслуживание очереди по "равноправному" принципу: пакеты сначала классифицируются по потокам и распределяются по очередям, выделенным соответствующим потокам, а затем очереди обслуживаются по круговому алгоритму. Пустые очереди пропускаются. Обслуживание очереди по равноправному принципу также называется обслуживанием очереди по каждому потоку или на основе потока.
– Обслуживание очереди по приоритетному принципу: пакеты сначала классифицируются, а затем помещаются в очереди с разными приоритетами. Пакеты обслуживаются начиная с "головы" данной очереди, если только все очереди более высокого приоритета пусты. В каждой из приоритетных очередей пакеты обслуживаются в порядке "первым вошел, первым вышел".
– Обслуживание очереди по взвешенному равноправному принципу: пакеты классифицируются по потокам и распределяются по очередям, выделенным для соответствующих потоков. Очереди присваивается некоторая процентная доля выходного диапазона передачи согласно диапазону, необходимому для соответствующего потока. Путем дифференцирования пакетов переменной длины в такой дисциплине также предотвращается распределение большого диапазона передачи для потоков с более длинными пакетами, чем для потоков с более короткими пакетами.
– Обслуживание очереди по принципу, опирающемуся на класс обслуживания: пакеты классифицируются по различным классам обслуживания, а затем присваиваются очередям, относящимся к соответствующим классам. Каждой очереди может быть присвоена своя процентная доля выходного диапазона передачи, и эта очередь обслуживается по круговому алгоритму. Пустые очереди пропускаются.

8.4 Маркировка пакетов

Пакеты могут маркироваться согласно конкретным классам обслуживания, которые им будут присваиваться в сети для каждого пакета. Маркировка пакетов, выполняемая, как правило, оконечным узлом, включает в себя присвоение стандартным способом некоторого значения предназначенному для этого полю заголовка пакета. (Например, тип услуги в заголовке IP-протокола или EXP-биты заголовка вставки при коммутации MPLS [IETF RFC 3032] используются для кодификации наблюдаемого внешним образом поведения маршрутизаторов в методах *DiffServ* [IETF RFC 2474] или *MPLS-DiffServ* [IETF RFC 3270].) При выполнении маркировки хост-узлом маркер должен быть проверен, и, при необходимости, может быть изменен оконечным узлом. Иногда для маркировки несовместимых пакетов могут быть использованы специальные значения, и эти пакеты могут быть позднее отброшены из-за перегрузки. На основе результатов измерений для пакетов также может быть повышен или понижен класс обслуживания.

Критерии для маркировки пакетов должны устанавливаться или динамически конфигурироваться, независимо от того, выполняется маркировка хост-узлом или оконечным узлом. Для динамической конфигурации может быть использован общий открытый протокол обслуживания на основе установленных правил (IETF RFC 2748) или протокола RSVP. В случае протокола RSVP маркирующий объект может его использовать для запроса к сети о маркировке, чтобы применить маркировку к пакетам, принадлежащим определенному потоку [IETF RFC 2996].

8.5 Классификация трафика

Классификация трафика может быть выполнена на уровне потока или пакета. На границе сети объект, отвечающий за классификацию трафика, обычно просматривает многокомпонентные поля (такие, как пять кортежей, связанных с IP-потоком) пакета, определяет агрегат данных, к которому принадлежит пакет, и просматривает соответствующее соглашение об уровне обслуживания.

8.6 Контроль трафика

Система контроля трафика принимает решение о том, соответствует ли поступающий от транзита к транзиту трафик с заранее согласованными правилами обработки или контрактами. Обычно несоответствующие пакеты отбрасываются. Отправители могут быть уведомлены об отброшенных пакетах и обнаруженных причинах, а также о соблюдении соответствия в будущем, обусловленного соглашениями SLA.

8.7 Моделирование трафика

Система формирования трафика управляет скоростью и объемом трафика, поступающего в сеть. Объект, отвечающий за моделирование трафика, будет помещать несоответствующие пакеты в буфер до тех пор, пока не приведет соответствующий агрегат данных в соответствие с трафиком. Таким образом, результирующий трафик не будет таким же неравномерным, как исходный трафик, и будет более предсказуемым. Моделирование трафика часто необходимо выполнять между выходными и входными узлами.

Существуют два основных метода для формирования трафика: метод с использованием "протекающего" блока и метод с использованием блока маркеров. В методе с "протекающим" блоком такой блок используется для регулирования скорости трафика, исходящего от узла. Независимо от скорости входного потока "протекающий" блок удерживает постоянную скорость выходного потока. Все излишние пакеты, переполняющие этот блок, отбрасываются. Характеристиками данного метода служат два параметра, обычно настраиваемые пользователем, а именно размер блока и скорость передачи.

Метод с использованием блока маркеров, с другой стороны, не является таким жестким в отношении регулирования скорости трафика, исходящего от узла. Он позволяет пакетам выходить так же быстро, как они поступают, при условии, что имеется достаточно *маркеров.* Маркеры генерируются с определенной скоростью и заносятся в блок маркеров до тех пор, пока он не заполнится. За счет маркера определенный объем трафика (то есть определенное число байтов) может покинуть узел. Если в блоке нет маркеров, то никакие пакеты переданы быть не могут. Одновременно может быть использовано несколько маркеров, что позволит проходить пачкам пакетов. В этом методе, непохожем на метод с "протекающим" блоком, нет заданных правил отбрасывания пакетов. Если блок маркеров заполнен, то обработкой пакетов занимается система управления буфером. Характеристиками метода с блоком маркеров служат два параметра, обычно настраиваемые пользователем, а именно размер блока маркеров и скорость генерирования маркеров.

Метод с "протекающим" блоком и метод с блоком маркеров могут быть использованы вместе. В частности, трафик может моделироваться сначала по методу с использованием блока маркеров, а затем по методу с использованием "протекающего" блока, чтобы устранить нежелательные пачки пакетов. Два блока маркеров могут также использоваться последовательно.

9 Механизмы плоскости административного управления

9.1 Соглашение об уровне обслуживания

Соглашение об уровне обслуживания (SLA) обычно представляет собой соглашение между пользователем и поставщиком услуги, который задает уровень доступности, удобства обслуживания, качества, эксплуатации или других атрибутов услуги. Оно может включать в себя такие вопросы, как назначение цены, которые носят коммерческий характер. Техническая часть такого соглашения называется Спецификацией уровня обслуживания (SLS) [IETF RFC 3198], которая, в частности, включает в себя набор параметров и их значения, которые вместе определяют услугу, предлагаемую сетью трафику пользователя. Параметры спецификации SLS могут носить общий характер, как параметры, которые определены в Рекомендации МСЭ-Т Y.1540, или быть характерными для технологии, как параметры качества и трафика, используемые в технологиях *IntServ* или *DiffServ*. В целом, в Рекомендации МСЭ-Т E.860 определяется структура соглашения SLA для сетевой инфраструктуры, построенной на оборудовании разных производителей.

9.2 Измерения и регистрация трафика

К измерениям относится слежение за временными свойствами (например, скоростью) потока трафика в сопоставлении с согласованным профилем трафика. Они включают в себя наблюдение за характеристиками трафика в заданном пункте сети, а также сбор и хранение информации о трафике для анализа и дальнейших действий. В зависимости от уровня соответствия измерительное устройство может инициировать необходимую обработку (например, отбрасывание или моделирование) для потока пакетов.

9.3 Восстановление трафика

Восстановление определяется в широком смысле в данной Рекомендации как смягчающая последствия реакция сети в условиях отказа, и оно должно рассматриваться на многих уровнях. В нижней части многоуровневого стека оптические сети в настоящее время могут предоставлять динамическую защиту с кольцевой и ячеистой структурой и восстановление выполняемых функций на уровне длины волны. На уровне иерархий SONET/SDH надежность обеспечивается автоматической защитной коммутацией (APS), а также самовосстанавливающимися кольцевыми и ячеистыми архитектурами. Режим ATM также предоставляет подобные возможности. Ремаршрутизация традиционно используется на уровне IP-протокола, чтобы восстановить обслуживание после отказов тракта и узла, и может быть сквозной или местной (быстрая ремаршрутизация). Маршрутизация на уровне IP-протокола возникает после периода конвергенции маршрутизации, которая может требовать для своего выполнения периода времени от секунд до минут. В настоящее время восстановление на уровне IP-протокола осуществляется перед конвергенцией с помощью коммутации MPLS.

Существуют два типа отказов сети:

- Отказ узла: отказ сетевого элемента (например, платы маршрутизатора) в узле сети или на станции коммутации. Для минимизации влияния отказа такого типа обычно используются избыточные функции в сетевых элементах, предусмотренные при проектировании. Однако катастрофические отказы, такие как отключения электропитания и природные катастрофы, могут вывести из строя весь узел сети. В этом случае проходящий трафик может быть ремаршрутизирован по свободным каналам, минуя поврежденный узел.
- Отказ транспортного звена: отказ транспортного канала (например, каналов T1, OC-3), соединяющего два узла сети. Обычно каналы могут отказывать из-за отказа элемента канала (например, линейной платы) (который может затем вывести из строя один канал) или, что более серьезно, из-за разрыва оптического волокна (что может затем вывести из строя большое число каналов). Для ослабления влияния таких отказов и восстановления потоков трафика, пока не будет устранена неисправность, поставщики услуг могут предусматривать при проектировании дополнительную свободную емкость.

Следует заметить, что некоторые из этих терминов, как правило, характерны для уровня, и требуется тщательное рассмотрение нескольких уровней, включенных в весь проект. Например, отказ канала на физическом уровне может влиять на множество каналов и трактов на уровне IP-протокола.

Также, как в случае управления допуском, определенные потоки трафика, относящиеся к "критическим" услугам, могут потребовать более высокого приоритета восстановления, чем другие потоки. Необходимо, чтобы поставщик услуг планировал свободные ресурсы на достаточно уровне, так чтобы соглашения SLA для качества услуг подчинялись условиям восстановления. Типовыми параметрами для измерения возможности восстановления обслуживания являются время восстановления и вероятность (в процентах) восстановления обслуживания. Более подробно об уровнях приоритета см. в Приложении A.

9.4 Правила обработки

Правила обработки – это набор правил, обычно используемых для администрирования, управления и административного управления доступом к сетевым ресурсам. Эти правила могут быть характерными для нужд поставщика услуг, либо отражать соглашение между пользователем и поставщиком услуг, которое может содержать требования по надежности и доступности за некоторый период времени и прочие требования по качеству услуг. На основе правил обработки поставщики услуг могут осуществлять реализацию механизмов в плоскости управления и плоскости данных. Некоторыми из возможных применений являются маршрутизация по заданным правилам (направление потока пакетов в порт адресата без использования таблицы маршрутизации), фильтрация пакетов на основе заданных правил (маркировка или отбрасывание пакетов на основе правил классификации), регистрация пакетов (позволяющая пользователям регистрировать заданные потоки) и заданные правила обработки, связанные с безопасностью.

Принятие решений по правилам обработки может быть инициировано разными событиями. Некоторые из них связаны с трафиком, а некоторые – не связаны с ним. Подробности обычно зависят от специфики применения. Например, в документе IETF RFC 2748 описывается простой протокол запросов и ответов, который может быть использован для обмена информацией о правилах обработки между сервером этих правил (или точкой принятия решения по заданным правилам) и его клиентом (или пунктом выполнения этих правил).

10 Взаимодействие между конструктивными блоками

В полном решении, обеспечивающем качество услуг (QoS), обычно используется несколько компоновочных блоков на всей плоскости управления, плоскости данных и плоскости

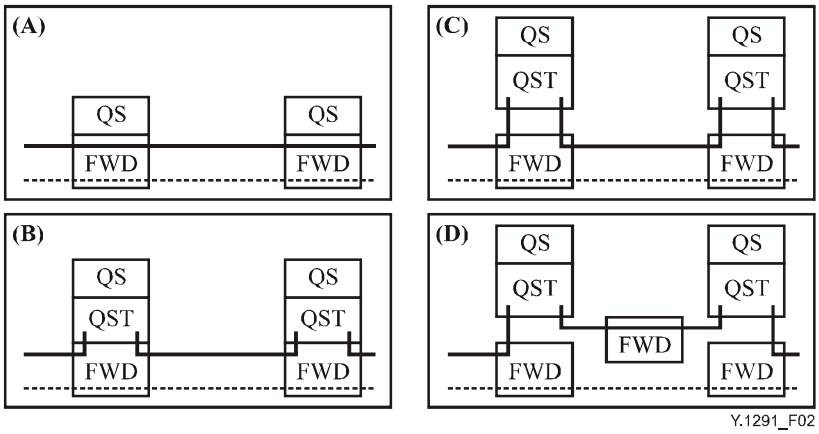
административного управления. Поэтому необходимо, чтобы между разными конструктивными блоками существовал обмен параметрами по качеству услуг. Эти параметры включают в себя показатели качества транзакций на уровне пакета (например, задержка и потери пакетов) и ожидания по надежности/доступности услуги в форме уровней приоритетов трафика для конкретных сетевых функций, таких как управление допуском и восстановление трафика. Примерами механизмов по переносу этих значений параметров являются сигнализация и просмотры без данных.

10.1 Сигнализация для качества услуг (QoS)

Сигнализация для качества услуг (QoS) служит, главным образом, для передачи требований приложений (или сети) для резервирования сетевых ресурсов по всей сети или для нахождения маршрутов для обеспечения качества услуг. В зависимости от того, является ли сигнальная информация частью ассоциированного трафика данных, она может быть внутриполосной или внеполосной:

– Внутриполосная сигнализация: сигнал для качества услуги (QoS) является частью ассоциированного трафика данных, обычно представленного в отдельном поле заголовка (например, поле TOS в протоколе IPv4, как в *DiffServ* и 802.1p) пакетов данных. На плоскости данных внутриполосная сигнализация ни вводит в сеть дополнительный трафик, ни приводит к задержке при установлении (соединения) для трафика данных. Естественно, что такой тип сигнализации не подходит для резервирования ресурсов или маршрутизации для качества услуг (QoS), что необходимо делать априори до передачи данных.

– Внеполосная сигнализация: сигнал для качества услуги (QoS), который переносится выделенными пакетами, отделяется от ассоциированного трафика данных. Кроме того. сигнализация для качества услуги может быть сквозной или передаваться через участки транзита. В случае передачи по участкам транзита (как показано на рисунке 2, случай B), сигнальная информация, вероятно, должна модифицироваться транзитными узлами. В противоположность этому, в случае сквозной передачи (как показано на рисунке, случай A) сигнальная информация не модифицируется транзитными узлами. В результате внеполосная сигнализация вносит в сеть дополнительный трафик и вызывает необходимость в дополнительной служебной информации для получения требуемых показателей качества сети. Кроме того, эта сигнализация влечет за собой использование протокола сигнализации и дальнейшую обработку на уровне выше сетевого, что приводит к не таким быстрым ответам, как при внутриполосной сигнализации. Тем не менее, естественно, что внеполосная сигнализация подходит для резервирования ресурсов и маршрутизации для обеспечения качества услуги (QoS).



QS Функции для сигнализации для QoS, отличные от QST
QST Функция для завершения сигнализации для QoS
FWD Функция для перенаправления данных
Сигнальный тракт для QoS
Тракт передачи данных

Рисунок 2/Y.1291 – Иллюстрация различных форм сигнализации для качества услуги (QoS)

Подобным образом, в зависимости от того, является ли сигнальный тракт тесно связанным с трактом ассоциированных данных, сигнализация для QoS может рассматриваться как сигнализация по связанному тракту или сигнализация по несвязанному тракту:

– Сигнализация по связанному тракту: сигнальные сообщения для качества услуги маршрутизируются только через узлы, потенциально находящиеся в тракте передачи данных. Как таковая, внутриполосная сигнализация по определению является сигнализацией по

связанному тракту, но внеполосная сигнализация может не быть таковой. Сигнализация по связанному тракту означает, что узлы сигнализации должны совмещаться с маршрутизаторами. С одной стороны, такое расположение имеет преимущество пониженной общей стоимости обработки сигнализации (поскольку оно выгодно использует задачи маршрутизации сетевого уровня), но, с другой стороны, оно имеет недостаток, связанный с отсутствием гибкости при модернизации маршрутизаторов или при объединении объектов управления (например, серверов правил обработки) вне тракта передачи данных (или при объединении нетрадиционных методов маршрутизации). Если механизм со связанным трактом включает в себя протокол сигнализации, то это означает, что маршрутизаторам требуется поддерживать этот протокол и они должны быть способны обрабатывать соответствующие сигнальные сообщения. Примером сигнализации по с вязанному тракту является протокол RSVP.

– Сигнализация по несвязанному тракту: сигнальные сообщения для качества услуги маршрутизируются через узлы, которые, как предполагается, не находятся в тракте передачи данных. Как таковая, только внеполосная сигнализация может быть сигнализацией по несвязанному тракту. Сигнализация по несвязанному тракту предусматривает, что объект, завершающий сигнализацию для качества услуги (QoS), должен быть предназначен для такой сигнализации и отделен от объекта, выполняющего переадресацию, который обычно находится в маршрутизаторах. В противоположность сигнализации по связанному тракту, сигнализация по несвязанному тракту обладает преимуществом гибкости при развертывании и модернизации узлов сигнализации независимо от маршрутизаторов или при объединении объектов управления вне тракта передачи данных, но она имеет недостаток, связанный с добавляемой сложностью и стоимостью всей обработки и с эксплуатационными задачами. На рисунке 2 случай C и случай D иллюстрируют сигнализацию по несвязанному тракту.

10.2 Взаимодействия внутри плоскостей

Данный вопрос подлежит дальнейшему изучению.

10.3 Взаимодействие между плоскостями

Плоскости управления и данных

Отображение класса качества QoS по Рекомендации МСЭ-Т Y.1541 в протоколе DSCP

В Добавлении VI/Y.1541 представлено объединение классов качества услуг (QoS) согласно Рекомендации Y.1541 с режимами каждого домена (PDB) для технологии Diffserv:

- PDB, основанный на режиме PHB срочной доставки: классы 0 и 1 согласно Рекомендации Y.1541.
- PDB, основанный на режиме PHB гарантированной доставки: классы 2, 3 и 4 согласно Рекомендации Y.1541.
- PDB, основанный на режиме PHB наилучшей из возможных доставки (по умолчанию): класс 3 согласно Рекомендации Y.1541.

11 Вопросы безопасности

В Рекомендации МСЭ-Т X.805 описана архитектура обеспечения безопасности сети, которую можно использовать для проверки характеристик обеспечения безопасности конструктивных блоков и технических решений для качества услуг (QoS) и для разработки защитных мер по отношению к конструктивным блокам и решениям.

11.1 Плоскость данных

Трафик на плоскости данных обычно обрабатывается в соответствии с информацией заголовка пакета. Пакеты могут быть промаркированы путем присвоения некоторого значения заданному полю заголовка или классифицированы на основе нескольких полей заголовка пакета (таких, как пять кортежей IP-протокола). На основе такой классификации и маркировки пакетов затем могут быть выполнены моделирование, отслеживание и организация очередей для трафика. Как таковая, целостность заголовков пакетов существенна для действительности и безопасности технологий обеспечения QoS. Злонамеренная модификация и фабрикация информации заголовков пакетов должна быть предотвращена.

Также важно отметить, что, хотя маркировка пакета может быть выполнена или изменена хост-узлами или любыми другими узлами сети, все-таки желательно иметь маркировку, выполненную оконечным узлом. Вообще, оконечный узел имеет надежную взаимосвязь с внутренними узлами. Таким образом, если маркировка пакета выполнена хост-узлом, то эта маркировка должна быть проверена и может быть изменена при необходимости оконечным узлом.

11.2 Плоскости управления и административного управления

Плоскость контроля и плоскость административного управления работают с трафиком на уровне потока или на агрегированном уровне. Поток также определяется и описывается, например, с помощью пяти кортежей IP-протокола или с помощью метки коммутации MPLS в заголовке пакета, который является постоянным в течение всего времени существования потока.

Управление допуском, выполняемое в оконечных узлах, подходит для препятствования замаскированным попыткам нарушения защиты и перегрузке, вызванной проникновением несанкционированного трафика. Оконечные узлы могут быть проверены внутренними узлами и могут иметь режим просмотра использования ресурсов всей сети. Управление допуском должно охватывать вопросы аутентификации и контроля прав доступа независимо от того, выполняется ли оно централизованным или распределенным образом.

Резервирование ресурсов тесно связано с управлением допуском. Запрос на резервирование может быть инициирован оконечным хост-узлом или узлом, поддерживающим услугу и расположенным в сети. Злонамеренные запросы ресурсов могут привести к незаконному чрезмерному резервированию ресурсов, исчерпанию ресурсов и к отказу в услуге. Защитные меры по предотвращению таких злонамеренных запросов являются необходимыми.

В общем, механизмы обеспечения безопасности сети, такие как системы защиты доступа и система обнаружения вмешательства, могут помочь в защите сетевых интерфейсов независимо от того, используются ли механизмы качества услуг (QoS) или не используются. Кроме того, объекты, отвечающие за аутентификацию, должны иметь средства защиты от попыток ее нарушения, приводящих к отказу в услуге.

11.3 Сигнализация для качества услуг (QoS)

Для защиты от попыток перехвата, модификации и подлога информации в системе сигнализации для качества услуг (QoS) должны использоваться механизмы обеспечения аутентификации и целостности, такие как RIPEMD160 или SHA-1 (защищенный алгоритм хеширования – 1). Использование механизмов обеспечения защиты может привести к последствиям для качества: поскольку сигнальный трафик по объему обычно намного меньше трафика данных, то влияние функционирования сети из-за защищенной внеполосной сигнализации (от сигнализации по несвязанному тракту) должно быть слабее, чем при внутриполосной сигнализации (или сигнализации по связанному объекту). Кроме того, объекты, "отвечающие" за сигнализацию, должны иметь средства защиты от попыток ее нарушения, приводящих к отказу в обслуживании.

12 Примеры методов

Чтобы показать, как взаимодействуют конструктивные блоки для обеспечения качества услуг (QoS) и как на их основе создаются методы обеспечения качества QoS, в данном разделе приводится описание четырех стандартизированных методов: метод интегрированных услуг (*IntServ*), метод дифференцированных услуг (*DiffServ*), метод многопротокольной коммутации с использованием меток (MPLS) и метод динамического качества услуг (QoS) IPCablecom. (Следует заметить, что в документе IETF RFC 2998 методы IntServ и DiffServ объединены.) Поскольку прочие, более проработанные методы только зарождаются и развиваются поэтапно, то примеры представлены в двух Добавлениях I и II.

12.1 Метод IntServ

Метод *IntServ* (см., например, [IETF RFC 1633]), предназначенный прежде всего для поддержки приложений, чувствительных к задержкам в реальном масштабе времени, построен на основе того, что поток, обслуживаемый со скоростью, которая немного выше его скорости передачи данных, имеет ограниченную задержку, и что сеть может гарантировать границу задержки для потока путем резервирования ресурсов для каждого потока. При таком методе приложение прежде, чем послать данные, сначала посылает в сеть сигналы запроса требуемой услуги, включая такие специфические параметры, как профиль ее трафика и требования к диапазону передачи и задержкам. Затем сеть определяет, может ли она выделить ресурсы достаточного объема (например, диапазон передачи и буферное пространство) для обеспечения требуемых показателей качества для запроса услуги. Только после того как запрос удовлетворен, приложение может начать передачу данных. Пока приложение придерживается своего профиля трафика, сеть выполняет свои обязательства по услуге путем поддержки состояния ресурсов по каждому потоку и путем использования дисциплин усовершенствованной организации очередей (например, принцип взвешенного равноправного обслуживания очереди) для совместного использования каналов. Конструктивные блоки, имеющие отношение к методу *IntServ*, включают в себя управление допуском, организацию очередей, резервирование ресурсов, классификацию и отслеживание трафика. В частности, для резервирования ресурсов используется протокол сигнализации RSVP. Сеть может принять или отклонить запрос резервирования средствами управления допуском на основании доступности ресурсов. Успешный запрос резервирования приводит к установке состояний ресурсов в узлах с протоколом RSVP. Конструктивные блоки взаимодействуют путем доступа к информации о состоянии ресурсов и к прочим предоставляемым (относительно статическим) объектам данных.

12.2 Метод DiffServ

В основе метода *DiffServ* лежит принцип анализа пакета на основе его класса обслуживания, указанного в кодах его IP-заголовка. Поставщик услуг заключает с каждым пользователем соглашение об уровне обслуживания (или определяет уровень обслуживания), которое, среди прочего, определяет, какой объем трафика может посылать пользователь в пределах любого заданного класса обслуживания. Исходящий трафик сортируется по каждому пакету и преобразуется в один из немногих агрегированных потоков или классов и отслеживается на границе сети поставщика услуг. Как только трафик поступает в сеть, маршрутизаторы проводят его дифференциальный анализ. В противоположность методу *IntServ*, анализ проводится не по каждому потоку, а исключительно по указанному классу обслуживания. Вся сеть организована так, чтобы удовлетворялись условия всех соглашений об уровне услуг. Соответствующие конструктивные блоки (в состав которых входит управление буферами, маркировка пакетов, соглашение об уровне обслуживания, измерение и регистрация трафика, отслеживание трафика, моделирование трафика и диспетчеризация) взаимодействуют в относительно статическом режиме, преимущественно через предоставляемые объекты данных.

12.3 Коммутация MPLS

Будучи первоначально разработанной в целях взаимодействия между сетями IP и ATM (или Frame Relay), коммутация MPLS [IETF RFC 3031] имеет большие преимущества в скорости передачи пакетов посредством использования коротких меток, подобных меткам уровня 2. При поступлении в сеть с коммутацией MPLS пакету раз и навсегда присваивается класс эквивалентности пересылки (FEC), который кодируется в форме строки фиксированной длины, называемой меткой. Когда пакет пересылается к следующему транзитному участку, то вместе с ним передается и эта метка. На следующем транзитном участке эта метка используется как указатель в заранее сконфигурированной таблице для определения следующего транзитного участка и новой метки. Старая метка заменяется на новую, и пакет передается на следующий транзитный участок. Этот процесс продолжается до тех пор, пока пакет не достигнет своего адресата. Иными словами, пересылка пакета при коммутации MPLS полностью управляется метками, посредством чего пакеты, которым присвоен один и тот же класс FEC, пересылаются по одному и тому же пути. Более того, метки имеют значение только для пары маршрутизаторов, совместно использующих тракт, и только в одном направлении – от отправителя до получателя. Получатель выбирает метку и согласует ее семантику с отправителем посредством протокола распределения меток. Коммутация MPLS в ее основной форме особенно удобна для расчета трафика. Для обеспечения явной поддержки качества услуг (QoS) в коммутации MPLS используются определенные элементы из методов *IntServ* и *DiffServ*. Например, протокол распределения меток может опираться на протокол резервирования ресурсов [IETF RFC 3209]. При этом требуемые ресурсы сети для коммутируемого по меткам тракта могут, таким образом, резервироваться в фазе его установления, чтобы гарантировать качество услуги для пакетов, проходящих по этому тракту. Кроме того, при использовании метки и определенных битов поля EXP заголовка вставки, который переносит метку для представления классов дифференцированных услуг, пакеты одного и того же класса FEC могут быть проанализированы по методу *DiffServ* [IETF RFC 3270]. Соответствующие конструктивные блоки для коммутации MPLS включают в себя управление буферами, маркировку пакетов, маршрутизацию для качества услуг (QoS), организацию очередей, резервирование ресурсов, классификацию и моделирование трафика. Они взаимодействуют посредством информации о состоянии коммутируемого по меткам тракта, имеющейся в каждом узле с коммутацией MPLS, используя протокол распределения меток и предоставляемые объекты данных.

12.4 Динамическое качество услуг (QoS) IPCablecom

В Рекомендации МСЭ-Т J.163 приводится описание метода, базирующегося на динамическом резервировании ресурсов для каждого потока, с целью поддержки интерактивных мультимедийных приложений, по сети доступа IPCablecom. Как определено в Рекомендации МСЭ-Т J.112, сеть доступа обеспечивает подключение терминального адаптера мультимедиа (MTA) к узлу доступа. На сети, соответствующей J.112, ресурсы распределяются для каждого индивидуального потока, связанного с прикладным сеансом связи для каждого абонента на основе аутентификации и подтверждения прав доступа.

Основным для динамического метода обеспечения качества услуг (QoS) являются шлюзы динамического качества услуг ((DQoS) и контроллер шлюзов. Используя общий открытый протокол обслуживания по заданным правилам (COPS), согласно документу IETF RFC 2748, контроллер шлюзов контролирует наличие и функционирование шлюзов.

Шлюзы для динамического качества услуги (DQoS) реализованы в узле доступа между сетью, соответствующей Рекомендации J.112, и опорной сетью с IP-протоколом, использующей функции классификации и фильтрации пакетов согласно Рекомендации J.112. Будучи однонаправленным, шлюз для динамического качества услуги (DqoS) является логическим объектом, связанным с сеансом связи. Если шлюз "закрыт", то транзитные данные в сети доступа, соответствующей Рекомендации J.112, могут быть либо отброшены, либо им просто может быть предоставлено лучшее из возможного обслуживание в зависимости от предопределенных действий поставщика.

Контроллер шлюзов реализован в Сервере управления вызовами, который обычно управляет мультимедийными сеансами, инициируемыми адаптерами MTA посредством сигнализации для управляемого сетью вызова (как определено в Рекомендации МСЭ-Т J.162) или посредством распределенной сигнализации для вызова (как определено в документе IETF RFC 3261). Контроллер "отвечает" за принятие решения по стратегии действий: создавать или открывать шлюз. Открытие шлюза предусматривает управление допуском при приеме запроса управления ресурсами (по протоколу RSVP) и резервирование в сети необходимых ресурсов. Следует отметить, что резервирование ресурсов осуществляется в два этапа. В конце первого этапа ресурсы резервируются, но они еще недоступны для адаптеров MTA. Только в конце второго этапа шлюзы в узлах доступа (AN) открыты, и ресурсы становятся доступными для адаптеров MTA. Модель резервирования и выполнения гарантирует, что ресурсы доступны для входящей стороны до получения сигнализации о том, что сеанс связи начинается и ресурсы гарантируются только тогда, когда они необходимы.

Соответствующие конструктивные блоки для метода динамического качества услуги (DQoS) IPCablecom включают в себя, в основном, управление допуском, организацию очередей, резервирование ресурсов, классификацию трафика, отслеживание трафика и заданные правила (стратегию). Для резервирования и гарантии предоставления ресурсов используются протоколы сигнализации RSVP и COPS. Сеть может принять или отклонить запрос резервирования ресурсов через управление допуском на основе доступности ресурсов или заданных правил. Успешный запрос резервирования ресурсов приводит к установке состояний ресурсов в узлах с протоколом RSVP. Конструктивные блоки взаимодействуют, получая доступ к информации о состоянии ресурсов и к другим предоставляемым объектам данных.

Приложение A

Уровни приоритетов трафика

Ожидания по качеству услуги (QoS) для услуг в сетях с передачей пакетов могут рассматриваться с двух сторон. Нормы качества пакетов транзакций (например, потеря пакета и задержка) регулируются классами транзакций, описанными в таких Рекомендациях МСЭ-Т, как Y.1541 для услуг IP и I.356 для услуг ATM. Эти классы охватывают широкий диапазон услуг, включая приложения по передаче речи, данных и мультимедиа. Приемлемые уровни качества определяются соответствующими параметрами (например, числом потерянных пакетов) для каждого класса транзакций. Ожидания по надежности выражаются в виде приоритета, связанного с установлением тракта или "соединения", такого как коммутируемый по меткам тракт (LSP) при многопротокольной коммутации с использованием меток (MPLS), по которому транзакция пакетов может быть маршрутизирована в сети. Механизмы, используемые для достижения этих норм качества услуги (QoS), включают в себя методы маршрутизации вызовов и соединений и методы выделения ресурсов для поддержки качества услуги, такие как выделение диапазона передачи, приоритетная маршрутизация, приоритетное обслуживание очереди и восстановление транспортировки. Областью применения данного приложения являются надежность таких трактов LSP, выраженная в форме приоритета, и потребность в точном определении уровней приоритетов для сигнализации по качеству услуги (QoS).

Приоритеты трафика играют важную роль в предоставлении клиентам сетей связи приемлемой надежности/доступности услуги. Например, экстренная связь требует наивысшего доступного приоритета управления допуском в условиях природных катастроф или нападения террористов. В современных коммутируемым телефонных сетях общего пользования (PSTN) этот уровень приоритета является единственным в своем роде. Требуемая надежность/доступность может быть запрошена как уровень приоритета для отдельной сетевой функции, которая, в свою очередь, определяет установление тракта LSP. Двумя сетевыми функциями для рассмотрения приоритетов в развивающихся сетях с коммутацией пакетов являются:

- Управление допуском для соединения: правила управления допуском отдают предпочтение потокам трафика, которые рассматриваются поставщиком услуг как более критические (например, экстренная связь) в условиях перегрузки. Приоритет для управления допуском – это способ отдать предпочтение при допуске трактам LSP с более высоким приоритетом по сравнению с трактами LSP с более низким приоритетом.
- Восстановление: восстановление в данной Рекомендации определяется в широком смысле как смягчающая последствия реакция сети в условиях отказа. Возможными методами для восстановления после отказа являются автоматическая защитная коммутация для защиты линий/трактов и методы восстановления совместно используемых узлов сети ячеистой структуры. Для критических потоков трафика услуги может запрашиваться восстановление с более высоким приоритетом. Такой поток трафика может быть затем маршрутизирован по тракту LSP, который имеет "помеченный" соответствующим образом уровень приоритета восстановления.

Установление приоритетов трафика должно позволить обеспечить максимальную гибкость для реализации с точки зрения поставщиков услуг. Уровни приоритетов должны отвечать следующим требованиям:

- Общее число классов приоритетов должно быть небольшим, чтобы обеспечивать расширяемость.
- Для простоты разбиение любого класса приоритетов следует исключить.
- Уровни приоритетов носят относительный характер и не связаны с конкретными параметрами (например, с временем восстановления) и их значениями.
- Поставщикам услуг должно быть позволено выбирать число уровней приоритетов из доступного набора для предоставления своих услуг. Соответственно, они могут разрабатывать соглашения по уровню услуги (SLA) по обработке любого заданного класса приоритетов для своих клиентов, включая других поставщиков услуг (интерфейс сеть–сеть).

В отношении трафика клиентской услуги для управления допуском для соединения определены четыре уровня приоритетов:

- Критический: единственный в своем роде уровень приоритета, зарезервированный для трафика экстренной связи для всех поставщиков услуг, как национальных, так и международных.
- Высокий: примерами такой услуги могут служить другие услуги государственного управления, услуги для важнейших абонентов делового сектора, услуги для виртуальных частных сетей.
- Нормальный: примерами таких услуг служат услуги телефонной связи для абонентов квартирного сектора.
- Лучший из возможных: примерами служат услуги поставщиков услуг доступа к Интернет.

Для восстановления определяются три уровня приоритетов: высокий, нормальный и лучший из возможных. Примеры услуг, приведенные выше, подходят и в этом случае; экстренная связь будет требовать высокого приоритета.

Как упомянуто выше, поставщик услуг может предложить конкретную приоритетную услугу на основе имеющихся возможностей сети и потребностей клиента. Например, поставщик услуг может выбрать для предоставления услугу со всеми четырьмя приоритетами, определяемыми для управления допуском для соединения, но только с высоким или нормальным приоритетами восстановления. С другой стороны, поставщик услуг доступа к Интернет (ISP) может выбрать для предоставления только приоритеты критического или наилучшего из возможных уровней для управления допуском для соединения и наилучший из возможных приоритет восстановления.

Добавление I

Комплексный подход к качеству услуг (QoS) на основе независимого управления ресурсами

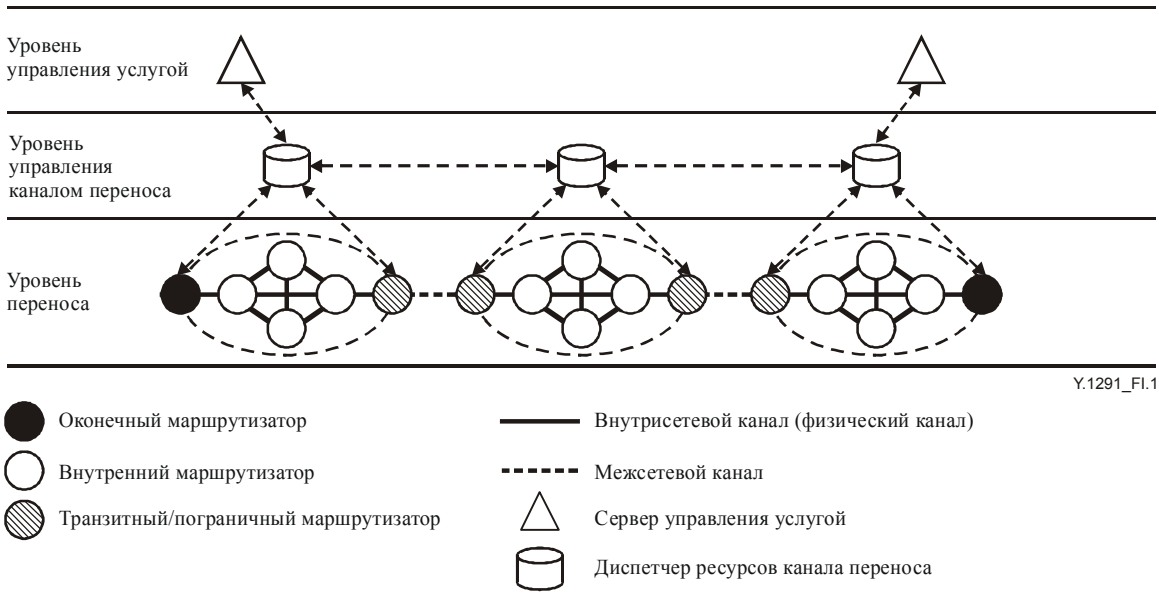


Рисунок I.1/Y.1291 – Комплексный подход к качеству услуг (QoS) на основе независимого управления ресурсами

На рисунке I.1 показан разработанный комплексный подход к качеству услуг (QoS) на основе независимого управления ресурсами для поддержки услуг при меняющихся требованиях к показателям качества для одной базовой сети с IP-протоколом и для гарантирования качества услуг (QoS) для ориентированных на соединение услуг и услуг в реальном масштабе времени (таких как IP-телефония). При данном подходе объединяются коммутация MPLS, технология DiffServ, расчет трафика и управление стратегией.

Услуги, требующие гарантии качества QoS, разбиты по категориям согласно общим типам услуг (например, передача речи) или согласно уровням анализа качества QoS (например, EF). В отношении управляемости и устойчивости сети опорная IP-сеть поставщика сетей разделяется на множество административных областей. Такое деление носит гибкий характер и может отличаться от деления на области маршрутизации. Например, административная область может быть настолько мала, что содержит только один оконечный маршрутизатор, или настолько большой, что содержит в себе всю сеть оператора.

Диспетчер ресурсов канала переноса (BRM) обладает функцией независимого управления ресурсами, с помощью которой осуществляется управление всеми ресурсами канала переноса в каждой административной области и которая может быть реализована в одном или в нескольких блоках. Диспетчер BRM регистрирует и сохраняет топологию сети и базу данных о ресурсах (NTRD). На основе топологии сети и базы данных о ресурсах диспетчер BRM производит выбор тракта внутри области распределения ресурсов, выделяет ресурс и осуществляет управление допуском для потока услуг. Диспетчеры BRM разных областей взаимодействуют через сигнализацию для управления ресурсами для потоков приложений, проходящих между областями. Кроме того, диспетчер BRM также может выполнять функции, подобные управлению стратегией, управлению соглашениями SLA, измерению трафика тракта LSP и взаимодействию с серверами по аутентификации, проверке прав доступа и учету (AAA).

Множество серверов управления услугами (SCS) "отвечает" за управление различными запросами услуг (например, за сигнализацию для вызова по передаче речи), за идентификацию исходящего и входящего пункта для каждого запроса услуги, за преобразование номера (имени) в IP-адрес и последующую передачу запросов ресурсов к диспетчеру BRM исходящей области. Для услуг с требованиями по качеству QoS, но без серверов управления услугами, подобно услугам при двухточечной передаче, хост-узлы могут инициировать запрос услуги для качества QoS через потоки RSVP или другие протоколы сигнализации для качества QoS. Протокол RSVP здесь предназначен только для хост-узлов, чтобы запрашивать гарантии QoS, и для маршрутизаторов, не требующих

поддержки протокола RSVP для резервирования ресурсов по каждому потоку. Оборудование, установленное для обработки запросов по обеспечению качества QoS, посылаемых хост-узлами, может рассматриваться как отдельный вид сервера SCS.

Диспетчер BRM принимает от сервера SCS в его административной области или от другого диспетчера BRM запросы ресурсов. Он их обрабатывает и затем посылает ответы к серверу SCS. В то же время, если запрос ресурсов для потока услуги принят, то диспетчер BRM сообщает входящим оконечным маршрутизаторам данные идентификации потока, тракта и атрибуты QoS. Входящий оконечный маршрутизатор идентифицирует, классифицирует, маркирует, отслеживает, формирует и инкапсулирует пакеты потока вместе с информацией о качестве QoS, заданной диспетчером BRM.

Для потоков услуг, проходящих через сети нескольких провайдеров, как правило, существуют шлюзы приложений и пограничные маршрутизаторы между сетями разных провайдеров, которые связаны между собой фиксированными ресурсами каналов и определенными межсетевыми соглашениями SLA. Разные провайдеры сетей могут использовать в своих сетях различные механизмы обеспечения качества QoS. В этом случае диспетчеры BRM только управляют ресурсами внутрисетевых каналов, тогда как шлюзы приложений и пограничные маршрутизаторы управляют ресурсами межсетевых каналов с помощью определенных соглашений SLA, а шлюз приложения или пограничный маршрутизатор действует как входящий или исходящий оконечный маршрутизатор.

При таком подходе соответствующие конструктивные блоки включают в себя почти все блоки, показанные на рисунке 1. Диспетчер BRM служит в качестве физически независимых плоскости управления и плоскости административного управления. Конструктивные блоки взаимодействуют, главным образом, через сигнализацию на уровне каждого потока и на основе управления ресурсами для каждой сети LBN. Это прозрачный интерфейс сигнализации между плоскостью управления и плоскостью данных.

I.1 Гибкость реализации для сетей с передачей пакетов и с поддержкой коммутации MPLS

В этом случае предполагается, что в базовых сетях с IP-протоколом поддерживается коммутация MPLS с использованием технологии DiffServ.

Технология трактов LSP с коммутацией MPLS используется для предварительной организации сети логических каналов переноса (LBN) для каждого класса услуг по базовой IP-сети вручную или автоматически с использованием оборудования TE с протоколом RSVP или через протокол LDP маршрутизатора CR. Что касается служебных потоков, принадлежащих некоторому классу услуг, то выбор тракта, распределение ресурсов, управление допуском и передача меток осуществляются в одной и той же сети LBN. Планирование топологии и резервирование диапазона передачи каждой сети LBN зависит от измерений трафика и прогнозирования данных, административной стратегии и соглашения SLA, которые могут быть установлены вручную или автоматически для защиты трактов LSP, изменений пропускной способности или оптимизации показателей качества сети в соответствии с ограничениями из расчета трафика.

В рамках остальных ресурсов базовых сетей с передачей пакетов трафик класса BE без требований к качеству QoS продолжает маршрутизироваться и пересылаться с помощью общепринятых методов маршрутизации по IP-протоколу и передачи с использованием технологии DiffServ или без нее.

Диспетчер BRM регистрирует и сохраняет топологию сети и базу данных для ресурсов (NTRD) отдельно для каждой сети LBN. На основе таких топологий и баз данных, а также стратегий, диспетчер BRM осуществляет выбор тракта внутри области, выделение ресурсов и управление допуском для потока услуги в рамках соответствующей ему сети LBN. Что касается остальных ресурсов базовых сетей с передачей пакетов, то диспетчер BRM мог бы также выполнять выделение ресурсов и управление допуском.

Информация тракта по качеству QoS для потока, определяемого диспетчером BRM, представляет собой многоуровневый стек меток, который представляет собой составной набор для тракта LSP. Оконечный маршрутизатор инкапсулирует пакеты вместе с этим стеком меток, который, в свою очередь, побуждает транзитные маршрутизаторы пересылать пакеты потока по определенному тракту в соответствии со стеком меток и заданным приоритетом.

I.2 Гибкость реализации для сетей с передачей пакетов без поддержки коммутации MPLS

В этом случае имеет место динамическое применение управления допуском и резервирования ресурсов при резервировании ресурсов от звена к звену, а для уровня канала переноса возможности коммутации MPLS не требуются. Маршрутизация и пересылка всего трафика находятся под управлением традиционных протоколов маршрутизации IP и технологии IP-Diffserv.

Диспетчер BRM устанавливается для непосредственного управления всеми ресурсами физического канала в каждой административной области. Диспетчер BRM запоминает и сохраняет топологию

сети и базу данных для ресурсов (NTRD). На основе информации, содержащейся в этой топологии и базе данных, диспетчер BRM обрабатывает информацию для поиска маршрута, резервирования ресурсов от звена к звену и управления допуском для каждого потока, требующего гарантии качества QoS. Если поток принят к обработке с высоким приоритетом, ему не будут мешать другие потоки трафика.

I.3 Гибкость реализации для распределенного управления ресурсами

В этом случае сети LBN являются виртуальными каналами (называемыми конвейерами QoS) между парами "входящий оконечный маршрутизатор – исходящий оконечный маршрутизатор" в области сети. Для переноса агрегированных потоков конкретной услуги или класса качества QoS устанавливается конвейер QoS.

Если функция диспетчера BRM реализована в оконечных маршрутизаторах (ER), то управление ресурсами для каждого потока распределено по окончаниям канала переноса. Функция управления ресурсами (RCF) маршрутизатора ER обслуживает таблицу состояний ресурсов соответствующих конвейеров QoS и соответственным образом управляет допуском и выделяет ресурсы. Она также обрабатывает сигнализацию QoS.

Конвейеры QoS устанавливаются вручную или автоматически на средний или долгий срок, что может быть реализовано системой управления сетью.

Добавление II

Схема повышения приоритета

Схема повышения приоритета (PPS) – это новая схема для управления трафиком, находящаяся еще на экспериментальном уровне. Вкратце, в схеме PPS используется некоторый вид управления допуском для получения сквозного качества QoS в сети с передачей пакетов. Основными приложениями для такой схемы являются интерактивные мультимедийные услуги, такие как передача речи по IP-протоколу, видеоразговоры и видеоконференцсвязь. В частности, эта схема основана на сквозных измерениях сетевых ресурсов оконечными системами. До установления сеанса или даже во время сеанса исходящая оконечная система определяет, измеряет или опробует доступность сетевых ресурсов путем посылки пакетов с приоритетом, на один уровень ниже приоритета нормальных пакетов. Результатом является модификация значения пункта кодирования для DiffServ (DSCP) в последующих IP-пакетах: приоритет возрастает или повышается, чтобы "твердо" установить сеанс, понижается, чтобы ресурсы остались у существующих сеансов связи, или, в противном случае, корректируется так, чтобы число пакетов не превышало доступную пропускную способность. Только предполагается, что сеть, то есть выходные каналы маршрутизаторов или коммутаторов L2, будет поддерживать управление приоритетами для каждого класса, сопровождающее архитектуру DiffServ. Если все оконечные системы будут следовать такому режиму функционирования, то сквозное качество QoS будет достигаться без обслуживания состояний ресурсов для каждого потока в узлах сети.

БИБЛИОГРАФИЯ

[IETF RFC 1633] BRADEN (R.), *et al*.: Integrated Services in the Internet Architecture: an Overview, June 1994.

[IETF RFC 2205] BRADEN (R.), *et al*.: Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification, September 1997.

[IETF RFC 2309] BRADEN (R.), *et al*.: Recommendations on Queue Management and Congestion Avoidance in the Internet, April 1998.

[IETF RFC 2386] CRAWLEY (E.), *et al*.: A Framework for QoS-based Routing in the Internet, August 1998.

[IETF RFC 2474] NICHOLS (K.), *et al*.: Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, December 1998.

[IETF RFC 2748] DURHAM (D.), *et al*.: The COPS (Common Open Policy Service) Protocol, January 2000.

[IETF RFC 2753] YAVATKAR (R.), *et al*.: A Framework for Policy-based Admission Control, January 2000.

[IETF RFC 2990] HUSTON (G.): Next Steps for the IP QoS Architecture, November 2000.

[IETF RFC 2996] BERNET (Y.): Format of the RSVP DCLASS Object, November 2000.

[IETF RFC 2998] BERNET (Y.), *et al*.: A Framework for Integrated Services Operation over Diffserv Networks, November 2000.

[IETF RFC 3031] ROSEN (E.), *et al*.: Multiprotocol Label Switching Architecture, January 2001.

[IETF RFC 3032] ROSEN (E.), *et al*.: MPLS Label Stack Encoding, January 2001.

[IETF RFC 3198] WESTERINEN (A.), *et al*.: Terminology for Policy-Based Management, November 2001.

[IETF RFC 3209] AWDUCHE (D.), *et al*.: RSVP-TE: Extensions to RSVP for LSP Tunnels, December 2001.

[IETF RFC 3261] ROSENBERG (J.), *et al*.: SIP: Session Initiation Protocol, June 2002.

[IETF RFC 3270] LE FAUCHEUR (F.), *et al*.: Multi-Protocol Label Switching (MPLS) Support of Differentiated Services, May 2002.

[IETF RFC 3272] AWDUCHE (D.): Overview and Principles of Internet Traffic Engineering, May 2002.

[Jacobson, 1988] JACOBSON (V.): Congestion Avoidance and Control*, Proceedings of ACM SIGCOMM'88*, pp. 314-329, August 1988.

[Lin *et al*., 1997] LIN (D.), MORRIS (R.): Dynamics of Random Early Detection*, Proceedings of ACM SIGCOMM'97*, pp. 127-138, September 1997.

[Chen] CHEN (Shigang), NAHRSTEDT (Klara): An Overview of Quality-of-Service Routing for the Next Generation High-Speed Networks: Problems and Solutions*, IEEE Network, Special Issue on Transmission and Distribution of Digital Video*, Vol. 12, No. 6, pp. 64-79, November/December 1998.

[Apostolopoulos] APOSTOLOPOULOS (D.), *et al*.: Intra domain QoS Routing in IP Networks: A Feasibility and Cost Benefit Analysis, *IEEE Network*, Vol. 13, No. 5, pp. 42, September/October 1999.

[Floyd] FLOYD (S.), JACOBSON (V.): Random Early Detection Gateways for Congestion Avoidance, *IEEE/ACM Transactions on Networking*, Vol. 1, No. 4, pp. 397-413, August 1993.

[Nagle] NAGLE (J.): On Packet Switches with Infinite Storage. *IEEE Trans. on communications*, Vol. COM-35, pp. 435-438. April 1987.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия B	Средства выражения: определения, символы, классификация
Серия C	Общая статистика электросвязи
Серия D	Общие принципы тарификации
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	TMN и техническое обслуживание сетей: международные системы передачи, телефонные, телеграфные, факсимильные и арендованные каналы
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	Сети передачи данных и взаимосвязь открытых систем
Серия Y	**Глобальная информационная инфраструктура, аспекты межсетевого протокола (IP) и сети последующих поколений**
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2005 г.