

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

У.3042

(04/2013)

СЕРИЯ У: ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ
ИНФРАСТРУКТУРА, АСПЕКТЫ МЕЖСЕТЕВОГО
ПРОТОКОЛА, СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ,
ИНТЕРНЕТ ВЕЩЕЙ И "УМНЫЕ" ГОРОДА

Будущие сети

**"Умные" повсеместно распространенные
сети – Функции "умного" управления
трафиком и ресурсами**

Рекомендация МСЭ-Т У.3042

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ Y

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА, АСПЕКТЫ МЕЖСЕТЕВОГО ПРОТОКОЛА, СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ, ИНТЕРНЕТ ВЕЩЕЙ И "УМНЫЕ" ГОРОДА

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА	
Общие сведения	Y.100–Y.199
Услуги, 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 ПРОТОКОЛА ИНТЕРНЕТ	
Общие сведения	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
Ведение расчетов	Y.1800–Y.1899
IPTV по СПП	Y.1900–Y.1999
СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ	
Структура и функциональные модели архитектуры	Y.2000–Y.2099
Качество обслуживания и рабочие характеристики	Y.2100–Y.2199
Аспекты обслуживания: возможности обслуживания и архитектура обслуживания	Y.2200–Y.2249
Аспекты обслуживания: функциональная совместимость услуг и сетей в СПП	Y.2250–Y.2299
Совершенствование СПП	Y.2300–Y.2399
Управление сетью	Y.2400–Y.2499
Архитектура и протоколы сетевого управления	Y.2500–Y.2599
Пакетные сети	Y.2600–Y.2699
Безопасность	Y.2700–Y.2799
Обобщенная мобильность	Y.2800–Y.2899
Открытая среда операторского класса	Y.2900–Y.2999
БУДУЩИЕ СЕТИ	Y.3000–Y.3499
ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ	Y.3500–Y.3999

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

Рекомендация МСЭ-Т Y.3042

"Умные" повсеместно распространенные сети – Функции "умного" управления трафиком и ресурсами

Резюме

В Рекомендации МСЭ-Т Y.3042 определены функции "умного" управления трафиком и ресурсами для сетей SUN. Описана мотивация и определены требования высокого уровня и функциональная архитектура для обеспечения соответствующих возможностей сети. В настоящей Рекомендации также описаны механизмы с учетом аспектов интеллектуальности и повсеместной распространенности сетей.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия
1.0	МСЭ-Т Y.3042	13.04.2013 год	13-я

Ключевые слова

"Умное" управление ресурсами, "умный" контроль трафика, "умные" повсеместно распространенные сети, SUN.

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 в целях стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются 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 осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" (shall) или некоторые другие обязывающие выражения, такие как "обязан" (must), а также их отрицательные формы. Использование этих слов не предполагает, что соблюдение положений данной Рекомендации является обязательным для какой-либо из сторон.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещения об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу <http://www.itu.int/ITU-T/ipr/>.

ITU 2019

Все права сохранены. Ни одна из частей данной публикации не может быть воспроизведена с помощью каких бы то ни было средств без предварительного письменного разрешения МСЭ.

Содержание

	Стр.
1 Сфера применения.....	1
2 Справочные документы	1
3 Определения.....	2
3.1 Термины, определенные в других документах	2
3.2 Термины, определенные в настоящей Рекомендации	2
4 Сокращения и акронимы.....	3
5 Условные обозначения.....	4
6 Введение	4
6.1 Мотивация.....	4
6.2	5
7 Многоуровневая классификация трафика.....	6
7.1 Многоуровневые показатели пропускной способности	6
7.2 Многоуровневая классификация по срокам предоставления услуг.....	7
7.3 Многоуровневые классы трафика.....	8
8 Требования	9
8.1 Требования более высокого уровня.....	9
8.2 Функциональные требования	10
9 Архитектура	11
9.1 Архитектура высокого уровня	11
9.2 Функциональная архитектура	11
9.3 Эталонные точки	14
10 Механизмы "умного" контроля трафика и управления ресурсами	17
10.1 Механизм на основе предельного объема передаваемых данных.....	17
10.2 Механизм для интенсивного трафика услуг	18
10.3 Механизм для интенсивного трафика сигнализации.....	19
10.4 Механизм для интенсивного пользовательского трафика	20
10.5 Механизм для трафика, содержащего всплески.....	21
10.6 Механизм для завышенного объема трафика.....	22
10.7 Механизм для трафика в час наибольшей нагрузки	24
10.8 Механизм на основе списков (пользователей).....	26
11 Аспекты безопасности	27
Дополнение I Взрывной рост объема данных и снижение качества обслуживания	28
I.1 Взрывной рост объема данных, вызванный небольшим числом пользователей в фиксированных и подвижных сетях	28
I.2 Снижение качества обслуживания для основного круга пользователей, вызванное небольшим числом активных пользователей	29

	Стр.
I.3 Необходимость "умного" управления сетью для обеспечения качества обслуживания обычных пользователей	29
Дополнение II. Примеры контекстной информации для STCRMF	31

"Умные" повсеместно распространенные сети – Функции "умного" управления трафиком и ресурсами

1 Сфера применения

В настоящей Рекомендации определены функции "умного" управления трафиком и ресурсами, обеспечивающие добросовестное использование сетевых ресурсов при помощи возможностей информирования о контексте в "умных" повсеместно распространенных сетях (SUN). В настоящей Рекомендации рассматриваются следующие вопросы:

- мотивы и цели "умного" контроля трафика и управления ресурсами;
- требования к "умному" контролю трафика и управлению ресурсами для сетей SUN;
- архитектура высокого уровня и функциональная архитектура;
- механизмы контроля.

ПРИМЕЧАНИЕ 1. – Использование информации о контексте не является обязательным, а подробное описание механизма по реализации возможностей информирования о контексте выходит за рамки сферы применения настоящей Рекомендации.

ПРИМЕЧАНИЕ 2. – Регуляторные аспекты контроля (например, наименьший уровень [depth] сигнала передаваемого IP-пакета, допустимый для контроля) не входят в сферу применения настоящей Рекомендации.

ПРИМЕЧАНИЕ 3. – В настоящей Рекомендации под трафиком понимается трафик пользователей или поставщиков услуг, а под ресурсами понимается состояние эксплуатационной готовности сетевых элементов (например, загрузка центрального процессора (ЦП), использование интерфейса и т. д.).

ПРИМЕЧАНИЕ 4. – Контроль трафика производится на уровне приложений и на сетевом уровне. Примерами контроля на уровне приложений являются регулирование видеотрафика, перекодировка видео и/или адаптивное потоковое вещание по HTTP (HAS).

2 Справочные документы

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 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 E.600] Recommendation ITU-T E.600 (1993), *Terms and definitions of traffic engineering.*
- [ITU-T Q.9] Recommendation ITU-T Q.9 (1988), *Vocabulary of switching and signalling terms.*
- [ITU-T Y.1541] Recommendation ITU-T Y.1541 (2011), *Network performance objectives for IP-based services.*
- [ITU-T Y.2701] Рекомендация МСЭ-Т Y.2701 (2007 год), *Требования к безопасности для сетей последующих поколений версии 1.*
- [ITU-T Y.3041] Рекомендация МСЭ-Т Y.3041 (2013 год), *"Умные" повсеместно распространенные сети – Обзор.*

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах.

3.1.1 "умные" повсеместно распространенные сети (smart ubiquitous networks (SUN)) [ITU-T Y.3041]: Сети пакетной передачи на основе IP, которые могут обеспечивать транспортирование и доставку широкого спектра существующих и появляющихся услуг для пользователей и вещей. Услуги, предоставляемые сетью SUN, могут охватывать такие аспекты, как контроль, обработка и хранение данных.

ПРИМЕЧАНИЕ 1. – Сеть является "умной" в том смысле, что она располагает надлежащей информацией, осведомлена о контексте, является адаптивной, автономной и программируемой, а также может предоставлять услуги эффективным и безопасным способом.

ПРИМЕЧАНИЕ 2. – Сеть является повсеместно распространенной в том смысле, что она предоставляет доступ в любое время в любом месте, при помощи различных технологий и устройств доступа, в том числе оконечных пользовательских устройств и интерфейсов "человек–машина".

3.1.2 контекст (context) [ITU-T Y.3041]: Информация, которая может использоваться для определения характеристик среды пользователя.

3.1.3 час наибольшей нагрузки (busy hour) [ITU-T E.600]: Непрерывный одночасовой период, целиком входящий в соответствующий временной интервал, с максимальным трафиком или количеством попыток вызова.

3.1.4 управление потоком трафика сигнализации (signalling traffic flow control) [ITU-T Q.9]: Действия и процедуры, предназначенные для ограничения трафика сигнализации в источнике в том случае, когда сеть сигнализации не способна передавать весь трафик сигнализации, предлагаемый пользовательскими подсистемами из-за сбоев сети или перегрузки.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяются следующие термины.

3.2.1 предельный объем трафика данных (data cap): Верхний предел общего объема трафика, допускаемый соглашением об уровне обслуживания (SLA), заключенным между источником трафика (например, поставщиком интернет-услуг (ISP)) и получателем (например, пользователем).

3.2.2 добросовестное использование (fair usage): Равное обращение к одной и той же услуге(ам), включая приложение (приложения), различными пользователями (например, конечными пользователями, приложениями) в рамках одного и того же соглашения об уровне обслуживания.

3.2.3 интенсивный трафик услуг (heavy service traffic): Уровень трафика, измеряемый как объем определенных услуг, который перегружает сетевые ресурсы на интерфейсе исходящих/входящих соединений с поставщиками услуг. Этот уровень влияет на трафик других услуг на одном и том же сетевом ресурсе (например, снижает качество обслуживания).

3.2.4 интенсивный трафик сигнализации (heavy signalling traffic): Уровень трафика, измеряемый как объем и частота, который запускает управление потоком трафика сигнализации [ITU-T Q.9] (например, интенсивный уровень трафика, вызванный сообщениями, подтверждающими активность (keep-alive)).

3.2.5 интенсивный пользовательский трафик (heavy user traffic): Уровень, измеряемый как объем трафика, инициированного конечным пользователем, который перегружает сетевые ресурсы на интерфейсе исходящих/входящих соединений с конечным пользователем. Этот уровень влияет на качество трафика других пользователей.

3.2.6 трафик, содержащий всплески (surge traffic): Уровень трафика, измеряемый как совокупный объем, инициированный несколькими пользователями, который перегружает сетевые ресурсы в случае особых событий, таких как резкое ухудшение погоды, отдельные

спортивные или музыкальные мероприятия, привлекающие большое число пользователей, и т. д.

3.2.7 монопольное использование (monopolization): Состояние перегрузки сетевых ресурсов, вызванное интенсивным трафиком услуг или пользователей. Такой режим влияет на качество трафика других услуг или пользователей.

3.2.8 завышенный трафик (over-sized traffic): Трафик, уровень которого превышает объем, рекомендованный для той или иной услуги. Рекомендованный объем трафика для такой услуги определяется соглашением об уровне обслуживания между источником и получателем трафика. Завышенный трафик является частным случаем интенсивного трафика услуг.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

3DTV	3 Dimensional TV	Трехмерное телевидение
CP	Contents Provider	Поставщик контента
DSCP	Differentiated Services Code Point	Точка кода дифференцированных услуг
HDTV	High Definition TV	Телевидение высокой четкости (ТВЧ)
IoT	Internet of Things	Интернет вещей
IPTV	Internet Protocol TV	Телевидение по протоколу Интернет (IP)
ISP	Internet Service Provider	Поставщик интернет-услуг
OTT	Over the Top	Технология ОТТ
PDL	Progressive Down Load	Прогрессивная загрузка
POP	Point of Presence	Точка входа в сеть
QCI	QoS Class Identifier	Идентификатор класса QoS
QoE	Quality of Experience	Оценка пользователем качества услуг
QoS	Quality of Service	Качество обслуживания
RA-FE	Resource Analysis Functional Entity	Функциональный объект анализа ресурсов
RMAF	Resource Monitoring and Analysis Function	Функция мониторинга и анализа ресурсов
RM-FE	Resource Monitoring Functional Entity	Функциональный объект мониторинга ресурсов
SCD-FE	Smart Correlation and Decision Functional Entity	Функциональный объект "умной" корреляции и принятия решений
SLA	Service Level Agreement	Соглашение об уровне обслуживания
SRC-FE	Smart Resource Control Functional Entity	Функциональный объект "умного" управления ресурсами
STC-FE	Smart Traffic Control Functional Entity	Функциональный объект "умного" контроля трафика
STCRM F	Smart Traffic Control and Resource Management Functions	Функции "умного" контроля трафика и управления ресурсами

STRCF	Smart Traffic and Resource Control Function	Функция "умного" контроля трафика и ресурсов
SUN	Smart Ubiquitous Network	"Умные" повсеместно распространенные сети
TA-FE	Traffic Analysis Functional Entity	Функциональный объект анализа трафика
TMAF	Traffic Monitoring and Analysis Function	Функциональный объект мониторинга и анализа трафика
TM-FE	Traffic Monitoring Functional Entity	Функциональный объект мониторинга трафика
TRAF	Traffic Control and Analysis Function	Функция контроля и анализа трафика
TRCMF	Traffic Resource Control and Management Function	Функция контроля трафика и управления ресурсами
VNO	Virtual Network Operator	Оператор виртуальной сети

5 Условные обозначения

В настоящей Рекомендации:

ключевые слова "требуется, чтобы" означают требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии настоящей Рекомендации;

ключевое слово "запрещается" означает требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии настоящей Рекомендации;

ключевые слова "рекомендуется, чтобы" означают требование, которое рекомендуется, но не является абсолютно необходимым. Таким образом для заявления о соответствии настоящей Рекомендации это требование не является обязательным;

слова "не рекомендуется, чтобы" означают требование действия, выполнение которого не рекомендуется, но не является прямо запрещенным. Таким образом даже при наличии данного требования может быть сделано заявление о соответствии настоящей Рекомендации;

ключевые слова "может факультативно" означают необязательное требование, которое допустимо, но не имеет рекомендательного значения. Данный термин не подразумевает, что вариант реализации поставщика должен обеспечивать выполнение этой функции и функция может быть активирована по желанию оператора сети/поставщика услуг дополнительно. Это означает лишь, что поставщик может факультативно предоставить эту функцию и по-прежнему заявлять о соответствии настоящей Рекомендации.

6 Введение

6.1 Мотивация

Разработка разнообразных "умных" устройств (таких как смартфоны, планшеты, устройства интернета вещей и т. д.) в пользовательской среде IP-сетей, а также появление новых услуг, таких как "умное" телевидение, трехмерное телевидение и сетевые игры, стали причиной роста трафика услуг. Эти "умные" устройства требуют, чтобы сети выделяли большой объем ресурсов для поддержки запрашиваемой пропускной способности и различных служебных

функций, в том числе в режиме реального времени, вне режима реального времени и в режиме промежуточного накопления.

Появление этих устройств – одна из причин взрывного роста объема данных. Кроме того, небольшое число пользователей и поставщиков услуг, генерирующих интенсивный трафик, могут монопольно использовать большую часть ресурсов сети. Подобного рода монополизация должна контролироваться для обеспечения добросовестного потребления ресурсов пользователями. Это монопольное использование ведет к снижению качества обслуживания и, кроме того, препятствует дальнейшему развитию "умных" устройств и сопутствующих услуг (см. Дополнение I). Таким образом, для обеспечения добросовестного использования конечных сетевых ресурсов необходимо определить более продуктивные способы.

В среде подвижной связи разработка "умных" пользовательских устройств позволила использовать различные широкополосные мультимедийные услуги, которые до сих пор предоставлялись по сетям фиксированной связи. Такого рода изменения в мобильных услугах вызывают перегрузку сети, что может привести к ограничению ресурсов доступа для новых пользователей. В этой среде сервисный трафик, создаваемый поставщиками услуг, транспортируется по фиксированным сетям и доставляется на устройства конечных пользователей по подвижным сетям доступа. Возможности мобильного доступа относительно ограничены по сравнению с возможностями фиксированного доступа. Таким образом следует отметить, что для добросовестного использования необходимо управлять входящим трафиком из среды фиксированных сетей в среду мобильного доступа.

6.2 Задачи

Для более эффективной работы сетей и служб необходимо понимание взаимосвязи различных факторов, в частности пропускной способностью, времени ожидания и сложности операций. На рисунке 6-1 показаны три различные области работы сетей на основе взаимосвязи этих факторов. Эти области обладают следующими характеристиками.

Область 1: Ситуация недоиспользования ресурсов – ситуация, в которой сетевые ресурсы используются недостаточно, а обеспечение качества обслуживания и управление сетью не представляют сложности. Однако сетевому оператору для экономичного использования сетевых ресурсов требуется большее число пользователей и трафик с потреблением высокой пропускной способности.

Область 2: Ситуация оптимального использования ресурсов – ситуация, в которой поддерживается оптимальный баланс между интенсивным использованием сетевых ресурсов, требованиями к качеству обслуживания и низкой сложностью управления сетью. Следует отметить, что эта ситуация является рекомендуемой для оптимального управления сетью.

Область 3: Ситуация повышенного использования ресурсов – ситуация, в которой обеспечивается высокая загрузка сетевых ресурсов, требования к качеству обслуживания могут не удовлетворяться, а сложность управления сетью высока. Многие пользователи в этой области могут испытывать трудности при подключении к сетям и/или использовании услуг. В частности, эта ситуация ухудшается в среде подвижных сетей. Для повышения эффективности доставки услуг и использования сетевых ресурсов рекомендуется внедрять систему контроля трафика и управления ресурсами.

Целью настоящей Рекомендации является предоставление функции контроля трафика и управления ресурсами для решения вопросов по области 3 в соответствии с потребностями области 2. Потребности области 1 связаны с экономической моделью и не входят в сферу применения настоящей Рекомендации.

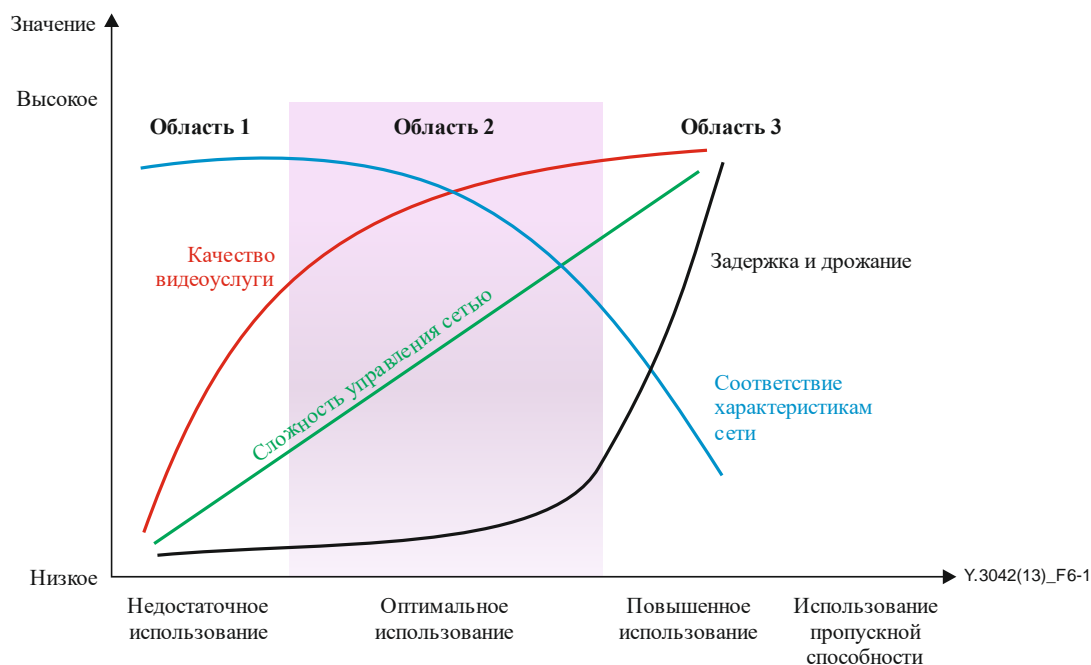


Рисунок 6.1 – Три различных области работы сети

7 Многоуровневая классификация трафика

Для определения характеристик трафика используется множество параметров, таких как пропускная способность, дрожание, задержка, неравномерность трафика и т. д. Эти параметры, определяемые в [ITU-T Y.1541], используются функциями "умного" контроля трафика и управления ресурсами в сетях SUN (STCRMF). Кроме того, в [ITU-T Y.1541] определяются новые параметры трафика и классификация вновь появляющихся типов трафика с высокой интенсивностью потока и долгосрочными характеристиками, генерируемых "умными" устройствами и поставщиками услуг.

7.1 Многоуровневые показатели пропускной способности

В средах традиционных сетей электросвязи трафик делится только на две категории на основе пропускной способности – широкополосная и узкополосная. Широкополосная связь относится к трафику с пропускной способностью не ниже 2 Мбит/с, а узкополосная – к пропускной способности ниже 2 Мбит/с. Эта классификация широко распространена в среде традиционных сетей электросвязи. Однако в сетях SUN критерии классификации усложнены вследствие факторов, описываемых в разделе 6.1.

Для решения указанных проблем применяется многоуровневая классификация по пропускной способности. В рамках этой классификации в качестве типов пропускной способности определяются три типа пропускной способности в узкополосной связи и два типа в широкополосной связи.

- Тип 0 (до 1 кбит/с). Этот тип используется при передаче небольших объемов данных со скоростью в несколько сотен битов в секунду. К этому типу может принадлежать трафик, генерируемый датчиками, или трафик сигнализации, например периодические сигналы от маяков.
- Тип 1 (от 1 до 128 кбит/с). Этот тип используется для традиционных услуг электросвязи, передающих голосовые сообщения и изображения низкого качества со скоростью менее 128 кбит/с. К этому типу могут принадлежать некоторые виды трафика сигнализации.
- Тип 2 (от 128 кбит/с до 2 Мбит/с). Этот тип используется для типичных мультимедийных услуг, передающих видеосигналы, а также аудио/голосовые сигналы и изображения высокого качества.

- Тип 3 (от 2 до 20 Мбит/с). Этот тип используется для усовершенствованных мультимедийных услуг, передающих видеосигналы с разрешением HD и full HD и т. д.
- Тип 4 (свыше 20 Мбит/с). Этот тип используется для новых появляющихся услуг, таких как услуги 3D-видео и современные конвергентные услуги, например моделирование работы сердца и дистанционные медицинские услуги в области хирургии.

7.2 Многоуровневая классификация по срокам предоставления услуг

Помимо объема трафика, его неравномерности (например, краткосрочный или постоянный трафик) и зависимости от фактора времени (например, в режиме реального времени или вне режима реального времени), еще одним важным фактором, который следует учитывать в сетях SUN, являются сроки предоставления услуг. С момента внедрения возможностей предоставления определенных услуг на постоянной основе и с фиксированной скоростью передачи (например, IP-телевидение, дистанционная хирургия, видеоконференции и сетевые игры) подключение пользователей длится намного дольше обычного независимо от фактического пользования услугой. Кроме того, специальные приложения, например одноранговые сети и приложения для онлайн-загрузки, позволяют пользователям подключаться без привязки к пропускной способности. Многие из вышеупомянутых услуг и приложений имеют продолжительность предоставления услуг свыше одного часа при пропускной способности типа 3 и/или 4. Таким образом сроки предоставления услуг следует рассматривать как один из важных факторов для осуществления контроля трафика и управления ресурсами.

Для решения этих вопросов применяется многоуровневая классификация по срокам предоставления услуг. Определяются следующие пять типов продолжительности предоставления услуг в диапазоне от очень короткого срока (например, менее 1 секунды) до очень длительного периода (например, более 1 часа).

- Тип 0 (менее 1 секунды). Этот тип используется для мгновенной передачи данных (например, автоматическая передача генерируемых сигналов датчика). Как правило, этот тип трафика влияет на работу сетей только в случае перегрузок, вызванных внезапным скачком объема данных (например, из-за стихийного бедствия).
- Тип 1 (от 1 секунды до менее чем 10 минут). Этот тип используется для традиционных услуг электросвязи, таких как голосовая телефония, факсимильная связь и передача сообщений. В большинстве из них используются двунаправленные симметричные услуги связи. В данный тип включены также однонаправленные услуги связи, такие как обмен сообщениями и музыкальные сервисы.
- Тип 2 (от 10 до менее чем 30 минут). Этот тип, как правило, используется для веб-услуг, но включает также голосовую и видеотелефонию.
- Тип 3 (от 30 минут до менее чем 1 часа). Этот тип используется главным образом для услуг передачи потокового видео (контентом являются обычные ТВ-программы длительностью менее 1 часа). Включены также услуги аудио- и видеоконференций.
- Тип 4 (свыше 1 часа). Этот тип используется главным образом для услуг передачи потокового видео (контентом являются HD и/или 3D-фильмы длительностью свыше одного часа). Этот тип включает также новые появляющиеся виды услуг, такие как дистанционная хирургия и т. д.

7.3 Многоуровневые классы трафика

В разделах 7.1 и 7.2 указано, что услуги могут сопоставляться по таким признакам, как пропускная способность и сроки предоставления услуг. Многоуровневые классы трафика показаны в таблице 7-1. Существует четыре класса трафика – от класса 0 до класса 3. Подробная информация приведена ниже. Если говорить более конкретно, классы 0, 2 и 3 являются приоритетными для целей контроля трафика и управления ресурсами, поскольку они оказывают существенное влияние на характеристики сети.

В таблице 7-1 определяются следующие многоуровневые классы трафика.

- Класс 0: Для этого класса характерны типы пропускной способности 0 и 1 и тип 0 сроков предоставления услуг. Например, часть трафика этого класса может представлять собой данные, полученные от датчиков системы электронного здравоохранения или систем обнаружения стихийных бедствий.
- Класс 1: Для этого класса характерна конкатенация пропускной способности типов от 0 до 4 и сроков предоставления услуг типа 1, пропускной способности типов 1 и 2 и сроков предоставления услуг типа 2, а также пропускной способности типа 1 и сроков предоставления услуг типов 3 и 4. К этому классу трафика принадлежит большинство услуг общего пользования, таких как голосовая телефонная связь.
- Класс 2: Для этого класса характерна конкатенация пропускной способности типов 3 и 4 и сроков предоставления услуг типа 2, а также пропускной способности типов от 2 до 4 и сроков предоставления услуг типов 3 и 4, исключая класс 3. К этому классу трафика принадлежат многие из новых услуг с расширенными возможностями мультимедийной передачи.
- Класс 3: Для этого класса характерна пропускная способность типа 4 и сроки предоставления услуг типа 4. К этому классу принадлежат услуги с высоким потреблением пропускной способности, такие как трехмерная дистанционная хирургия.

Таблица 7-1 – Многоуровневые классы трафика

		Сроки оказания услуги				
		Тип 0 (менее 1 секунды)	Тип 1 (от 1 секунды до менее чем 10 минут)	Тип 2 (от 10 до менее чем 30 минут)	Тип 3 (от 30 минут до менее чем 1 часа)	Тип 4 (свыше 1 часа)
Пропускная способность	Тип 0 (до 1 кбит/с)	Простые данные датчика	Данные датчика	NYI	NYI	NYI
	Тип 1 (1–128 кбит/с)	Усложненные текстовые данные датчика (SMS)	MMS Голосовая телефония/ сообщения	Голосовая телефония	Голосовая телефония Голосовая конференц-связь	Голосовая конференц-связь
	Тип 2 (от 128 кбит/с до 2 Мбит/с)	NYI	Передача видео- сообщений и клипов низкого качества, Музыка высокого качества	Видеотелефония/ конференц-связь низкого качества Передача файлов среднего размера	Одноранговая загрузка Интернет-TV Интернет-вещание	Одноранговая загрузка TV и вещание через интернет Теле- и видеонаблю- дение
	Тип 3 (2–20 Мбит/с)	NYI	Передача видео- сообщений и клипов в HD	Видеотелефония и конференц-связь в HD, передача больших файлов	IP TV (пьесы) Одноранговая загрузка Сетевые игры Видеоконференции Прилож. эл. здраво- охранения	IP TV (фильм) Одноранговая загрузка Сетевые игры Видеоконференции Прилож. эл. здраво- охранения
	Тип 4 (свыше 20 Мбит/с)	NYI	Обмен видео- сообщениями в 3D	Веб-контент на основе 3D	3D TV 3D-телеприсутствие Прилож. по ядерным исследованиям	Прилож. эл. здраво- охранения Прилож. по ядерным исследованиям

NYI – не определено

Y.3042(13)_F7-1



Некоторые виды трафика, принадлежащие к классу 0, требуют обработки с наиболее высоким приоритетом, а поддержка трафика класса 1 важна при предоставлении услуг общего пользования. Трафик класса 2 влияет на системы электросвязи, в том числе коммерческие (новые модели, например, технология OTT), на функционирование соответствующих ресурсов и управление ими. Трафик класса 3 оказывает серьезное влияние на операторов сетей электросвязи и поставщиков интернет-услуг (ISP). Ожидается, что наилучшим решением по поддержке на данном этапе будет использование арендованной связи.

8 Требования

8.1 Требования более высокого уровня

К функции STCRMF в сетях SUN применяются следующие требования более высокого уровня по контролю трафика и управлению ресурсами:

- требуется осуществлять мониторинг сквозных IP-пакетов на сетевых элементах при передаче по фиксированным/подвижным сетям;
- требуется осуществлять мониторинг использования ресурсов сетевых элементов;
- требуется предоставлять механизмы для контроля трафика и управления ресурсами, обеспечивающие добросовестное использование сетевых ресурсов;
- рекомендуется обеспечивать сбор контекстной информации для детализированного контроля трафика и управления ресурсами.

8.2 Функциональные требования

Функциональные требования для функции STCRMF в сетях SUN делятся на шесть областей: мониторинг трафика, анализ трафика, мониторинг ресурсов, анализ ресурсов, "умный" контроль трафика и обеспечение ресурсами. Для каждой области определены следующие подробные функциональные требования.

- Требования, связанные с мониторингом трафика:
 - требуется собирать информацию о потоках (например, 5-элементные кортежи; SrcIP, DestIP, протокол, SrcPort и DestPort);
 - требуется собирать данные об общем объеме трафика потоков;
 - рекомендуется собирать контекст трафика (см. Дополнение II).
- Требования, связанные с анализом трафика:
 - требуется классифицировать трафик следующим образом: поток в расчете на пользователя/пользовательское устройство, объем в расчете на поток, объем в расчете на пользователя/пользовательское устройство и объем в расчете на поставщика услуг;
 - требуется определять пользователей/пользовательские устройства, которые генерируют многопоточный трафик;
 - требуется определять класс собранного объема трафика;
 - рекомендуется генерировать статистику трафика по времени (например, режим реального времени, час, день, неделя, месяц);
 - рекомендуется генерировать статистику трафика по расположению (например, последняя миля, сеть доступа, POP, базовая сеть).
- Требования, связанные с мониторингом ресурсов:
 - требуется собирать информацию об использовании пропускной способности (например, используемая и доступная пропускная способность) в расчете на сетевой элемент;
 - требуется собирать информацию об использовании пропускной способности в расчете на один поток в сетевом элементе;
 - рекомендуется собирать прочую информацию по ресурсам (например, использование процессора, использование интерфейса, использование памяти, использование хранилища и т. д.).
- Требования, связанные с анализом ресурсов:
 - требуется классифицировать информацию об использовании ресурсов на пользователя/пользовательское устройство или поставщика услуг;
 - требуется определять состояние перегрузки сети, вызванное интенсивным пользовательским трафиком;
 - требуется определять состояние перегрузки сети, вызванное интенсивным трафиком услуг;
 - требуется определять состояние перегрузки сети, вызванное интенсивным трафиком сигнализации;
 - требуется определять состояние перегрузки сети, вызванное трафиком, который содержит всплески.
- Требования, связанные с "умным" контролем трафика:
 - требуется частично или полностью контролировать потоки пользовательского трафика, вызывающие перегрузку сети;

- может дополнительно поддерживаться регулирование видеотрафика (преобразование), перекодировка видео и/или HAS, что позволяет избежать перегрузки сети.
- Требования, связанные с управлением ресурсами:
 - требуется поддержка управления на основе приоритетов (например, метки DSCP или распределение каналов QCI);
 - требуется поддержка формирования ресурсов, постановки в очередь, определения общих концепций, управления буфером и допуском.

9 Архитектура

9.1 Архитектура высокого уровня

В [ITU-T Y.3041] описываются шесть наборов функциональных возможностей для реализации сетей SUN, а именно: функциональные возможности информирования о контексте, функциональные возможности информирования о контенте, программируемые функциональные возможности, функциональные возможности "умного" управления ресурсами, функциональные возможности автономного управления сетями и функциональные возможности для повсеместно распространенных сетей. Из указанных возможностей в настоящей Рекомендации определяются функциональные возможности "умного" управления ресурсами, реализуемые при помощи функции "умного" контроля трафика и управления ресурсами.

На рисунке 9-1 показана архитектура высокого уровня для целей "умного" контроля трафика и управления ресурсами. Мониторинг и анализ трафика выполняются на интерфейсах поставщиков услуг (например, CP, VNO, Portal и т. д.) и пользователей подвижных или фиксированных сетей доступа. Кроме того, по всем сетям также проводится мониторинг и анализ ресурсов. Состояние перегрузки может контролироваться при помощи контроля трафика и управления ресурсами, а также функциональных возможностей информирования о контексте. Функции и функциональные объекты "умного" контроля трафика и управления ресурсами описываются в разделе 9.2.

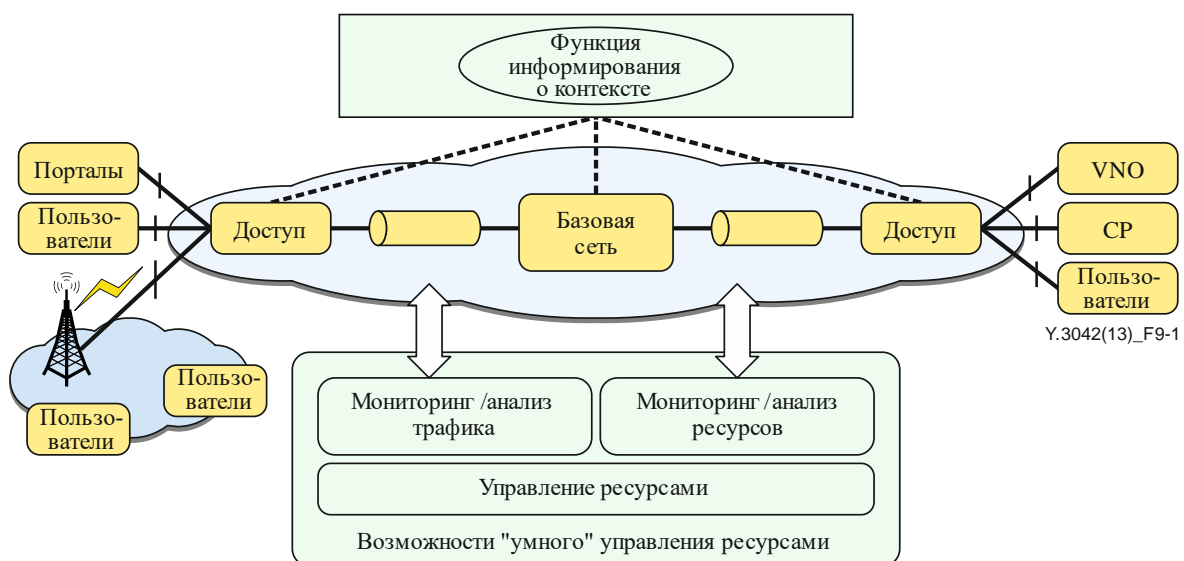
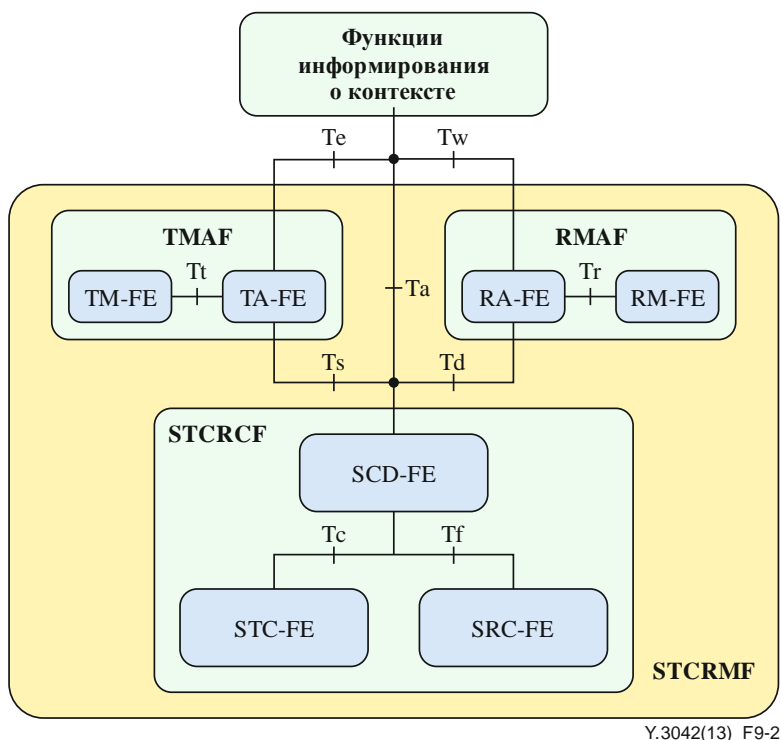


Рисунок 9-1 – Архитектура высокого уровня для STCRMF

9.2 Функциональная архитектура

В данном разделе определена функциональная архитектура, а также описаны функции и функциональные объекты. Функция STCRMF включает в себя функцию мониторинга и

анализа трафика (TMAF), функцию мониторинга и анализа ресурсов (RMAF), а также функцию "умного" управления трафиком и ресурсами (STRCF), как показано на рисунке 9-2. Функция STCRMF обеспечивает эталонные точки взаимодействия с функциями информирования о контексте для получения контекстной информации.



Y.3042(13)_F9-2

Рисунок 9-2 – Функциональная архитектура STCRMF

9.2.1 Функция мониторинга и анализа трафика (TMAF)

Функция TMAF осуществляет мониторинг и анализирует трафик выгрузки/загрузки от поставщиков услуг и пользователей или в направлении к ним. Эта функция состоит из функционального объекта по мониторингу трафика (TM-FE) и функционального объекта по анализу трафика (TA-FE).

- Объект TM-FE осуществляет мониторинг трафика выгрузки и загрузки на интерфейсах поставщиков услуг и пользователей соответственно. Кроме того, он устанавливает связь с объектом TA-FE для проведения анализа трафика.
 - 1) Объект TM-FE осуществляет мониторинг объема трафика услуг в целях идентификации поставщика, генерирующего интенсивный трафик услуг.
 - 2) Данный объект осуществляет мониторинг объема трафика пользователей в целях идентификации интенсивного трафика пользователей.
 - 3) Этот объект осуществляет мониторинг объема трафика пользователей и услуг в целях идентификации интенсивного трафика сигнализации.
 - 4) Объект осуществляет мониторинг объема трафика пользователей и услуг в целях идентификации трафика, содержащего всплески.
 - 5) Результаты мониторинга трафика отправляются объекту TA-FE для анализа трафика.
- Объект TA-FE анализирует и классифицирует результаты мониторинга трафика. С этой целью он поддерживает связь с функциями информирования о контексте.

- 1) Данный объект классифицирует и анализирует результаты мониторинга трафика в расчете на одного пользователя и одного поставщика услуг в соответствии с заранее определенными установками (например, пороговым значением).
- 2) Этот объект может генерировать временную статистику классифицируемого трафика (например, режим реального времени, час, день, неделю и месяц).
- 3) Для более точного анализа этот объект может запрашивать контекстную информацию у функций информирования о контексте.
- 4) Данный объект отправляет результаты анализа объекту SCD-FE.

9.2.2 Функция мониторинга и анализа ресурсов (RMAF)

Функция RMAF выполняет мониторинг сетевых ресурсов (использование пропускной способности), а также анализирует каждый поток или пользователя. Функция RMAF включает в себя функциональный объект мониторинга ресурсов (RM-FE) и функциональный объект анализа ресурсов (RA-FE).

- Объект RM-FE осуществляет мониторинг использования пропускной способности для каждого пользователя или потока, а также поддерживает связь с объектом RA-FE.
 - 1) Объект RM-FE осуществляет мониторинг информации об использовании пропускной способности для каждого сетевого элемента.
 - 2) Данный объект осуществляет мониторинг информации об использовании пропускной способности для каждого потока в сетевом элементе.
 - 3) Этот объект осуществляет мониторинг прочей информации по ресурсам (например, использование процессора, использование памяти, использование хранилища, использование линии связи и т. д.).
 - 4) Данный объект информирует объект RA-FE о результатах анализа ресурсов.
- Объект RA-FE анализирует информацию об использовании контролируемых ресурсов и определяет состояние перегрузки сети. С этой целью он также поддерживает связь с функциями информирования о контексте.
 - 1) Данный объект классифицирует и анализирует информацию об использовании контролируемых ресурсов в целях идентификации интенсивного трафика услуг/пользователей/сигнализации, а также трафика, содержащего всплески, что вызывает перегрузку сети.
 - 2) Этот объект также определяет сбои в сети, информация о которых может помочь в анализе перегрузки сети.
 - 3) Для более точного анализа этот объект запрашивает контекстную информацию у функций информирования о контексте.
 - 4) Данный объект отправляет результаты анализа объекту SCD-FE.

9.2.3 Функции "умного" управления трафиком и ресурсами (STRCF)

Функция STRCF определяет оптимальный механизм для управления интенсивным трафиком и трафиком, содержащим всплески. Эта функция также управляет пользователями или потоками, монопольно использующими ресурсы. Функция STRCF включает в себя функциональный объект "умной" корреляции и принятия решений (SCD-FE), функциональный объект "умного" управления трафиком (STC-FE) и функциональный объект "умного" управления ресурсами (SRC-FE).

- Объект SCD-FE определяет оптимальный механизм управления путем анализа корреляции между статусом трафика, ресурсами и контекстной информацией. Он кроме того поддерживает связь с функциями информирования о контексте, а также с объектами TA-FE и RA-FE.
 - 1) Объект SCD-FE получает контекстную информацию (например, поведение пользователей, тип устройства, тип услуги, расположение, а также тип контента и время и т. д.) от функций информирования о контексте.

- 2) Данный объект выполняет корреляцию объема трафика, использования ресурсов и контекстной информации.
 - 3) Этот объект определяет, какие из поставщиков услуг или пользователей генерируют или принимают интенсивный трафик. Кроме того, он определяет, какой пользователь или поток монополично используют сетевой ресурс, а также на каких пользователей или на какие потоки это влияет.
 - 4) Данный объект определяет оптимальный механизм для "умного" управления трафиком и ресурсами.
- Объект STC-FE управляет трафиком выгрузки/загрузки от поставщиков услуг и пользователей (или в направлении к ним), которые генерируют интенсивный трафик. Он также поддерживает связь с объектом SCD-FE.
 - 1) Объект STC-FE осуществляет управление интенсивным трафиком на уровне приложений и сетей (например, фильтрацию пакетов, блокировку потока, регулирование и перекодирование видео).
 - 2) В качестве средства непрямого управления трафиком этот объект посылает обратный сигнал предупреждения поставщику услуг или пользователю.
 - Объект SRC-FE управляет использованием пропускной способности и ресурсами. Он также поддерживает связь с объектом SCD-FE.
 - 1) Данный объект выполняет перераспределение пропускной способности в целях обеспечения добросовестного использования соответствующих сетевых ресурсов для каждого пользователя.
 - 2) Этот объект поддерживает прежние механизмы управления ресурсами (например, метки, определение концепций, формирование ресурсов и управление по приоритетам) для осуществления управления ресурсами в случае монопольного использования пропускной способности сети.

9.3 Эталонные точки

9.3.1 Эталонная точка Та

Эталонная точка Та позволяет объекту SCD-FE получать от функций информирования о контексте контекстную информацию, необходимую для определения оптимального механизма управления. Кроме того, функция SCD-FE может предоставлять уведомление об обработке результатов управления.

Через эталонную точку Та происходит обмен следующими информационными потоками.

9.3.1.1 Запрос контекстной информации

Этот запрос отправляется объектом SCD-FE функциям информирования о контексте для запроса контекстной информации.

9.3.1.2 Ответ по контекстной информации

Этот ответ отправляется функциями информирования о контексте объекту SCD-FE для подтверждения запроса контекстной информации и содержит запрашиваемую контекстную информацию.

9.3.1.3 Уведомление о контексте

Информационный поток уведомления о контексте отправляется объектом SCD-FE функциям информирования о контексте для передачи информации о результатах обработки механизмом управления.

9.3.2 Эталонная точка Те

Эталонная точка Те позволяет объекту ТА-FE получать контекстную информацию по услуге, необходимую для анализа контролируемого трафика, от функций информирования о контексте. Через эталонную точку Те происходит обмен следующими информационными потоками.

9.3.2.1 Запрос контекста услуги

Этот запрос отправляется объектом TA-FE функциям информирования о контексте для запроса контекстной информации по услуге.

9.3.2.2 Ответ по контексту услуги

Этот ответ отправляется функциями информирования о контексте объекту TA-FE для подтверждения запроса на контекст услуги и содержит запрашиваемую контекстную информацию по услуге.

9.3.3 Эталонная точка Tw

Эталонная точка Tw позволяет объекту RA-FE получать от функций информирования о контексте контекстную информацию по пользователям, необходимую для мониторинга и анализа использования ресурсов. Подробная контекстная информация по пользователям приведена в Дополнении II.

Через эталонную точку Tw происходит обмен следующими информационными потоками.

9.3.3.1 Запрос контекста пользователя

Этот запрос отправляется объектом RA-FE функциям информирования о контексте для запроса контекстной информации по услуге.

9.3.3.2 Ответ по контексту пользователя

Этот ответ отправляется функциями информирования о контексте объекту RA-FE для подтверждения запроса на контекст услуги и содержит запрашиваемую контекстную информацию по услуге.

9.3.4 Эталонная точка Tt

Эталонная точка Tt позволяет объекту TA-FE получать от объекта TM-FE информацию по контролируемому трафику для анализа. Информация по контролируемому трафику содержит объем контролируемого трафика каждой услуги.

Через эталонную точку Tt происходит обмен следующими информационными потоками.

9.3.4.1 Запрос анализа трафика

Этот запрос отправляется объектом TM-FE объекту TA-FE для запроса анализа контролируемого трафика.

9.3.4.2 Ответ по анализу трафика

Этот ответ отправляется объектом TA-FE объекту TM-FE для подтверждения запроса на анализ трафика.

9.3.5 Эталонная точка Tr

Эталонная точка Tr позволяет объекту RA-FE получать от объекта RM-FE информацию по использованию контролируемых ресурсов, необходимую для анализа использования ресурсов. Информация по мониторингу использования ресурсов содержит данные об использовании пропускной способности для каждого пользователя (или потока).

Через эталонную точку Tr происходит обмен следующими информационными потоками.

9.3.5.1 Запрос анализа ресурсов

Этот запрос отправляется объектом RM-FE объекту RA-FE для запроса анализа контролируемого использования ресурсов.

9.3.5.2 Ответ по анализу ресурсов

Этот ответ отправляется объектом RA-FE объекту RM-FE для подтверждения запроса по анализу ресурсов.

9.3.6 Эталонная точка Ts

Эталонная точка Ts позволяет объекту SCD-FE получать от объекта TA-FE информацию о решениях по механизму контроля, необходимую для определения оптимального механизма контроля. Информация о решениях по механизму контроля содержит тип услуги и объем трафика в единицу времени для каждой услуги, а также прочую актуальную информацию.

Через эталонную точку Ts происходит обмен следующими информационными потоками.

9.3.6.1 Запрос решения по "умному" контролю

Этот запрос отправляется объектом TA-FE объекту SCD-FE для запроса решения по оптимальному механизму контроля.

9.3.6.2 Ответ по решению об "умном" контроле

Этот ответ отправляется объектом SCD-FE объекту TA-FE для подтверждения запроса по решению об "умном" контроле.

9.3.7 Эталонная точка Td

Эталонная точка Td позволяет объекту SCD-FE получать от объекта RA-FE информацию о решениях по механизму контроля, необходимую для определения оптимального механизма контроля. Информация о решениях по механизму контроля содержит тип пользователя и сведения об использовании пропускной способности в единицу времени для каждого пользователя, а также прочую актуальную информацию.

Через эталонную точку Td происходит обмен следующими информационными потоками.

9.3.7.1 Запрос решения по "умному" контролю

Этот запрос отправляется объектом RA-FE объекту SCD-FE для запроса решения по оптимальному механизму контроля.

9.3.7.2 Ответ по решению об "умном" контроле

Этот ответ отправляется объектом SCD-FE объекту RA-FE для подтверждения запроса по решению об "умном" контроле.

9.3.8 Эталонная точка Tc

Эталонная точка Tc позволяет объекту STC-FE получать от объекта SCD-FE информацию по запросу контроля трафика, необходимую для реализации контроля трафика. Информация по запросу контроля трафика содержит выбранный механизм и данные для контроля, а также другую актуальную информацию.

Через эталонную точку Tc происходит обмен следующими информационными потоками.

9.3.8.1 Запрос контроля трафика

Этот запрос отправляется объектом SCD-FE объекту STC-FE для запроса по реализации контроля трафика.

9.3.8.2 Ответ по контролю трафика

Этот ответ отправляется объектом STC-FE объекту SCD-FE для подтверждения запроса по реализации контроля трафика.

9.3.9 Эталонная точка Tf

Эталонная точка Tf позволяет объекту SRC-FE получать от объекта SCD-FE информацию по запросу насчет управления ресурсами, необходимую для реализации управления ресурсами. Информация по запросу насчет управления ресурсами содержит выбранный механизм и данные для управления, а также другую необходимую информацию.

Через эталонную точку Tf происходит обмен следующими информационными потоками.

9.3.9.1 Запрос по управлению ресурсами

Этот запрос отправляется объектом SCD-FE объекту SRC-FE для запроса по реализации управления ресурсами.

9.3.9.2 Ответ по управлению ресурсами

Этот ответ отправляется объектом SRC-FE объекту SCD-FE для подтверждения запроса по реализации управления ресурсами.

10 Механизмы "умного" контроля трафика и управления ресурсами

10.1 Механизм на основе предельного объема передаваемых данных

Ниже описываются процедуры контроля трафика и механизм управления ресурсами на основе предельного объема передаваемых данных.

- 1) Объект TM-FE осуществляет мониторинг общего объема трафика активных пользователей (см. Дополнение I).
- 2) Одновременно объект RM-FE осуществляет мониторинг использования пропускной способности и других ресурсов сетевых элементов, связанных с пользователями (или потоками) этих услуг.
- 3) Объект TA-FE анализирует и определяет общий уровень объема трафика в плане того, достигается ли предельное значение в рамках заранее определенных установок (например, 70%, 90% или 100% от предельного объема передаваемых данных). Затем результат анализа отправляется объекту SCD-FE. Для более точного анализа может дополнительно использоваться контекстная информация, полученная от функций информирования о контексте.
- 4) Объект RA-FE также анализирует информацию о контролируемых ресурсах. Этот объект определяет уровень использования сетевых ресурсов в плане того, ухудшается ли качество обслуживания других пользователей (или потоков). Для более точного анализа может дополнительно использоваться контекстная информация, полученная от функций информирования о контексте.
- 5) Объект SCD-FE получает результаты анализа от объектов TA-FE и RA-FE. Этот объект выполняет корреляцию объемов трафика и использования ресурсов, а также определяет механизм контроля трафика и управления ресурсами на основе предельного объема передаваемых данных. Для более точного анализа может дополнительно использоваться контекстная информация, полученная от функций информирования о контексте.
- 6) Объект SRC-FE обеспечивает выполнение решений в соответствии с заранее определенными установками следующим образом.
 - Если предельный объем передаваемых данных составляет 70%, необходимо уведомить пользователя и установить ограничение скорости для доступных ресурсов, равное 50%.
 - Если предельный объем передаваемых данных составляет 90%, необходимо уведомить пользователя и установить ограничение скорости для доступных ресурсов, равное 30%.
 - Если предельный объем передаваемых данных составляет 100%, необходимо уведомить пользователя и установить ограничение скорости для доступных ресурсов, равное 1% (минимум 1 Мбит/с).

На рисунке 10-1, ниже, показаны процедуры для этого механизма.

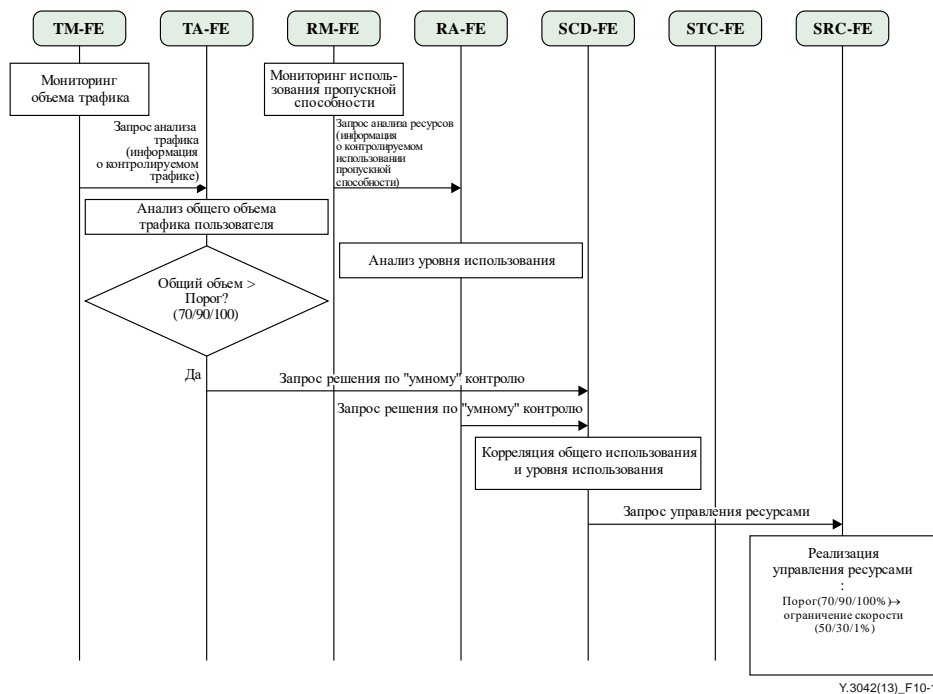


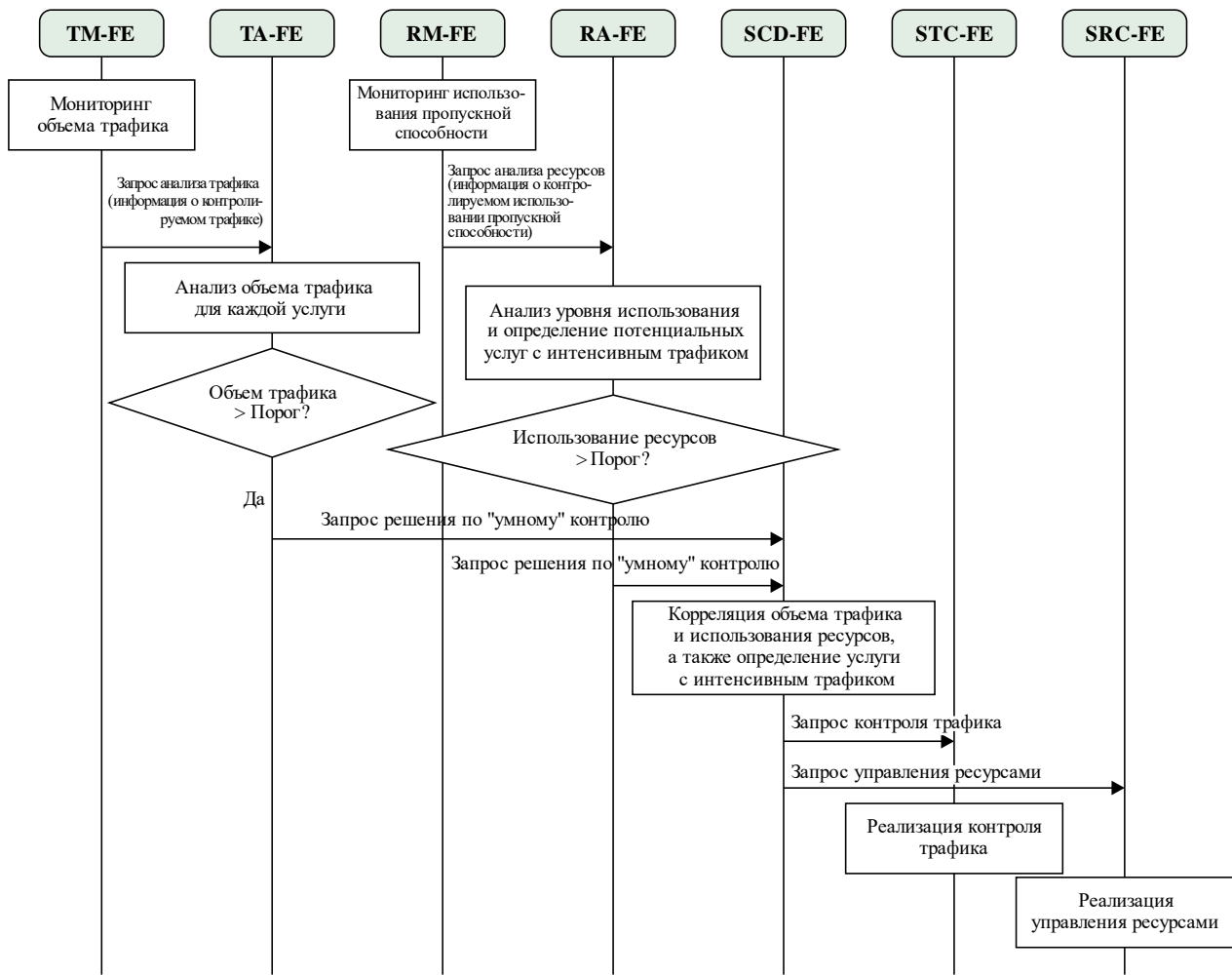
Рисунок 10-1 – Процедуры для механизма на основе предельного объема передаваемых данных

10.2 Механизм для интенсивного трафика услуг

Ниже описываются процедуры механизма по контролю трафика и управлению ресурсами для интенсивного трафика услуг.

- 1) Объект TM-FE осуществляет мониторинг объема трафика и отправляет объекту TA-FE запрос анализа трафика, содержащий информацию о контролируемом трафике.
- 2) Объект TA-FE анализирует объем трафика для каждой услуги.
- 3) Объект TA-FE проверяет, не превышает ли объем трафика за час пороговое значение. В случае превышения объект TA-FE отправляет объекту SCD-FE запрос решения об "умном" контроле.
- 4) Одновременно объект RM-FE осуществляет мониторинг использования пропускной способности сетевых ресурсов и отправляет объекту RA-FE запрос анализа ресурсов, содержащий информацию о контролируемом использовании ресурса.
- 5) Объект RA-FE анализирует уровень использования и определяет потенциальные услуги с интенсивным трафиком.
- 6) Объект RA-FE проверяет, не превышает ли использование ресурсов пороговое значение. В случае превышения объект RA-FE отправляет объекту SCD-FE запрос решения об "умном" контроле.
- 7) Затем объект SCD-FE сопоставляет объем трафика и использование ресурсов. Объект SCD-FE определяет услугу с интенсивным трафиком.
- 8) Объект SCD-FE отправляет объекту STC-FE запрос контроля трафика. Объект STC-FE выполняет функцию контроля трафика (например, отклонение потока (из нескольких потоков) и формирование потока).
- 9) Одновременно объект SCD-FE отправляет объекту SRC-FE запрос управления ресурсами. Объект SRC-FE выполняет функцию управления ресурсами (например, определение концепций, формирование ресурсов и контроль приоритетов).

На рисунке 10-2 показаны процедуры для этого механизма.



Y.3042(13)_F10-2

Рисунок 10-2 – Процедуры для механизма контроля интенсивного трафика услуг

10.3 Механизм для интенсивного трафика сигнализации

Ниже описываются процедуры контроля трафика и управления ресурсами для интенсивного трафика сигнализации.

- 1) Объект TM-FE измеряет пакеты сигнализации.
- 2) Объект TA-FE анализирует частоту сигнализации.
- 3) Если частота превышает пороговое значение, объект SCD-FE выполняет корреляцию объема контролируемого трафика и использования ресурсов. Этот объект принимает оптимальные решения по контролю трафика и управлению ресурсами применительно к интенсивному трафику сигнализации. Для более точного анализа может дополнительно использоваться контекстная информация, полученная от функций информирования о контексте.
- 4) Объект STC-FE уведомляет клиента и сервер о необходимости регулировки частоты сигнализации. Этот объект также управляет пакетами (например, блокировкой пакетов).

На рисунке 10-3, ниже, показаны процедуры для этого механизма.

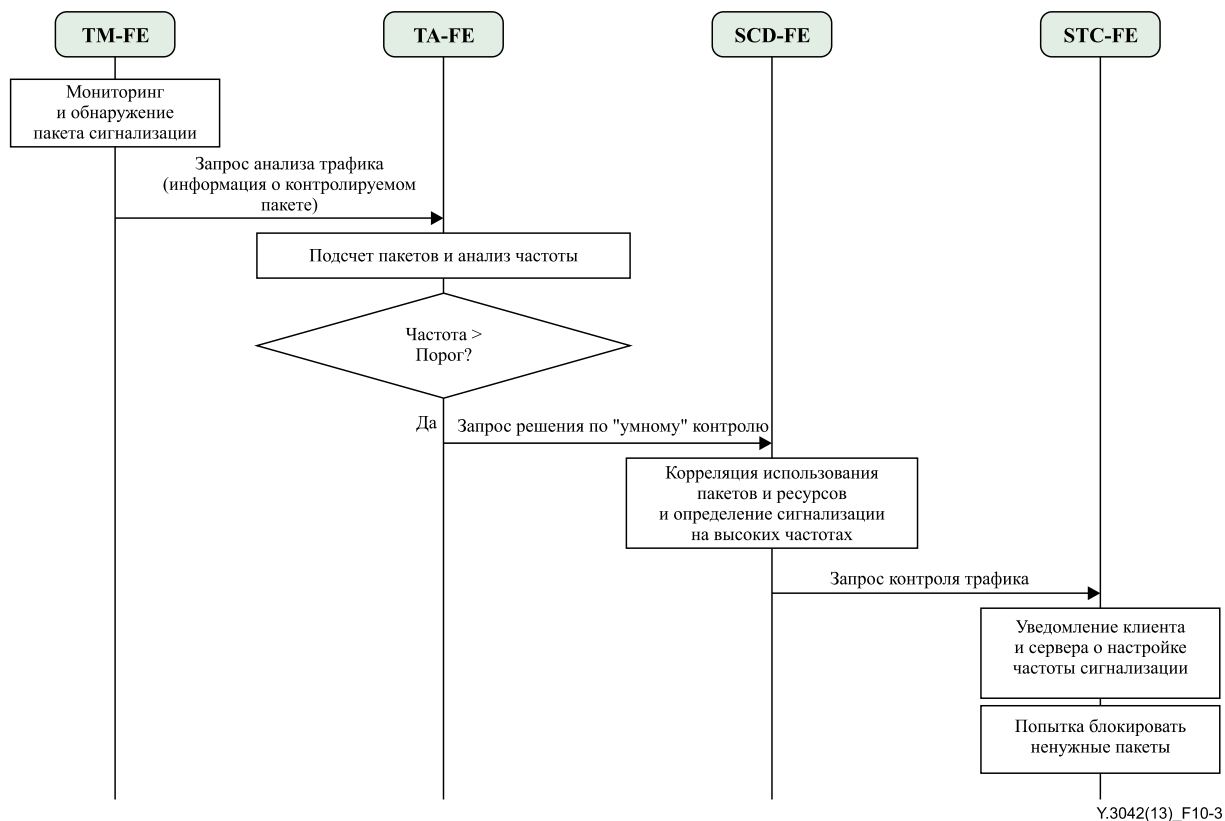


Рисунок 10-3 – Процедуры для интенсивного трафика сигнализации

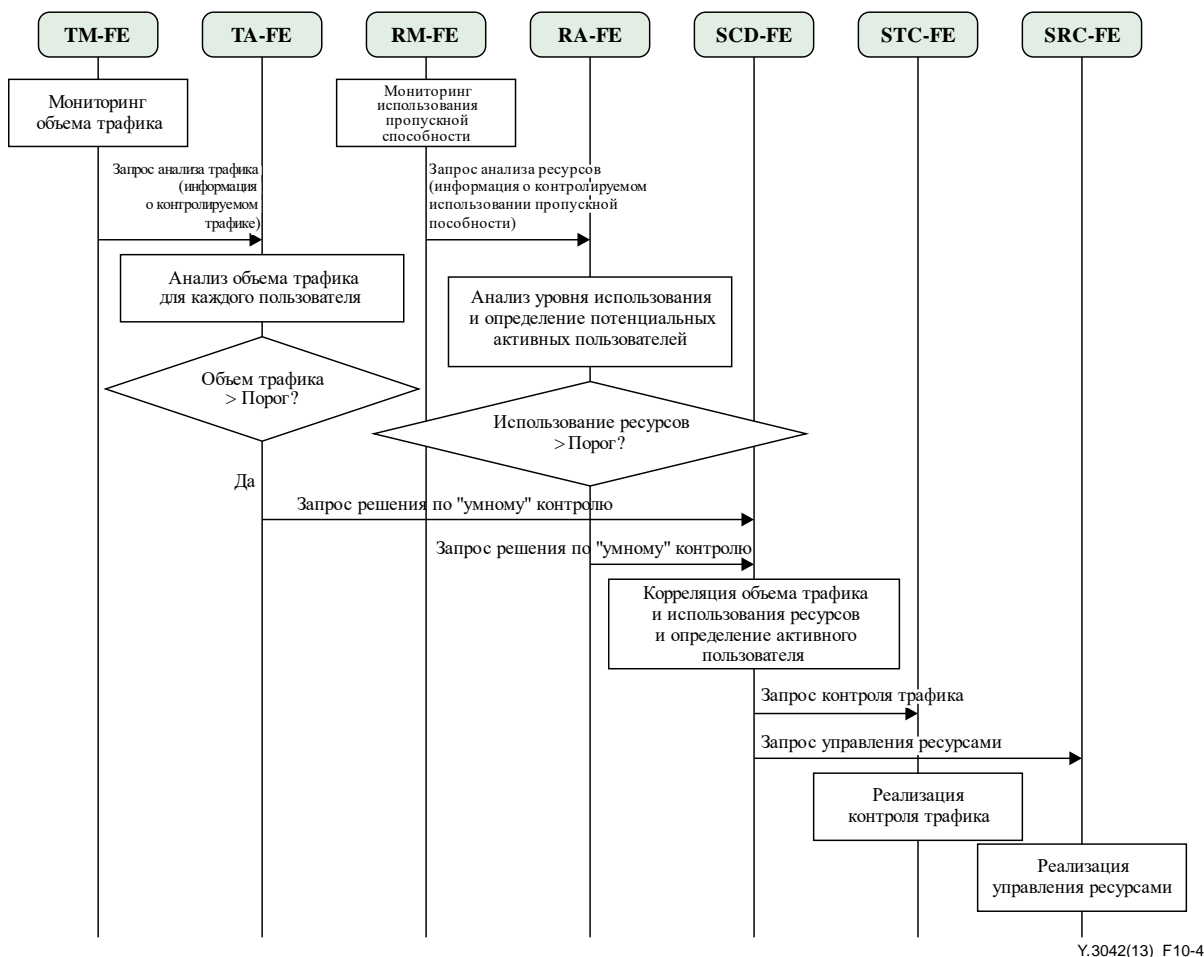
10.4 Механизм для интенсивного пользовательского трафика

Ниже описываются процедуры механизма контроля трафика и управления ресурсами для интенсивного пользовательского трафика.

- 1) Объект TM-FE осуществляет мониторинг объема трафика и отправляет объекту TA-FE запрос по анализу трафика, содержащий информацию о контролируемом трафике.
- 2) Объект TA-FE анализирует объем трафика для каждой услуги.
- 3) Объект TA-FE проверяет, не превышает ли объем трафика за час пороговое значение. В случае превышения объект TA-FE отправляет объекту SCD-FE запрос решения об "умном" контроле.
- 4) Одновременно объект RM-FE осуществляет мониторинг использования пропускной способности сетевых ресурсов и отправляет объекту RA-FE запрос анализа ресурсов, содержащий информацию об использовании контролируемого ресурса.
- 5) Объект RA-FE анализирует уровень использования и определяет потенциальных пользователей с интенсивным трафиком.
- 6) Объект RA-FE проверяет, не превышает ли использование ресурсов пороговое значение. В случае превышения объект RA-FE отправляет объекту SCD-FE запрос решения об "умном" управлении.
- 7) Затем объект SCD-FE выполняет корреляцию объема трафика и использования ресурсов и определяет пользователя с интенсивным трафиком.
- 8) Объект SCD-FE отправляет объекту STC-FE запрос контроля трафика. Объект STC-FE выполняет контроль трафика (например, отклонение потока (из нескольких потоков) и формирование потока).

- 9) Одновременно объект SCD-FE отправляет объекту SRC-FE запрос управления ресурсами. Объект SRC-FE выполняет функцию управления ресурсами (например, определение общей концепции, формирование ресурсов и контроль приоритетов).

На рисунке 10-4 показаны процедуры для этого механизма.



Y.3042(13)_F10-4

Рисунок 10-4 – Процедуры для механизма контроля интенсивного пользовательского трафика

10.5 Механизм для трафика, содержащего всплески

Ниже описываются процедуры механизма контроля трафика и управления ресурсами для трафика, содержащего всплески.

- 1) Объект TM-FE осуществляет мониторинг объема трафика и отправляет объекту TA-FE запросы по анализу трафика, содержащие информацию о контролируемом трафике.
- 2) Объект TA-FE анализирует характеристики услуги (то есть зависимость и независимость от времени) и объем трафика для каждой услуги.
- 3) Объект TA-FE проверяет, не превышает ли общий объем трафика за час пороговое значение. В случае превышения объект TA-FE отправляет объекту SCD-FE запрос о принятии решения об "умном" контроле.
- 4) Одновременно объект RM-FE осуществляет мониторинг использования пропускной способности сетевых ресурсов и отправляет объекту RA-FE запрос анализа ресурсов, относящийся к информации об использовании контролируемого ресурса.

- 5) Объект RA-FE анализирует характеристики услуги (то есть зависимость и независимость от времени) и уровень использования.
- 6) Объект RA-FE проверяет, не превышает ли общее использование ресурса пороговое значение. В случае превышения объект RA-FE отправляет объекту SCD-FE запрос решения об "умном" управлении.
- 7) Затем объект SCD-FE выполняет корреляцию характеристик услуги (то есть зависимость и независимость от времени), объема трафика и использования ресурсов. SCD-FE определяет методы контроля в соответствии с целями и задачами контроля.
- 8) Объект SCD-FE отправляет объекту STC-FE запрос контроля трафика. Объект STC-FE выполняет контроль трафика (например, отклонение потока (из нескольких потоков) и/или формирование потока).
- 9) Одновременно объект SCD-FE отправляет объекту SRC-FE запрос управления ресурсами. Объект SRC-FE осуществляет управление ресурсами (например, определение общей концепции, формирование ресурсов и контроль приоритетов).

На рисунке 10-5 показаны процедуры для этого механизма.

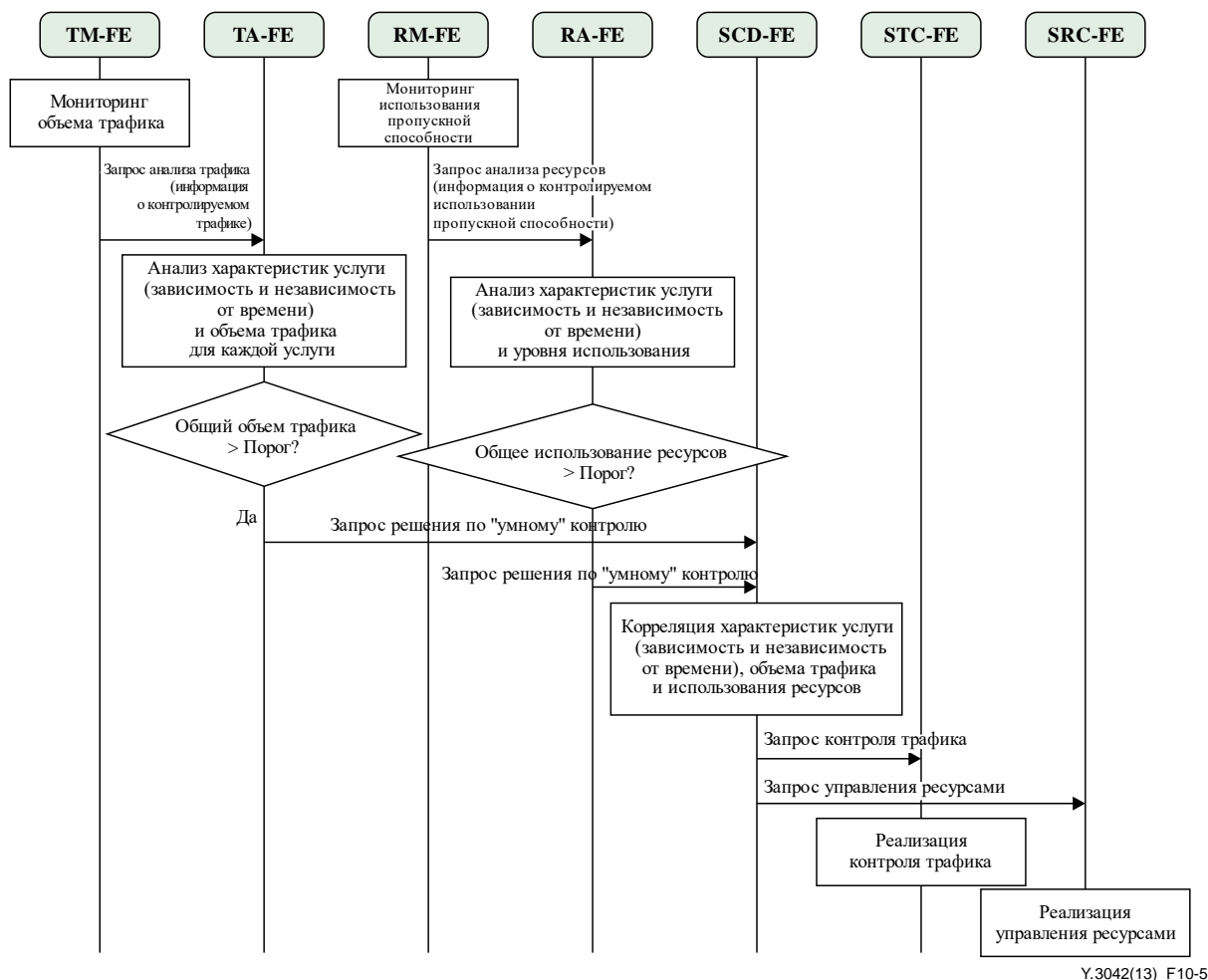


Рисунок 10-5 – Процедуры для механизма контроля трафика, содержащего всплески

10.6 Механизм для завышенного объема трафика

Ниже описываются процедуры контроля трафика и управления ресурсами для завышенного объема трафика.

- 1) Объект TM-FE осуществляет контроль услуг и объема их трафика.

- 2) Одновременно объект RM-FE осуществляет мониторинг использования пропускной способности других ресурсов сетевых элементов, связанных с пользователями (или потоками) этих услуг.
- 3) Объект TA-FE анализирует контролируемый трафик и классифицирует его в соответствии с заранее определенным объемом трафика, частотой использования и типом устройства. Для более точного анализа может дополнительно использоваться контекстная информация, полученная от функций информирования о контексте.
- 4) Объект RA-FE также анализирует контролируемый трафик. Этот объект определяет уровень использования сетевых ресурсов в плане того, снижается ли качество обслуживания других пользователей (или потоков). Для более точного анализа может дополнительно использоваться контекстная информация, полученная от функций информирования о контексте.
- 5) Объект SCD-FE получает результаты анализа от объектов TA-FE и RA-FE. Этот объект выполняет корреляцию объема трафика и использования ресурсов, а также принимает решения по оптимальному контролю трафика и управлению ресурсами в отношении трафика, содержащего всплески. Для более точного анализа может также использоваться контекстная информация, полученная от функций информирования о контексте.
- 6) Объект STC-FE обеспечивает выполнение принятого решения по контролю трафика, основываясь на заранее определенных общих концепциях или механизмах (например, пороговом значении, фильтрации пакетов или перекодировке).
- 7) Объект SRC-FE обеспечивает выполнение решений по пропускной способности и управлению ресурсами, основываясь на заранее определенных общих концепциях или механизмах (например, пороговом значении, общих концепциях, формировании ресурсов и контроле приоритетов).

На рисунке 10-6 ниже показаны процедуры для этого механизма.

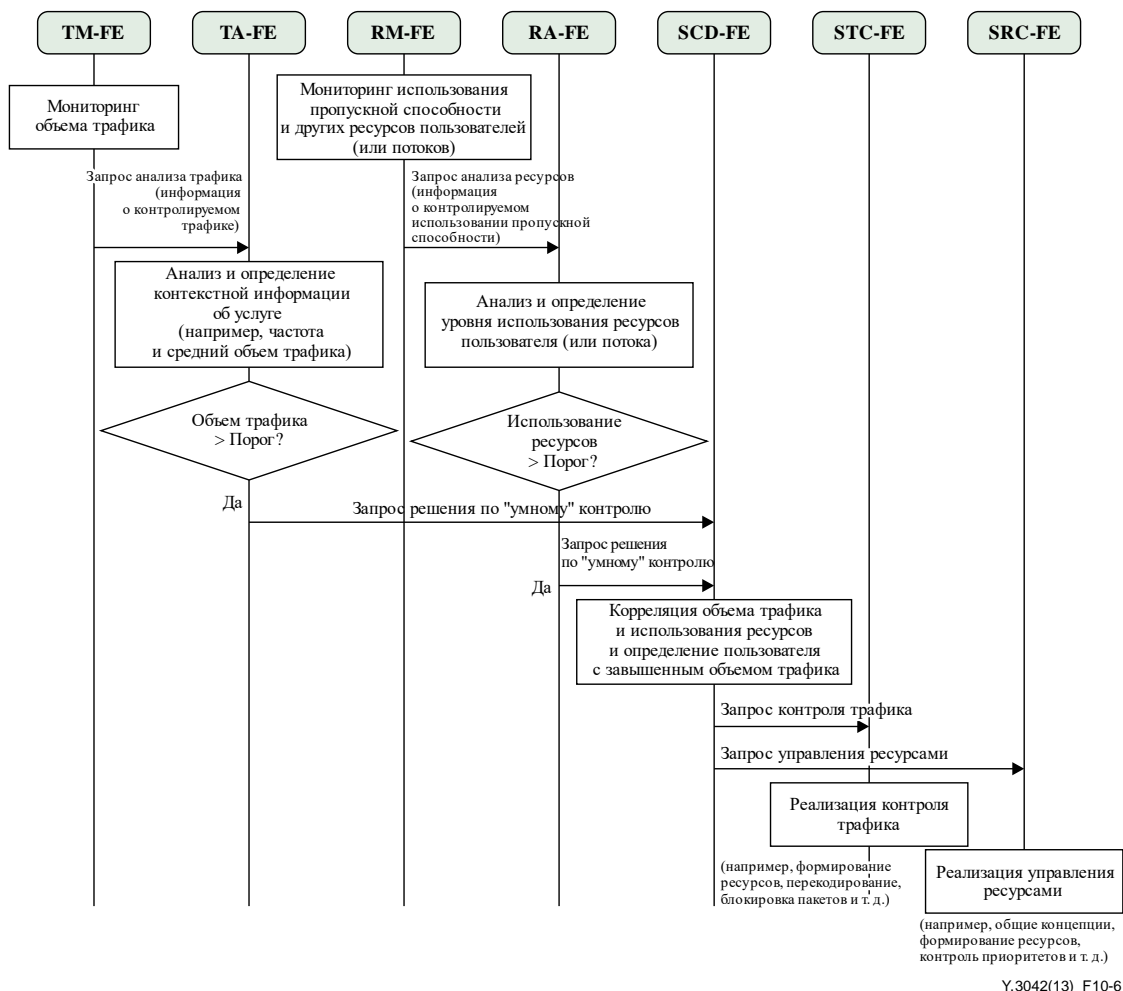


Рисунок 10-6 – Процедуры для завышенного объема трафика

10.7 Механизм для трафика в час наибольшей нагрузки

Общий объем трафика в IP-сети непрерывно изменяется во времени (время/день/неделя/месяц/год) [ITU-T E.600]. В частности, сеть может быть перегружена в течение определенного периода времени, когда одновременно подключается множество пользователей. Контроль трафика и управление ресурсами в такой период наибольшей нагрузки позволяют снизить перегрузку.

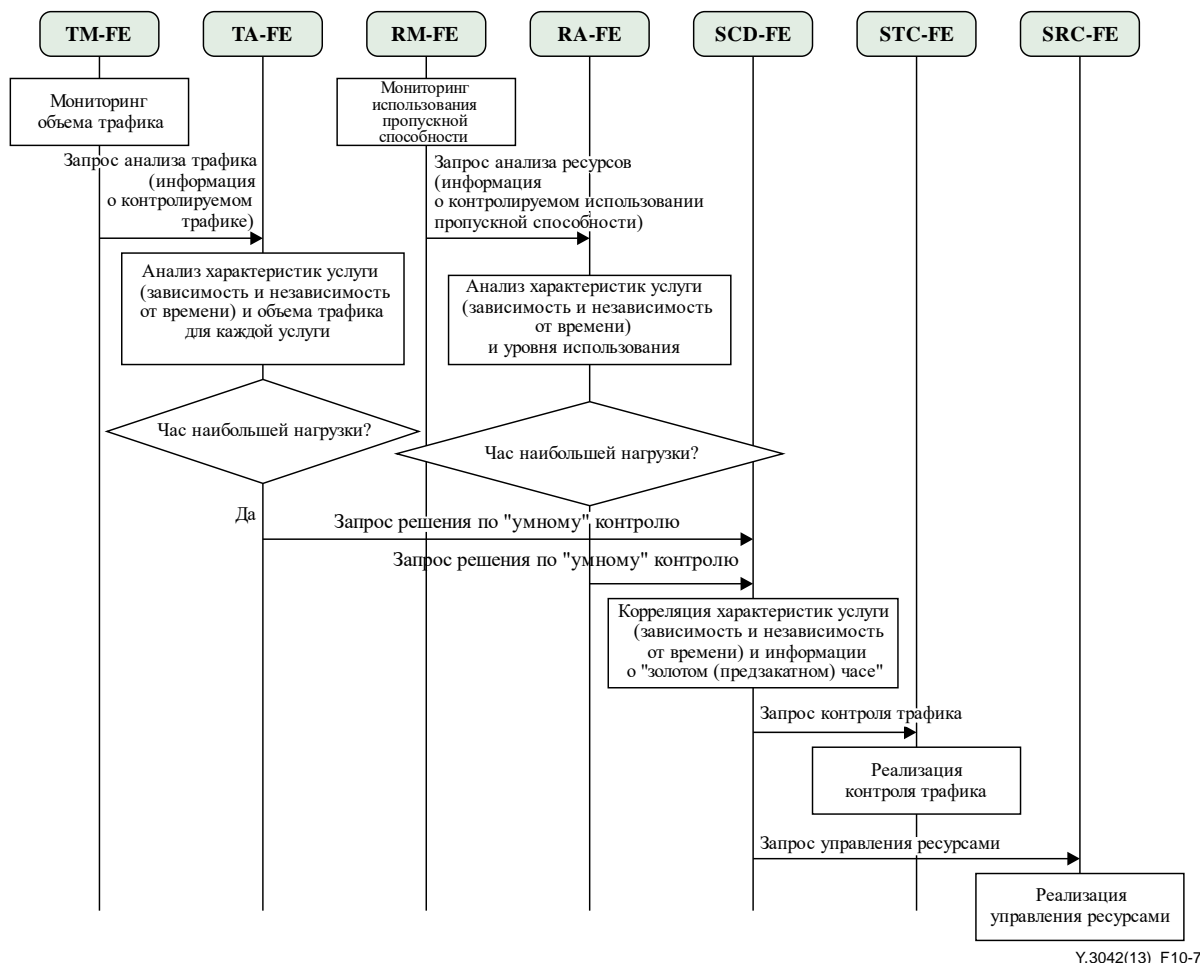
Может использоваться механизм контроля трафика и управления ресурсами в час наибольшей нагрузки для услуг, не зависящих от времени.

Ниже описаны процедуры механизма контроля трафика и управления ресурсами для трафика в час наибольшей нагрузки.

- 1) Объект TM-FE осуществляет мониторинг услуг и объемов их трафика.
- 2) Одновременно объект RM-FE осуществляет мониторинг использования пропускной способности и других ресурсов сетевых элементов, связанных с пользователями (или потоками) этих услуг.
- 3) Объект TA-FE анализирует характеристики услуг (зависимые и независимые от времени) и объем контролируемого трафика каждой услуги. Для более точного анализа может дополнительно использоваться контекстная информация, полученная от функций информирования о контексте.

- 4) Объект RA-FE анализирует характеристики услуг (зависимые и независимые от времени) и контролируемый трафик, который генерируют пользователи (или потоки). Этот объект определяет уровень использования сетевых ресурсов в плане того, ухудшается ли качество обслуживания других пользователей (или потоков). Для более точного анализа может дополнительно использоваться контекстная информация, полученная от функций информирования о контексте.
- 5) Объект SCD-FE получает результаты анализа от объектов TA-FE и RA-FE. Этот объект выполняет корреляцию характеристик услуги, объема информации в час наибольшей нагрузки и использования ресурсов. Кроме того, этот объект принимает оптимальные решения по контролю трафика и управлению ресурсами. Для более точного анализа может дополнительно использоваться контекстная информация, полученная от функций информирования о контексте.
- 6) Объект STC-FE обеспечивает выполнение принятого решения по контролю трафика, основываясь на predetermined механизмах (например, фильтрации пакетов или перекодировке).
- 7) Объект SRC-FE обеспечивает выполнение принятого решения по пропускной способности и управлению ресурсами, основываясь на заранее определенных механизмах (например, общей концепции, формировании ресурсов и контроле приоритетов).

На рисунке 10-7, ниже, показаны процедуры для этого механизма.



Y.3042(13)_F10-7

Рисунок 10-7 – Процедуры для трафика в час наибольшей нагрузки

10.8 Механизм на основе списков (пользователей)

Услуги в одноранговых соединениях могут приводить к монопольному использованию пропускной способности и снижению качества обслуживания. Для эффективного контроля таких услуг может использоваться механизм контроля трафика и управления услугами на основе списков.

Механизм контроля трафика и управления услугами на основе списков формирует список целевых активных пользователей и контролирует конкретный трафик на основе этого списка. Далее приведены два примера данного механизма специально для одноранговых соединений (P2P) в сетях CDN.

- Ограничение числа одноранговых пользователей, подключенных к сетям P2P, и ограничение скорости выгрузки – ограничение максимального числа (например, 5–10) одноранговых пользователей на каждый тип контента и ограничение скорости выгрузки (например, 500 кбит/с) по одноранговому соединению для определенного типа контента.
- Ограничение однорангового трафика путем блокирования сигналов keep-alive подтверждения активности (сигнал с сервера, содержащий информацию о статусе клиента) в определенной одноранговой сети CDN – блокирование сигналов keep-alive среди управляющих сигналов между сервером одноранговой сети и клиентом гибридной одноранговой сети.

Процедуры контроля трафика на основе списков в одноранговых сетях CDN можно обобщить следующим образом.

- 1) Объект TM-FE осуществляет мониторинг трафика на основе IP-адреса получателя пакетов.
- 2) Объект TA-FE проверяет, находится ли в данном списке IP-адрес получателя обнаруженного пакета.
- 3) Если IP-адрес получателя этого пакета находится в данном списке, объект TA-FE проверяет, имеет ли пакет статус keep-alive.
- 4) Если пакет имеет статус keep-alive, объекту SCD-FE посылается запрос анализа. Объект SCD-FE выполняет корреляцию пакетов и использования ими ресурсов, а также определяет механизм оптимального контроля трафика и управления ресурсами. Для более точного анализа может дополнительно использоваться контекстная информация, полученная от функций информирования о контексте.
- 5) Объект STC-FE обеспечивает выполнение решений, принятых объектом SCD-FE по отношению к целевым пакетам (например, блокирование пакетов).

На рисунке 10-8, ниже, показаны процедуры для этого варианта.

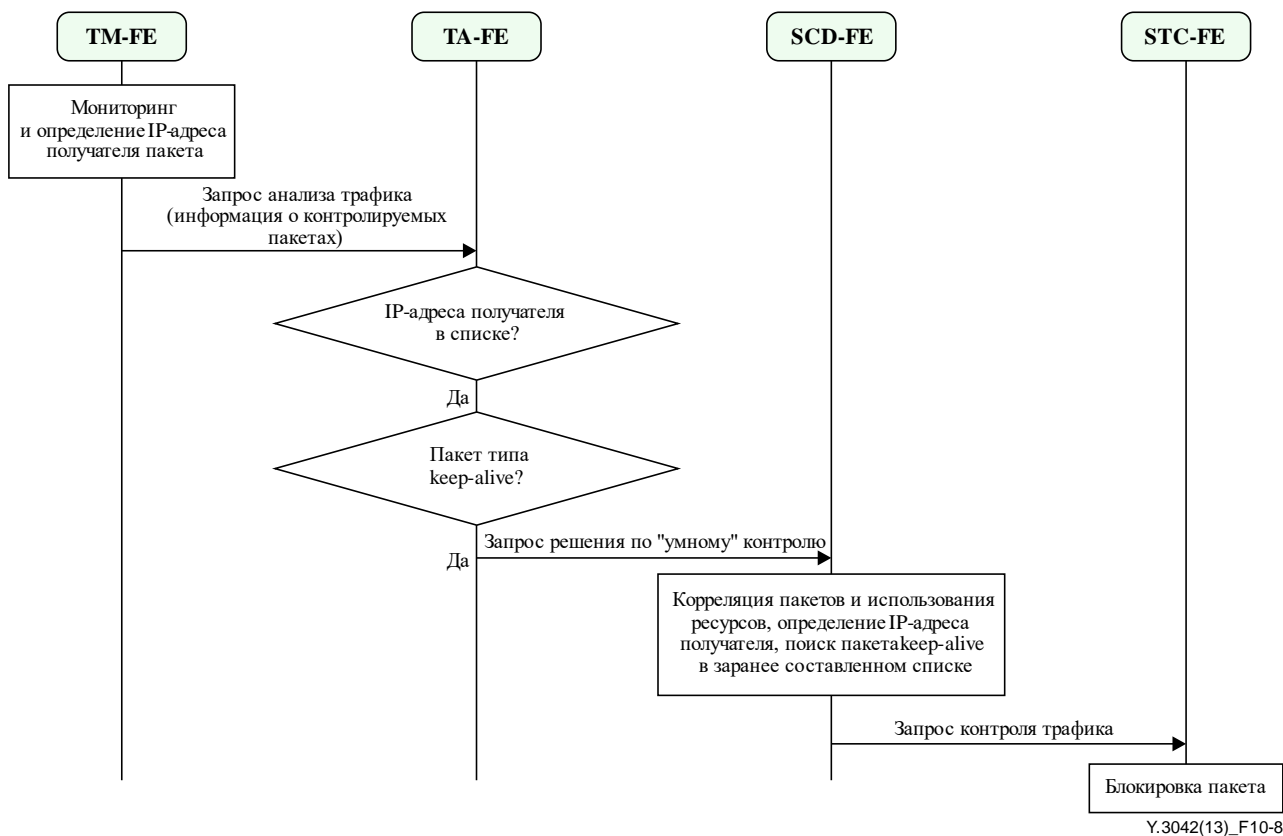


Рисунок 10-8 – Процедуры контроля трафика в одноранговых сетях CDN на основе списков

11 Аспекты безопасности

Сеть SUN считается усовершенствованным вариантом сетей на основе IP. Таким образом настоящая Рекомендация соответствует требованиям по безопасности, изложенным в [ITU-T Y.2701].

Дополнение I

Взрывной рост объема данных и снижение качества обслуживания

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации)

I.1 Взрывной рост объема данных, вызванный небольшим числом пользователей в фиксированных и подвижных сетях

Появление смартфонов вызвало дополнительное увеличение трафика данных в подвижных сетях. Разработка новых "умных" устройств с расширенными функциональными возможностями приведет к еще большему росту трафика данных, источником которого послужат подвижные сети (3G, Wi-Fi и WiMax). Это в свою очередь вызовет рост трафика данных как в подвижных, так и в фиксированных сетях. Кроме того, значительная часть сетевых ресурсов занята небольшим числом активных пользователей. Это оказывает серьезное влияние на основной круг пользователей.

На рисунках I.1 и I.2 показано монопольное использование трафика в подвижных и фиксированных сетях. В фиксированных сетях 5% абонентов генерируют почти 50% трафика, а 20% абонентов генерируют 95%. Это указывает на то, что соответствующие сетевые ресурсы не используются должным образом всеми абонентами, а заняты небольшим числом пользователей. Ситуация усугубляется в подвижных сетях, где всего 1% абонентов генерируют 45% трафика, а 10% абонентов используют 95% ресурсов, что говорит о нерациональном использовании крайне ограниченных ресурсов спектра.



Рисунок I.1 – Монопольное использование трафика в фиксированных сетях, 2010 год

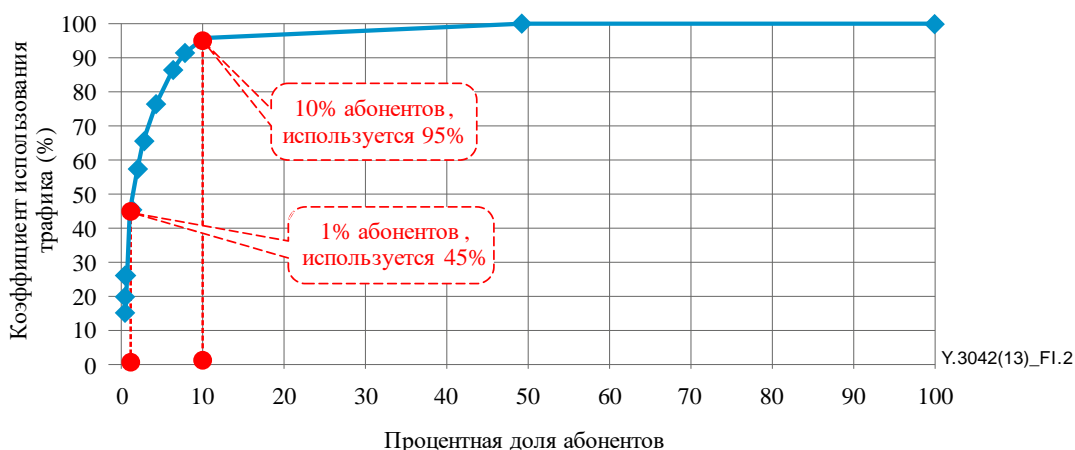


Рисунок I.2 – Монопольное использование трафика в подвижных сетях, 2010 год

I.2 Снижение качества обслуживания для основного круга пользователей, вызванное небольшим числом активных пользователей

В общем случае небольшое число активных пользователей оказывают существенное влияние на общее качество обслуживания, приводя к значительному ухудшению предоставляемых услуг для остальных пользователей. На рисунке I.3 показано существенное снижение качества обслуживания, вызванное одним активным пользователем, который использует 6 линий связи по 100 Мбит/с и занимает почти 97% пропускной способности. Показанный на этом рисунке уровень снижения качества обслуживания изменяется от минимального снижения в 29 раз до максимального – в 265 раз. Согласно данным анализа, обычные пользователи, испытывающие такое снижение качества обслуживания, сталкиваются с серьезными затруднениями даже при выполнении простого поиска в интернете.

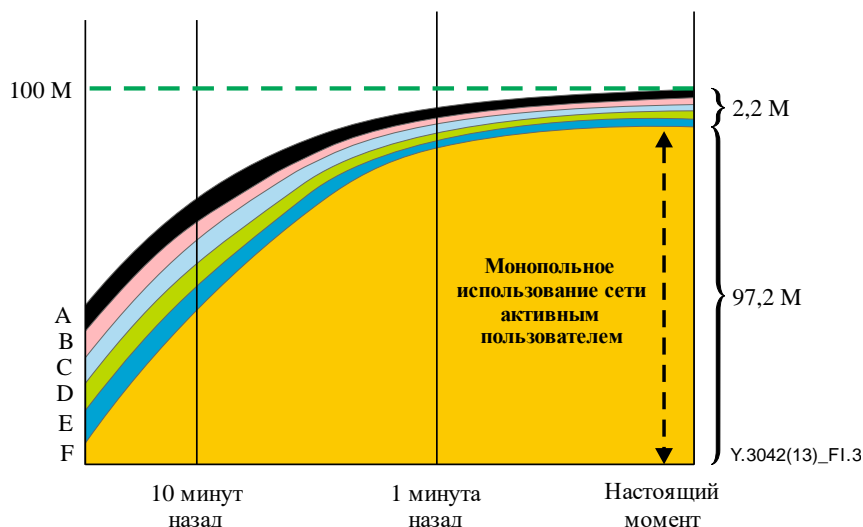


Рисунок I.3 – Снижение качества обслуживания при интенсивном и монопольном использовании

Далее в таблице I.1 подробно показана ситуация, возникающая при монопольном использовании пропускной способности.

Таблица I.1 – Снижение эксплуатационных характеристик при интенсивном и монопольном использовании

Пользователь	10 минут назад	1 минута назад	Настоящий момент
Пользователь А	0,14 Мбит/с	0,15 Мбит/с	0,01 Мбит/с
Пользователь В	11,74 Мбит/с	2,45 Мбит/с	0,04 Мбит/с
Пользователь С	13,51 Мбит/с	1,86 Мбит/с	1,74 Мбит/с
Пользователь D	0,52 Мбит/с	0,35 Мбит/с	0,39 Мбит/с
Пользователь E	0,36 Мбит/с	0,06 Мбит/с	0,05 Мбит/с
Пользователь F	29,14 Мбит/с	94,85 Мбит/с	97,24 Мбит/с

I.3 Необходимость "умного" управления сетью для обеспечения качества обслуживания обычных пользователей

После рассмотрения вышеприведенных сценариев использования очевидно, что для обеспечения качества обслуживания как минимум обычного пользователя требуются специальные механизмы, функционирующие с высокой степенью прозрачности и на основе

добросовестного подхода. Эти проблемы должны решаться с использованием возможностей "умного" контроля и управления сетями.

Дополнение II

Примеры контекстной информации для STCRMF

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации)

Функция STCRMF позволяет взаимодействовать с функциями информирования о контексте для получения контекстной информации. Эта информация содержит данные, относящиеся к соответствующим пользователям, устройствам, услугам и контенту. Тем не менее в функциональной архитектуре, рассматриваемой в разделе 9.2, не существует подробного примера контекстной информации. Поэтому в данном Дополнении приводятся примеры каждого типа контекста и информации.

В таблице II.1 показаны примеры контекстной информации, используемой для функции STCRMF.

Таблица II.1 – Контекстная информация для STCRMF

Тип контекста	Контекстная информация
Контекст услуги	<ul style="list-style-type: none">• Тип услуги – VoIP, потоковые аудиоданные, потоковое видео, мгновенные сообщения, интерактивные игры, просмотр веб-страниц• Разрешение видео – SD, HD720p, HD1080p, VGA (Video Graphics Array)• Кодирование видео (скорость передачи данных, бит/с)• Скорость передачи видеокадров• Кодеки – ITU-T H.264, MPEG4 (Экспертная группа 4 по вопросам движущегося изображения)
Контекст пользователей	<ul style="list-style-type: none">• Тип устройства – смартфон, планшет, "умное" телевидение, мобильный ПК• Предел трафика – верхний предел трафика• Тип пользователя – активный (с интенсивным трафиком), злонамеренный, обычный (по результатам поведения пользователя)
Контекст сети (трафика)	<ul style="list-style-type: none">• Тип трафика – управляемый, неуправляемый• Тип сетевого соединения – 3G, LTE, WiMax, Wi-Fi, фиксированное• Расположение, время• Атрибут трафика – объем, частота, количество потоков

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

- Серия А Организация работы МСЭ-Т
- 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 Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
- Серия M Управление электросвязью, включая СУЭ и техническое обслуживание сетей
- Серия N Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
- Серия O Требования к измерительной аппаратуре
- Серия P Оконечное оборудование, субъективные и объективные методы оценки
- Серия Q Коммутация и сигнализация, а также соответствующие измерения и испытания
- 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, взаимосвязь открытых систем и безопасность
- Серия Y Глобальная информационная инфраструктура, аспекты межсетевого протокола, сети последующих поколений, интернет вещей и "умные" города**
- Серия Z Языки и общие аспекты программного обеспечения для систем электросвязи