Международный союз электросвязи

МСЭ-Т Y.1540

(12/2019)

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

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

Аспекты протокола Интернет – Качество обслуживания и сетевые показатели качества

Служба передачи данных по межсетевому протоколу (IP) – Параметры рабочих характеристик переноса и доступности IP-пакетов

Рекомендация МСЭ-Т Y.1540

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ Y

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

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА	
Общие положения	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 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
IPTV по NGN	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 услуг и архитектура услуг	Y.2200–Y.2249
Аспекты обслуживания: взаимодействие услуг и СПП	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
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
ИНТЕРНЕТ ВЕЩЕЙ И "УМНЫЕ" ГОРОДА И СООБЩЕСТВА	
Общие положения	Y.4000–Y.4049
Определения и терминология	Y.4050–Y.4099
Требования и сценарии использования	Y.4100–Y.4249
Инфраструктура, возможность установления соединений и сети	Y.4250–Y.4399
Структуры, архитектуры и протоколы	Y.4400–Y.4549
Услуги, приложения, вычисления и обработка данных	Y.4550–Y.4699
Управление, контроль и рабочие характеристики	Y.4700–Y.4799
Идентификация и безопасность	Y.4800–Y.4899
Анализ и оценка	Y.4900–Y.4999

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

Рекомендация МСЭ-Т Y.1540

Служба передачи данных по межсетевому протоколу (IP) – Параметры рабочих характеристик переноса и доступности IP-пакетов

Резюме

В Рекомендации МСЭ-Т Y.1540 определены параметры, которые могут использоваться при описании и оценке эксплуатационных показателей скорости, точности, функциональной надежности и готовности передачи IP-пакетов региональных и международных услуг передачи данных на основе протокола Интернет (IP). Определенные параметры применяются к сквозным IP-услугам и IP-услугам связи пункта с пунктом, а также к частям сети, которые обеспечивают такие услуги или способствуют предоставлению таких услуг, в соответствии с нормативными документами, указанными в разделе 2. Транспортирование без установления соединения является отличительным аспектом услуги IP, которая рассматривается в настоящей Рекомендации.

После более чем 20 лет существования в качестве действующей Рекомендации издание 2019 года отражает многочисленные изменения в подходе к разработке IP-услуг и протоколов, используемых конечными пользователями. В него включено новое Приложение A, в котором определены параметры пропускной способности IP-уровня с учетом возможности проведения оценки и содержатся требования к методам измерения пропускной способности IP-уровня. Это новое Приложение является результатом многолетних исследований и применения разработанных 12-й Исследовательской комиссией МСЭ-Т принципов точной оценки параметров рабочих характеристик и методов измерения в сравнении с эталонной "реальной ситуацией" в лабораторных и полевых измерениях. Связанные с потоком параметры пропускной способности и методы измерения (надежный транспорт доставки) остаются для дальнейшего изучения, и в тексте проводится четкое различие между этими параметрами пропускной способности IP-уровня. Точно так же параметры, описывающие рабочие характеристики конкретного надежного протокола транспортного уровня (TCP), остаются для дальнейшего изучения, и признается, что надежные транспортные протоколы для интернета постоянно меняются и являются предметом непрерывных исследований.

В Приложении B представлен второй, более мощный алгоритм поиска для метода измерения пропускной способности IP-уровня, определенного в Приложении A.

Хронологическая справка

Издание	Рекомендация	Утверждено	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т I.380	26.02.1999	13-я	11.1002/1000/4573
1.0	МСЭ-Т Y.1540	26.02.1999	13-я	11.1002/1000/5302
2.0	МСЭ-Т Y.1540	14.12.2002	13-я	11.1002/1000/6189
2.1	МСЭ-Т Y.1540 (2002) Попр. 1	01.08.2003	13-я	11.1002/1000/6975
3.0	МСЭ-Т Y.1540	13.11.2007	12-я	11.1002/1000/9270
3.1	МСЭ-Т Y.1540 (2007) Попр. 1	19.03.2009	12-я	11.1002/1000/9727
4.0	МСЭ-Т Y.1540	01.03.2011	12-я	11.1002/1000/11079
4.1	МСЭ-Т Y.1540 (2011) Попр. 1	21.01.2016	12-я	11.1002/1000/12761
5.0	МСЭ-Т Y.1540	29.07.2016	12-я	11.1002/1000/12975
6.0	МСЭ-Т Y.1540	05.12.2019	12-я	11.1002/1000/13933
6.1	МСЭ-Т Y.1540 (2019) Попр. 1.	06.02.2020	12-я	11.1002/1000/14161

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL http://handle.itu.int/, после которого укажите уникальный идентификатор Рекомендации.
Например, http://handle.itu.int/11.1002/1000/11830-en.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). 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. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

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/.

СОДЕРЖАНИЕ

Рекомендация МСЭ-T Y.1540

Служба передачи данных по межсетевому протоколу (IP) – Параметры рабочих характеристик переноса и доступности IP-пакетов

1 Сфера применения

В настоящей Рекомендации определены параметры, которые могут использоваться при описании и оценке эксплуатационных показателей скорости, точности, функциональной надежности и готовности передачи IP-пакетов региональных и международных услуг передачи данных на основе протокола Интернет (IP). Определенные параметры применяются к сквозным IP-услугам и IP-услугам связи пункта с пунктом, а также к частям сети, которые обеспечивают такие услуги или способствуют предоставлению таких услуг, в соответствии с нормативными документами, указанными в разделе 2. Транспортирование без установления соединения является отличительным аспектом IP-услуги, которая рассматривается в настоящей Рекомендации.

В тексте настоящей Рекомендации сквозная IP-услуга обозначает передачу IP-датаграмм, сформированных пользователем (в настоящей Рекомендации они называются IP-пакетами) между двумя оконечными станциями, обозначенными их полными IP-адресами. В некоторых других Рекомендациях термином "сквозной" обозначены иные границы. Например, в Рекомендации [ITU-T P.10] сквозное качество определяется как качество, относящееся к работе системы связи, включая все оконечное оборудование. Для услуг передачи голоса оно эквивалентно качеству "рот – ухо".

ПРИМЕЧАНИЕ 1. – В настоящей Рекомендации определяются параметры, которые можно использовать для характеристики IP-услуг, предоставляемых с использованием протокола Интернет версии 4 (IPv4) и протокола Интернет версии 6 (IPv6); вопрос о применимости или распространению настоящей Рекомендации на другие протоколы (например, протокол резервирования ресурсов (RSVP)) подлежит дальнейшему изучению.

ПРИМЕЧАНИЕ 2. – Рекомендации по качеству IP-услуг связи пункта с несколькими пунктами в настоящее время находятся в стадии разработки.

Параметры рабочих характеристик [ITU-T Y.1540] и методы измерения (где они указаны) предназначены для использования при планировании и предоставлении как региональных, так и международных IP-услуг. К предполагаемым пользователям настоящей Рекомендации относятся поставщики IP-услуг, производители оборудования, конечные пользователи (абоненты IP-услуг) и все те, кому нужно осуществлять оценку IP-услуг и/или контроль за ними. Настоящая Рекомендация будет полезна поставщикам услуг при планировании, разработке и оценке IP-услуг, отвечающих потребностям пользователей в отношении качества, производителям оборудования в качестве источника информации о рабочих характеристиках, которая повлияет на конструкцию оборудования, а также конечным пользователям при оценке качества IP-услуг.

Обобщенная информация о сфере применения настоящей Рекомендации представлена на рисунке 1. Параметры рабочих характеристик IP-услуг определяются на основе эталонных событий передачи IP-пакетов (IPRE), которые можно наблюдать в пунктах измерения (MP), с учетом указанных функциональных и юрисдикционных границ. В целях обеспечения сопоставимости и полноты рабочие характеристики IP-услуг рассматриваются в контексте матрицы рабочих характеристик 3×3, определенной в [ITU-T I.350]. В этой матрице определены три не зависящие от протокола функции связи: получение доступа, перенос информации пользователя и разъединение. Каждая функция рассматривается с учетом трех основных аспектов рабочих характеристик (или "критериев качества"): скорости, точности и надежности. Соответствующая модель с двумя состояниями обеспечивает основу для описания доступности IP-услуг.

ПРИМЕЧАНИЕ 3. – В настоящей Рекомендации функция переноса информации пользователя, показанная на рисунке 1, относится к попытке передачи любого IP-пакета, независимо от его типа или содержимого.

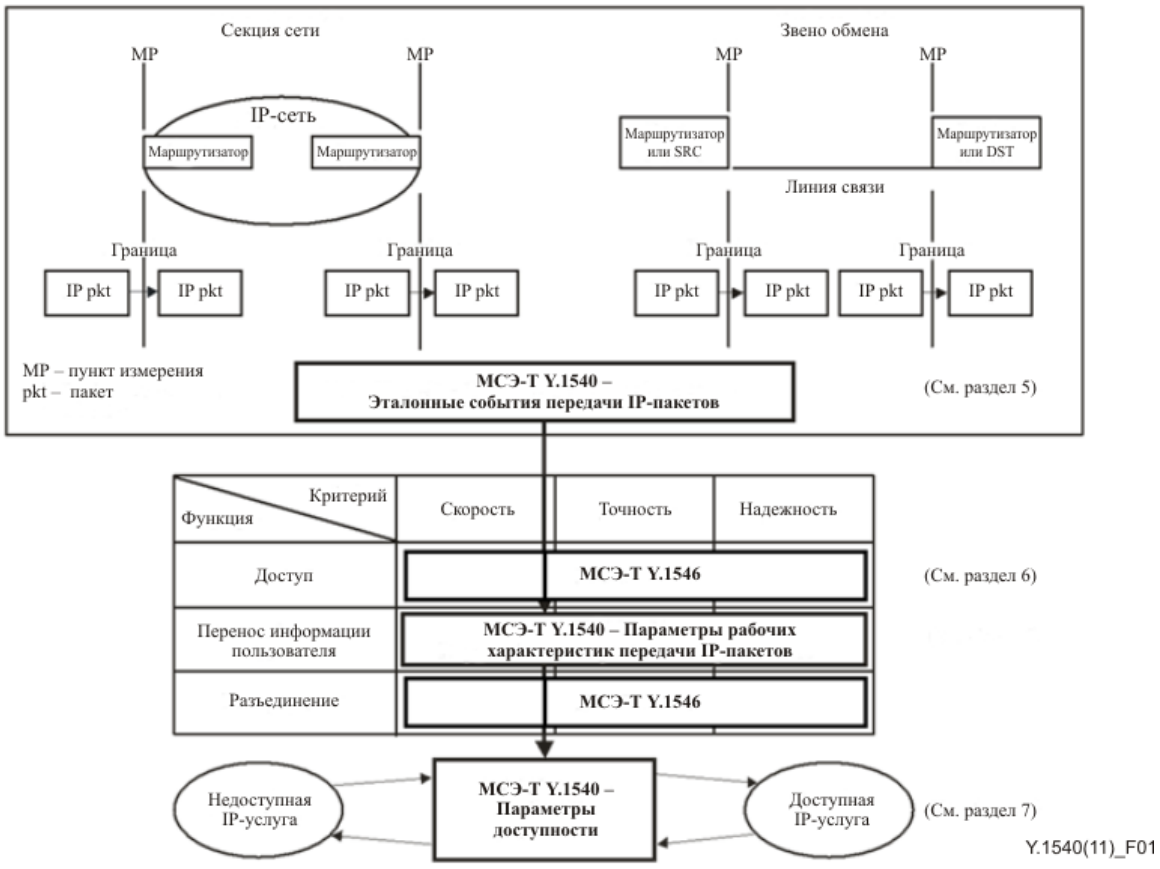


Рисунок 1 – Сфера применения настоящей Рекомендации

Рабочие параметры, определенные в настоящей Рекомендации, описывают скорость, точность, надежность и доступность передачи IP-пакетов, обеспечиваемые службой передачи данных по протоколу Интернет. Сквозные рабочие характеристики региональных и международных IP-услуг, обеспечивающих функции получения доступа и разъединения (например, служба доменных имен) и транспортные возможности более высокого уровня (например, протокол управления передачей), рассматриваются в отдельных Рекомендациях, таких как Приложение C к [ITU-T Y.1546] о доступности IP-услуг.

Настоящая Рекомендация имеет следующую структуру: в разделе 1 определяется сфера ее применения; в разделе 2 приводятся нормативные ссылки; в разделе 3 содержится список сокращений; в разделе 4 описывается многоуровневая модель, которая служит контекстом для спецификации рабочих характеристик IP-услуг; в разделе 5 определяется модель рабочих характеристик IP-услуг, включая сегменты сети и пункты измерения, эталонные события и результаты; в разделе 6 эта модель используется для определения параметров рабочих характеристик переноса IP-пакетов; а затем в разделе 7 определяются параметры доступности IP-услуг.

В Приложении A определяются параметры пропускной способности IP-уровня с учетом возможности проведения оценки и приводятся требования к методам измерения наряду с планом оценки возможных методов измерения в лаборатории и в производственных (действующих) сетях (новое в версии 2019 года). В Дополнении I описываются аспекты маршрутизации IP-пакетов и их влияние на рабочие характеристики. В Дополнении II приводится дополнительная терминология по вариации задержки IP-пакетов. Дополнение III (Параметры, связанные со скоростью и пропускной способностью) в версии 2019 года признано устаревшим. В Дополнении IV описывается процесс оценки доступности IP-услуг. В Дополнении V представлены соображения по измерению параметров, определенных в [ITU-T Y.1540]. В Дополнении VI дается некоторая базовая информация о доступности IP-услуг. В Дополнении VII содержится базовая информация о параметрах восстановления потока,

а в Дополнении VIII – информация о параметрах пропускной способности (включая сопоставление с предыдущими показателями IETF и вопросы для дальнейшего изучения). В Дополнении IX объясняется, почему измерения на основе TCP не соответствуют нормативным требованиям, изложенным в пункте 6.12.

В версию 2019 года добавлено много новых дополнений. Новое Дополнение X содержит важный справочный материал, подтверждающий параметры пропускной способности IP-уровня и методы их измерения, в том числе сводную информацию о результатах лабораторных и полевых испытаний со сравнением разных методов измерения. В Дополнении XI содержится обзор научных статей, описывающих кампании по измерению, в котором проводятся аналогичные сравнения. В Дополнении XII дается подробная информация о расчетах, необходимых для выполнения точных измерений и сравнений скорости передачи данных на разных уровнях стека протоколов. В Дополнении XIII приводится информация о параметрах и методах измерения, связанных с IP-потоком, которая подлежит дальнейшему изучению, и указывается их дополнительная роль в отношении показателей и методов измерения пропускной способности IP-уровня.

ПРИМЕЧАНИЕ 4. – Параметры, определенные в МСЭ-T Y.1540, могут быть дополнены или изменены в результате дальнейшего изучения требований, предъявляемых поддерживаемыми IP-приложениями (например, интерактивными, блочными, потоковыми).

ПРИМЕЧАНИЕ 5. – Параметры скорости, точности и надежности, определенные в МСЭ-T Y.1540, характеризуют IP-услугу в состоянии доступности.

ПРИМЕЧАНИЕ 6. – Параметры, определенные в настоящей Рекомендации, могут применяться к одной сквозной IP-услуге между двумя конечными станциями, определяемыми их IP-адресами. Эти параметры также могут применяться к тем IP-пакетам данной сквозной IP-услуги, которые предлагаются для данной сети или звена обмена (EL).

ПРИМЕЧАНИЕ 7. – Параметры МСЭ-T Y.1540 характеризуют рабочие характеристики услуги, обеспечиваемые элементами сети в указанных границах секции. Однако пользователям настоящей Рекомендации следует знать о том, что элементы сети за пределами указанных границ иногда могут влиять на измеряемые рабочие характеристики элементов, находящихся в этих границах. Примеры описаны в Дополнении V.

ПРИМЕЧАНИЕ 8. – Параметры, определенные в настоящей Рекомендации, могут также применяться к любому подмножеству IP-пакетов, поступающих в данный комплект сетевого оборудования. Методы агрегирования рабочих характеристик по комплекту сетевого оборудования или по всей сети выходят за рамки сферы применения настоящей Рекомендации.

ПРИМЕЧАНИЕ 9. – В настоящей Рекомендации не предлагаются инструменты для прямой оценки стабильности маршрутизации. Однако влияние нестабильности маршрута можно количественно оценить с помощью определенных в настоящей Рекомендации параметров потери пакетов, задержки и потери значительного блока пакетов.

ПРИМЕЧАНИЕ 10. – Спецификация значений показателей качества для некоторых параметров рабочих характеристик, рассматриваемых в Рекомендации МСЭ-T Y.1540, приведена в [ITU-T Y.1541].

ПРИМЕЧАНИЕ 11. – Слово "предварительный", используемое в настоящей Рекомендации, означает, что существует соглашение о стабильности указанного значения, но что в результате дальнейшего изучения или на основе реального опыта эксплуатации сети это значение может измениться.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-T и другие справочные документы содержат положения, которые путем ссылок на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие справочные документы могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Перечень действующих на настоящий момент Рекомендаций МСЭ-T регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус Рекомендации.

[ITU-T I.350] Recommendation ITU-T I.350 (1993), *General aspects of quality of service and network performance in digital networks, including ISDNs.*

[ITU-T P.10] Рекомендация МСЭ-T P.10/G.100 (2017 г.), *Словарь по рабочим характеристикам, качеству обслуживания и оценке пользователем качества услуги.*

[ITU-T Y.1541] Рекомендация МСЭ-Т Y.1541 (2011 г.), *Требования к сетевым показателям качества для служб, основанных на протоколе IP.*

[ITU-T Y.1546] Recommendation ITU-T Y.1546 (2014), *Hand-over performance among multiple access networks.*

[ITU-T Y.1565] Recommendation ITU-T Y.1565 (2011), *Home network performance parameters.*

[IETF RFC 791] IETF RFC 791 (1981), *Internet Protocol*.
<http://www.ietf.org/rfc/rfc791.txt>

[IETF RFC 4737] IETF RFC 4737 (2006), *Packet Reordering Metrics.*
<http://www.ietf.org/rfc/rfc4737.txt>

[IETF RFC 5136] IETF RFC 5136 (2008), *Defining Network Capacity.*
<http://www.ietf.org/rfc/rfc5136.txt>

[IETF RFC 5481] IETF RFC 5481 (2009), *Packet Delay Variation Applicability Statement.*
<http://www.ietf.org/rfc/rfc5481.txt>

[IETF RFC 8200] IETF RFC 8200 (2017), *Internet Protocol, Version 6 (IPv6) Specification.*
<http://www.ietf.org/rfc/rfc8200.txt>

[IETF RFC 8337] IETF RFC 8337 (2018), *Model-Based Metrics for Bulk Transport Capacity.*
<http://www.ietf.org/rfc/rfc8337.txt>

3 Сокращения и акронимы

В настоящей рекомендации используются следующие сокращения и акронимы.

ARQ	Automatic Repeat-request	Автоматический запрос повторной передачи
ATM	Asynchronous Transfer Mode	Асинхронный режим передачи
BTC	Bulk Transfer Capacity	Пропускная способность службы транспортировки массивов данных
DSCP	Differentiated Services Code Point	Указатель кода дифференцированных служб
DST	Destination host	Хост-получатель
EL	Exchange Link	Звено обмена
ER	Edge Router	Граничный маршрутизатор
FEC	Forward Error Correction	Прямая коррекция ошибок
FTP	File Transfer Protocol	Протокол передачи файлов
HTTP	Hypertext Transfer Protocol	Протокол передачи гипертекста
IP	Internet Protocol	Протокол Интернет
IPDR	Internet Protocol packet Duplicate Ratio	Коэффициент дублирующих IP-пакетов
IPDV	Internet Protocol packet Delay Variation	Вариация задержки IP-пакетов протокола Интернет
IPER	Internet Protocol packet Error Ratio	Коэффициент ошибочных IP-пакетов
IPIBR	Internet Protocol packet Impaired Block Ratio	Коэффициент блоков IP-пакетов с нарушениями
IPIIR	Internet Protocol packet Impaired Interval Radio	Коэффициент интервалов IP-пакетов с нарушениями
IPLR	Internet Protocol packet Loss Ratio	Коэффициент потери IP-пакетов

IPOR	Octet-based IP packet Rate		Скорость побайтовой передачи IP-пакетов
IPPM	IP Performance Metrics		Показатели рабочих характеристик IP-услуг
IPPR	Internet Protocol Packet Rate		Скорость передачи IP-пакетов
IPRE	Internet Protocol packet transfer Reference Event		Эталонное событие переноса (передачи) IP-пакетов
IPRR	Internet Protocol packet Reordered Ratio		Коэффициент переупорядоченных IP-пакетов
IPSLB	Internet Protocol packet Severe Loss Block outcome		Результат "блок с серьезными потерями IP-пакетов"
IPSLBR	Internet Protocol packet Severe Loss Block Ratio		Коэффициент блоков с серьезными потерями IP-пакетов
IPTD	Internet Protocol packet Transfer Delay		Задержка передачи IP-пакетов протокола Интернет
IPv4	Internet Protocol version 4		Протокол Интернет версии 4
IPv6	Internet Protocol version 6		Протокол Интернет версии 6
ISP	Internet Service Provider	ПУИ	Поставщик услуг интернета
LL	Lower Layers (protocols and technology supporting the Internet protocol layer)		Нижние (нижележащие) уровни (протоколы и технологии, поддерживающие уровень протокола Интернет)
M_{av}	The minimum number of packets recommended for assessing the availability state		Минимальное количество пакетов, рекомендуемое для оценки состояния доступности
MBM	Model-Based Metrics		Показатели на основе модели
MP	Measurement Point		Пункт измерения
MTBISO	Mean Time Between IP Service Outages		Среднее время между перебоями в работе IP-услуги
MTTISR	Mean Time To Internet protocol Service Restoral		Среднее время до восстановления IP-услуги
N	The number of packets in a throughput probe of size N		Количество пакетов в пробе размера N при проверке пропускной способности
NS	Network Section		Сетевая секция
NSE	Network Section Ensemble		Совокупность сетевых секций
NSP	Network Service Provider		Поставщик сетевых услуг
PDH	Plesiochronous Digital Hierarchy		Плезиохронная цифровая иерархия
PDV	Packet Delay Variation		Вариация задержки пакетов
PIA	Percent Internet protocol service Availability		Доля времени доступности IP-службы
PIU	Percent Internet protocol service Unavailability		Доля времени недоступности IP-службы
QoS	Quality of Service		Качество обслуживания
R	Router		Маршрутизатор

RIPR	Replicated Internet protocol Packet Ratio	Коэффициент дублируемых IP-пакетов
RSVP	Resource reservation Protocol	Протокол резервирования ресурсов
RTCP	Real-Time Control Protocol	Протокол управления в режиме реального времени
RTO	Retransmission Time Out	Тайм-аут повторной передачи
RTP	Real-time Transport Protocol	Транспортный протокол реального времени
RTT	Round-Trip Time	Время передачи в прямом и обратном направлениях
SDH	Synchronous Digital Hierarchy	Синхронная цифровая иерархия
SPRT	Sequential Probability Ratio Test	Последовательный тест на основе отношения вероятностей
SRC	Source host	Хост-источник
STD	Standard	Стандарт
T_{av}	Minimum length of time of Internet protocol availability; minimum length of time of Internet protocol unavailability	Минимальный интервал времени доступности протокола Интернет; минимальный интервал времени недоступности протокола Интернет
TBF	Token Bucket Filter	Фильтр на основе буфера маркеров
TCP	Transmission Control Protocol	Протокол управления передачей
T_{max}	Maximum Internet protocol packet delay beyond which the packet is declared to be lost	Максимальная задержка IP-пакетов, при превышении которой пакет объявляется потерянным
ToS	Type of Service	Тип службы (услуги)
T_s	Length of time defining the block in the severe loss block outcome	Интервал времени, определяющий блок в результате "блок с серьезными потерями пакетов"
TTL	Time To Live	Время существования
UDP	User Datagram Protocol	Протокол передачи датаграмм пользователя

4 Многоуровневая модель рабочих характеристик IP-службы

На рисунке 2 иллюстрируется многоуровневый характер рабочих характеристик IP-службы. Рабочие характеристики, которые обеспечиваются для пользователей IP-службы, зависят от рабочих характеристик других уровней:

– нижележащие уровни (LL), которые обеспечивают (через "звенья") транспорт, ориентированный на соединения или без установления соединений, поддерживающий IP-уровень. Звенья оканчиваются в пунктах, в которые направляются IP-пакеты (то есть в маршрутизаторах SRC и DST), и поэтому не организованы "от конца до конца". В звеньях могут применяться различные технологии, например асинхронный режим передачи (ATM), ретрансляция кадров, синхронная цифровая иерархия (SDH), плезиохронная цифровая иерархия (PDH), ЦСИС или выделенные линии. Ниже уровня IP может находиться несколько уровней протоколов и служб, и в конечном счете они используют различные типы физической среды передачи;

– IP-уровень, обеспечивающий транспортировку IP-датаграмм (то есть IP-пакетов) без организации соединений. IP-уровень организуется "от конца до конца" для заданной пары IP-адресов источника и получателя. Определенные элементы в заголовках IP-пакетов могут изменяться сетями, но данные IP-пользователя не могут быть изменены на IP-уровне или ниже;

– более высокие уровни, поддерживаемые протоколом IP, которые обеспечивают дальнейшие связи "от конца до конца". Верхние уровни могут содержать, например, протокол управления передачей (TCP), протокол датаграмм пользователя (UDP), протокол передачи файлов (FTP), транспортный протокол реального времени (RTP) и протокол передачи гипертекста (HTTP). Более высокие уровни будут изменять и могут улучшить рабочие характеристики "от конца до конца", которые обеспечивает IP-уровень.

ПРИМЕЧАНИЕ 1. – В разделе 5 описывается модель рабочих характеристик IP-службы и точнее определяются ключевые термины, используемые в этой многоуровневой модели.

ПРИМЕЧАНИЕ 2. – Соотношение рабочих характеристик между этими уровнями подлежит дальнейшему изучению.

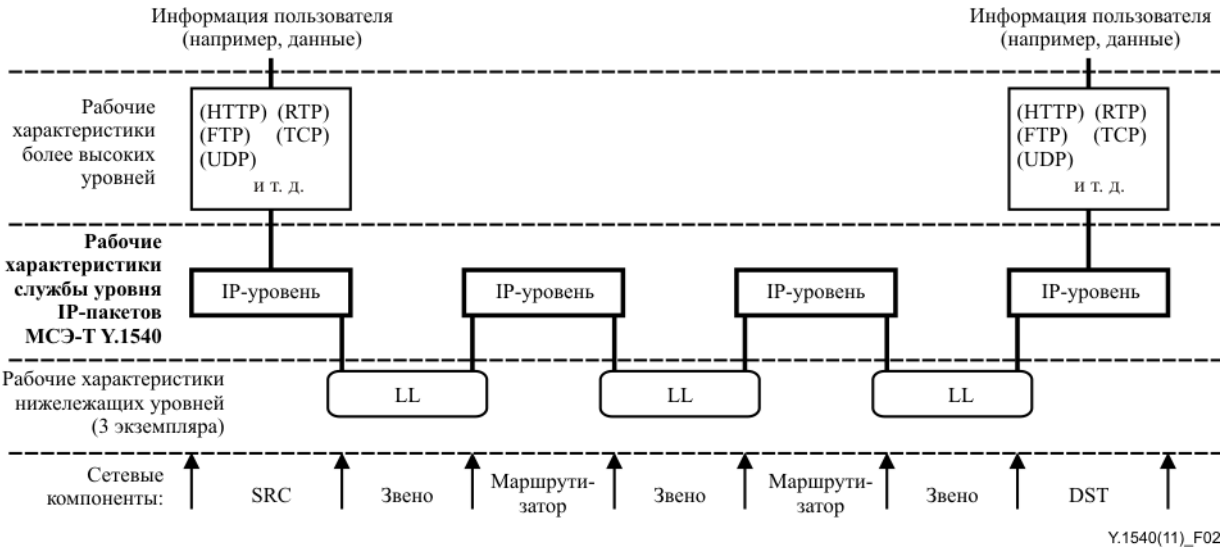


Рисунок 2 – Многоуровневая модель рабочих характеристик IP-службы – пример

5 Общая модель рабочих характеристик IP-службы

В данном разделе определяется общая модель рабочих характеристик IP-службы. Эта модель состоит главным образом из секций двух типов – звеньев обмена и сетевых секций (NS). Они определены в пункте 5.2. Это конструктивные блоки, с помощью которых можно представить любую сквозную IP-службу. Каждый из параметров рабочих характеристик, определенных в настоящей Рекомендации, может применяться к однонаправленной передаче IP-пакетов по секции или группе соединенных секций.

В пункте 5.4 перечислены эталонные события передачи IP-пакетов, составляющие основу определения параметров рабочих характеристик. Эти эталонные события выведены из соответствующих определений IP-службы и протоколов и согласуются с ними. Затем в пункте 5.5 эти эталонные события используются для перечисления возможных результатов, когда пакет доставляется в секцию.

ПРИМЕЧАНИЕ. – Вопрос о включении всей определяемой в МСЭ-Т Y.1540 модели рабочих характеристик или ее части и эталонных событий в [b-ITU-T I.353] подлежит дальнейшему изучению.

5.1 Сетевые компоненты

5.1.1 Хост

Хост (хост-компьютер) – это компьютер, который пользуется связью с помощью протоколов Интернет. Он реализует функции маршрутизации (то есть работает на IP-уровне) и может реализовать дополнительные функции, включая протоколы вышележащих уровней (например, протокол TCP в хост-источнике или в хост-получателе (DST)) и протоколы нижележащих уровней (например, ATM).

5.1.2 Маршрутизатор

Маршрутизатор (router) – это хост, который создает возможность связи между другими хостами путем пересылки IP-пакетов, используя содержимое их полей IP-адреса получателя.

5.1.3 Хост-источник (SRC)

Хост-источник (source host) – это хост и полный IP-адрес пункта, из которого выдаются IP-пакеты "от конца до конца". Обычно хост может иметь более одного IP-адреса; однако хост-источник (SRC) является уникальным хостом, связанным с одним IP-адресом. Хосты-источники выдают также протоколы более высокого уровня (например, TCP), когда такие протоколы реализованы.

5.1.4 Хост-получатель (DST)

Хост-получатель (destination host) – это хост и полный IP-адрес пункта назначения, в который поступают IP-пакеты "от конца до конца". Обычно хост может иметь более одного IP-адреса; однако хост-получатель (DST) является уникальным хостом, связанным с одним IP-адресом. Хосты-получатели также заканчивают протоколы более высокого уровня (например, TCP), когда такие протоколы реализованы.

5.1.5 Звено

Звено (link) – это двухточечное соединение (физическое или виртуальное), используемое для транспортировки IP-пакетов между парой хостов. Оно не включает в себя какие-либо части этих хостов или какие-либо другие хосты; оно действует ниже IP-уровня. Например, звено может представлять собой выделенную линию или может быть реализовано в виде логического соединения по сети Ethernet, сети с ретрансляцией кадров, сети ATM или посредством любой другой сетевой технологии, работающей ниже IP-уровня.

На рисунке 3 показаны сетевые компоненты, относящиеся к IP-службе между SRC и DST. Звенья, которые могут представлять собой коммутируемые линии, выделенные линии, кольца или сети, показаны в виде линий между хостами. Маршрутизаторы показаны в виде окружностей, а SRC и DST – в виде треугольников.

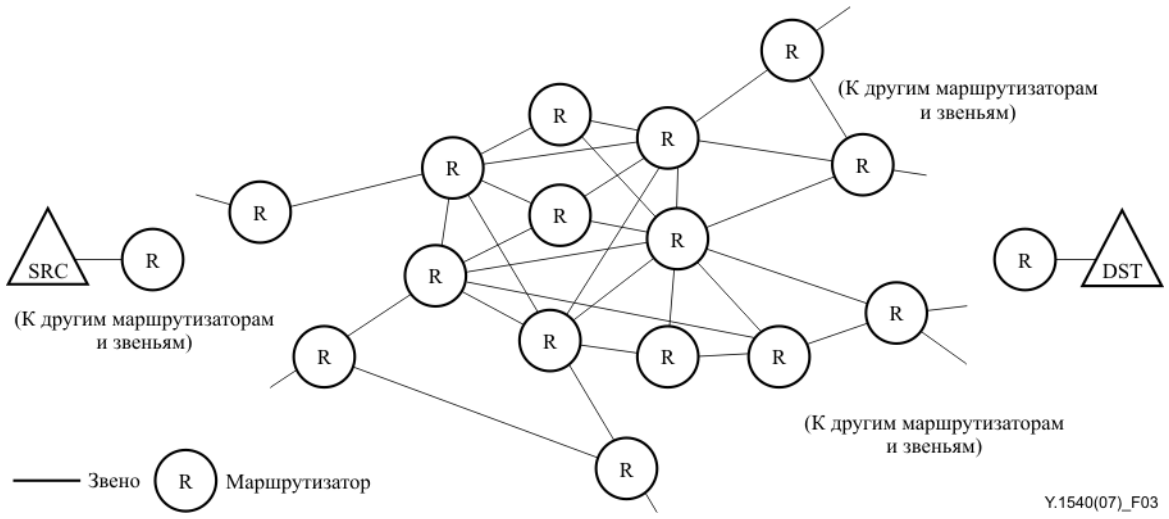


Рисунок 3 – Компоненты IP-сети

5.2 Звенья обмена и сетевые секции

5.2.1 Звено обмена (exchange link, EL)

Это звено соединяет:

1) хост-источник или хост-получатель со смежным хостом (например, маршрутизатором), возможно находящимся в другом подчинении, который иногда называют звеном доступа, входным звеном или выходным звеном; либо

2) маршрутизатор одной сетевой секции с маршрутизатором другой сетевой секции.

Следует отметить, что ответственность за звено обмена, его пропускную способность и его рабочие характеристики обычно распределяется между соединяемыми сторонами.

ПРИМЕЧАНИЕ. – "Звено обмена" приближенно эквивалентно термину "exchange" (обмен, передача), определенному в [b-IETF RFC 2330].

5.2.2 Сетевая секция (network section, NS)

Сетевая секция – это набор хостов вместе со всеми соединяющими их звеньями, которые в совокупности образуют часть IP-службы между SRC и DST и находятся под одной (или совместной) полномочной ответственностью. Некоторые сетевые секции содержат один хост без соединительных звеньев. Частными случаями сетевых секций являются NS-источник и NS-получатель. Две сетевые секции соединяются с помощью звеньев обмена.

ПРИМЕЧАНИЕ. – "Сетевая секция" приближенно эквивалентна термину "cloud" (облако, сеть), определенному в [b-IETF RFC 2330].

Любой набор хостов, взаимно соединенных звеньями, может рассматриваться как сетевая секция. Однако для (будущих) целей назначения IP-рабочих характеристик будет уместно сосредоточиться на наборе хостов и звеньев, находящихся под одной (или совместной) полномочной ответственностью (например, поставщика услуг интернета (ПУИ) или поставщика сетевых услуг (NSP)). Эти хосты обычно имеют один и тот же идентификатор сети в своих IP-адресах. Обычно они имеют собственные правила внутренней маршрутизации. Выбор маршрутизации к получателям за пределами такой сетевой секции (к другой NS через звенья обмена) диктуется глобальными процессами и местной политикой. Эти сетевые секции обычно ограничиваются маршрутизаторами, которые реализуют внешние IP-протоколы шлюза.

5.2.3 NS-источник

NS-источник – это NS, которая содержит SRC, находящийся под ее полномочной ответственностью. В некоторых случаях SRC является единственным хостом в NS-источнике.

5.2.4 NS-получатель

NS-получатель – это NS, которая содержит DST, находящийся под ее полномочной ответственностью. В некоторых случаях DST является единственным хостом в NS-получателе.

На рисунке 4 показаны возможности соединения сети, относящиеся к IP-службе, между SRC и DST. Маршрутизаторы-шлюзы на границах каждой NS получают и передают пакеты через звенья обмена.

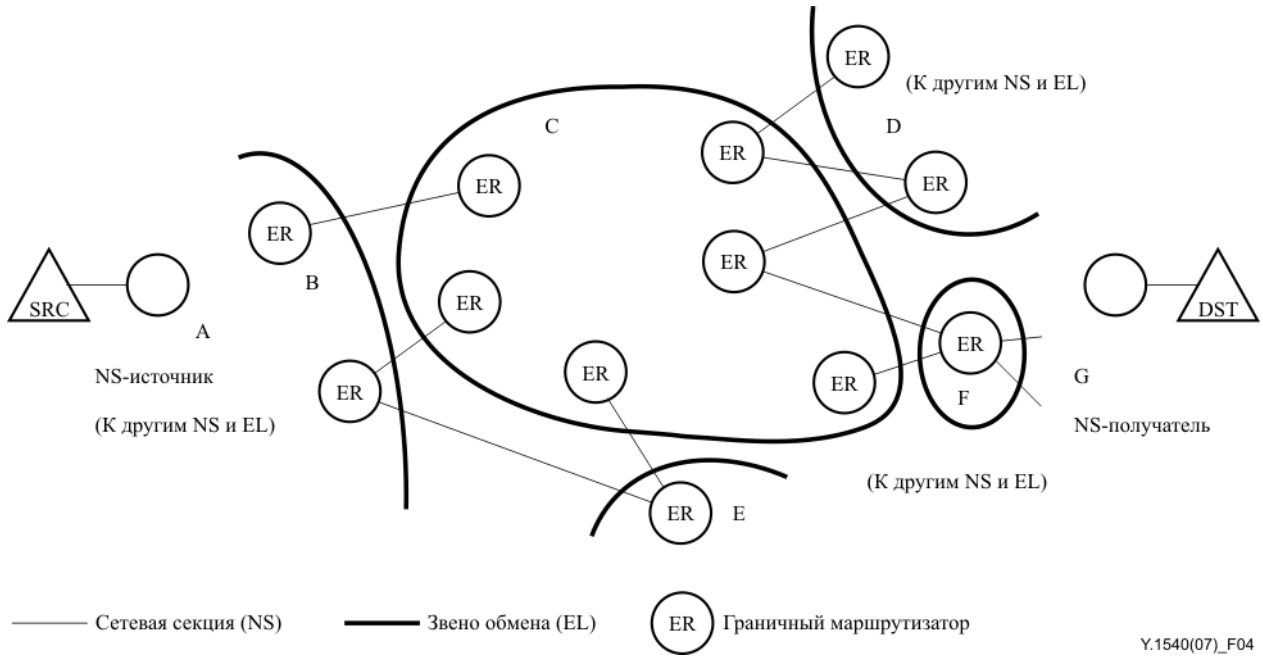


Рисунок 4 – Возможности соединения IP-сети

5.3 Пункты измерения и измеряемые секции

5.3.1 Пункт измерения (MP)

Пункт измерения – это граница между хостом и смежным звеном, на которой могут наблюдаться и измеряться эталонные рабочие параметры. В пункте измерения IP-службы (MP) может соблюдаться стандартный протокол Интернет, согласующийся с [b-ITU-T I.353]. Более подробная информация об MP для цифровых услуг содержится в [b-ITU T I.353].

ПРИМЕЧАНИЕ. – Вопрос точного местоположения MP IP-службы в стеке протокола IP подлежит дальнейшему изучению.

Секцию или комбинацию секций можно измерить, если она ограничена набором MP. Согласно настоящей Рекомендации можно измерять следующие секции.

5.3.2 Базовая секция

Базовые секции представляют собой EL, NS, SRC или DST. Базовые секции ограничиваются MP.

Рабочие характеристики любой EL или NS можно измерить относительно любой конкретной однонаправленной сквозной IP-службы. *Входные MP* представляют собой набор MP, через которые проходят пакеты из этой службы при их вхождении в базовую секцию. *Выходные MP* представляют собой набор MP, через которые проходят пакеты из этой службы при выходе из базовой секции.

5.3.3 Сквозная IP-сеть

Набор EL и NS, которые обеспечивают транспортировку IP-пакетов, передаваемых из SRC в DST. Пунктами MP, которые связывают сквозные IP-сети, являются MP в SRC и DST.

Рабочие параметры сквозной IP-сети могут измеряться относительно любой конкретной однонаправленной сквозной IP-службы. К *входным MP* относятся те MP, через которые проходят пакеты из этой службы при их поступлении в сквозную сеть в SRC. К *выходным MP* относятся те MP, через которые проходят пакеты из этой службы при выходе из сквозной сети в DST.

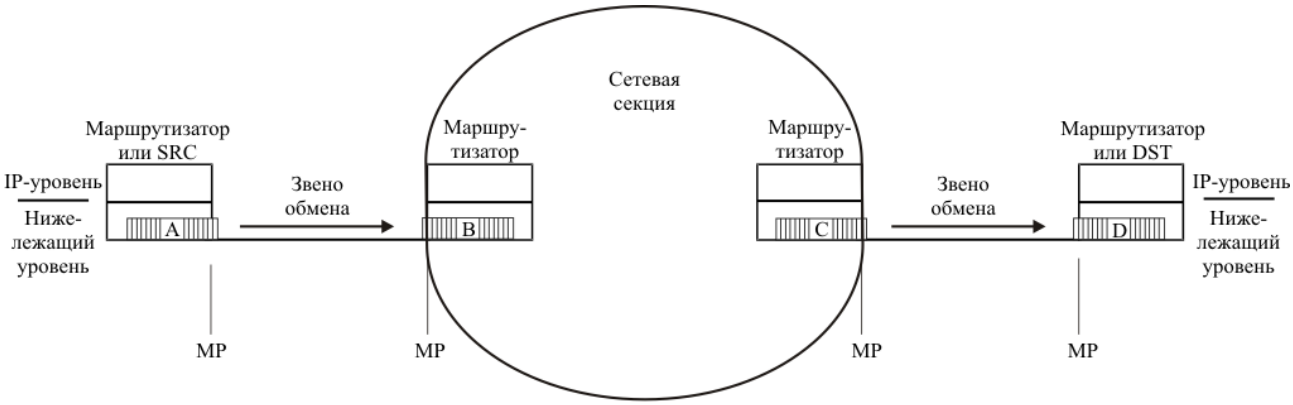
5.3.4 Совокупность сетевых секций (NSE)

Совокупностью сетевых секций (NSE) называется любой соединенный набор NS вместе со всеми соединяющими их EL. Термин "NSE" может использоваться для обозначения одной NS, двух NS или любого числа NS и соединяющих их EL. Пара различных NSE соединяется звеньями обмена. Термин "NSE" может использоваться также для представления всей сквозной IP-сети. NSE ограничиваются MP.

Рабочие характеристики любой конкретной NSE могут измеряться относительно любой конкретной однонаправленной сквозной IP-службы. *Входные MP* представляют собой набор MP, через которые проходят пакеты от этой службы при их вхождении в данную NSE. *Выходные MP* представляют собой набор MP, через которые проходят пакеты от этой службы при выходе из данной NSE.

5.4 Эталонные события передачи IP-пакетов (IPRE)

В контексте настоящей Рекомендации к заданной сквозной IP-службе применимы следующие определения. Определяемые термины показаны на рисунке 5.



ПРИМЕЧАНИЕ 1. – События выхода IP-пакета для пакетов A и C.
ПРИМЕЧАНИЕ 2. – События выхода IP-пакета для пакетов B и D.

Y.1540(07)_F05

Рисунок 5 – Пример эталонных событий передачи IP-пакетов

Событие передачи IP-пакета происходит, когда:

– IP-пакет проходит через MP; и

– стандартные IP-процедуры, применяемые к пакету, подтверждают, что контрольная сумма заголовка является действительной; и

– поля адресов отправителя и получателя в заголовке IP-пакета представляют собой IP-адреса предполагаемых SRC и DST.

ПРИМЕЧАНИЕ. – Заголовок IP-пакета содержит информацию, включающую тип службы (ToS) или указатель кода дифференцированных служб (DSCP). Вопрос о том, как такая информация может повлиять на рабочие характеристики при передаче пакетов, подлежит дальнейшему изучению.

Эталонные события передачи IP-пакетов определяются безотносительно фрагментации пакетов. Они относятся к каждому IP-пакету, проходящему через любой MP, независимо от значения, содержащегося во флаге "дополнительные фрагменты".

Определены четыре типа событий передачи IP-пакетов.

5.4.1 Событие входа IP-пакета в хост

Событие входа IP-пакета в хост при передаче IP-пакетов происходит, когда пакет проходит через MP на входе в хост (маршрутизатор NS или DST) из подключенного EL.

5.4.2 Событие выхода IP-пакета из хоста

Событие выхода IP-пакета из хоста при передаче IP-пакетов происходит, когда IP-пакет проходит через MP, выходя из хоста (маршрутизатор NS или SRC) в подключенное EL.

5.4.3 Событие входа IP-пакета в базовую секцию или NSE

Событие входа IP-пакета в базовую секцию или NSE при передаче IP-пакетов происходит, когда IP-пакет проходит через входной MP в базовую секцию или NSE.

5.4.4 Событие выхода IP-пакета из базовой секции или NSE

Событие выхода IP-пакета из базовой секции или NSE при передаче IP-пакета происходит, когда IP-пакет проходит через выходной MP из базовой секции или NSE.

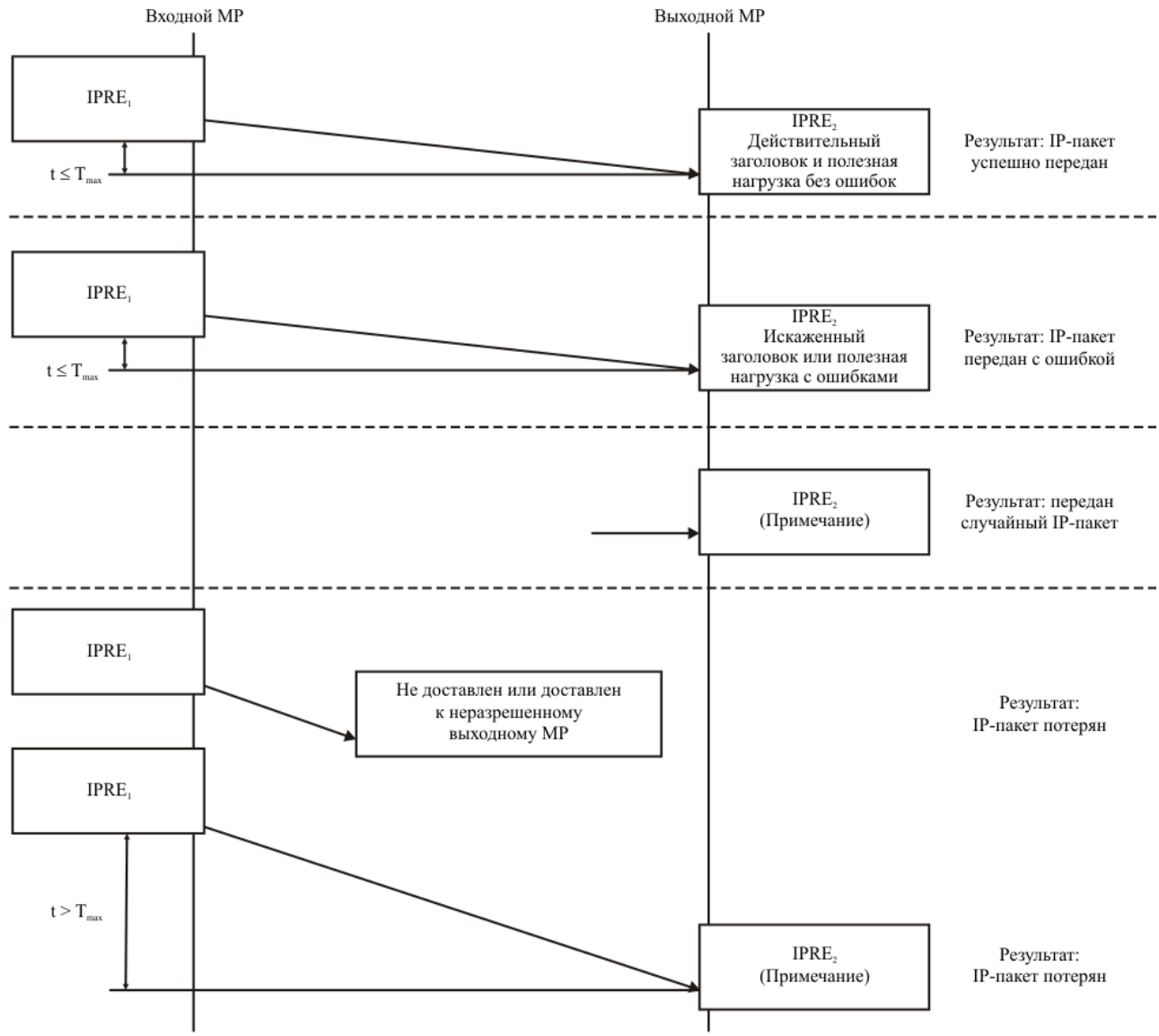
ПРИМЕЧАНИЕ 1. – События входа и выхода IP-пакета всегда представляют собой вход в хост и выход из хоста соответственно. События входа IP-пакета и события выхода IP-пакета всегда представляют собой вход в секцию или NSE и выход из секции или NSE. Для иллюстрации этого следует заметить, что вход в EL создает событие выхода из предыдущего хоста, тогда как вход в NS является событием входа, поскольку по определению NS всегда имеют хосты на своих границах.

ПРИМЕЧАНИЕ 2. – Для целей практических измерений эталонные события передачи IP-пакетов не должны наблюдаться в рамках стека IP-протоколов хоста. Вместо этого время появления таких эталонных событий может быть приблизительно определено путем наблюдения IP-пакетов, проходящих через соответствующий физический интерфейс. Однако такой физический интерфейс должен быть расположен как можно ближе к требуемому MP. В тех случаях, когда эталонные события контролируются на физическом интерфейсе, время возникновения события выхода из хоста приближенно определяется путем наблюдения первого бита IP-пакета, поступающего из хоста или из испытательного оборудования. Время возникновения события входа в хост приближенно определяется путем наблюдения последнего бита IP-пакета, поступающего в хост или в испытательное оборудование.

5.5 Результаты передачи IP-пакетов

Рассматривая эталонные события передачи IP-пакетов, можно определить ряд возможных результатов передачи для любого IP-пакета, пытающегося пройти через базовую секцию или NSE. Передаваемый IP-пакет будет либо *успешно передан*, либо *передан с ошибкой*, либо *потерян*. Доставленный IP-пакет, для которого не было выдано соответствующего исходного IP-пакета, считается *случайным*. На рисунке 6 показаны результаты передачи IP-пакетов.

Определение результатов передачи IP-пакетов основывается на концепциях *разрешенных входных MP, разрешенных выходных MP* и *соответствующих пакетов*.



ПРИМЕЧАНИЕ. – Результат определяется независимо от содержимого IP-пакета

Рисунок 6 – Результаты передачи пакетов

5.5.1 Глобальная информация маршрутизации и допустимые выходные звенья

Теоретически в присоединенной IP-сети пакет может быть доставлен в любой маршрутизатор, NS или NSE и все равно поступить к получателю. Однако в рамках глобальной информации маршрутизации определяется ограниченный набор адресов получателей, которые каждая сеть (автономная система) готова и способна обслуживать от имени каждой из примыкающих к ней NS. Разумно предположить, что (в худшем случае) NS будет полностью отбрасывать любые пакеты с адресами получателей о неспособности (или неготовности) обслуживать, которые она объявила. Поэтому все IP-пакеты (и фрагменты пакетов), выходящие из базовой секции, должны продвигаться к другим базовым секциям только так, как это *допускается* имеющейся глобальной информацией маршрутизации.

С точки зрения рабочих характеристик транспортировка IP-пакета совокупностью NSE может рассматриваться как успешная только в том случае, если данная NSE продвигает все содержимое пакета к другим базовым секциям, как это допускается имеющейся в настоящее время глобальной информацией маршрутизации. Если адрес получателя соответствует адресу хоста, подключенного непосредственно к данной NSE, то единственно допустимый успешный результат и единственный успешный способ передачи IP-пакетов состоит в их продвижении к хосту-получателю.

ПРИМЕЧАНИЕ 1. – Процедуры IP включают обновление глобальной информации маршрутизации. NS, которая раньше была допустимой, может больше не быть допустимой после обновления этой информации маршрутизации, которая совместно используется NS. И наоборот, NS, которая прежде была недопустимой, может стать допустимой после обновления глобальной информации маршрутизации.

ПРИМЕЧАНИЕ 2. – Информация маршрутизации может быть дополнена информацией об относительной пригодности каждого из разрешенных выходных звеньев. Влияние этой дополнительной информации на рабочие характеристики подлежит дальнейшему изучению.

В любой заданный момент времени относительно заданной сквозной IP-службы и базовой секции или NSE:

– входной MP является *разрешенным входным MP*, если прохождение через этот MP в данную базовую секцию или в NSE разрешено глобальной информацией маршрутизации;

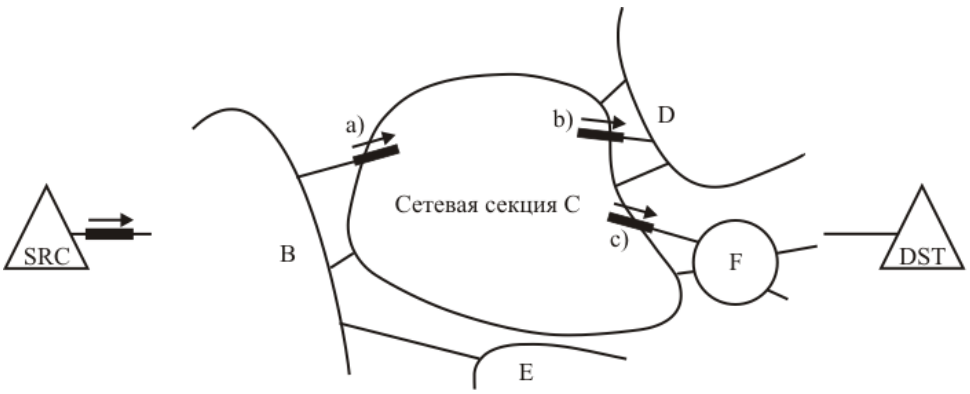
– выходной MP является *разрешенным выходным MP*, если прохождение через этот MP ведет к другой базовой секции, что разрешено глобальной информацией маршрутизации.

5.5.2 Соответствующие события

Для анализа рабочих характеристик необходимо увязывать пакеты, проходящие через один MP, с пакетами, проходящими через другой MP. Маршрутизация без установления соединения означает, что пакет может выйти из базовой секции по любому одному из (возможно) нескольких разрешенных выходных MP. Фрагментация пакета означает, что пакет, входящий в базовую секцию, может поступить из нее во фрагментах в несколько других базовых секций. И наконец, при IP-маршрутизации в режиме без установления соединения пакет или его фрагмент может быть даже послан обратно в базовую секцию, которую он уже прошел (возможно, из-за обновления таблиц маршрутизации).

Считается, что событие выхода IP-пакета *соответствует* более раннему событию входа, если они были обусловлены "одним и тем же IP-пакетом". Эта концепция применима независимо от того, является ли пакет на выходном MP целым пакетом или только фрагментом первоначального пакета. На рисунке 7 приведен пример, где пакет входит в NS C из NS B и фрагментируется на две части в NS C. Один из фрагментов передается в NS D, а другой – в NS F. Оба этих события выхода *соответствуют* одному событию входа. Во избежание путаницы из-за повторного входа пакетов в NSE данная концепция *соответствия* требует также, чтобы это был первый раз (с момента входа), когда конкретное содержимое было выведено из NSE.

Определение на практике соответствия эталонных событий передачи IP-пакетов обычно является *специальным* и часто может основываться на IP-адресах, глобальной информации маршрутизации, поле идентификации IP-пакета, другой информации заголовка и содержимом IP-пакета.



IP-пакет, передаваемый из SRC в DST, входит в NS C, создает событие входа, фрагментируется и образует два соответствующих события выхода – b) и c).

Y.1540(07)_F07

Рисунок 7 – Соответствующие события при выполнении фрагментации

5.5.3 Замечания относительно определений результатов "успешная передача пакетов", "ошибочный пакет", "потерян пакет" и "случайный пакет"

Каждое из следующих определений результатов передачи отдельных пакетов основывается на наблюдении эталонных событий передачи IP-пакетов в пунктах измерения IP. Путем выбора подходящих пунктов измерений IP каждое определение можно использовать для оценки характеристик конкретного EL, конкретной NS, конкретной NSE, и эти определения можно применить к оценке рабочих характеристик сквозных служб.

Эти результаты определяются без наложения ограничений на конкретный тип пакета (ToS, DSCP, протокол и т. д.). Рабочие характеристики IP-службы будут различаться в зависимости от типа пакетов.

В каждом определении возможность фрагментации пакетов принимается во внимание путем учета возможности того, что отдельное эталонное событие передачи IP-пакета может привести к нескольким последующим событиям. Следует отметить, что, если какой-либо фрагмент потерян, весь исходный пакет считается потерянным. Если ни один из фрагментов не потерян, но некоторые из них получены с ошибками, весь исходный пакет считается ошибочным. Для того чтобы доставка исходного пакета рассматривалась как успешная, каждый фрагмент должен быть успешно доставлен на один из разрешенных выходов EL.

5.5.4 Результат "успешная передача IP-пакетов"

Результат "успешная передача пакетов" имеет место тогда, когда одно эталонное событие передачи IP-пакета в разрешенном входном MP_0 приводит к появлению одного соответствующего эталонного события (или нескольких таких событий) в одном (или нескольких) выходном MP_i, в пределах максимального периода времени T_{max} исходного эталонного события, и:

1) все выходные MP_i, где возникает соответствующее эталонное событие, являются разрешенными; и

2) в состав доставленного пакета (пакетов) входит все содержимое исходного пакета, наблюдаемое в MP_0; и

3) двоичное содержимое поля (полей) информации доставленного IP-пакета в точности соответствует содержимому исходного пакета; и

4) поле (поля) заголовка доставленного пакета (пакетов) действительно (действительны).

ПРИМЕЧАНИЕ. – В общем случае величину T_{max} рекомендуется установить в значение 3 секунды. Для некоторых глобальных сквозных маршрутов может потребоваться большее значение T_{max}, чтобы обеспечить адекватную возможность доставки пакетов с более длительным временем передачи. На практике используется значение 3 секунды.

5.5.5 Результат "ошибочный IP-пакет"

Результат "ошибочный пакет" получается, когда отдельное эталонное событие передачи IP-пакета в разрешенном входном MP_0 приводит к появлению одного соответствующего эталонного события (или нескольких таких событий) в одном (или нескольких) выходном (выходных) MP_i, в пределах максимального периода времени T_{max} исходного эталонного события, и:

1) все выходные MP_i, где возникает соответствующее эталонное событие, являются разрешенными; и

2) в состав доставленного пакета (пакетов) входит все содержимое исходного пакета, наблюдаемое в MP_0; и

3) либо:

   – двоичное содержимое поля (полей) информации доставленного IP-пакета не соответствует в точности содержимому исходного пакета; либо

   – одно или несколько полей заголовка доставленного пакета (пакетов) искажены.

ПРИМЕЧАНИЕ. – Большая часть пакетов с ошибочными заголовками, которые не обнаруживаются контрольной суммой заголовка на IP-уровне, может быть аннулирована или переадресована другими процедурами IP-уровня (например, по причине искажения адреса или полей ToS/DSCP). В результате ни одно из эталонных событий не будет создано для протоколов более высоких уровней, ожидающих поступления данного пакета. По причине отсутствия эталонного события передачи IP-пакета эти попытки передачи пакетов могут быть отнесены к

категории результатов "потерян пакет". Ошибочные заголовки, которые не приводят к аннулированию или неправильной адресации, могут рассматриваться как результат "ошибочный пакет".

5.5.6 Результат "потерян IP-пакет"

Результат "потерян IP-пакет" имеет место, когда происходит одно эталонное событие передачи IP-пакета на разрешенном входном MP_1, если часть или все содержимое, соответствующее этому входному пакету, не приводит к эталонному событию передачи IP-пакета на разрешенном выходном MP_n в течение времени T_{max}.

Результат "потерян IP-пакет" фактически может представлять собой один или несколько результатов "*неправильная адресация пакета"* (которые не были замечены), определенных ниже.

Неправильная адресация пакета происходит, когда отдельное эталонное событие передачи IP-пакета в разрешенном входном MP_0 приводит к возникновению одного соответствующего эталонного события (или нескольких таких событий) на одном (или нескольких) выходном (выходных) MP_i, в пределах максимального периода времени T_{max} исходного входного события, и:

1) в состав доставленного пакета (пакетов) входит все содержимое исходного пакета, наблюдаемое в MP_0; но
2) один или несколько выходных MP_i, где возникают соответствующие эталонные события, не является (не являются) разрешенным выходным MP (разрешенными выходными MP).

5.5.7 Результат "случайный IP-пакет"

Результат "случайный IP-пакет" имеет место для базовой секции или NSE в сквозной IP-службе, когда отдельный IP-пакет создает выходное событие, для которого не было соответствующего входного события.

5.5.8 Вторичные результаты передачи IP-пакетов

Следующие результаты базируются на описанных выше основных результатах.

5.5.8.1 Результаты "упорядоченные IP-пакеты" и "переупорядоченные IP-пакеты"

Определение этих результатов передачи IP-пакетов требует некоторого предварительного обсуждения.

Упорядоченная доставка пакетов – это свойство успешных попыток передачи пакетов, когда порядок, в котором отправляются пакеты, сохраняется по их поступлении в хост-получатель (или в пункт измерения). Порядок поступления пакетов определяется их позицией (положением) относительно других представляющих интерес пакетов, хотя степень переупорядочения данного пакета может быть количественно определена в единицах позиции, времени и расстояния в байтах полезной нагрузки. Параметр рабочей характеристики, определяющий переупорядочение пакетов, важен для большинства приложений, особенно при оценке поддержки сетью медиапотоков в режиме реального времени из-за их ограниченной способности восстанавливать порядок следования или когда рабочие характеристики подразумевают отсутствие такой возможности. Обычно пакеты содержат некоторый уникальный идентификатор, применяемый в SRC, который иногда считается порядковым номером, так что этот номер или другая информация (например, метки времени из MP_0) указывает на исходный порядок пакетов в источнике. Для оценки порядка поступления пакетов также требуется возможность определения того, какой конкретный пакет является "следующим ожидаемым" пакетом, а это значительно упрощается, когда порядковые номера представляют собой последовательные возрастающие целые числа.

Результат "упорядоченные пакеты" имеет место тогда, когда отдельное эталонное событие передачи IP-пакетов в разрешенном выходном пункте измерения приводит к следующему:

– порядковый номер пакета больше или равен следующему ожидаемому значению. В ответ на поступление этого пакета следующее ожидаемое значение увеличивается и становится новым ожидаемым значением.

Результат "переупорядоченные пакеты" имеет место тогда, когда отдельное эталонное событие передачи IP-пакетов в разрешенном выходном пункте измерения приводит к следующему:

– порядковый номер пакета меньше следующего ожидаемого значения, означая, что порядок следования пакетов был изменен. По поступлении этого пакета следующее ожидаемое значение не изменяется.

5.5.8.2 Результат "блок с серьезными потерями IP-пакетов"

Результат "блок с серьезными потерями IP-пакетов" (IPSLB) имеет место для блока пакетов, наблюдаемого в интервале времени T_s на входном MP_0, когда отношение потерянных пакетов в выходном MP_i к общему числу пакетов в блоке превышает величину s1.

Интервал времени T_s предварительно устанавливается в значение 10 секунд. Пороговая величина s1 предварительно устанавливается в значение 0,2. Оценка последовательных блоков (интервалов времени) не должна перекрывать эти значения.

ПРИМЕЧАНИЕ. – Эти значения предназначены для выявления изменений маршрута IP-пакетов из-за обновлений схемы маршрутизации, что вызывает значительное ухудшение качества работы большинства пользовательских приложений. Эти значения могут быть изменены после проведения дальнейших исследований и накопления опыта. Пониженные значения s1 приведут к захвату дополнительных событий сети, которые могут влиять на работу чувствительных к связности применений. Кроме того, значительное ухудшение работы аудио- и видеоприложений может хорошо коррелировать с результатом IPSLB при использовании длины блока T_s приблизительно в 1 секунду, а в будущем использование этого значения может оказаться важным.

Минимальное число пакетов, которое должно использоваться при оценке результата "блок с серьезными потерями", равно M_{lb}, и эти пакеты должны быть распределены в интервале T_s. Определение конкретного значения M_{lb} подлежит дальнейшему изучению.

5.5.8.3 Результат "дублирующий IP-пакет"

Результат "дублирующий пакет" представляет собой подмножество результатов "успешная передача пакета" и имеет место тогда, когда одно эталонное событие передачи IP-пакета в разрешенном входном MP_0 приводит к двум соответствующим эталонным событиям или более по крайней мере в одном разрешенном выходном MP_i, причем двоичная информация в полях всех выходных пакетов идентична информации исходного пакета. Выходное эталонное событие в MP_i для дублирующего пакета происходит после как минимум одного другого соответствующего выходного эталонного события для исходного пакета (обычно также в MP_i).

Следует отметить, что при связи пункта с пунктом существует только один разрешенный выходной MP_i, где хост-получатель подсоединен непосредственно к NSE. При связи пункта с многими пунктами может быть несколько разрешенных выходных MP_i для разных получателей.

5.5.8.4 Результат "дублируемый IP-пакет"

Результат "дублируемый IP-пакет" имеет место тогда, когда одно эталонное событие передачи IP-пакета в разрешенном входном MP_0 приводит к двум соответствующим эталонным событиям или более по крайней мере в одном разрешенном выходном MP_i, причем двоичная информация в полях всех выходных пакетов идентична информации исходного пакета. Выходное эталонное событие в MP_i для дублируемого пакета происходит впервые для данного исходного пакета и по крайней мере перед одним выходным эталонным событием для дублирующего пакета (обычно также происходящим в MP_i).

5.5.9 Результаты "восстановление потока IP-пакетов"

Следующие результаты базируются на основных результатах и предполагают дополнительный анализ на основе модели систем восстановления потока. Более подробная базовая информация по этой теме и рассматриваемым методам уменьшения нарушений (выше IP-уровня) содержится в Дополнении VII.

5.5.9.1 Простая модель восстановления потока на уровне приложений

В Дополнении VII также определяется простая модель, описанная ниже. Каждый поток пакетов уровня приложений моделируется как содержащий пакеты двух категорий:

- интервалы или блоки информационных пакетов;
- максимальное количество восстанавливаемых пакетов, связанных с информационным блоком.

Задача разработчика метода восстановления состоит в том, чтобы выбрать такой размер информационного блока в сочетании с (максимальной) возможностью восстановления, который будет достаточным для компенсации высокого процента нарушений в пакетной сети (потери, чрезмерная задержка и искажение) при работе в пределах общих ограничений пропускной способности при передаче пакетов в системе и при обеспечении достаточного качества в потоке приложения.

Новые параметры рабочих характеристик должны помочь в поиске таких решений.

5.5.9.2 Результаты "пакет с нарушениями" и "интервал IP-пакетов с нарушениями"

Результат "интервал IP-пакетов с нарушениями" возникает для набора пакетов, наблюдаемых в течение временного интервала T_I во входном MP_0, когда количество результатов "пакет с нарушениями" на выходном MP_i превышает величину x. Следует отметить, что временной интервал T_I включает в себя как информационные, так и служебные или восстановительные пакеты (если они встроены во входящий поток).

Результаты "пакет с нарушениями" представляют собой сумму следующих результатов:

- результаты "потерян пакет", полученные с использованием значения T_{max}, связанного с T_I и номинальным временем передачи и, возможно, равного минимальной задержке передачи пакетов для представляющей интерес совокупности, плюс (кратная) величина T_I. Сюда входят пакеты, слишком долго ожидавшие в очереди, а также так и не поступившие пакеты;
- результаты "ошибочный пакет".

Следует отметить, что одним из факторов, отличающих этот результат от других показателей, связанных с потерей/блокировкой пакетов, является объединение чрезмерно задержанных пакетов (с превышением порога вариации задержки) с так и не поступившими пакетами (действительно потерянными во время передачи) в одну категорию – "пакеты с нарушениями".

Предварительные значения временного интервала T_I и порога x не устанавливаются. Вместо этого анализ может включать диапазон значений для интервала T_I и порога x. Также должна быть указана длина полезной нагрузки IP-пакета, поскольку она влияет на время сериализации и, следовательно, на временной интервал, занимаемый блоком пакетов.

5.5.9.3 Результат "блок IP-пакетов с нарушениями"

Результат "*блок IP-пакетов с нарушениями*" имеет место тогда, когда для набора пакетов с размером блока b, наблюдаемых во входном MP_0, количество результатов "пакет с нарушениями" в блоке в выходном MP_i превышает величину x. Предварительные значения размера блока b и порога восстановления x не устанавливаются.

6 Параметры рабочих характеристик передачи IP-пакетов

В данном разделе определяется набор параметров рабочих характеристик передачи информации с использованием результатов передачи IP-пакетов, определенных в пункте 5.5. Все другие параметры могут быть оценены на основе наблюдений в MP, которые ограничивают базовую секцию или испытуемую NSE.

ПРИМЕЧАНИЕ. – Определения дополнительных параметров рабочих характеристик передачи IP-пакетов (например, коэффициент блоков IP-пакетов с серьезными ошибками) подлежат дальнейшему изучению.

6.1 Классификация пакетов

В данном пункте определяется основная терминология, используемая для определения применимости параметров рабочих характеристик к наборам пакетов.

6.1.1 Представляющая интерес совокупность

Большая часть параметров рабочих характеристик определяется через наборы пакетов, называемых *представляющими интерес совокупностями*. Для *случая сквозной связи* представляющая интерес совокупность – это обычно полный набор пакетов, передаваемых из SRC в DST. В случае сквозной связи пунктами измерения служат MP в SRC и DST.

Для базовой секции или NSE и относительно конкретной пары SRC и DST представляющая интерес совокупность в конкретном разрешенном входном MP – это набор пакетов, передаваемых из SRC в DST, которые маршрутизируются в базовую секцию или NSE через конкретный MP. Эта ситуация получила название *"специфический для входа случай"*.

Суммарная представляющая интерес совокупность для базовой секции или NSE относительно конкретной пары SRC и DST – это полный набор пакетов, передаваемых из SRC в DST, которые доставляются в секцию или NSE через любой из разрешенных входных MP. Эта ситуация получила название *"независимый от входа случай"*.

Каждый из этих параметров рабочих характеристик IP определен без ссылки на конкретный тип пакетов (ToS, DSCP, протокол и т. д.). Рабочие характеристики будут различаться по типам пакетов, и любые сообщения об измеренных рабочих характеристиках должны содержать информацию относительно типа или типов пакетов, входящих в данную совокупность.

6.1.2 Поток пакетов

Потоком пакетов является набор пакетов, связанный с заданным потоком, имеющим соединение или без логического соединения, который имеет одинаковые адрес хоста-источника (SRC), адрес хоста-получателя (DST), класс обслуживания и идентификатор сеанса (например, номера портов в протоколе более высокого уровня). В других документах при обращении к потокам с данной степенью классификации могут использоваться термины "микропоток" или "вложенный поток". Поток пакетов служит наиболее распространенным примером представляющей интерес совокупности.

В пакетах IPv6 имеется дополнительное поле, в котором хост-источник может помечать последовательности пакетов, подлежащих особой обработке в маршрутизаторах IPv6. Это поле называется меткой потока и в сочетании с адресом источника однозначно определяет поток пакетов.

6.2 Задержка передачи IP-пакетов

Задержка передачи IP-пакетов (IPTD) определена для всех результатов "успешная передача пакетов" и "ошибочный пакет" в базовой секции или NSE. Параметр IPTD представляет собой период времени ($t_2 – t_1$) между появлением двух соответствующих эталонных событий передачи IP-пакетов – входным событием $IPRE_1$ в момент t_1 и выходным событием $IPRE_2$ в момент t_2, где ($t_2 > t_1$) и ($t_2 – t_1$) ≤ T_{max}. Если пакет фрагментируется в пределах NSE, t_2 – это время последнего соответствующего выходного события. Задержка сквозной передачи IP-пакетов – это однонаправленная задержка между MP в SRC и DST, как показано на рисунке 8.

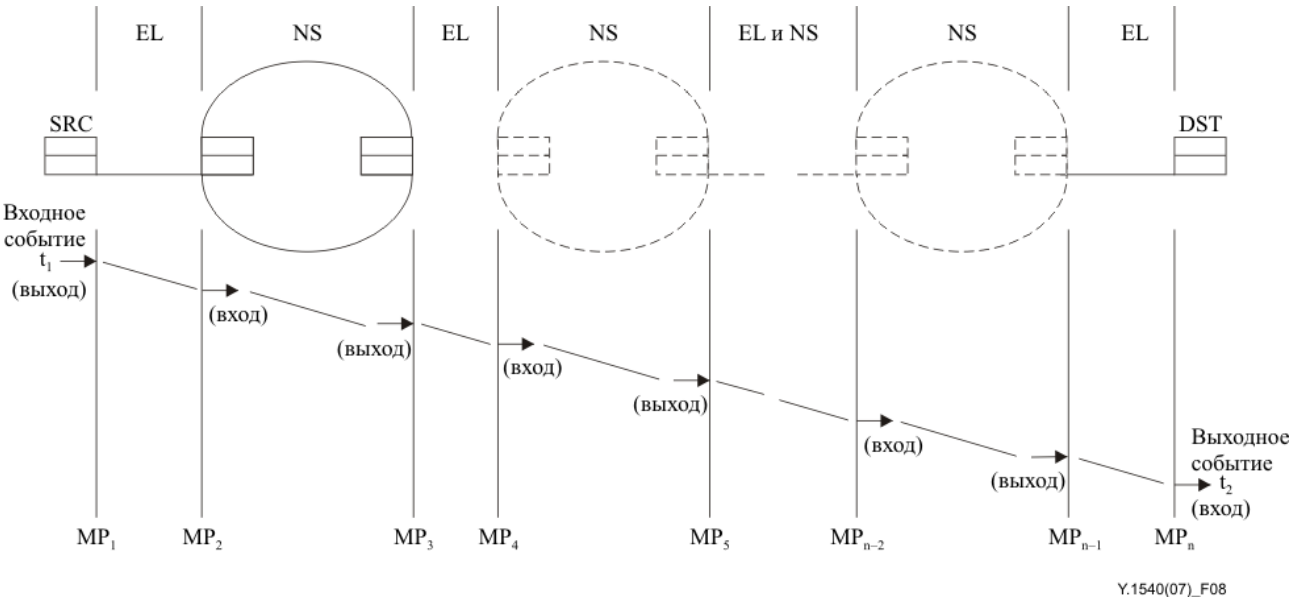


Рисунок 8 – События задержки при передаче IP-пакетов (показана сквозная передача одного IP-пакета)

6.2.1 Средняя задержка передачи IP-пакетов

Средняя задержка передачи IP-пакетов представляет собой среднее арифметическое задержек передачи IP-пакетов для представляющей интерес совокупности.

6.2.2 Минимальная задержка передачи IP-пакетов

Минимальная задержка передачи IP-пакетов – это наименьшее из всех значений задержки передачи IP-пакетов в представляющей интерес совокупности. Сюда относятся задержка распространения и задержки ожидания в очереди, общие для всех пакетов. Следовательно, этот параметр может не отражать теоретическую минимальную задержку на пути между MP.

6.2.3 Медианная задержка передачи IP-пакетов

Медианная задержка передачи IP-пакетов представляет собой 50-й процентиль частотного распределения значений задержки передачи IP-пакетов из представляющей интерес совокупности. Медиана – это серединное значение после ранжирования значений задержки передачи. Чтобы получить это серединное значение, когда совокупность содержит четное количество значений, используется среднее значение двух центральных значений.

6.2.4 Вариации задержек сквозной двухточечной передачи IP-пакетов

Вариации задержек передачи IP-пакетов также являются важным фактором. Потоковые приложения могут использовать информацию обо всем диапазоне вариаций задержек IP-пакетов для исключения недогрузки и перегрузки буферов. Экстремальные вариации задержек IP-пакетов могут привести к увеличению порогов таймера повторных передач TCP, а также задержать повторные передачи IP-пакетов или вызвать ненужную повторную передачу пакетов.

Вариации задержек IP-пакетов (PDV) при сквозной двухточечной передаче определяются на основе наблюдений поступления соответствующих IP-пакетов на входные и выходные MP (например, MP_{DST}, MP_{SRC}). Эти наблюдения характеризуют варьируемость в комбинации событий поступления IP-пакетов на выходных MP относительно комбинации соответствующих событий на входном MP по отношению к эталонной задержке.

PDV (v_k) при двухточечной передаче IP-пакета k между SRC и DST представляет собой разницу между абсолютной задержкой передачи IP-пакетов (x_k) пакета k и определенной эталонной задержкой передачи IP-пакетов $d_{1,2}$ между теми же MP (см. рисунок 9): $v_k = x_k – d_{1,2}$.

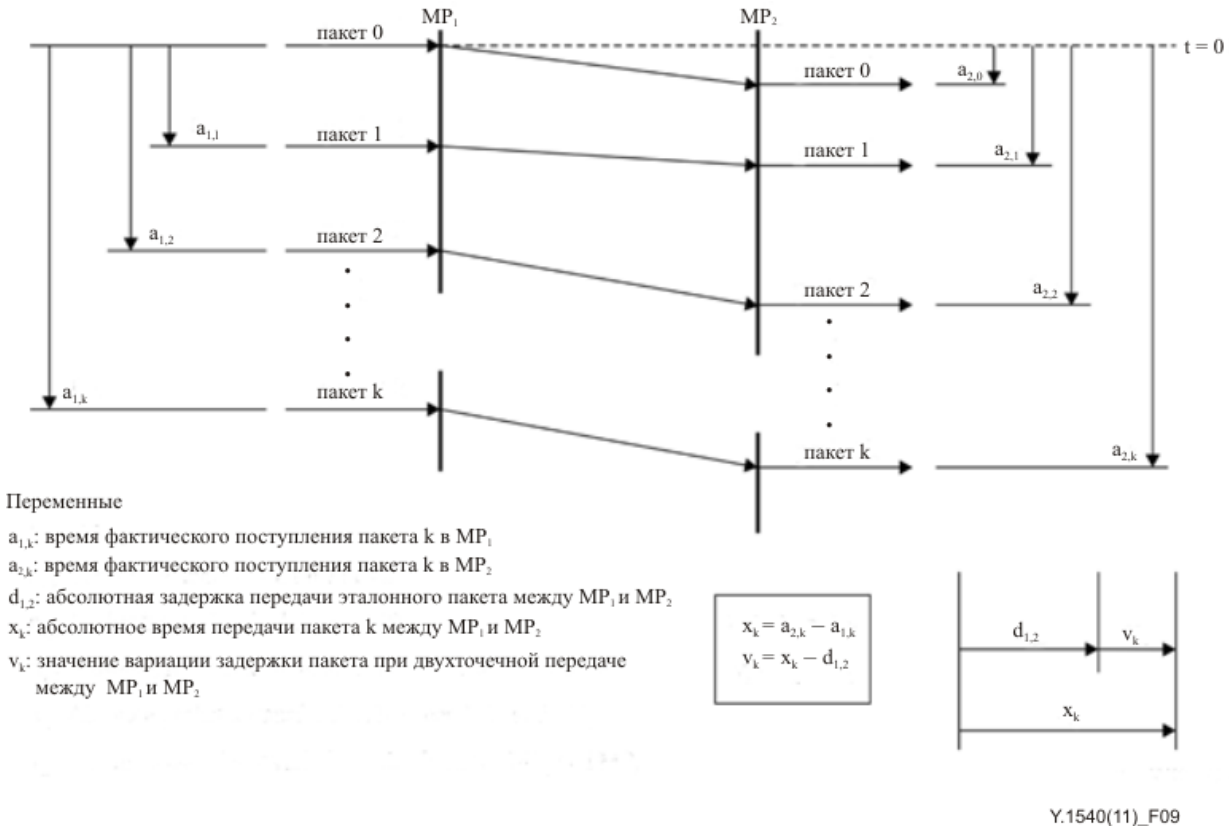


Рисунок 9 – Вариация задержки IP-пакетов при двухточечной передаче

Эталонная задержка передачи IP-пакетов, $d_{1,2}$, между SRC и DST – это абсолютная задержка передачи IP-пакетов, которой подвергается выбранный IP-пакет между этими двумя MP.

Положительные значения вариации задержки IP-пакетов (IPDV) при двухточечной передаче соответствуют задержкам передачи IP-пакетов, превышающим те, которым подвергается эталонный IP-пакет; отрицательные значения при двухточечной передаче соответствуют задержкам передачи пакетов меньше тех, которым подвергается эталонный IP-пакет. Распределение PDV при двухточечной передаче идентично распределению абсолютных задержек передачи IP-пакетов, выражаемых постоянным значением, равным $d_{1,2}$.

6.2.4.1 Использование минимальной задержки в качестве основы для определения вариаций задержек

Как показано на рисунке 9, вариация задержек отдельного пакета естественно определяется как разница между фактической задержкой, которой подвергается пакет, и номинальной или эталонной задержкой. Предпочтительной эталонной задержкой (которая используется в требованиях к IPDV в Рекомендации МСЭ-Т Y.1541) является минимальная задержка представляющей интерес совокупности. Это гарантирует, что все вариации будут регистрироваться как положительные значения, и упрощает отчетность о диапазоне вариации (максимальное значение вариации равно диапазону). Распределения вариации задержки в IP-сетях часто демонстрируют смещение в сторону минимума (например, минимум и мода равны). Многие другие полезные возможности этой формы вариации задержки – PDV с использованием минимальной задержки в качестве эталонной – подробно описаны в [IETF RFC 5481].

Использование средней задержки в качестве эталонной вариации задержки в данной версии настоящей Рекомендации не рекомендуется.

В предыдущих версиях настоящей Рекомендации альтернативой использованию минимальной задержки пакета в качестве номинальной или эталонной задержки служило использование в качестве таковой средней задержки представляющей интерес совокупности. Это сказывается на центрировании распределения значений вариации задержек на нулевом уровне (если распределение является симметричным) и приводит как к положительным, так и к отрицательным значениям вариации. Вместе

с тем средняя задержка совокупности может заметно отличаться от задержки любого отдельного пакета, что создает искусственный эталон для вариации (например, когда присутствует бимодальное распределение).

6.2.4.2 Пределы вариации задержек IP-пакетов, основанные на квантилях

Предпочтительным методом обобщения вариаций задержек представляющей интерес совокупности (который используется в требованиях МСЭ-T Y.1541) является выбор верхнего и нижнего квантилей распределения вариаций задержек с последующим измерением расстояния между этими квантилями. Например, выбрать квантиль $1–10^{-3}$ и нулевой квантиль (или минимум), провести измерения и определить разницу между значениями вариаций задержек при этих двух квантилях. Этот пример может помочь разработчикам приложений определить размер буфера компенсации вариации задержки, чтобы перегрузка общей буферной емкости не превышала 0,1%.

Норма вариации задержек передачи IP-пакетов может быть установлена путем выбора верхней границы для разницы между заранее определенными квантилями распределения вариации задержек. Например, "Разница между квантилем 99,9 и минимумом вариации задержек пакета не должна превышать 50 мс".

6.2.4.3 Пределы вариации задержек передачи IP-пакетов, основанные на интервале

Альтернативным методом обобщения вариаций задержек передачи IP-пакетов, которым подвергается представляющая интерес совокупность, служит предварительное определение интервала вариации задержек, например 50 мс, и последующее наблюдение процента вариаций задержек отдельного пакета, которые находятся внутри и за пределами этого интервала. При использовании интервала 50 мс приложение с буфером фиксированного размера, равного или близкого к 50 мс, может затем приблизительно узнать, сколько пакетов может вызвать перегрузку или недогрузку буферов.

ПРИМЕЧАНИЕ. – Если этот метод используется для обобщения вариаций задержек IP-пакетов, то вариант задержек отдельных пакетов должен быть вычислен с использованием минимальной задержки в качестве номинальной, как определено в пункте 6.2.4.1, вместо использования первого пакета, как определено в пункте 6.2.4. При использовании определения из пункта 6.2.4 предварительно определенный интервал (например, 50 мс) может быть случайно зафиксирован на необычно большом или малом значении.

Норма вариации задержек передачи IP-пакета может быть установлена путем выбора нижней границы для процента вариаций задержек отдельного пакета, которые попадают в заранее определенный интервал. Например, "$\geq$ 99,9% вариаций задержек пакета должны находиться в интервале [0 мс, 50 мс]".

6.2.4.4 Вторичные параметры для вариации задержек передачи IP-пакетов

Один или несколько параметров, которые охватывают влияние вариации задержек передачи IP-пакетов на различные приложения, могут оказаться полезными. Они могут оказаться пригодными для дифференциации (обычно небольших) межпакетных вариаций задержек из потенциально более длительных перерывов в задержках, которые могут возникнуть в результате изменений в маршрутизации IP-пакетов. В Дополнении II приведены несколько производных определений вариации задержек и руководящие указания по их применению.

6.3 Коэффициент ошибочных IP-пакетов (IPER)

Коэффициент ошибочных IP-пакетов (IPER) – это отношение общего количества результатов передачи ошибочных IP-пакетов к общему количеству результатов успешной передачи IP-пакетов плюс результаты "ошибочные IP-пакеты" в представляющей интерес совокупности.

6.4 Коэффициент потери IP-пакетов (IPLR)

Коэффициент потери IP-пакетов (IPLR) – это отношение общего количества результатов потерянных IP-пакетов к общему количеству переданных IP-пакетов в представляющей интерес совокупности.

ПРИМЕЧАНИЕ. – Показатели для описания моделей односторонних потерь приведены в [b-IETF RFC 3357]. Последовательная потеря пакетов представляет особый интерес для некоторых неэластичных приложений реального времени, таких как передача голоса и видео.

6.5 Коэффициент случайных IP-пакетов

Коэффициент случайных IP-пакетов в выходном MP представляет собой общее число случайных IP-пакетов, наблюдаемых в данном выходном MP в течение заданного интервала времени, деленное на длительность интервала времени (эквивалентно – на число случайных IP-пакетов на секунду обслуживания)[1].

6.6 Коэффициент переупорядоченных IP-пакетов (IPRR)

Коэффициент переупорядоченных IP-пакетов (IPRR) – это отношение общего количества результатов с нарушением порядка следования пакетов к общему количеству успешных результатов передачи IP-пакетов в представляющей интерес совокупности.

На рисунке 10 представлены результат с нарушением пакетом 2 порядка следования пакетов и гипотетический допуск по времени поступления в случае применения буфера воспроизведения, позволяющего восстановить первоначальный порядок.

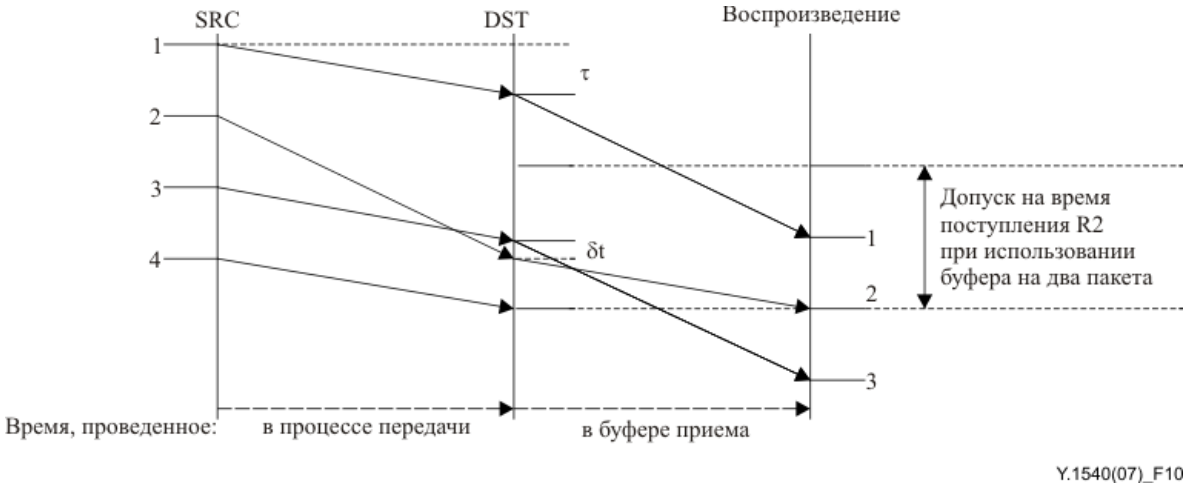


Рисунок 10 – Иллюстрация поступления с нарушением порядка следования

Если можно различить отдельные события переупорядочения, то можно также представить информацию о количестве событий (вместе с их критериями).

Кроме того, можно установить степень переупорядочения пакетов. Любой пакет, порядковый номер которого приводит к увеличению следующего ожидаемого значения больше чем на стандартное приращение, указывает на нарушение порядка поступления. С этого момента можно подсчитывать все (переупорядоченные) пакеты с порядковыми номерами меньше следующего ожидаемого значения, учитывая при этом расстояние от нарушившего порядок пакета. Это расстояние можно выразить в позициях, единицах времени или суммой байтов полезной нагрузки промежуточных пакетов. Например, на рисунке 10 пакет 2 "опаздывает" на δt секунд или на одну позицию пакета.

Дополнительные параметры переупорядочения определены в [IETF RFC 4737].

6.7 Коэффициент блоков с серьезными потерями IP-пакетов (IPSLBR)

Коэффициент блоков с серьезными потерями IP-пакетов (IPSLBR) представляет собой отношение результатов "блоки с серьезными потерями IP-пакетов" к общему количеству блоков в представляющей интерес совокупности.

ПРИМЕЧАНИЕ. – Этот параметр может идентифицировать множество изменений маршрута IP-пакетов, обусловленных обновлениями маршрутизации, и иначе называется нестабильностью маршрута. Нестабильность маршрута вызывает значительное ухудшение качества большинства приложений пользователя.

---

[1] Поскольку предполагается, что механизмы, которые вызывают появление случайных IP-пакетов, слабо связаны с количеством IP-пакетов, передаваемых через испытуемые секции, этот рабочий параметр рассматривается не как отношение, а только как коэффициент.

6.8 Коэффициент дублирующих IP-пакетов (IPDR)

Коэффициент дублирующих IP-пакетов (IPDR) – это отношение общего количества результатов "дублирующий IP-пакет" к общему количеству успешных результатов передачи IP-пакетов за вычетом результатов "дублирующий IP-пакет" в представляющей интерес совокупности.

6.9 Коэффициент дублируемых IP-пакетов (RIPR)

Коэффициент дублируемых IP-пакетов (RIPR) – это отношение общего количества результатов "дублированный IP-пакет" к общему количеству успешных результатов передачи IP-пакетов за вычетом результатов "дублированный IP-пакет" в представляющей интерес совокупности.

6.10 Параметры восстановления потока

В идеале хотелось бы знать вероятность того, что данный интервал пакетов (или информационный блок b) будет содержать более чем x пакетов с нарушениями.

$$P(b, x) = p, \text{ или } P(T_I, x) = p.$$

Измерение результатов "пакет с нарушениями" в *представляющей интерес совокупности* обеспечило бы эмпирическую оценку вероятности в течение времени доступности.

6.10.1 Коэффициент интервалов IP-пакетов с нарушениями (IPIIR)

Коэффициент интервалов IP-пакетов с нарушениями представляет собой отношение количества результатов "интервал IP-пакетов с нарушениями" к общему количеству неперекрывающихся интервалов в представляющей интерес совокупности.

6.10.2 Коэффициент блоков IP-пакетов с нарушениями (IPIBR)

Коэффициент блоков IP-пакетов с нарушениями (IPIBR) представляет собой отношение количества результатов "блок IP-пакетов с нарушениями" к общему количеству неперекрывающихся блоков в представляющей интерес совокупности.

6.11 Параметры пропускной способности

Служба сквозной передачи IP-пакетов прокладывает путь через упорядоченную последовательность базовых секций от хоста-источника к хосту-получателю. Описанные ниже параметры пропускной способности определяют свойства базовых секций с точки зрения их способности передавать IP-трафик и соответствующие свойства NSE, также называемых "маршрутами". Важно отметить, что базовая секция, равно как и последовательность базовых секций, связана с определенным направлением. Направление важно, поскольку свойства последовательности секций в прямом направлении могут быть не такими, как в обратном направлении.

Следует отметить, что в отличие от параметров, связанных с потоком и определенных в пункте 6.12, параметры, связанные с пропускной способностью, не зависят от протоколов более высокого уровня поверх IP (например, TCP). Следует также отметить, что параметры используемой пропускной способности, степени использования и доступной пропускной способности не поддаются внешнему измерению, и требуется поддержка со стороны систем мониторинга с доступом к измерениям степени использования звеньев и т. д.

6.11.1 Показатели секции

6.11.1.1 Число переданных битов IP-уровня

Для данной представляющей интерес совокупности число переданных битов IP-уровня определяется как восьмикратное количество октетов во всех IP-пакетах с результатом "успешная передача IP-пакетов" в выходном пункте измерения, начиная с первого октета заголовка IP и до последнего октета полезной нагрузки IP-пакета включительно.

Следует отметить, что это определение идентично определению числа битов IP-уровня, приведенному в [IETF RFC 5136]. Следует также отметить, что определение битов IP-уровня не зависит от версии IP.

6.11.1.2 Пропускная способность секции IP-уровня

Для данной представляющей интерес совокупности пропускная способность секции IP-уровня составляет:

$$C(t,\Delta t) = \frac{n_0(t,\Delta t)}{\Delta t}$$

где n_0 – наибольшее (общее) количество битов IP-уровня, которое может быть передано по базовой секции с результатом "успешная передача IP-пакета" в выходном пункте измерения в течение заданного интервала времени $[t, t + \Delta t]$.

Следует отметить, что это концептуальное определение, а не показатель, который можно многократно измерять. Выражение "наибольшее количество" битов несколько расплывчато, за исключением случаев повторных оценок. Скорее всего, это относится к сумме битов в успешных результатах передачи в течение интервала $[t, t + \Delta t]$. Нормативное определение измеримой пропускной способности секции IP-уровня см. в Приложении A.

6.11.1.3 Используемая пропускная способность секции IP-уровня

Для данной представляющей интерес совокупности используемая пропускная способность секции IP-уровня составляет:

$$U(t,\Delta t) = \frac{n(t,\Delta t)}{\Delta t},$$

где n – фактическое количество битов IP-уровня, которое может быть передано по базовой секции с результатом "успешная передача IP-пакета" в выходном пункте измерения в течение заданного интервала времени $[t, t + \Delta t]$.

6.11.1.4 Степень использования секции IP-уровня

Для данной представляющей интерес совокупности степень использования секции IP-уровня, $V(t, \Delta t)$, определяется как отношение используемой пропускной способности секции IP-уровня $U(t, \Delta t)$ к пропускной способности секции IP-уровня $C(t, \Delta t)$, то есть:

$$V(t,\Delta t) = U(t,\Delta t) / C(t,\Delta t).$$

6.11.1.5 Доступная пропускная способность секции IP-уровня

Для данной представляющей интерес совокупности доступная пропускная способность секции IP-уровня, $A(t, \Delta t)$, представляет собой неиспользованную часть пропускной способности секции IP-уровня в течение интервала времени $[t, t + \Delta t]$. Ее можно рассчитать как разность пропускной способности секции IP-уровня и используемой пропускной способности секции IP-уровня, то есть:

$$A(t,\Delta t) = C(t,\Delta t) - U(t,\Delta t)$$

или, что то же самое,

$$A(t,\Delta t) = C(t,\Delta t)(1 - V(t,\Delta t)).$$

6.11.2 Показатели NSE

6.11.2.1 Пропускная способность NSE IP-уровня

Определение пропускной способности секции IP-уровня можно распространить на NSE, также называемую маршрутом. Для данной представляющей интерес совокупности пропускная способность NSE IP-уровня $C_{NSE}(t, \Delta t)$ в течение заданного интервала времени $[t, t + \Delta t]$ определяется как наименьшая пропускная способность секции IP-уровня вдоль этой NSE. То есть пропускная способность NSE IP-уровня составляет:

$$C_{NSE}(t,\Delta t) = \min_{i=1..n} C_i(t,\Delta t),$$

где C_i – пропускная способность секции IP-уровня секции с номером i ($i = 1..n$) в NSE.

6.11.2.2 Доступная пропускная способность NSE IP-уровня

Определение доступной пропускной способности секции IP-уровня можно распространить на NSE, также называемую маршрутом. Для данной представляющей интерес совокупности доступная пропускная способность NSE IP-уровня $A_{NSE}(t, \Delta t)$ в течение заданного интервала времени $[t, t + \Delta t]$ определяется как наименьшая доступная пропускная способность секции IP-уровня вдоль этой NSE, то есть:

$$A_{NSE}(t, \Delta t) = \min_{i=1..n} A_i(t, \Delta t),$$

где A_i – доступная пропускная способность секции IP-уровня секции с номером i (i = 1..n) в NSE. Следует отметить, что номер секции, определяющий доступную пропускную способность NSE IP-уровня, может отличаться от номера секции, определяющей пропускную способность NSE IP-уровня.

6.11.2.3 Пропускная способность ограничивающей секции IP-уровня

Для данной представляющей интерес совокупности ограничивающая секция IP-уровня определяется как секция NSE с наименьшей доступной пропускной способностью IP-уровня. Следует отметить, что если этому условию удовлетворяют несколько секций, то ограничивающая секция IP-уровня однозначно не определяется.

Для данной представляющей интерес совокупности пропускная способность ограничивающей секции IP-уровня NSE – это пропускная способность секции IP-уровня ограничивающей секции IP-уровня.

Следует отметить, что доступная пропускная способность секции IP-уровня для ограничивающей секции IP-уровня равна доступной пропускной способности IP-уровня NSE. То есть пропускная способность ограничивающей секции IP-уровня составляет:

$$C_{TL}(t, \Delta t) = C_i(t, \Delta t) \text{ , так что } A_i(t, \Delta t) = A_{NSE}(t, \Delta t).$$

Следует отметить, что ограничивающая секция IP-уровня не обязательно совпадает с секцией, определяющей пропускную способность NSE IP-уровня.

6.11.3 Изменчивость

Каждый показатель пропускной способности P представляет собой среднее значение за временной интервал $[t, t + \Delta t]$. Для набора последовательных наблюдений $P_1..P_N$ данного параметра P в интервале $[T, T + \Delta T]$, где $T > t$, в целях описания изменчивости можно использовать среднее значение, стандартное отклонение и квантили.

6.11.3.1 Среднее значение

Среднее значение рассчитывается следующим образом:

$$a_P(T, \Delta T) = \frac{1}{n} \sum_{i=1..n} P_i(t, \Delta t).$$

6.11.3.2 Среднеквадратичное отклонение

Стандартное отклонение рассчитывается следующим образом:

$$s_P(T, \Delta T) = \sqrt{\sum_{i=1..n} \left(P_i(t, \Delta t) - a_P(T, \Delta T)\right)^2}.$$

6.11.3.3 Квантили

Для отсортированного списка N значений $P1..P_n$ k-й 100-квантиль (то есть k-й процентиль) определяется следующим образом:

$$P_I : I = \left\lceil N \frac{k}{100} \right\rceil$$

где P_I – соответствующее значение данных для k-го 100-квантиля. (Символ $\lceil\ \rceil$ означает, что если $N\frac{k}{100}$ – не целое, то, для того чтобы получить индекс списка I, его следует округлить до следующего большего целого числа.)

Квантили минимума ($k = 0$), медианы ($k = 50$) и максимума ($k = 100$) представляют особый интерес и регистрируются. Также могут использоваться другие квантили, такие как $k = 95$ или $k = 99$.

6.12 Параметры, связанные с потоком

Рабочие параметры полезно характеризовать с помощью параметров, связанных с потоком или пропускной способностью, которые оценивают способность IP-сетей или секций передавать определенное количество IP-пакетов. Следует отметить, что параметр, предназначенный для характеристики пропускной способности IP-приложения, не равен объему ресурсов (пропускной способности), доступных этому приложению (как он определен количественно в пункте 6.11 и измеряется с использованием методов, описанных в Приложении A). Это связано с тем, что на пропускную способность IP-уровня также влияют протоколы более высокого уровня, использующие управление потоком с обратной связью по IP (например, управление потоком TCP).

В настоящей версии данной Рекомендации рекомендуется, чтобы все параметры, связанные с потоком или пропускной способностью, отвечали следующим требованиям.

1) Параметр, характеризующий пропускную способность, доступную IP-службе, должен соотносить количество IP-пакетов, успешно переданных в IP-сети или секции, с количеством IP-пакетов, доставленных в эту сеть или секцию.

2) Параметр, связанный с пропускной способностью, должен применяться к сквозной IP-сети и к IP-транспорту через EL, NS или NSE.

Некоторые параметры, связанные с потоком или пропускной способностью, представляют собой попытку охарактеризовать пропускную способность IP-сети, то есть ее способность поддерживать заданную скорость передачи IP-пакетов. Рекомендуется, чтобы любые такие параметры и методы измерения отвечали следующим дополнительным требованиям.

1) Следует описать структуру трафика, предлагаемого для IP-сети или секции, поскольку от нее зависит способность IP-сети или секции успешно доставить эти пакеты.

2) Скорость поступления трафика не должна превышать пропускную способность (в битах в секунду) канала, соединяющего испытуемые (тестируемые) секции с неиспытуемыми секциями назначения.

3) В любом отдельном заявлении о характеристиках пропускной способности должен быть объявлен тип рассматриваемого IP-пакета (с указанием версия IP, наличия заголовков расширения, протокола транспортного уровня, заголовков других протоколов и любой другой значимой информации, такой как длина используемых пакетов).

4) Некоторые формы управления потоком, применяемые на уровне IP или выше, могут приводить к ошибкам измерения. Например, при измерении пропускной способности IP-уровня в условиях отслеживания подтверждений более высокого уровня, ограничения размера окна и/или управления потоком для смягчения перегрузки (например, TCP) требуется оценка и представление отчета о соответствующей погрешности измерения. Погрешность измерения указывает на возможную неиспользуемую пропускную способность IP-уровня по сравнению со спецификацией интернет-службы и с результатами применения методов, использующих управление потоком. Также рекомендуется следовать руководящим указаниям в отношении параметров, связанных с пропускной способностью, и их измерения, которые приведены в системе показателей пропускной способности службы транспортировки массивов данных (BTC) IETF RFC 3148.

Параметры, связанные с потоком и пропускной способностью, приведены в Приложении A. В Дополнении IX объясняется, почему измерения с использованием TCP не соответствуют требованиям этого пункта.

ПРИМЕЧАНИЕ. – Дополнение III (Параметры, связанные со скоростью и пропускной способностью) в издании 2019 года признано устаревшим.

7 Доступность IP-услуг

Показатель доступности IP-услуг применим к сквозным IP-услугам, базовым секциям и NSE.

Функция доступности (определенная в пункте 7.1) служит для подразделения общего запланированного времени обслуживания для IP-услуг на периоды доступности и недоступности. На основе этой классификации в пункте 7.2 определяются доля времени доступности IP-услуг и доля времени недоступности IP-услуг. Наконец, основой для определения соответствующих параметров доступности в пункте 7.2 служит модель доступности IP-услуг с двумя состояниями.

ПРИМЕЧАНИЕ. – Если только поставщиком IP-услуг не оговорено иное, то планируемое время обслуживания для IP-услуг предполагается равным 24 часам в сутки, семи дням в неделю.

7.1 Функция доступности IP-услуг

В основе функции доступности IP-услуг лежит порог показателя IPLR.

IP-услуга готова к сквозной передаче, если IPLR для этой сквозной передачи меньше порогового значения c_1, определенного в таблице 1.

Таблица 1 – Функция доступности IP-услуг

Критерий недоступности	Порог
IPLR > c_1	c_1 = 0,20
ПРИМЕЧАНИЕ. – Значение c_1 = 0,20 считается предварительным и определяется как требующее дальнейшего изучения. Предыдущее предварительное значение c_1 составляло 0,75. Также предлагались значения c_1, равные 0,9 и 0,99. Однако на момент утверждения настоящей Рекомендации большинство причин недоступности, как представляется, связаны с отказами, когда коэффициент потерь составляет практически 100%, а многие приложения для IP-сетей перестают работать, когда коэффициент потерь > 0,20. Когда IP-сети поддерживают различные классы качества обслуживания, может оказаться целесообразным рассматривать разные значения c_1 для разных служб. В этом случае для служб, обеспечивающих класс 0 или класс 1 по Рекомендации МСЭ-Т Y.1541, предлагались значения c_1 от 0,03 до 0,2 (в зависимости от устойчивости различных кодеров речи), а для служб, обеспечивающих класс 5 по Рекомендации МСЭ-Т Y.1541, – значение c_1 = 0,75. Порог c_1 следует использовать только для определения того, что ресурсы IP-сети неспособны (временно) поддерживать полезную службу передачи IP-пакетов. Значение c_1 не следует рассматривать как заявление о величине IPLR и как требование к IPLR, подходящее для любого IP-приложения. Требования, установленные для IPLR, должны исключать все периоды недоступности службы, то есть все временные интервалы, когда IPLR > c_1.	

Относительно конкретной пары SRC и DST *базовая секция или NSE доступна в независимом от входа случае*, если IPLR для этой пары меньше порогового значения c_1, измеренного во всех разрешенных входных MP.

Относительно конкретной пары SRC и DST *базовая секция или NSE доступна в специфическом для входа случае*, если IPLR для этой пары меньше порогового значения c_1, измеренного в конкретных разрешениях входных MP.

ПРИМЕЧАНИЕ 1. – В процессе эксплуатации можно измерять и/или отслеживать доступность в конкретном входном MP, а затем использовать эту информацию для того, чтобы сделать заключение о независимой от входа доступности.

ПРИМЕЧАНИЕ 2. – Количественная связь между доступностью сквозных IP-услуг и доступностью IP-услуг базовой секции или NSE подлежит дальнейшему изучению.

Если критерии отказа, приведенные в таблице 1, удовлетворены (то есть IPLR превышает пороговое значение), то IP-служба находится в состоянии недоступности (отказа). Если критерии отказа не удовлетворены, IP-служба находится в состоянии доступности (отсутствия отказа). Минимальное количество пакетов, которое следует использовать при оценке функции доступности IP-службы, равно M_{av} (значение M_{av} подлежит дальнейшему изучению. Когда при испытании доступности используется трафик, генерируемый конечным пользователем, предлагается считать M_{av} равным 60 пакетам, распределенным в пределах интервала времени T_{av}, при скорости передачи один пакет в секунду). Минимальная продолжительность интервала времени, в течение которого должна оцениваться

функция доступности IP-службы, равна T_{av}. Значение T_{av} предварительно принято равным одной минуте. Исследование показало, что это значение согласуется с практическими ограничениями операций IP-уровня. Мониторинг рабочих характеристик нижнего уровня и отказов элементов сети позволяет выявить надвигающееся состояние недоступности за более короткое время и принять меры по устранению неполадок. В Дополнении VI дается обоснование текущего определения функции доступности IP-службы и значений T_{av} и c_1.

ПРИМЕЧАНИЕ 3. – Ожидается, что критерий отказа, основанный на IPLR, будет удовлетворительно характеризовать доступность IP-службы. Однако при определении доступности IP-службы можно также учитывать резкое ухудшение значения IPER и/или коэффициента случайных IP-пакетов. Учет дополнительных параметров при принятии решения о доступности и связанные с ними пороговые значения подлежат дальнейшему изучению.

ПРИМЕЧАНИЕ 4. – Это одностороннее определение доступности мотивировано тем фактом, что IP-пакеты часто проходят из SRC в DST по совершенно другим маршрутам, чем из DST в SRC. Если с точки зрения пользователя IP-сети требуется определение доступности в обоих направлениях, его можно легко получить из этого одностороннего определения путем суммирования с неперекрывающимся интервалом времени недоступности обратного пути.

Предполагается, что это определение доступности IP-службы применимо как к IP-трафику, генерируемому конечным пользователем (то есть к обычному потоку IP-пакетов между SRC и DST), так и к трафику, генерируемому испытательными установками и методами тестирования. В любом случае при составлении отчета о доступности должен быть задокументирован источник IP-трафика. Такая документация должна включать конкретные типы пакетов, используемых в каждом направлении потока.

Трафик, генерируемый специально для проверки состояния доступности, должен быть ограничен, чтобы не вызывать перегрузки. Такая перегрузка может повлиять на другой трафик и/или значительно повысить вероятность превышения критериев отказа.

Более подробная информация по определению состояния доступности приведена в Дополнении IV.

7.2 Параметры доступности IP-службы

7.2.1 Доля времени недоступности IP-службы (PIU)

Доля времени недоступности IP-службы (PIU) – это доля в процентах общего запланированного времени работы IP-службы (доля интервалов T_{av}), которая рассматривается как время "недоступности" с использованием функции доступности IP-службы.

7.2.2 Доля времени доступности IP-службы (PIA)

Доля времени доступности IP-службы (PIA) – это доля в процентах общего запланированного времени работы IP-службы (доля интервалов T_{av}), которая рассматривается как время "доступности" с использованием функции доступности IP-службы:

$$PIU = 100 – PIA.$$

ПРИМЕЧАНИЕ. – Поскольку IPLR обычно увеличивается с возрастанием предлагаемой нагрузки в направлении от SRC к DST, то вероятность превышения порогового значения c_1 также увеличивается с возрастанием предлагаемой нагрузки. Следовательно, с ростом требований к пропускной способности между SRC и DST значения PIA, вероятно, будут уменьшаться.

В Дополнении IV содержится информация выборке для определения PIA и PIU.

Приложение A

Параметры, связанные с пропускной способностью и потоком IP-пакетов, и методы их измерения

(Данное Приложение является неотъемлемой частью настоящей Рекомендации.)

A.1 Базовая информация

Стандартизация архитектуры измерений, характеризующих "интернет-услуги", началась в 2013 году. Система доступа потребителей к сети, поддерживающая протокол Интернет, служит распространенным способом подключения к интернету. Традиционно большинство потребительских приложений взаимодействуют с использованием транспорта TCP. TCP обеспечивает надежную передачу датаграмм. При попытке охарактеризовать интернет-услуги с помощью стандартизированных измерений для суждения о свойствах интернета или канального уровня, таких как пропускная способность услуг доступа, использовались методы описания свойств транспортного уровня TCP. Высказывались опасения, что этот подход может не работать должным образом, и предлагались альтернативные методы оценки характеристики потребительских услуг доступа в интернет на основе измерений.

В то же время наблюдается сильная тенденция к замене транспорта TCP транспортом UDP, к полезной нагрузке с открытой и шифрованной частями, а также к повторной передаче на уровне приложений с контролем перегрузки. Использование протокола Google QUIC и предстоящее утверждение IETF QUIC [b-QUIC] быстро изменят среду передачи интернета, и одними из первых пользователей станут потребители, применяющие популярные браузеры.

В данном Приложении определены параметры и методы измерения пропускной способности услуг доступа для оценки максимальной пропускной способности IP-уровня. В будущем после дальнейшего изучения здесь могут быть указаны параметры и методы измерения (пропускной способности транспортного уровня), связанные с потоком. Эти параметры и методы измерения полностью применимы как к абонентам (конечным пользователям), так и к поставщикам услуг интернета, с той оговоркой, что их применимость при сравнении результатов измерений со спецификациями служб IP-уровня полностью определяется выбранными входными и выходными пунктами измерения.

12-я Исследовательская комиссия МСЭ-Т (ИК12) обладает опытом разработки стандартов измерения и моделирования для электросвязи. Кроме того, имеется опыт в области статистических методов и наборов инструментов, позволяющих проводить объективное сравнение предлагаемых методов измерения и моделирования. Использование знаний и методов ИК12 для принятия решения о применимости конкурирующих предложений, связанных с характеристикой "потребительских интернет-услуг", считается хорошим способом перейти от обмена мнениями к проверке и сравнению концепций в воспроизводимых условиях испытаний. В [b-ITU-T P.800] предъявляются следующие требования.

> Важно, чтобы до и после каждого эксперимента были правильно описаны и созданы, а также точно измерены условия, моделируемые в процессе испытания; …и чтобы точно регистрировались результаты каждого испытания.

В марте 2018 года IETF утвердил и опубликовал документ RFC 8337 "Показатели на основе моделей пропускной способности служб транспортировки массивов данных" [IETF RFC 8337]. Работа над показателями на основе моделей (MBM) стала результатом многолетнего изучения проблемы измерения пропускной способности транспортного уровня, прежде всего в рабочей группе IETF IP Performance Metrics (IPPM). В спецификации подробно описаны многие проблемы и трудности, связанные с повторяемостью при испытаниях с использованием стандартного TCP (раздел 4), и эти проблемы решаются главным образом путем разработки метода и набора диагностических тестов, в которых управление потоком TCP запрещено. Метод включает в себя оценку рабочих характеристик целевого транспорта с точки зрения скорости передачи и времени передачи в прямом и обратном направлениях (RTT).

До настоящей Рекомендации существовали инструменты для измерения пропускной способности IP-уровня на основе UDP (например iPerf), и встречались отдельные упоминания о таких измерениях в публикуемых стандартах и отчетах. Сегодня отрасль рассматривает в качестве идеального способа

предложения новых показателей и методов измерения предоставление как стандарта, так и совместимого с ним инструмента. В данном Приложении содержится достаточно подробная для реализации спецификация модели, которая дает статистически эквивалентные результаты (как описано в [b-IETF RFC 6576] по итогам работы IPPM). Инструмент измерения, соответствующий настоящему Приложению, будет представлен отдельно.

В данное Приложение включен план испытаний для оценки соответствующих методов измерения. В этом плане в целях создания эталонной "реальной ситуации" для сравнения возможных методов измерения используются принципы ИК12, приведенные в [b-ITU-T P.800]. Испытания проводились в два этапа: в соответствии с планом первого этапа проводились лабораторные испытания, в ходе которых в контролируемых условиях проверялись реализация эталонной "реальной ситуации", предельные показатели испытательной платформы и возможные методы измерения. В соответствии с планом второго этапа проводились полевые испытания.

Обобщенные результаты (с использованием плана испытаний) как лабораторных испытаний первого этапа, так и полевых испытаний второго этапа представлены в Дополнении X (информативном). В других Дополнениях содержатся информация, собранная в поддержку выработанного здесь консенсуса, а также дополнительные сведения по расчетам и коэффициентам преобразования между измерениями на разных уровнях.

A.2 Параметры и методы измерения пропускной способности услуг доступа IP-уровня (потребительского доступа в интернет)

A.2.1 Определение измеримого показателя пропускной способности IP-уровня

В пункте 6.11.1.2 определяется идеализированный параметр пропускной способности секции IP-уровня, оценивающий "наибольшее (общее) количество битов IP-уровня, которое может быть передано… в течение заданного интервала времени $[t, t + \Delta t]$". В данном же пункте приведена измеримая (более практичная) версия идеализированного определения.

Для данной представляющей интерес совокупности максимальная пропускная способность секции IP-уровня в течение интервала времени $[t, t + \Delta t]$ составляет:

$$Maximum\_C(t, \Delta t) = \frac{\max\limits_{[t,\Delta t]}\left(n_0(dt_n, dt_{n+1})\right)}{dt},$$

где:

интервал времени $[t, t + \Delta t]$ состоит из x равных промежуточных интервалов *длительностью dt*;

n_0 – общее количество битов заголовка и полезной нагрузки IP-уровня, которые могут быть переданы по базовой секции с результатом "успешная передача IP-пакета" в выходном пункте измерения в течение заданного интервала времени, начиная с $[dt_1, dt_2]$ или других интервалов длительностью *dt*, и

максимум $C(t, \Delta t)$ соответствует максимальному значению n_0, измеренному за любой промежуточный интервал времени $[dt_n, dt_{n+1}]$ в пределах интервала времени $[t, t + \Delta t]$, деленному на продолжительность промежуточного интервала.

Следует отметить, что при оценке измеримого показателя пропускной способности IP-уровня должен использоваться транспорт UDP.

Для этого метода измерения также используется приведенное ниже определение скорости передачи.

A.2.1.1 Битовая скорость передачи IP-пакетов (IPSBR)

Для данной представляющей интерес совокупности битовая скорость передачи IP-пакетов (IPSBR), обеспечиваемая отправителем во входном MP, равна восьмикратному общему количеству октетов, передаваемых в заголовках и полезной нагрузке IP-пакетов, которое приводит к одному эталонному событию передачи IP-пакета в этом входном MP в течение заданного интервала времени, деленному на продолжительность интервала времени. Это соответствует количеству битов в заголовках и полезной нагрузке IP-пакетов, приводящему к эталонным событиям передачи IP-пакета, за секунду работы службы.

A.2.2 Метод измерения

Метод (процедура) измерения состоит из следующих шагов.

- Отправитель организует передачу и прием потока IP-пакетов с использованием транспортного уровня UDP с определенными ключевыми параметрами, включая:

  тип пакетов, в том числе длину заголовка и полезной нагрузки, присутствующие заголовки и опции, а также любые маркеры для специальной обработки в сети;

  начальную/переменную скорость передачи пакетов в течение заданного интервала времени (например, интервала, соответствующего параметру HZ, намного меньшему, чем *dt*, который представляет собой промежуточный интервал для регистрации во время тестирования);

  длину, продолжительность и характеристики преамбулы или подготовительной фазы тестирования (это важно для сетей определенного типа, таких как подвижные сети);

  конкретный порядок передачи, в том числе допустимую или предполагаемую неравномерность трафика).

- Во время испытаний скорость передачи варьирует в соответствии с заданным алгоритмом поиска с учетом:

  заданной цели поиска, включая один или несколько измеряемых показателей и соответствующие им рабочие пороги, а также допуск выше и ниже этих порогов;

  заданной продолжительности испытаний, состоящих из отдельных шагов алгоритма поиска;

  набора измерений в промежуточных интервалах *dt*, которые поддерживают итоговые измерения, проводимые по завершении каждого испытания;

  максимальной продолжительности процесса поиска (предела времени).

  В настоящем Приложении приведен один обязательный алгоритм поиска; другие алгоритмы обязательны к применению или факультативны (как указано в пункте или Приложении с описанием алгоритма). То, какой именно алгоритм поиска применяется – обязательный или факультативный, сообщается пользователю вместе с результатами.

- Данные всех измерений (результаты испытаний), собранные в ходе поиска, должны храниться в виде временны́х рядов, чтобы можно было анализировать процесс поиска.

- Должен быть определен способ последующей обработки данных всех измерений (результатов испытаний), собранных в ходе поиска, для определения итогового значения (итоговых значений) конкретного процесса поиска. Примерами (для скорости приема или – в данном случае – измеренной пропускной способности; в число других параметров входят задержка, потери и переупорядочение) могут служить:

  вычисление среднего значения скорости приема по всем измерениям во всех испытаниях;

  вычисление среднего значения скорости приема по всем измерениям, в которых цель поиска достигнута;

  вычисление максимального значения скорости приема по всем измерениям, в которых цель поиска достигнута;

  вычисление среднего значения скорости приема по всем измерениям во всех испытаниях, в которых были удовлетворены заданные критерии исключения результатов (например, исключение выпадающих значений, как указано в заданных критериях);

  обобщение связанных параметров (см. пункт A.2.3 ниже).

- Должны быть определены критерии аннулирования результатов данного процесса поиска, такие как обнаружение невозможности достижения требуемой скорости передачи или обнаружение конкурирующего трафика (но этот трафик не может быть полностью выявлен при всех обстоятельствах).

- Когда тесты повторяются для проверки согласованности результатов или по другим причинам, процесс обобщения результатов должен включать соответствующий последующий анализ для обеспечения качества данных, а также для обнаружения и исключения (по возможности)

искажений данных. Методы последующего анализа при их использовании публикуются вместе с результатами.

- Безопасность: тестовый получатель (или сервер) должен быть устроен так, чтобы он принимал тестовые запросы только от авторизованных пользователей и отклонял все прочие.
- Пропускная способность: тестовый получатель (или сервер) должен быть устроен так, чтобы он принимал тестовые запросы только при наличии достаточных ресурсов хоста и интерфейса и отклонял запросы, когда это условие не выполняется.
- Представление результатов: система измерения должна выдавать такую информацию, как максимальная пропускная способность IP-уровня, коэффициент потери тестовых IP-пакетов и другие показатели, если таковые имеются (см. пункт A.2.4). Система измерения также может предоставлять информацию о пропускной способности UDP в виде доставленных битов полезной нагрузки UDP, поскольку это пропускная способность, доступная пользовательским приложениям, после удаления заголовков IP и UDP.

A.2.2.1 Обязательный алгоритм поиска

Система измерения соответствует требованиям пункта A.2.2 с добавлением следующих возможностей для поддержки алгоритма поиска.

1. Испытатель дает рекомендацию по максимальному размеру тестовых пакетов и допускает некоторую непредвиденную служебную нагрузку во избежание фрагментации.
2. Имеется таблица скоростей передачи (IPSBR), количества пакетов, передаваемых в течение каждого интервала времени, и размеров пакетов. В этой таблице представлены в возрастающем порядке значения предлагаемых скоростей передачи нагрузки – от минимальной поддерживаемой скорости передачи нагрузки до максимальной включительно.
3. Получатель предлагаемой нагрузки измеряет следующие показатели: скорость приема, потери, переупорядочение, вариацию задержки (в соответствии с настоящей Рекомендацией) и двустороннюю задержку [Y.1565].
4. Получатель предлагаемой нагрузки периодически передает отправителю сообщения о состоянии с результатами измерения показателей.
5. На основе результатов, содержащихся в сообщении о состоянии, отправитель корректирует предлагаемую нагрузку в соответствии с блок-схемой, приведенной на рисунке A.1. В блок-схеме "1 шаг" – это изменение скорости в таблице предлагаемых скоростей нагрузки с использованием нового значения (в строке, расположенной выше или ниже текущей строки для передачи).

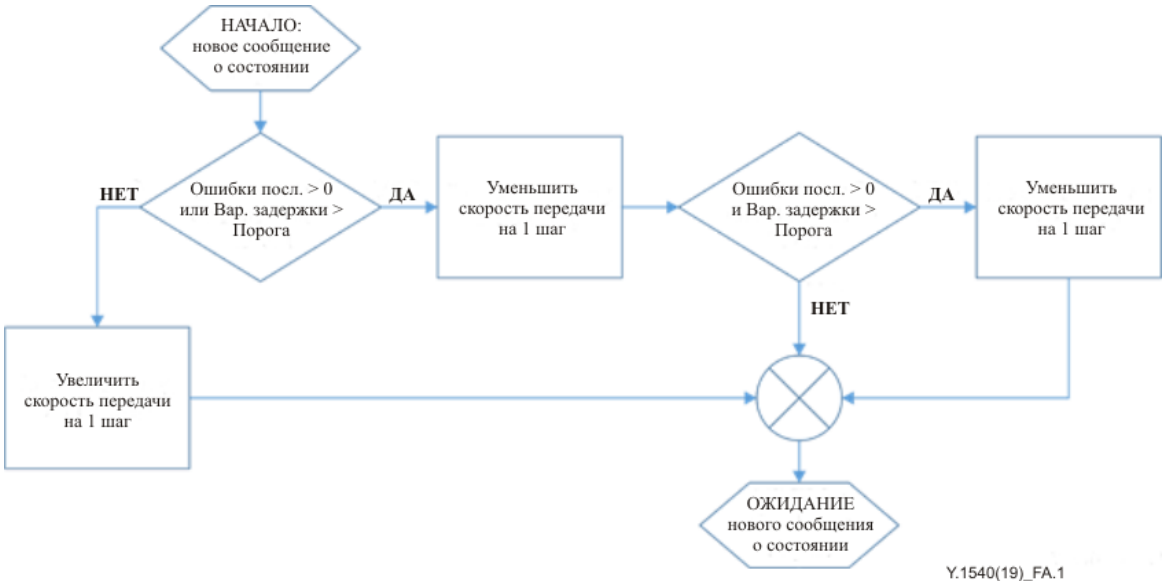


Рисунок A.1 – Блок-схема корректировки предлагаемой нагрузки в процессе поиска алгоритма

ПРИМЕЧАНИЕ. – При выполнении алгоритма решения могут приниматься одним из двух хостов системы измерения, что значительно упрощает реализацию на другом хосте и делает ее независимой от версии алгоритма. Это также позволяет обновлять алгоритм на более легкодоступном хосте.

Впоследствии в отдельных Приложениях будут приведены альтернативные обязательные или факультативные алгоритмы поиска.

A.2.3 Показатель коэффициента потери IP-пакетов (IPLR) при испытаниях

Для данной представляющей интерес совокупности коэффициент потери IP-пакетов (IPLR) при испытаниях – это отношение общего количества потерянных IP-пакетов к общему количеству потерянных и успешно переданных IP-пакетов во время каждого испытания (или промежуточного интервала *dt*).

Следует отметить, что определение IPLR при испытаниях несколько отличается от определения IPLR, данного в основном тексте, поскольку невозможно использовать длительное время ожидания (T_{max}), чтобы при оценке результатов каждого испытания (или промежуточного интервала, *dt*) отличить успешные результаты передачи пакетов от результатов с потерей пакетов и немедленно передать их алгоритму поиска. Необычно длительные задержки или переупорядоченные пакеты будут учитываться при измерениях в ходе последующих испытаний по всем параметрам, включая IPDV.

A.2.4 Связанные параметры и методы

Очевидно, интерес представляют значения IPLR, IPTD (оцениваемого как время передачи в прямом и обратном направлениях, или двусторонняя задержка, в соответствии с параметром, определенным в [Y.1565]) и IPDV, полученные во время испытаний, и их следует представлять вместе с итоговым значением скорости приема (измеренной пропускной способности).

Дополнительные измеряемые параметры:

- фактическая продолжительность процесса поиска (должна быть равна Δt);
- общее количество потерянных пакетов за время поиска;
- диапазон и вариация результатов при повторяющихся процессах поиска.

A.3 Связанные с потоком параметры и методы измерения пропускной способности (надежный транспорт доставки)

В данном разделе, который подлежит дальнейшему изучению, определены связанные с потоком показатели и методы измерения пропускной способности в соответствии с пунктом 6.12 настоящей Рекомендации. Следует отметить, что в Дополнении X к настоящей Рекомендации объясняется, почему стандарт TCP с управлением потоком с обратной связью не удовлетворяет этим требованиям. Возможные показатели и метод описаны в Дополнении XIII к настоящей Рекомендации и соответствуют требованиям пункта 6.12.

A.3.1 Определение параметров

Подлежит дальнейшему изучению; см. Дополнение XIII.

A.3.2 Метод измерения

Подлежит дальнейшему изучению.

A.3.3 Связанные параметры и методы

Подлежит дальнейшему изучению.

A.4 План оценки и сравнения методов измерения услуг доступа

В Рекомендации МСЭ-T P.800 и других Рекомендациях этой серии, хотя они в первую очередь относятся к голосовой связи, содержатся общие руководящие указания по организации, проведению и оценке результатов измерительных кампаний с целью сравнения моделей, основанных на данных измерений в реальных условиях. Аналогичный процесс, который описан ниже, полезен для оценки возможностей и ограничений испытаний, инструментов и результатов, характеризующих типы доступа в интернет.

Для передачи данных в процессе лабораторных испытаний следует создать ряд условий. Сначала следует определить условия передачи, близкие к реальным условиям эксплуатации. Эти условия должны быть стабильными и поддающимися проверке во время испытаний с использованием лабораторного измерительного оборудования. Затем можно протестировать при разных условиях каждый метод, предназначенный для определения характеристик различных типов доступа в интернет. Можно определить погрешность измерения. По характеристикам каждого параметра и метода можно определить рабочие области (условия), в которых данный метод измерения имеет преимущества и где он менее надежен (а также количественно определить источники погрешности измерения).

Условия испытаний перечислены ниже.

A.4.1 Пункты измерения

В [b-IETF RFC 7398] определены эталонный маршрут и пункты измерения общепринятых рабочих характеристик. Описанные здесь расширения для определения местоположения пункта измерения могут использоваться и в других подобных проектах по измерению. Целью [b-IETF RFC 7398] является создание эффективного способа описания местоположения пунктов измерения, используемых для проведения конкретных измерений, особенно указание того, когда в измерение входят управляемые и неуправляемые участки маршрута (частные сети).

Следует отметить, что от маршрута измерения, ограниченного пунктами измерения [b-IETF RFC 7398], зависит применимость абонентских параметров, таких как типичные предлагаемые скорости передачи данных, а также влияние абонентских параметров на выбор параметров, таких как MBM target_data_rate (целевая скорость передачи данных) [IETF RFC 8337]. Кроме того, таких параметров, как размер кадра, используемого в тестах UDP, при определении уровня, на котором вводится тестовый трафик, во избежание фрагментации.

A.4.2 Условия испытаний

Все конфигурации и поведение фонового трафика должны быть максимально приближены к рабочим условиям сети. Рекомендуется определить базовый тест, а затем варьировать параметры испытаний. Это первый этап испытаний.

A.4.2.1 Условия лабораторных испытаний первого этапа

Согласно требованиям BEREC [b-BEREC], первый этап испытаний проводится с применением формирователей (и ограничителей до 10 Мбит/с, см. [b-Google-Police]), и испытатель должен знать уровень, на котором пакеты измеряются в формирователях, ограничителях, пассивных наблюдателях, отправителях, получателях и по окончании испытаний. Кроме того, в сеть вносятся и тестируются нарушения, такие как задержка.

На приведенном ниже рисунке показаны две разные утилиты, обеспечивающие гибкое управление трафиком/скоростью передачи на вычислительной платформе общего назначения. Различные утилиты управления трафиком можно применять тремя способами.

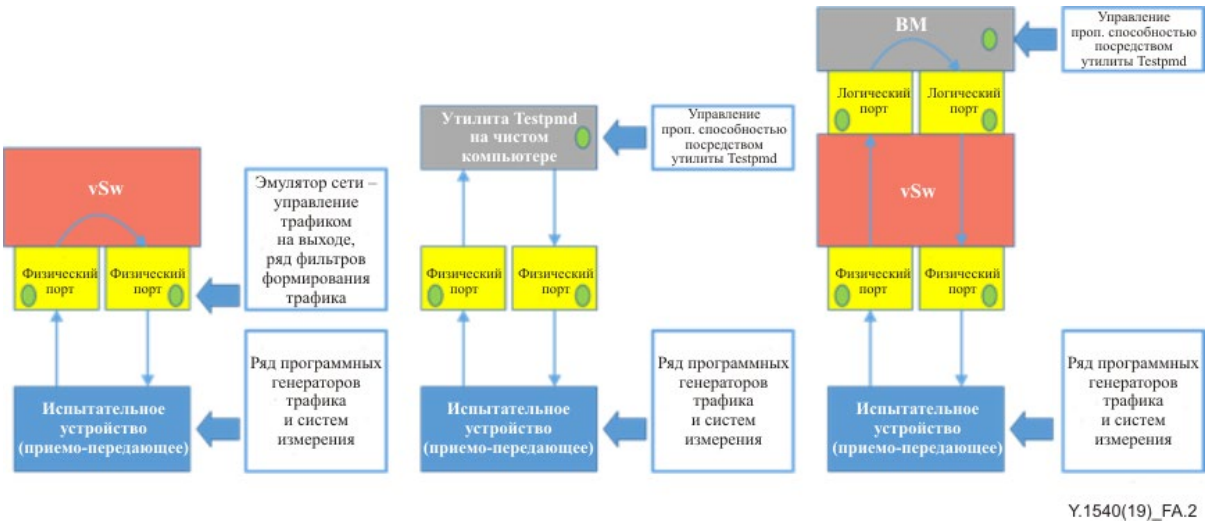


Рисунок A.2 – Три альтернативных способа испытаний на вычислительной платформе общего назначения

На рисунке A.2 испытательное устройство подключено к компьютеру общего назначения через физические каналы с пропускной способностью 10 Гбит/с. Испытательное устройство также представляет собой компьютер общего назначения, но он полностью изолирован от компьютера, регулирующего трафик, что позволяет каждому узлу выделять ресурсы для решения своих задач в тестовой среде. Можно устанавливать и тестировать через узел управления трафиком разные реализации предлагаемых методов измерения.

Имеется три варианта реализации функции формирования трафика. В первой слева схеме используется эмулятор сети с ядром Linux, который может эмулировать задержку и помогает управлять трафиком после настройки подходящей сетевой карты и физических интерфейсов. Виртуальный коммутатор (vSw) просто коммутирует кадры между двумя своими портами. Эту конфигурацию обычно называют "phy2phy".

Второй вариант (средняя схема) предполагает, что для переадресации кадров между соответствующими физическими интерфейсами, а также для управления пропускной способностью маршрута передачи установлена и настроена утилита Intel DPDK testpmd.

В последнем варианте (справа) используются утилита testpmd, установленная на виртуальной машине, или ВМ, и виртуальный коммутатор с конфигурацией для подключения физических интерфейсов к нужным портам ВМ. Опять же, пропускная способность маршрута между логическими портами управляется утилитой testpmd (или другой утилитой, работающей на виртуальной машине).

Все три конфигурации можно реализовать на модуле проекта OPNFV VSPERF, предназначенном для тестирования, разработки и оценки с использованием инструмента VSPERF [b-Pod12].

Для отдельных тестов могут применяться разные условия. В каждом тесте изменяется только один параметр по сравнению с базовым тестом, все остальные параметры конфигурации остаются неизменными.

– Полоса пропускания формирователя/ограничителя настраивается на значения скоростей, предложенные BEREC, вплоть до гигабитного диапазона, и проверяется.
– Для RTT устанавливаются следующие значения: 5, 10, 20, 40 мс.
– Для коэффициента случайной потери пакетов устанавливаются следующие значения: 0, 10**−4. 10**−5.
– Для устойчивости формирователя к неравномерности трафика передачи может быть установлено значение 0 или максимальное значение, допускаемое формирователем (5 кбит).
– В качестве методов ограничения скорости используются формирование или ограничение (но не то и другое одновременно).

– Стратегией управления переполнением очереди является отбрасывание конца очереди ("отбрасывание хвоста").

– Тесты выполняются без фонового трафика. Может быть выполнен дополнительный тест с фоновым (конкурирующим) трафиком. Средняя фоновая нагрузка публикуется вместе с полученными результатами.

– Весь тестовый и фоновый трафик обрабатывается с максимально возможной эффективностью.

– Максимальный интервал для отдельного измерения составляет 30 с.

– Для того чтобы значение полосы пропускания было признано как правильно измеренное предлагаемой измерительной системой, допуск на установленную полосу пропускания по сравнению с полосой пропускания, измеренной во время испытания, должен быть в пределах 5% для каждого отдельного измерения.

– Программное обеспечение измерения, используемое для испытаний, должно быть доступно по лицензии ПО с открытым исходным кодом. При использовании коммерческих продуктов выполнение этого требования можно отложить до тех пор, пока не начнется стандартизация метода. Тестовые системы должны быть откалиброваны, и в РГ17 должны знать предельные возможности любой системы, представленной для оценки. Кроме того, должны быть предоставлены сведения о среде разработки и требуемой операционной системе.

– Результаты будут опубликованы в качестве Приложения к настоящей Рекомендации.

– Размеры кадра ETH соответствуют размеру кадра уровня 2, равному 64 байтам, и дополнительно максимальному размеру ETH MTU, равному 1512 байтам (или 1516, включая ETH CRC).

– Желательно проводить испытания с использованием семейства адресов IPv6 в дополнение к IPv4.

Для калибровки параметров сети [b-TST 009], таких как максимальная пропускная способность IP-уровня, минимальное и максимальное время передачи в прямом и обратном направлениях, глубина буфера и т. д., перед каждым отдельным измерением при каждом условии тестирования сети может использоваться стандартное лабораторное испытательное оборудование. Таким образом, можно получить информацию о контрольных показателях рабочих характеристик сети для сравнения результатов инструментов измерения с соответствующими оценками.

Эталоном правильной работы формирователя в соответствии с конфигурацией и, в конечном счете, правильной оценки условий канала (в соответствии с [b-PAM-12]) служит передача UDP с постоянной битовой скоростью (CBR). Если пропускная способность UDP и конфигурация формирователя различаются, то третьим "арбитром" правильности может служить ввод пакетов потока UDP. Важное значение в процессе сравнения с эталоном имеет выявление и обсуждение любых обнаруженных ошибок.

Были выполнены предварительные лабораторные испытания для оценки метода калибровки и измерения. Руководствуясь существующим текстом Приложения A к настоящей Рекомендации и требованиями BEREC по проверке инструментов измерения, компания AT&T протестировала одну из трех альтернативных конфигураций с использованием вычислительной платформы общего назначения, которая соответствует требованиям (phy2phy).

Основные итоги этого тестирования:

- пропускная способность в обоих направлениях составила 213,85 Мбит/с, что довольно близко к установленному значению 100 Мбит/с x2. Превышение можно отнести на счет допустимой неравномерности трафика.
- Двоичный поиск с проверкой потерь был настроен так, чтобы допускать довольно большой разброс скорости передачи данных в гигабитах в секунду для принятия результата. При тестировании скоростей ниже 1 Гбит/с этот допуск следует пересмотреть.

A.4.2.2 Условия испытаний второго этапа

На следующем этапе программы испытаний по этому плану используется эталон UDP в действующих сетях (с проверенными спецификациями параметров обслуживания) для дальнейшего сравнения спецификаций и методов обслуживания, таких как методы TCP iPerf 2 и методы на основе UDP. Это аналогично [b-PAM-12] и другим стандартам, указанным ниже.

Тестирование конфигураций сетевого оборудования, находящегося в эксплуатации, МОЖЕТ также проводиться в лабораторных условиях, когда это возможно и желательно.

Испытания второго этапа проводятся, как описано в работе Гоги и Тейшейры 2012 года [b-PAM-12]. Судя по имеющимся сведениям о широко используемых сегодня системах измерения, ни в одной из них не используется метод, который, как было продемонстрировано в прошлом, дает наиболее точную оценку пропускной способности IP-уровня – измерения на основе UDP [b-PAM-12]. К сожалению, испытания [b-PAM-12] проводились, когда типичные значения пропускной способности службы доступа были меньше 50 Мбит/с, а сейчас (более пяти лет спустя) этот диапазон превышается даже для подвижного доступа в интернет. Основные выводы [b-PAM-12].

- Для эмуляции инструментов, работающих по принципу заполнения канала, использовалась утилита iperf, поскольку она позволяет задавать, среди прочих параметров, количество параллельных соединений, продолжительность или размер передачи.
- "Эталон. В первой строке таблицы 1 показана пропускная способность UDP, полученная при заполнении канала с помощью iperf в UDP….. Пропускная способность UDP – это максимально достижимая скорость передачи IP-пакетов для каждого звена".
- Spruce, нагрузка маршрута большими зондами и параллельный TCP – наиболее точные инструменты для оценки доступной пропускной способности (то есть остаточной пропускной способности), но есть регионы, где параллельные TCP-тесты не дают полезных результатов, а именно места, где присутствует неопознанный параллельный трафик.

Общие недостатки существующих систем измерения, которые использовались в 2012 году, проанализированы в [MortonPQS].

Испытания второго этапа следует проводить для каждого из основных типов доступа.

Основные типы доступа:

Проводной доступ: потребительский доступ DSL, широкополосный доступ по кабелю, волоконно-оптический доступ и др.

Беспроводной доступ: точка доступа Wi-Fi, UMTS, беспроводной доступ LTE и др.

Основу испытаний второго этапа составляют результаты и маршруты, использовавшиеся на первом этапе. Второй этап охватывает несколько типов доступа в интернет, например доступ с типичными свойствами для национального рынка электросвязи. То же относится и ко всем другим параметрам, например, следует принять RTT, типичное для популярного контента, типичный фоновый трафик и т. д. Таким образом, условия сети должны быть приближены к реальной абонентской среде передачи.

Для отдельных тестов могут применяться разные условия. В каждом тесте изменяется только один параметр по сравнению с базовым тестом, все остальные параметры конфигурации остаются неизменными.

– В службу доступа может быть введен фоновый трафик (с функциями Diffserv или без них, как можно ожидать на конкретном рынке).

Дополнительно для исследования измеренных свойств сети можно использовать стандартное лабораторное испытательное оборудование.

Если известны размеры пакетов, они должны быть указаны, но возможно, что пакеты будут иметь переменный размер, и эта изменчивость может быть результатом условий сети, требующих повторной передачи (в основном для TCP, другие инструменты могут использовать пакеты фиксированного или переменного размера).

Приложение B

Дополнительный алгоритм поиска для параметров и методов измерения пропускной способности на базе IP

(Данное Приложение является неотъемлемой частью настоящей Рекомендации.)

B.1 Алгоритм поиска

Эта система измерения соответствует требованиям пункта A.2.2 с добавлением следующих возможностей для поддержки альтернативного и обязательного к реализации алгоритма поиска, называемого алгоритмом поиска по Приложению B (который не зависит от протокола испытаний).

1. Испытатель дает рекомендацию по максимальному размеру тестовых пакетов и допускает некоторую непредвиденную служебную нагрузку во избежание фрагментации.
2. Таблица скоростей передачи, которые представляют собой количество пакетов, передаваемых в течение каждого временного интервала (в соответствии с битовой скоростью и указанным уровнем протокола), и размеров пакетов. В этой таблице представлены в возрастающем порядке значения предлагаемых скоростей передачи нагрузки – от минимальной поддерживаемой скорости передачи нагрузки до максимальной включительно.
3. Получатель предлагаемой нагрузки измеряет следующие показатели: скорость приема, потери, переупорядочение, вариацию задержки (в соответствии с настоящей Рекомендацией) и двустороннюю задержку [МСЭ-T Y.1565].
4. Получатель предлагаемой нагрузки периодически передает отправителю сообщения о состоянии с результатами измерения показателей.
5. На основе результатов, содержащихся в сообщении о состоянии, отправитель корректирует предлагаемую нагрузку в соответствии с блок-схемой, приведенной на рисунке B.1. В блок-схеме "1 шаг" – это изменение скорости в таблице предлагаемых скоростей нагрузки с использованием нового значения (из строки, расположенной выше или ниже текущей строки для скорости передачи и размера пакетов).

В блок-схеме на рисунке B.1 используется множество имен переменных и в некоторых случаях настраиваемые пороги, определяющие принимаемые решения. Блок-схема предусматривает три основных пути: когда сообщение обратной связи указывает на отсутствие измеренных ухудшений; когда ухудшения измерены впервые и может присутствовать некоторая перегрузка, но изменение скорости передачи откладывается; и когда измеренные ухудшения подтверждаются повторными измерениями.

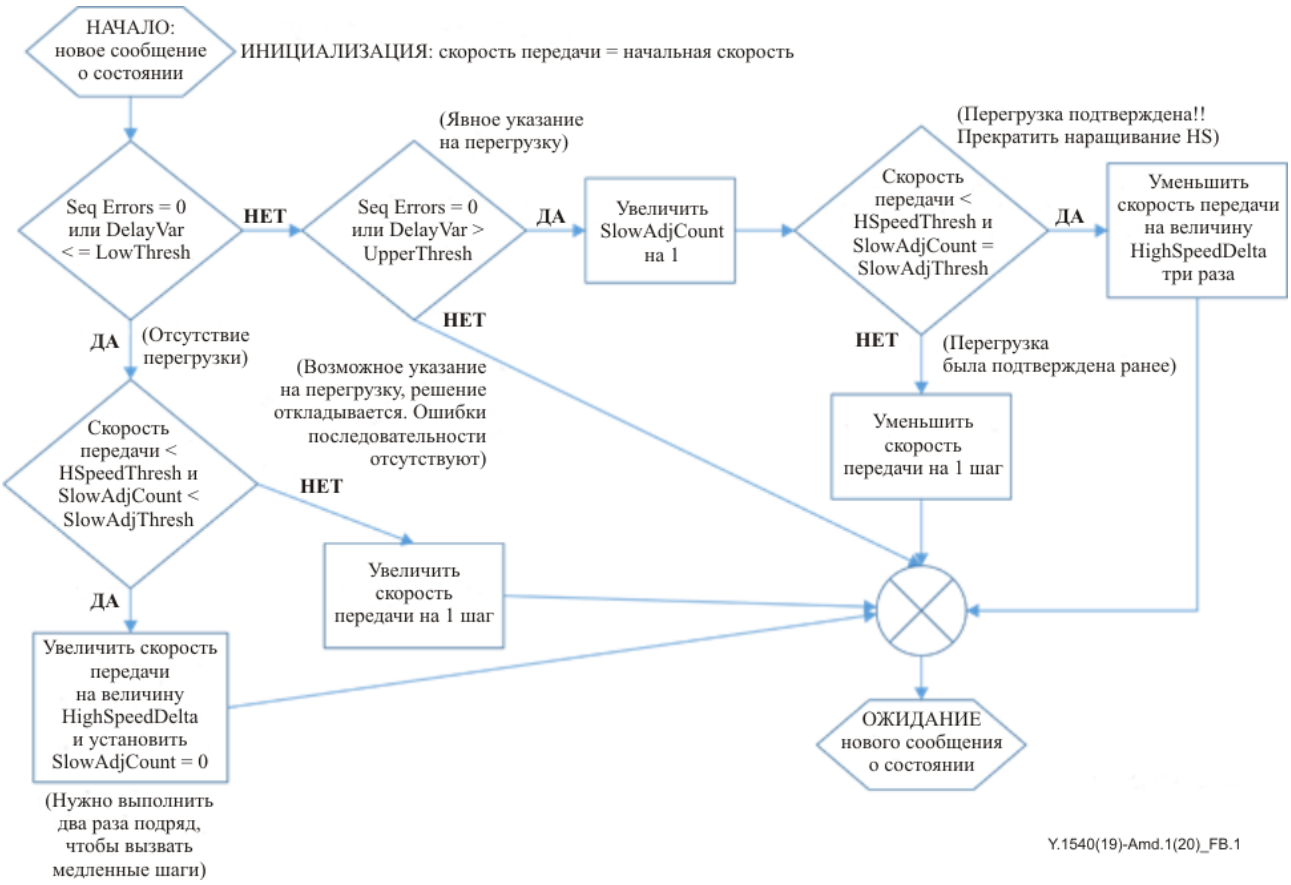


Рисунок B.1 – Блок-схема предлагаемого алгоритма регулирования нагрузки, алгоритм поиска типа B

ПРИМЕЧАНИЕ. – Решения при выполнении алгоритма могут приниматься одним из хостов системы измерения, что значительно упрощает реализацию на другом хосте и делает ее независимой от версии алгоритма.

Переменные и пороговые значения, используемые на рисунке B.1, поясняются в таблице B.1.

Таблица B.1 – Переменные на блок-схеме, их описание, диапазоны значений и значения по умолчанию

Категория/ имя переменной	Описание	Единицы измерения	Диапазон значений	Значение по умолчанию
Скорость передачи	Текущая скорость передачи (эквивалент на строке таблицы), начальное значение которой равно минимальной скорости передачи из таблицы скоростей передачи	кбит/с	500–10 000 000 (10 Гбит/с)	См. начальную скорость
Начальная скорость передачи	Начальное значение скорости передачи	кбит/с	Неприменимо	500 кбит/с
Seq Errors	Количество всех измеренных потерь или изменений порядка следования (событий, при которых порядковый номер полученного пакета не увеличился на единицу)	Число	Неприменимо	0 (ошибки последовательности отсутствуют)

Таблица B.1 – Переменные на блок-схеме, их описание, диапазоны значений и значения по умолчанию

Категория/ имя переменной	Описание	Единицы измерения	Диапазон значений	Значение по умолчанию
DelayVar	Диапазон времени передачи в прямом и обратном направлениях, RTT (или вариация задержки передачи пакета в одном направлении сверх минимального значения задержки, когда измерения DelayVar в одном направлении надежны)	мс	Неприменимо	Неприменимо
LowThresh	Нижний порог диапазона изменения RTT (диапазон – это значения, превышающие минимальное значение RTT)	мс	5–250	По умолчанию 30 мс
UpperThresh	Верхний порог диапазона изменения RTT (диапазон – это значения, превышающие минимальное значение RTT)	мс	5–250	По умолчанию 90 мс
HighSpeedDelta	Количество строк, на которые необходимо переместиться за один шаг регулирования при первоначальном увеличении предлагаемой нагрузки (для быстрого повышения)	Количество строк	≥ 2	10 строк таблицы (в настоящее время 10 Мбит/с)
SlowAdjCount	Количество последовательных сообщений о состоянии, указывающих на потери и/или вариацию задержки сверх порога UpperThreshold	Число событий	Неприменимо	См. SlowAdjThresh
SlowAdjThresh	Пороговое значение величины SlowAdjCount, используемое для определения перегрузки. Во избежание неправильной интерпретации кратковременных потерь следует использовать значения > 1	Число событий	> 1	2
HSpeedThresh	Порог для перехода между шагами изменения скорости передачи малого и большого размера (например, 1 Мбит/с и 100 Мбит/с). Может привести к использованию крупных кадров, если это разрешено	Гбит/с		1 Гбит/с

В таблице B.2 приведены значения по умолчанию входных коэффициентов для метода, описанного в Приложении A, при использовании Приложения B.

Таблица B.2 – Измеряемые переменные, их диапазоны значений и значения по умолчанию

Категория/ имя переменной	Параметр	Единицы измерения	Диапазон	Значение по умолчанию
Максимальная пропускная способность IP-уровня				
	Количество параллельных соединений	Целое число	1–10	1 соединение
	Продолжительность времени ожидания в начале испытаний	с	0–5	~2 с
Δt	Продолжительность испытаний (в нисходящем или восходящем направлении) с использованием алгоритма поиска, составляющая максимальную продолжительность процесса поиска	с	5–60	10 с
Δt	Продолжительность испытаний с фиксированной скоростью передачи (в нисходящем или восходящем направлении)	с	5–60	10 с
dt	Продолжительность интервалов между промежуточной отчетностью	с	0,1–10	1 с
	Значение тайм-аута	с	5–30	5 с
	Тип тестовых пакетов, включая длину заголовка и полезной нагрузки, присутствующие заголовки и опции, а также любые маркеры для специальной обработки в сети	Неприменимо	IPv4 или IPv6 UDP DSCP	Значение по умолчанию отсутствует UDP 00 = наилучшее из возможного
	Эталонный размер полезной нагрузки UDP	КБ	Минимум 1 кбайт, максимум 1472 байта (максимум 9000 при использовании крупных кадров)	Значение по умолчанию отсутствует, рекомендуется наибольшее значение, позволяющее избежать фрагментации
	Период между сообщениями обратной связи о состоянии (получатель предлагаемой нагрузки передает отправителю сообщения с результатами измерения показателей)	с	0,005–0,250	0,050 с
Вспомогательные показатели	Это показатели, измеряемые в том же потоке, в котором измеряется пропускная способность IP-услуг			

Таблица B.2 – Измеряемые переменные, их диапазоны значений и значения по умолчанию

Категория/ имя переменной	Параметр	Единицы измерения	Диапазон	Значение по умолчанию
IPLR	Y.1540, RFC 7680			
T_{max}	Максимальное время ожидания поступления пакетов	с	0,05–3	1 с
Выборка RTT	Y.1545, RFC 2681: RTT использует сообщения обратной связи о состоянии, поступающие от получателя			
T_{max}	Максимальное время ожидания поступления пакетов	с	0,05–3	3 с
	Разрешение меток времени	мс	0,001–1	Предлагаемое значение для фиксированного доступа: 0,001 (на основе текущей реализации)
Вспомогательный показатель: IPDV	Y.1540, RFC 3393, RFC 5481(PDV)			
T_{max}	Максимальное время ожидания поступления пакетов	с	0,05–3	1 с
	Разрешение меток времени	мс	0,001–1	Предлагаемое значение для фиксированного доступа: 0,001 (на основе текущей реализации)

Параллельные соединения вносят усложнение, но позволяют достигать более высоких скоростей.

Возможные преимущества:

- для получения совокупной скорости, необходимой при параллельных соединениях, могут использоваться параллельные системы;
- параллельные соединения могут использоваться как способ насыщения тестируемого маршрута при одной паре испытательных хостов;
- Можно получить дополнительную информацию для диагностических целей или для проверки процесса испытаний. Например, сравнение скоростей передачи данных в каждом соединении может дать полезную информацию, когда значительное различие скоростей передачи данных помогает выявить неисправность.

В настоящее время предполагается необходимость наличия для каждого соединения собственного канала обратной связи, системы обработки измерений и блок-схемы, а также необходимость предоставления сводного отчета о результатах испытаний по всем соединениям.

Дополнение I

Вопросы маршрутизации IP-пакетов

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

В данном Дополнении описываются аспекты маршрутизации IP-пакетов, относящиеся к оценке рабочих характеристик IP-услуг.

Маршрутизация IP-пакетов определяется правилами и конфигурациями протоколов маршрутизации каждого оператора сети, а также выбором самих протоколов. Например, операторы настраивают параметр "стоимости" прохождения пакетом каждого звена своей сети, и алгоритм маршрутизации вычисляет маршрут до получателя с наименьшей стоимостью на основе своего знания текущего состояния топологии сети. Очевидно, что путь, который проходит пакет от источника к получателю, оказывает значительное влияние на время задержки его передачи (как при транспортировке, так и в процессе ожидания в очереди), а также на его подверженность другим нарушениям, таким как потери, ошибки, дублирование и переупорядочение.

Еще одним способом влияния протоколов маршрутизации на характеристики передачи пакетов является автоматическое реагирование на изменения в топологии сети, такие как отказ канала или маршрутизатора или процедуры технического обслуживания с выводом сетевого элемента из эксплуатации. Когда топология сети изменяется из-за отказа, процесс восстановления по возможности восстанавливает нарушенную связь с использованием оставшейся топологии сети. Этот процесс называется "перемаршрутизацией" или "реконвергенцией" и обычно состоит из следующих шагов (для выполнения каждого из которых требуется время):

1) обнаружение отказа/события;
2) вычисление пути;
3) объявление;
4) обновление таблицы переадресации.

К тому же продолжительность процесса перемаршрутизации в значительной степени определяется параметрами таймеров, установленными оператором. Операторы также могут устанавливать время ожидания между прогонами алгоритма маршрутизации, что позволяет экономить ресурсы обработки, но в некоторых случаях может увеличить время реагирования на отказ.

Сетевые технологии вложенного IP-уровня, такие как кольца SONET и быстрая перемаршрутизация MPLS-TE, обеспечивают восстановление после отказа канала или маршрутизатора менее чем за секунду.

Дополнение II

Дополнительная терминология по вариации задержки IP-пакетов

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

II.1 Введение

В настоящей Рекомендации содержится единое основное/нормативное определение для оценки вариации последовательности задержек по отношению к эталонной задержке. В данном Дополнении приводятся два информативных/дополнительных определения (на основе определения IETF вариации задержки между пакетами и модификации вариации задержки элементов в одном пункте). В нем также даются указания о том, когда каждый параметр можно считать наиболее подходящим, и приводится соотношение между результатами наблюдений и различными параметрами. Дополнительное сравнение различных форм вариации задержки подробно описано в [IETF RFC 5481].

Существует два дополнительных подхода к количественной оценке вариации задержки:

1) параметр, основанный на [b-IETF RFC 3393], который устанавливает вариацию задержки между пакетами;

2) параметр, аналогичный вариации задержки элементов в одном пункте, описанной в [b-ITU-T I.356], который оценивает интервал поступления пакетов в одном интерфейсе относительно идеального интервала поступления.

Следует отметить, что в [b-ITU-T I.356] даны два разных определения вариации: в двух пунктах и в одном пункте.

В настоящей Рекомендации требования к характеристикам IP [ITU-T Y.1541] касательно PDV выражены в отношении нормативного параметра вариации задержки пакетов в двух пунктах.

II.2 Определение вариации задержки между пакетами

В [b-IETF RFC 3393] дано следующее определение вариации задержки.

– Может быть дано определение IPDV для пакетов внутри потока пакетов.

– IPDV пары пакетов в потоке пакетов определяется для выбранной пары пакетов в потоке из пункта измерения MP1 в пункт измерения MP2.

– IPDV – это разность между значениями задержки передачи выбранных пакетов в одном направлении.

Функция выбора однозначно определяет пару пакетов, используемых при каждом расчете показателя вариации задержки. В расчетах IPDV используются только успешно доставленные пакеты.

Первая определенная функция выбора относится к соседним пакетам в потоке. Для определения IPDV текущего пакета из задержки передачи текущего пакета в одном направлении вычитается задержка передачи предыдущего пакета в одном направлении. Если один из пакетов пары (или оба) потерян, то IPDV не определена.

Другим важным примером является функция выбора, производящая эквивалентную оценку вариации задержки для параметра PDV в двух пунктах, определенного в пункте 6.2.4. Пара пакетов всегда включает текущий пакет и пакет с минимальной задержкой передачи в одном направлении в потоке. PDV в двух пунктах для всех поступивших пакетов рассчитывается путем вычитания из их значений задержки передачи в одном направлении минимальной задержки (эталонная задержка равна минимальной задержке).

II.3 Определение вариации задержки пакетов в одном пункте

В основе параметра вариации задержки в одном пункте лежит сравнение фактического цикла поступления пакетов с требуемым (обычно периодическим). В некоторые варианты этого определения входит подстройка "срывающейся тактовой синхронизации" (когда элементы или пакеты приходят с опозданием/отставанием относительно идеального времени поступления), как указано в [b-ITU-T I.356]. В приведенном ниже определении функция срывающейся тактовой синхронизации не используется, поскольку из-за произвольного установления эталонного цикла точное значение смещения отсутствует.

PDV в одном пункте (y_k) для пакета k в MP представляет собой разность между эталонным временем поступления пакета (c_k) и фактическим временем его поступления в MP (a_k): $y_k = c_k - a_k$. Эталонное время поступления (c_k) определяется следующим образом:

$$c_0 = a_0 = 0,$$

$$c_{k+1} = c_k + T \ ,$$

где T – идеальный интервал между пакетами.

Положительные значения PDV в одном пункте ("раннее" поступление пакетов) соответствуют концентрации пакетов; отрицательные значения PDV в одном пункте ("позднее" поступление пакетов) соответствуют разрывам в потоке пакетов.

II.4 Руководящие указания по применению различных параметров

Следующие руководящие указания относятся к практической стороне измерения.

– Когда синхронизация в измерительных устройствах невозможна (или временно отсутствует):

  1) вариация задержки пакетов в одном пункте (PDV в одном пункте) служит возможной заменой диапазона/гистограммы задержки передачи в одном направлении, применимой для измерения потоков периодически передаваемых пакетов (когда надлежащим образом установлено эталонное время поступления);

  2) показатель рабочих характеристик IP-услуг (IPPM) "вариация задержки между пакетами" применим ко всем типам потоков трафика;

  3) при постоянной ошибке синхронизации можно рассчитать и использовать PDV в двух пунктах согласно Рекомендации МСЭ-T Y.1540.

– Когда в измерительных устройствах обеспечивается синхронизация:

  1) вычисление диапазона/гистограммы PDV задержки передачи в одном направлении по Рекомендации МСЭ-T Y.1540 полезно для ряда задач оценки, включая оценку размера буфера компенсации вариации задержки;

  2) IPPM "вариация задержки между пакетами" вводит параметр, чувствительный к последовательным/кратковременным изменениям и отличающийся некоторой невосприимчивостью к изменениям маршрута.

Межпакетный показатель IPDV, определенный рабочей группой (РГ) IPPM IETF, аналогичен расчету при измерении вариации времени поступления в отчетах протокола управления в режиме реального времени (RTCP). RTP рассчитывает вариацию времени поступления, как указано в пункте 6.4 [b-IETF RFC 3550], с примером реализации, приведенным в Дополнении. Несмотря на некоторые различия в методах (в вариации между поступлениями RTCP используется порядок поступления, а не последовательность передачи, как в IPDV), во многих случаях удобно сравнить "сглаженную вариацию задержки", вычисленную с использованием одиночных сигналов IPDV, с отчетами по вариации задержки RTCP (в случае переупорядочения большого количества пакетов результаты, вероятно, не совпадут). Полезно иметь параметр, который можно связать с измерениями, выполненными оконечными устройствами пользователя. Показатель IPDV с использованием пар соседних пакетов также менее чувствителен к изменениям маршрута в течение интервала измерения, эффект от которых будет наблюдаться только в парах, захваченных изменением маршрута.

Преимуществом параметра PDV в одном пункте является его простота. Возможность оценки периодических потоков в одном элементе сети чрезвычайно полезна.

Момент, который необходимо четко прописать во всех спецификациях параметров вариации, – это зависимость от длины пакета. Поскольку в задержку передачи входит время ввода (от первого бита до последнего), пакеты переменного размера имеют присущую им вариацию задержки. Для того чтобы упростить интерпретацию результатов, в спецификациях сетей и при испытаниях следует использовать пакеты одного и того же размера (и этот размер должен быть указан).

Дополнение III

Параметры, связанные со скоростью и пропускной способностью

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Данное Дополнение в версии 2019 года признано устаревшим.

Дополнение IV

Тесты состояния доступности IP-услуг и выборочная оценка параметров доступности IP-услуг

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

В данном Дополнении, которое подлежит дальнейшему изучению, описываются тесты, определяющие, находится ли IP-услуга, базовая секция или NSE в состоянии доступности или недоступности. В следующей версии в ней будут представлены методы выборочной оценки параметров доступности IP-услуг.

IV.1 Минимальный тест для оценки состояния доступности IP-услуг (для методик тестирования и испытательного оборудования)

Согласно пункту 7.1 требуется, чтобы для оценки состояния доступности использовалось как минимум M_{av} пакетов. Методики тестирования и испытательное оборудование должны пытаться распространить по крайней мере M_{av} пакетов в течение интервала времени T_{av}. Для трафика, создаваемого конечным пользователем, последовательные интервалы времени T_{av} можно объединять до тех пор, пока не будет выполнено требование наличия по крайней мере M_{av} событий приема. Этот вопрос подлежит дальнейшему изучению.

Ниже приводится описание минимально необходимых усилий для определения состояния доступности в течение одного интервала времени T_{av}. Для определения значений PIA и PIU требуется повторение этого теста. Данный минимальный тест для оценки доступности IP-услуг применим к методикам тестирования и испытательному оборудованию; некоторые требования к трафику, создаваемому конечным пользователем, представлены в пункте 7.1. Приемлем любой другой тест для оценки доступности IP-услуг, который работает не хуже, чем этот (статистически). Этот тест для оценки доступности IP-услуг применим как для сквозной передачи, так и для измерения на входе определенной базовой секции или NSE.

– Шаг 1. Определить SRC и DST.

– Шаг 2. Разместить испытательное оборудование или активировать сценарии испытаний в соответствующих пунктах измерения.

– Шаг 3. В заданное время начать передачу M_{av} IP-пакетов, распределенных по интервалу времени T_{av}.

– Шаг 4. Если количество потерянных пакетов превышает $c_1 \times M_{av}$, то IP-услуга недоступна в течение интервала времени T_{av}.

– Шаг 5. Если IP-услуга (базовая секция или NSE) не объявлена недоступной по результатам шага 4, то она доступна в течение этого интервала времени T_{av}.

Минимальный тест обеспечивает неопределенный уровень достоверности, который зависит от размера выборки M_{av}, поэтому предпочтительным является следующий тест.

IV.2 Тест для оценки доступности IP-услуг (с использованием последовательного теста на основе отношения вероятностей)

В данном пункте содержится описание непараметрического теста, в котором не делается никаких предположений об исходном распределении потерь, а используется последовательный тест на основе отношения вероятностей (SPRT) для определения того, был ли превышен порог потерь c_1 при заданном уровне ошибок. SPRT также позволяет испытателю прекратить тестирование, когда среди определенного количества последовательных пакетов и в течение определенного интервала времени наблюдается гораздо более низкий коэффициент потерь. Результат также может быть неопределенным, и в этом случае требуется дальнейшее тестирование. SPRT был впервые применен в [b-Morton] для оценки коэффициента потерь пакетов и связан с целевыми показателями при тестировании интернета.

В качестве нулевой гипотезы H0 установим вероятность потерь (или дефектов) c_1 = p0 = 0,20. В качестве альтернативной гипотезы H1 установим коэффициент потерь p1 = 0,05. Наконец, пусть уровни ошибок типа I и II равны альфа = бета = 0,001.

Уравнения SPRT [b-Montgomery], [b-Wald]:

$$X_A = -h_1 + sn \text{ (граница приемлемости);} \quad (1)$$

$$X_R = h_2 + sn \text{ (критическая граница),} \quad (2)$$

где n линейно возрастает для всех переданных пакетов и

$$h_1 = \left(\log \frac{1-\text{alpha}}{\text{beta}}\right) k^{-1}; \quad (3)$$

$$h_2 = \left(\log \frac{1-\text{beta}}{\text{alpha}}\right) k^{-1}; \quad (4)$$

$$k = \log \frac{p_1(1-p_0)}{p_0(1-p_1)}; \quad (5)$$

$$s = \left(\log \frac{(1-p_0)}{(1-p_1)}\right) k^{-1} \quad (6)$$

для p_0 и p_1, определенных в нулевой и альтернативной гипотезах, выше.

Используя приведенные выше уравнения, рассчитаем минимальное количество пакетов, необходимое для принятия H0 при наличии x дефектов, например x = 0 (без потерь).

$$X_A = 0 = -h_1 + sn; \quad (7)$$

$$n = \frac{h_1}{s}. \quad (8)$$

При использовании c1 = p0 = 0,20 в качестве уровня H0, p0 = 0,05 для альтернативного уровня H1 и при уровне ошибок 0,001 установлено, что предпочтение гипотезе H1 (с нулевыми потерями) отдается в случае наличия не менее 41 пакета, а наличие 9 потерь среди этого 41 пакета ведет к выбору гипотезы H0.

На рисунке IV.1 показаны результаты работы инструмента R [b-Rdev] с пакетом ПО [b-CVST], настроенным на указанные выше значения.

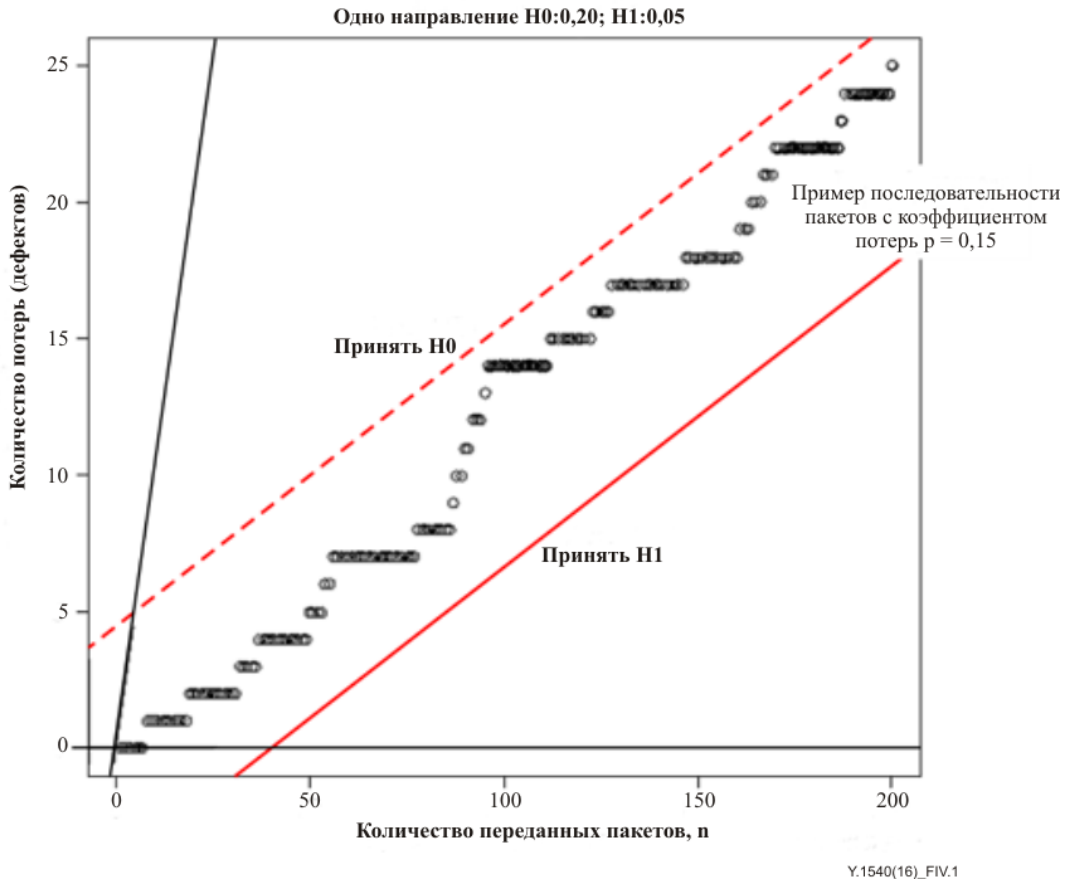


Рисунок IV.1 – Пример последовательного теста на основе отношения вероятностей

На рисунке IV.1 показано, что для выбора гипотезы H1 (с нулевыми потерями) требуется не менее 41 пакета, а при наличии 9 потерь среди этого 41 пакета предпочтение следует отдать гипотезе H0.

IV.3 Альтернативный тест для определения доступности IP-услуг на основе статистической значимости

Согласно определению [ITU-T Y.1540], IP-услуга доступна в течение интервала измерения, если IPLR для этого интервала меньше порогового значения c_1. Поскольку пакет бывает либо успешно переданным, либо потерянным, потерю пакета можно смоделировать биноминальным распределением.

Нулевая гипотеза H_0 заключается в том, что IP-услуга доступна в течение интервала измерения. Гипотеза H_0 считается верной, если средний коэффициент потери пакетов в течение интервала измерения меньше или равен c_1 (z-тест предполагает, что IP-услуга доступна, если коэффициент потери пакетов равен c_1). Гипотеза H_1 заключается в том, что IP-услуга недоступна в течение интервала измерения (коэффициент потери пакетов > c_1 в течение интервала измерения). Для того чтобы определить, поддерживается ли в процессе измерения гипотеза H_0 или H_1, предлагается использовать z-тест. Следуя [b-C-298], примем уровень достоверности равным 95% (имеется в виду уровень значимости $\alpha = 0{,}05$).

Тест состоит из одной выборки, сравниваемой с порогом c_1. Пороговое среднее $\mu_0 = c_1$, а его дисперсия, применимая к тесту, равна $\sigma = c1 * (1 - c_1)$.

Количество пакетов $n = packets_{transmitted} + packets_{dropped}$ (число переданных пакетов + число отброшенных пакетов). Тогда средний коэффициент потери пакетов равен $x_{mean} = packets_{dropped} / n$.

Статистический результат теста для определения порога: $z_{available} = sqrt(n) * (x_{mean} - \mu_0) / \sigma$.

Для уровня достоверности 95% и $\alpha = 0{,}05$ при тестировании в одном направлении в отношении значения z принимается гипотеза H_1 (IP-услуга недоступна в течение времени измерений), если $z_{available} > 1{,}645$.

Для уровня достоверности 99,9% и $\alpha = 0{,}001$ при тестировании в одном направлении в отношении значения z принимается гипотеза H_1 (IP-услуга недоступна в течение времени измерений), если $z_{available} > 3{,}09$.

IV.4 Выборочная оценка доступности IP-услуг

Для оценки PIA и PIU может быть достаточно случайной выборки измерений состояния доступности с использованием приведенного выше минимального теста. Чтобы оценить продолжительность непрерывного времени доступности или недоступности, выборка должна быть намного более частой. В [b-ITU-T X.137] представлены процедуры для сетей МСЭ-Т X.25/МСЭ-Т X.75, которые могут подойти и для IP-услуг.

Дополнение V

Сведения, касающиеся методов измерения рабочих характеристик протокола IP

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Данное Дополнение, которое подлежит дальнейшему изучению, описывает важные вопросы, связанные с развитием методов измерения рабочих характеристик протокола IP. В нем описано влияние внешних по отношению к испытуемым секциям условий, включая вопросы, связанные с трафиком, на измеряемые рабочие характеристики.

Следующие условия должны быть заданы и проконтролированы во время измерений рабочих характеристик протокола IP:

1) Измерение точных секций:
   - SRC и DST для сквозных измерений;
   - ограничение MP для измерения NSE.

ПРИМЕЧАНИЕ. – Нет необходимости выполнять измерения между всеми парами MP или всеми парами SRC и DST для определения рабочих характеристик.

2) Время измерения:
   - как долго собирались образцы;
   - когда выполнялось измерение.

3) Точные характеристики трафика:
   - скорость, на которой SRC предлагает трафик;
   - модель трафика SRC;
   - конкурирующий трафик на SRC и DST;
   - размер пакета IP.

4) Тип измерения:
   - в процессе обслуживания или вне процесса обслуживания;
   - активный или пассивный.

5) Результаты измеренных данных:
   - значения, наихудшие значения, эмпирические квантили;
   - итоговый период:
     – короткий период (например, один час);
     – длительный период (например, день, неделя, месяц).

Дополнение VI

Исходные принципы для доступности услуг IP

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

VI.1 Введение

В настоящем Дополнении дается обоснование имеющегося определения функции доступности услуг IP, приведенного в разделе 7. Целью данного документа являются предоставление дополнительной исходной информации и помощь в понимании этого сложного и важного вопроса.

VI.2 Исходные принципы

Имеется множество путей для определения доступности и множество направлений, которые ведут к оценке с использованием некоторого диапазона чувствительности и шкал времени. В настоящей Рекомендации используется простое и достаточное определение (с точки зрения сетевого оператора), которое устанавливает минимальные условия оценки. Чтобы понять, почему эта функция доступности услуг IP достаточна, необходимо понимание причин недоступности.

На рисунке VI.1 показана диаграмма Венна, на которой область отображает все время службы. В основной части настоящей Рекомендации отмечено, что поставщики услуг IP могут указывать интервалы технического обслуживания, в которые доступность услуг не гарантируется. Поэтому область времени обслуживания обычно не совпадает с областью *всего* времени.

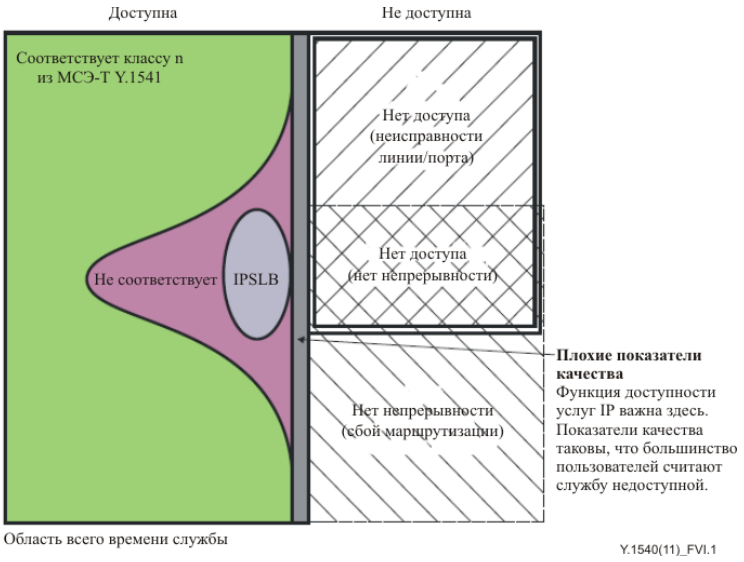


Рисунок VI.1 – Иллюстрация времени обслуживания в виде диаграммы Венна

Мы отмечаем, что время службы разделяется на две главные категории: время доступности (слева) и время недоступности (справа). Отметим также, что относительные размеры указаны не в масштабе, поскольку время доступности обычно намного больше, чем время недоступности.

VI.3 Определения зон на рисунке VI.1

Время **недоступности** состоит из следующих зон.

– **Нет доступа**. Пользователь услуг не имеет возможности связаться с IP-сетью из-за неисправности в транспортных или сетевых элементах сети доступа. Неисправность самой линии доступа или интерфейса маршрутизатора является распространенной причиной. Коэффициент потери пакетов обычно равен 100%, а время на исправление часто значительно превышает 1 минуту. Персонал технического обслуживания будет почти немедленно оповещаться системами управления при повреждении.

– **Нет непрерывности**. Пользователь услуг не имеет возможности связаться с желательным пунктом назначения из-за неисправности в системе информации IP-сети о глобальной маршрутизации. Пользователь может связаться с некоторыми пунктами назначения, но не с желательным пунктом назначения. Коэффициент потери пакетов обычно равен 100%, а время на исправление часто значительно превышает 1 минуту.

– **Нет доступа, нет непрерывности**. Пользователь услуг не имеет возможности связаться из-за обоих вышеприведенных состояний, присутствующих одновременно.

– **Плохие показатели качества**. Пользователь услуг не имеет возможности связаться надежно с желательным пунктом назначения. Коэффициент потери пакетов равен 20% или более, а пользователь будет считать услугу недоступной для связи с почти любой формой приложения в IP-сети. Когда первичной причиной такого уровня потери пакетов является перегрузка, для ее уменьшения должно запускаться сквозное управление потоком (обеспечиваемое протоколом TCP).

Время **доступности** состоит из следующих зон.

– **Соответствует классу n из [ITU-T Y.1541]**. Пользователь услуг имеет возможность связаться с желательным пунктом назначения, а показатели качества переноса пакетов соответствуют нормам согласованного класса. Оценка этого состояния обычно проводится за 1-минутные интервалы. Заметим, что любое пользовательское приложение будет иметь специфические потребности в пропускной способности; должна также учитываться способность поддерживать контракт о трафике (определенный в [b-ITU-T Y.1221]).

– **Не соответствует**. Пользователь услуг имеет возможность связаться с желательным пунктом назначения, но показатели качества переноса пакетов не удовлетворяют одной или нескольким нормам согласованного класса. Оценка этого состояния обычно проводится за 1-минутные интервалы.

– **Блок с серьезными потерями IP-пакетов (IPSLB)**. Пользователь услуг имеет возможность связаться с желательным пунктом назначения, но показатели качества переноса пакетов не удовлетворяют одной или нескольким нормам согласованного класса. В частности, коэффициент потерь достаточен для обнаружения появления блока IPSLB (предварительно определен как блок с более чем 20% потерь за 10-секундный интервал).

VI.4 Резюме

Замечено, что критерии для функции доступности услуг IP важны только в зоне "плохие показатели качества" и что время недоступности, вносимое этой зоной, мало по сравнению с другими причинами недоступности. Поэтому оценка состояния на базе только потерь и критерии, предварительно согласованные для оценки состояния (1 минута, потери 20%), считаются достаточными.

Дополнение VII

Параметры, определяющие характеристики пакетов для оценки и оптимизации методов восстановления потока

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

VII.1 Введение

Параметры рабочих характеристик IP-уровня имеют множество применений, одним из классов которых является мониторинг сети и выявление неисправностей. Эти параметры также используются в качестве основы для соглашений об уровне обслуживания (SLA). В обеих вышеупомянутых областях передача пакетов считается характеристикой сети, обеспечивающей транспортировку UNI-UNI.

Имеется и второй ракурс: параметры рабочих характеристик IP-уровня также характеризуют сети с точки зрения разработчиков приложений. Хотя им полезны многие параметры, используемые при мониторинге сетей, вероятно, что для каждой области применения имеются свои уникальные параметры. Рисунок VII.1 иллюстрирует два разных подхода или две области применения параметров рабочих характеристик IP-уровня.

В Рекомендации МСЭ-T Y.1540 определены параметры рабочих характеристик и доступности IP-сетей. В ней определены первичные и вторичные результаты передачи пакетов и ряд параметров рабочих характеристик пакетов на основе этих результатов, включая функцию доступности IP-услуг.

Настоящая версия Рекомендации МСЭ-T Y.1540 основывается на фундаментальных определениях и концепциях для стандартизации нового набора нормативных параметров рабочих характеристик системы восстановления потока. Целью новых параметров является предоставление информации, относящейся к разработке и настройке методов верхнего уровня (уровня приложений) для компенсации потери пакетов по различным причинам (включая ошибки и вариацию задержки). Таким образом, если эти новые параметры для оценки рабочих характеристик пакетов достигнут своей цели, то проектирование и/или оптимизация и оценка рабочих характеристик методов восстановления потока в приложениях должны упроститься.

Настоящее Дополнение начинается с краткого описания методов восстановления потока на уровне приложений. Затем предлагается очень простая модель, предназначенная для применения в отношении многих разных методов восстановления.

Рисунок VII.1 – Две различные области применения параметров рабочих характеристик IP-услуг

Обычная процедура заключается во введении новых показателей в качестве информативных дополнений, чтобы потенциальные пользователи получили возможность оценить их до включения в основную часть Рекомендации в качестве нормативных параметров. Эти новые показатели включены в Рекомендацию МСЭ-Т Y.1540 по принципу "сначала как информативные". В своих исследованиях МСЭ-Т рассмотрел множество вкладов с подробным описанием опыта работы с параметрами рабочих характеристик системы восстановления потока, который послужит основой для повышения статуса этих параметров до нормативного.

VII.2 Краткое описание методов восстановления потока на уровне приложений

Существует три основных типа методов компенсации нарушений при передаче пакетов на уровне приложений. Мы уделим основное внимание непрерывно работающим приложениям в режиме реального или близкого к реальному времени (аудио, видео), которые неэластичны – доставка информации происходит по заранее установленному графику, – а не классу эластичных приложений передачи данных, обычно обслуживаемых TCP и основанными на нем надежными службами передачи потока октетов.

Прямая коррекция ошибок (FEC). Это метод, при котором потоки пакетов перед передачей организуются в блоки. Для каждого блока выполняются определенные вычисления, и к потоку добавляются служебные пакеты, которые получатель может использовать для восстановления некоторой части пакетов блока, если они потеряны, переданы успешно, но с задержкой или повреждены при транспортировке. Обычно объем служебных данных составляет от 5 до 20% размера информационного блока. В *идеальной* схеме FEC количество потерянных пакетов, которые можно восстановить, *равно* количеству служебных пакетов. Основные характеристики этой схемы:

- размер информационного блока, указанный в пакетах и в единицах времени;
- количество служебных пакетов по отношению к информационному блоку, что приблизительно соответствует восстановительной способности схемы.

Автоматический запрос повторной передачи (ARQ). При этом методе имеется канал обратной связи, по которому получатель, обнаружив, что некоторые пакеты потеряны, задержаны или повреждены, может запросить повторную передачу (так называемый выборочный ARQ). Потерянные пакеты повторно отправляются в отведенное для них время, чтобы занять свое место, когда информация передается на более высокие уровни для декодирования и воспроизведения. Иногда в TCP вносят изменения, чтобы он обслуживал неэластичные потоки в роли ARQ. Предусмотрено время ожидания для определения того, потеряны ли пакеты или только задержаны, что подобно информационному блоку, используемому в схемах FEC. Также может быть наложено ограничение на количество повторно передаваемых пакетов, которые могут добавляться в первичный поток за любой промежуток времени, и это соответствует накладным расходам в схемах FEC. Метод ARQ позволяет повторно передавать потерянные пакеты в блоке в пределах заданного объема повторной передачи. Следует отметить, что повторно передаваемые пакеты добавляются к следующему блоку информационных пакетов, но идея остается той же.

Таким образом, оба метода ARQ и FEC можно описать с использованием одних и тех же основных переменных, характеризующих размер информационного блока и максимальный размер, подлежащий восстановлению.

Маскировка ошибок на уровне приложений. Это метод, при котором декодеры пытаются компенсировать потерянную или поврежденную информацию, используя различные методы для конкретных приложений, часть которых стандартизирована. Применимость простой модели (выведенной ниже) к этому классу методов подлежит дальнейшему изучению.

VII.3 Простая модель восстановления потока на уровне приложений

Каждый поток пакетов уровня приложений моделируется как содержащий две категории пакетов:

1) временные интервалы T_I или блоки b информационных пакетов;
2) служебные пакеты или максимальное количество восстанавливаемых пакетов x, связанные с информационным блоком.

Задача разработчика метода восстановления состоит в том, чтобы выбрать такой размер информационного блока в сочетании с (максимальным) количеством служебных пакетов, который будет достаточным для компенсации высокого процента нарушений в пакетной сети (потери, чрезмерная задержка и искажение) при работе в пределах общих ограничений пропускной способности при передаче пакетов в системе и при обеспечении достаточного качества в потоке приложения.

Новые параметры рабочих характеристик (описанные в пункте 6.10) должны помочь в принятии этих решений.

VII.4 Пример параметров рабочих характеристик для оценки переменных восстановления потока

На рисунке VII.2 приведен пример расчета параметров восстановления потока, где b = 9 пакетам, а x = 3 пакетам.

Рисунок VII.2 – Иллюстрация расчета параметров рабочих характеристик для восстановления потока

VII.5 Обсуждение вопросов измерения и использования параметров

При попытке оценить рабочие характеристики системы восстановления с неизвестным способом выравнивания блоков временные интервалы T_I или блоки b могут перекрываться, чтобы можно было оценить разные способы выравнивания интервалов времени в зависимости от количества нарушений (анализ со скользящими интервалами). Использование одного фиксированного, неперекрывающегося интервала для оценки и анализа рабочих характеристик проблематично, так как разница в выравнивании информационного блока с дополнительными данными может приводить к худшим рабочим характеристикам.

Существует два подхода к анализу потоков пакетов для определения оптимальной комбинации переменных восстановления потока:

1) использование (нескольких) произвольно установленных интервалов между пакетами (в единицах времени или количества пакетов), как это сделано выше;

2) подсчет интервалов между последовательными поврежденными пакетами и интервалов при передаче неповрежденных пакетов.

Подход с подсчетом последовательных интервалов, по-видимому, обладает гибкостью, недоступной при оценке, основанной на фиксированных интервалах; он позволяет определить фактический размер интервалов с нарушениями/без нарушений в потоке и не подвержен влиянию проблемы выравнивания интервалов. Однако результирующие параметры, описывающие длину интервалов с нарушениями/без нарушений, не зависят от их фактической последовательности. Эта последовательность изменений между интервалами с нарушениями и без нарушений может иметь большое значение. Кроме того, для метода подсчета последовательных интервалов требуется определенный способ оценки того, было ли превышено пороговое значение x, поскольку это важно для определения результата с нарушениями. Если необходимо оценить более одного значения x, то может потребоваться несколько прогонов с сохраненными данными.

В любом случае результаты можно выразить в виде распределений вероятностей или накопленных вероятностей по зависимым и независимым переменным, как показано в приведенном ниже примере (рисунок VII.3).

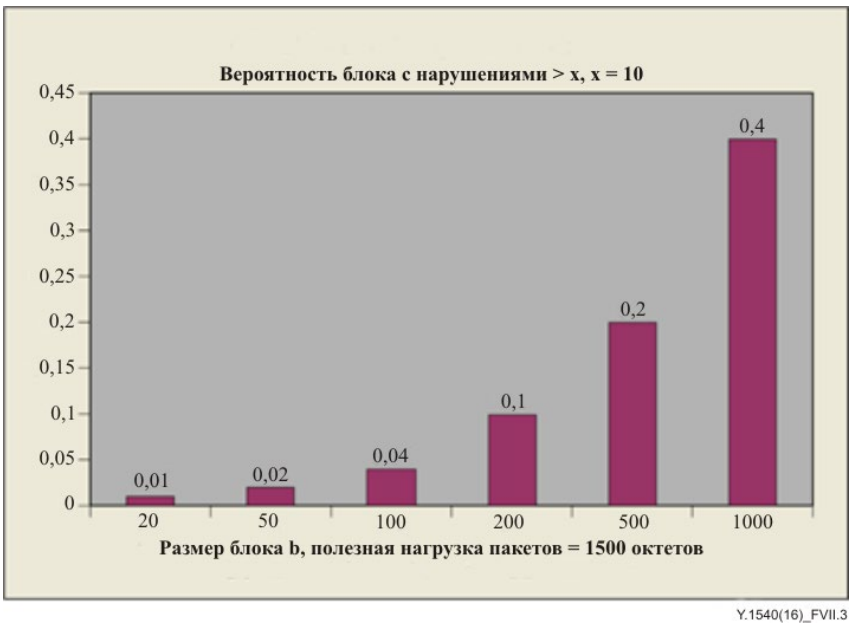


Рисунок VII.3 – Пример графика результатов оценки параметров восстановления потока для диапазона размеров блоков при фиксированном значении x и фиксированном размере пакетов

VII.6 Дополнительные соображения

Хотя определение характеристик сети с использованием описанных выше параметров может быть полезным, для прогнозирования качества, обеспечиваемого для пользователей, необходимо знать детали системы восстановления данного приложения. Когда методы FEC и ARQ работают за пределами своей способности выполнять полное восстановление потерь, они создают разные шаблоны потери пакетов. Типичные размеры блоков, связанные с каждым методом, различаются, при этом ARQ часто характеризуется большими размерами блоков.

Схемы FEC организуют информационный блок и служебные пакеты разными способами (иногда их называют одномерными или двумерными формами), при этом менее сложные схемы демонстрируют большую зависимость между конкретным шаблоном потерь и способностью восстановления этих потерь. Разработчику должна быть известна и приниматься во внимание разница между рабочими характеристиками простых схем FEC и идеальной схемы, работающей в соответствии с приведенными выше параметрами.

В некоторых приложениях может использоваться последовательность, состоящая из разных описанных выше методов. Например, система может использовать FEC или ARQ в сочетании с маскированием ошибок на уровне приложения. В еще одном примере на одном участке маршрута может использоваться FEC, на другом – ARQ или иная схема FEC и, наконец, схема маскирования ошибок на уровне приложения.

Наконец, определенные выше кратковременные параметры рабочих характеристик могут быть полезны при устранении неполадок, помогая определить характер проблем в сети, но этот вопрос подлежит дальнейшему изучению.

Дополнение VIII

Структура пропускной способности IP-уровня

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

VIII.1 Введение

В этом Дополнении дается более подробная информация, относящаяся к показателям пропускной способности, определенным в пункте 6.11.

Сведения о пропускной способности IP-уровня, доступной в режиме реального времени в IP-сети (перегруженной или нет), представляют собой ценную информацию для операторов сетей и пользователей приложений. Этот параметр можно использовать для оптимизации и мониторинга сети, устранения неполадок, выбора сервера или шлюза, выравнивания нагрузки, управления доступом, контроля перегрузки или проверки выполнения соглашения об уровне обслуживания (SLA) для сетевых услуг гарантированного или повышенного качества, предоставляемых поставщиком таких услуг.

Параметры и методы измерения, определенные в нормативном Приложении A, заменяют перечень научных проектов и примеров инструментов, приводившийся в данном Дополнении ранее, и касаются нескольких вопросов, указанных ниже как подлежащие дальнейшему изучению.

VIII.2 Терминология и связь с IETF RFC 5136

В литературе на английском языке используются взаимозаменяемые термины "available capacity" и "available bandwidth" (доступная пропускная способность). В [IETF RFC 5136] обсуждается соответствующая терминология, в основном вопрос о том, какой термин следует использовать для описания характеристик IP – "capacity" или "bandwidth". В [IETF RFC 5136] предлагается использовать термин "capacity", и для согласования с IETF в Рекомендации МСЭ-T Y.1540 также используется термин "capacity".

В [IETF RFC 5136] определены параметры, связанные с пропускной способностью, аналогичные тем, которые определены в пункте 6.11. Однако одно из основных различий между определениями МСЭ-T и IETF заключается в том, что в Рекомендации МСЭ-T Y.1540 учитывается возможность влияния хостов сети на значения параметров пропускной способности IP-уровня. В [IETF RFC 5136] этот вопрос не рассматривается, но в IETF он обсуждался. Параметры МСЭ-T Y.1540 определены для базовых секций, так что они, по существу, учитывают пропускную способность как каналов, так и узлов в этой секции.

В таблице VIII.1 приведено сопоставление определений параметров, приведенных в пункте 6.11 и в [IETF RFC 5136].

Таблица VIII.1 – Сопоставление определений параметров в МСЭ-T Y.1540 и в IETF RFC 5136

Пункт 6.11 МСЭ-T Y.1540	IETF RFC 5136
Число переданных битов IP-уровня (IP-layer bits transferred)	Число битов IP-уровня (IP-layer Bits)
Пропускная способность секции IP-уровня (IP-layer section capacity)	Пропускная способность канала IP-уровня (IP-type-P Link Capacity)
Используемая пропускная способность секции IP-уровня (IP-layer used section capacity)	Использование канала IP-уровня (IP-type-P Link Usage)
Степень использования секции IP-уровня (IP-layer section utilization)	Степень использования канала IP-уровня (IP-type-P Link Utilization)
Доступная пропускная способность секции IP-уровня	Доступная пропускная способность канала IP-уровня

Таблица VIII.1 – Сопоставление определений параметров в МСЭ-Т Y.1540 и в IETF RFC 5136

Пункт 6.11 МСЭ-Т Y.1540	IETF RFC 5136
(IP-layer available section capacity)	(IP-type-P Available Link Capacity)
Пропускная способность NSE IP-уровня (IP-layer NSE capacity)	Пропускная способность маршрута IP-уровня (IP-type-P Path Capacity)
Доступная пропускная способность NSE IP-уровня (IP-layer available NSE capacity)	Доступная пропускная способность маршрута IP-уровня (IP-type-P Available Path Capacity)
Пропускная способность ограничивающей секции IP-уровня (IP-layer tight section capacity)	Определение отсутствует

VIII.3 Вопросы для дальнейшего изучения

Определения параметров пропускной способности, приведенные в настоящей Рекомендации, не относятся явно к многопунктовым маршрутам; однако эти вопросы определены как подлежащие дальнейшему изучению.

Обсудите и определите методы измерения, отвечающие требованиям операторов в отношении точности измерения, скорости и накладных расходов.

Есть ли способ создать систему для определения ограничивающего звена IP-уровня?

Регулирующие функции вызывают потерю пакетов, и из-за этого ограничения для будущих методов измерения может потребоваться другой метод оценки, отличный от методов, основанных на дисперсии пакетов.

Дополнение IX

Объяснение неадекватности измерения на основе TCP для удовлетворения нормативных требований

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

IX.1 Введение

Для читателей настоящей Рекомендации может оказаться полезным знание последствий применения нормативных требований, приведенных в пункте 6.12, при рассмотрении методик измерения, особенно тех, которые основаны на имеющихся реализациях протокола TCP. Хотя измерения на основе TCP считаются полезными для информативных исследований опыта пользователей, они не составляют основу для стандартных показателей, методов измерения или целевых числовых значений. Сравнение в данном Дополнении протокола TCP с требованиями, изложенными в пункте 6.12, проясняет его статус как метода измерения.

IX.2 Сравнение с нормативными требованиями

Требования, изложенные в пункте 6.12, представлены в виде двух пронумерованных списков. Первый список требований относится ко всем параметрам, а второй – к параметрам, которые оценивают способность поддерживать заданную скорость передачи IP-пакетов.

По первому списку требований (все параметры):

1) в отношении обязательного учета доставки пакетов в сеть и их успешной передачи: в некоторых версиях TCP может вестись подсчет повторно переданных сегментов во время соединения (через интерфейс управления), но повторные передачи основаны на адаптивном тайм-ауте повторной передачи (RTO), а не на проверке того, действительно ли пакеты были потеряны, или подтверждение поступило по истечении этого тайм-аута и не было ли сообщение подтверждения ACK потеряно после успешной доставки. Получатели TCP не различают, доставлены ли успешно исходные или повторно переданные пакеты (или те и другие). Кроме того, разные алгоритмы управления перегрузкой TCP различаются методами достижения равноправия по отношению к другим потокам и пропускной способностью, что приводит к большему количеству потерянных пакетов при использовании агрессивных алгоритмов или к излишнему снижению скорости передачи, когда потеря пакетов неправильно интерпретируется как сигнал перегрузки (отметим, что при управлении потоком TCP постоянное отображение потери пакетов интерпретируется как перегрузка);

2) в отношении требуемой возможности измерения частичных маршрутов: механизм контроля перегрузки TCP очень чувствителен ко времени передачи в прямом и обратном направлениях (RTT) и реагирует на него нелинейным и иногда неожиданным образом. Поэтому измерение частичного маршрута (EL или NS) на основе TCP обычно не позволяет спрогнозировать характеристику всего маршрута, и одна из основных причин – зависимость TCP от RTT.

По списку требований для оценки устойчивой скорости передачи пакетов:

1) в отношении требуемого описания структуры трафика, предлагаемого сети: структура передачи пакетов определяется фазами затяжного пуска и предотвращения перегрузки TCP, и эта структура варьирует в широких пределах в зависимости от условий на маршруте, особенно от наличия перекрестного трафика и от характеристик любых встречающихся "узких мест". Таким образом, эту структуру трудно или невозможно ограничить или спрогнозировать при работающем механизме управления потоком TCP;

2) в отношении требования ограничить скорость трафика до значения, которое меньше пропускной способности соединительных звеньев: механизм управления потоком TCP постоянно проверяет доступную пропускную способность, предполагая, что условия могут измениться. Ограничивать отправителя TCP точным значением пропускной способности с использованием известных параметров нецелесообразно, отчасти из-за изменения RTT в течение времени существования TCP-соединения. Другими словами, TCP всегда может передавать трафик со скоростью, превышающей пропускную способность соединительных звеньев.

Все трудности, вызванные механизмом управления потоком TCP, еще больше усугубляются тем, что одновременно работают несколько TCP-соединений, каждое из которых независимо оценивает свое соединение на одном и том же маршруте.

В заключение следует отметить, что транспортный протокол определяется и реализуется в хостах пользователей и находится вне поля зрения поставщиков услуг передачи пакетов на основе IP. Стандартные оценки рабочих характеристик услуг поставщика должны исключать вклад уровней, выбранных другими, и соответствовать нормативным требованиям, изложенным в пункте 6.12.

Дополнение X

Сводные результаты лабораторных (первый этап) и полевых (второй этап) испытаний: план оценки согласно Приложению A

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

X.1 Введение

На своем промежуточном собрании в апреле 2018 года и на специальных собраниях во время Пленарного заседания ИК12, которое состоялось в мае 2018 года, рабочая группа по Вопросу 17/12 согласовала план разработки показателей (или параметров) и методов измерения для оценки пропускной способности IP-уровня (наряду с задержкой и потерей пакетов и другими ключевыми показателями качества). Работа началась с составления плана лабораторной оценки некоторых существующих показателей и методов. В новом Приложении A содержится план оценки и сравнения показателей, методов, моделей и инструментов для измерения услуг доступа в стабильных и воспроизводимых лабораторных условиях. Работа опирается на текущие параметры, изложенные в пункте 6.11, и требования, изложенные в пункте 6.12.

По мере продолжения работы стало ясно, что для обеспечения широкого и быстрого внедрения в отрасли потребуются параллельные усилия нескольких ОРС по согласованию стандартизированных рабочих характеристик IP-уровня. К этим усилиям относятся предложение новой работы в ТК по STQ ETCИ и призыв к сотрудничеству в рамках рабочей группы IETF по измерению показателей IP (с двумя добровольцами). Другие ОРС (ИК 11 МСЭ-Т, ТК INT ETCИ и BBF) получили несколько заявлений о взаимодействии с описанием текущего состояния дел.

На собраниях осенью 2018 года было принято решение разделить план оценки на два этапа, и были собраны первые результаты испытаний первого этапа. План испытаний первого этапа основан на оценке BEREC систем измерения доступа в интернет, приведенной в [b-BEREC], где Требование 127 предусматривало обязательное испытание для определения точности скорости передачи данных с использованием "программного или аппаратного обеспечения формирования трафика" на нескольких скоростях до 500 Мбит/с. Другие подробности отсутствовали, и критический фактор задержки был исключен. В новом Приложении A это и другие упущения плана BEREC устранены. На втором этапе оценки будут исследоваться выводы первого этапа по сетям доступа.

Вклады по Вопросу 17/12 также включали два обзора научных исследований по измерению характеристик доступа в интернет. В одном приведены итоги последнего обзора, а также заметки с семинара-практикума ИК12, проводившегося в ноябре 2018 года, и в конце этого вклада резюмируется несколько ключевых моментов, наиболее важным из которых является то, что эталонными для измерения пропускной способности считаются испытания на основе UDP.

В этом вкладе обобщаются описания и результаты испытаний ИК12-C275, TD627 и TD701 R2, полученные по январь 2019 года. В другом вкладе содержатся обсуждение и вопросы, рассмотренные на промежуточном собрании рабочей группы по Вопросу 17 (виртуальном, в январе 2019 года), и представлены новые результаты лабораторных испытаний по нескольким показателям, инструментам и методам измерения.

X.2 Установка для лабораторных испытаний первого этапа

В данном разделе описаны два основных способа создания контролируемой и изолированной тестовой среды в качестве основы для повторяемых сравнений методов испытаний.

На приведенном ниже рисунке показаны две разные утилиты, обеспечивающие гибкое управление трафиком/скоростью передачи данных на вычислительной платформе общего назначения. Различные утилиты управления трафиком можно применять тремя способами.

Рисунок X.1 – Три возможных способа тестирования на вычислительной платформе общего назначения

На рисунке X.1 испытательное устройство подключено к хост-компьютеру общего назначения физическими каналами с пропускной способностью 10 Гбит/с. Испытательное устройство также представляет собой хост-компьютер общего назначения, но он полностью изолирован от хост-компьютера, осуществляющего управление трафиком, что позволяет каждому узлу выделять ресурсы для решения своих задач в тестовой среде. Можно устанавливать и тестировать через узел управления трафиком разные реализации возможных методов измерения.

Имеется три варианта реализации функции формирования трафика. В первой слева схеме используется эмулятор сети с ядром Linux, который может эмулировать задержку и помогает управлять трафиком после настройки подходящей сетевой карты и физических интерфейсов. Виртуальный коммутатор просто коммутирует кадры между двумя своими портами. Эту конфигурацию обычно называют "phy2phy".

Конфигурация phy2phy использовалась для испытаний, описание и результаты которых приведены ниже. Описание остальных конфигураций (с использованием утилиты Intel DPDK testpmd) см. в Приложении A.

X.3 Подробное описание тестовой установки

На приведенном ниже рисунке показаны детали тестовой установки phy2phy с двумя хост-узлами, системами измерения, сетевыми интерфейсами с каналами передачи данных 10 Гбит/с, а также конфигурации, включая пространство имен сети и виртуальный коммутатор с открытым исходным кодом (OVS). Хосты расположены в лаборатории OPNFV, организованной компанией Intel [b-Pod12].

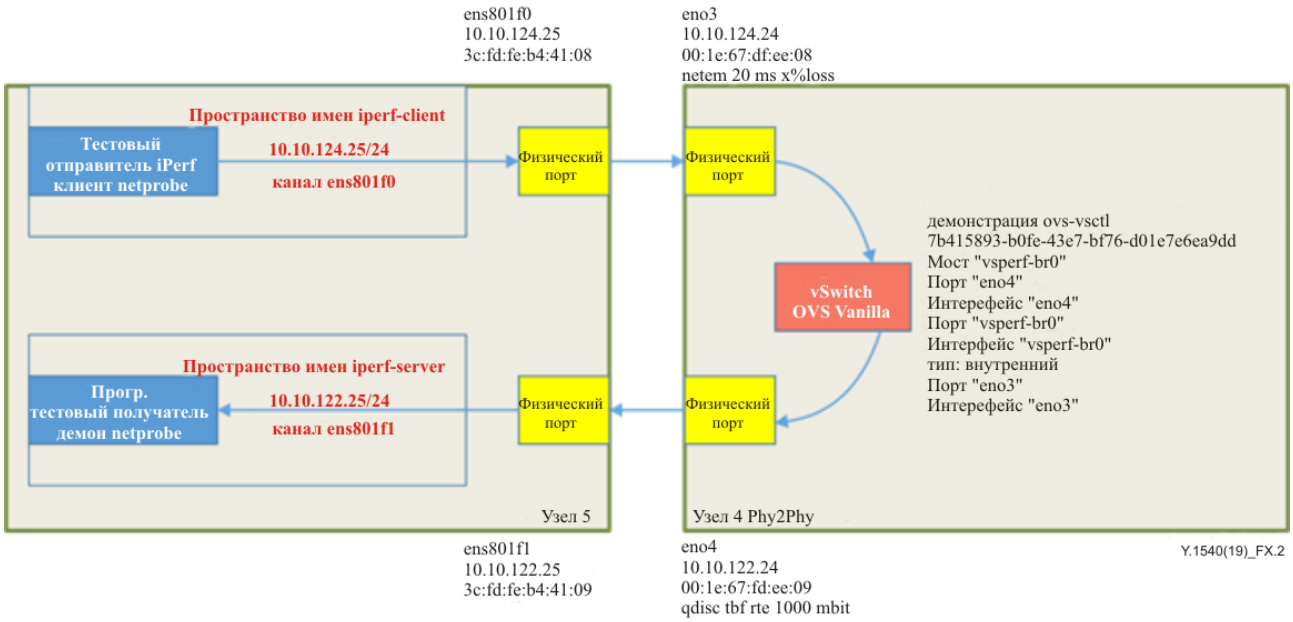


Рисунок X.2 – Тестовая установка, состоящая из утилиты iPerf, калиброванной сети (DUT) и средств генерирования (измерения) конкурирующего трафика

Пространство сетевых имен необходимо для принудительного вывода трафика через соответствующие сетевые интерфейсы и недопущения внутренней маршрутизации через ядро. Инструмент Netprobe может обеспечивать как конкурирующий UDP-трафик, так и подпоток общего трафика с измерением потерь и задержек по каждому пакету (как в одном направлении, так и в обоих направлениях с миллисекундным разрешением).

X.4 Инструменты тестирования

В оценках, которые привели к настоящему резюме и текущим решениям, использовались многие измерительные инструменты с открытым исходным кодом. Это такие инструменты, как Cisco T-rex, iPerf 2, iPerf 3, NetProbe, а также новый, еще не имеющий названия инструмент. Функции формирователя и ограничителя трафика, как и эмулятора сетевых искажений netem, присущи типичному дистрибутиву Linux.

Оценку на первом этапе испытаний обеспечили ранние тесты UDP с использованием инструмента T-rex и усовершенствованный алгоритм поиска, основанный на бинарном поиске с проверкой на потери (BSwLV), который описан в [b-TST 009]. Однако выбор методики (потери определялись с помощью несинхронизированных счетчиков в пунктах передачи и приема) и трудность организации тестирования TCP побудили к исследованию других инструментов.

Хотя на смену iPerf 2 пришла разработка iPerf 3, текущие испытания показали, что iPerf 2 более предсказуем в настройке, если освоить некоторые соответствующие приемы. В этом обзоре используется iPerf 2 (если не указано иное). Везде используются пакеты размера MTU. iPerf 3 на платформе Linux имеет некоторые "особенности", которые, по-видимому, нуждаются в сортировке (некоторые конфигурации сталкиваются с ограничениями скорости передачи). В настоящее время имеются параллельные разработки iPerf 3, и, для того чтобы различать разные исходные коды, необходим номер подверсии.

NetProbe использовался исключительно как дополнительная система измерения (обеспечивающая измерение задержки, которое в iPerf 2/3 отсутствует) и как генератор конкурирующего трафика (с возможностью измерения).

X.5 Калибровка сообщаемых результатов с помощью iPerf 2

iPerf 2 сообщает результаты измерения скорости по количеству доставленных байтов полезной нагрузки транспортного уровня (поверх уровня UDP или TCP). Скорость фильтра на основе буфера маркеров (TBF) указывается в "битах в кадрах уровня 2 без ETH CRC", так что в расчеты TBF включаются заголовки, добавляемые к полезным нагрузкам транспортного уровня (скорость рассчитывается с учетом битов заголовка ETH, IP и транспортного уровня).

В расчеты скорости приема "со служебными данными" входят октеты служебных данных на каждый пакет в следующих заголовках: ETH (14), IP(20) и UDP(8) или TCP(20). Типичная скорость полезной нагрузки UDP 972 Мбит/с с поправкой на служебные данные (1,0286) составляет 999,799 Мбит/с.

Размер кадра TCP является переменным, поскольку iPerf 2 передает отправителю блок размером 8 КБ, в результате чего получается пять кадров размером MTU и 892 байта в оставшемся кадре для завершения блока. Однако при наблюдении в процессе трассировки пакетов размер пакета отличается от этой модели. Простейший поправочный коэффициент для служебных данных (OH) в потоках TCP учитывает при расчете только максимальный размер сегмента (MSS):

54 + 1446 = 1500; 1500/1446 = 1,0373 * измеренная скорость полезной нагрузки TCP.

Максимальная скорость полезной нагрузки TCP при трех соединениях по 956 Мбит/с с поправкой на служебные данные (и без усложняющих факторов, таких как задержка) составляет 991 Мбит/с. В большинстве случаев скорость полезной нагрузки TCP, измеренная при выверенной скорости формирователя 1 Гбит/с, оказывается заметно меньше 956 Мбит/с (см. рисунки X.4 и X.5).

Также имеет место некоторое несоответствие между расчетным максимальным размером окна приема TCP (RWIN), сообщаемым iPerf 2, и измеренным значением с RTT 20 мс. Один тест с тремя соединениями TCP дал следующий результат:

956 Мбит/с/3 соединения = 318 666 666 бит/с на соединение;

318 666 666/50 окон в секунду = 6 373 333,32 бита в RWIN

или 796 666 байтов ~ 0,8 Мбайт (а не 0,08 Мбайт, как сообщает iPerf 2).

X.6 Обзор подхода к тестированию и результатов

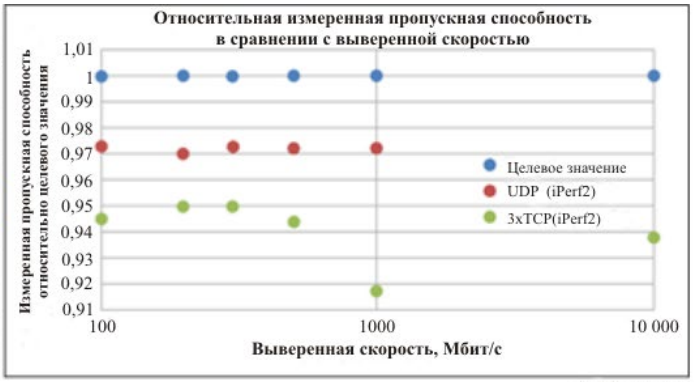
Часть процесса первоначального тестирования (до ноября 2018 года) показана на следующем рисунке.

Рисунок X.3 – Обзор первоначального тестирования

X.7 Обзор испытаний, в которых измеренная пропускная способность сравнивалась с выверенными скоростями физического уровня

В тестовой установке и конфигурации испытаний (описаны на рисунке X.2, выше) используется фильтр на основе маркеров буфера (TBF) в узле 4 eno4 с настраиваемой целевой скоростью и допускается некоторая неравномерность трафика, но также устанавливается максимальное время, в течение которого любой пакет может оставаться в обработке (обычно 4 мс). Одна из самых высоких скоростей, которую предполагалось использовать в [b-BEREC] для проверки согласно требованию 127, – 100 Мбит/с. На большинство результатов, представленных в данном разделе, повлияла смоделированная (в эмуляторе сети) задержка.

	C-Rate, M	Целевое значение: UDP (iPerf	3xTCP(iPerf2))		Задержка, мс
29 нояб.	100	1	0,973	0,945	40
29 нояб.	200	1	0,97	0,95	40
29 нояб.	300	1	0,973	0,95	40
29 нояб.	500	1	0,972	0,944	40
24 янв.	1000	1	0,972	0,917	20
11 дек.	10 000	1		0,9379	0
			2 янв.		



Y/1540(19)_FX.4

Рисунок X.4 – Сводная информация об измеренной пропускной способности в сравнении с выверенными скоростями

Как показано на рисунке X.4, методы iPerf 2, основанные на UDP, работают практически без потерь на скорости, настроенной в TBF, например 972 Мбит/с в полезных нагрузках UDP (которая с учетом заголовков корректируется до 1001 Мбит/с). Измерения с тремя соединениями TCP чувствительны к задержке в обоих направлениях, особенно когда скорость TBF увеличивается до 1000 Мбит/с, и коррекции на заголовки недостаточно для ее компенсации (хотя здесь влияет начальная задержка TCP, скорость 956 Мбит/с достигается через 2 с).

Весьма полезным источником информации об ограничении скорости являются измерения только каналов 10 000 Мбит/с (10 Гбит/с) (без TBF или эмулятора сети). После применения поправочных коэффициентов на заголовки тесты с тремя и пятью соединениями TCP в этих реалистичных условиях продолжали занижать скорость физического уровня. В этой тестовой конфигурации iPerf 2 и T-rex не смогли сгенерировать ни одного потока UDP со скоростью выше ~5 Гбит/с (этот результат был изучен дополнительно: два клиента iPerf 2 одновременно генерировали трафик 3,94 + 4,18 = 8,12 Гбит/с, и, по-видимому, нужен третий поток).

X.8 Обзор тестов для сравнения измеренной пропускной способности в зависимости от двусторонней задержки

При использовании одной целевой скорости TBF 1 Гбит/с с помощью эмулятора сети эмулировалась постоянная задержка на прямом и обратном маршрутах (в узле 4 eno3).

	Задержка, мс	Целевое значение: IG UDP (iPerf 3xTCP(iPerf2))		
27 янв.	40	1	0,972	0,62
27 янв.	40	1	0,972	0,312
27 янв.	40	1	0,972	0,313
27 янв.	40	1	0,972	
27 янв.	20	1	0,972	0,786
27 фев.	20	1		0,906
27 фев.	10	1		0,952
27 фев.	10	1		0,792
27 фев.	5	1		0,953
27 фев.	5	1		0,948
11 дек.	0	1	0,972	0,9379
27 фев.	0	1		0,956

Рисунок X.5 – Сводная информация об измеренной пропускной способности в зависимости от двусторонней задержки при целевой скорости 1 Гбит/с

Измерения задержки с помощью Netprobe (см. следующий раздел) подтверждают, что, когда TBF ограничивает скорость (и некоторые пакеты отбрасываются), настроенная задержка TBF для некоторых пакетов добавляет к задержке эмулятора сети (20 или 40 мс, см. выше) целых 4 мс. Результаты теста пропускной способности UDP не зависят от задержки, но позволяют удобно добавлять измерения задержки UDP. Однако контур управления потоком TCP чувствителен к задержке (в частности, времени передачи в прямом и обратном направлениях), и с увеличением задержки результаты измерения его пропускной способности ухудшаются (особенно когда интегральный показатель задержки передачи (BW*Delay) превышает установленный максимальный размер окна приема, см. измерения при 40 мс на рисунке X.5).

По запросу членов STQ ETCИ были проведены тесты TCP при значениях задержки 5 и 10 мс и повторены все тесты при задержке от 0 до 20 мс. Результаты показывают, что измерение на основе TCP дает изменчивые результаты, а задержка имеет тенденцию увеличивать их потенциальную изменчивость. Эта проблема измерений с управлением потоком TCP отмечается в разделе 4 [IETF RFC 8337].

X.9 Обзор испытаний с конкурирующим трафиком

В данном разделе обобщаются результаты трех тестов, в которых предпринимается попытка измерить пропускную способность IP-уровня с помощью потоков UDP и TCP в присутствии конкурирующего потока трафика (поток с постоянной скоростью передачи от NetProbe, который позволяет измерять задержку пакетов и вариацию задержки пакетов (PDV)).

Таблица X.1 – Конкурирующий поток 1 Мбит/с с фильтром на основе буфера маркеров 1000 Мбит/с + задержка "phy2phy"

Примечания	Скорость TBF	Пачка TBF, задержка	Двусторонняя задержка эмулятора сети	Инструмент	Размер кадра, байты	Скорость приема, Мбит/с	Изм. задержка	Количество потерянных пакетов	Точность оценки
27 января, с эмулятором сети, передача 1 156 800 бит/с	1000 Мбит/с	5КБ 4,0 мс	40 мс (eno3)	iPerf2; UDP uni-dir **–b 972000000**	1470, пакеты данных	971 Мбит/с	Рис. X.6	798 в большинстве тестов	0,971
27 января, с эмулятором сети, передача 1 156 800 бит/с			40 мс (eno3)	iPerf2; UDP uni-dir **–b 971000000**	1470, пакеты данных	971 Мбит/с	Рис. X.7	245 (только в 1-ю секунду)	0,971
27 января, с эмулятором сети, передача 1 156 800 бит/с			20 мс (eno3)	iPerf2; TCP 3 соединения однонапр. (uni-dir) 12 с	5@MTU + остальные 892	**786 Мбит/с средн.** достигла 955 Мбит/с через 10 с	Рис. X.8	X	0,786 средн. 0,955 пик.

Рисунок X.6 – Измерение с помощью NetProbe вариации задержки пакетов в течение 11 с; UDP, 972 Мбит/с

Измерения с помощью инструмента NetProbe демонстрируют задержку, возникающую при превышении скорости фильтра на основе буфера маркеров (примерно на 1 Мбит/с) в течение 11-секундного теста UDP iPerf (во время 30-секундного теста NetProbe). В потоке NetProbe было потеряно 3 пакета, скорость передачи данных составила 1 156 800 бит/с. Оценка скорости UDP уменьшена на объем конкурирующего трафика в этом тесте. Результаты измерения задержки (PDV при передаче в одном направлении), приведенные на рисунке X.6, показывают, что максимальная задержка TBF была достигнута через несколько секунд с момента начала потока iPerf 2.

Рисунок X.7 – Измерение с помощью NetProbe вариации задержки пакетов в течение 11 с; UDP, 971 Мбит/с

Измерения с помощью инструмента NetProbe демонстрируют задержку, возникающую при достижении скорости фильтра на основе буфера маркеров в течение 11-секундного теста UDP iPerf (во время 30-секундного теста NetProbe). В потоке NetProbe не было потеряно ни одного пакета, скорость передачи данных составила 1 156 800 бит/с.

Скорость передачи UDP была снижена для обеспечения конкурирующего трафика, что указывает на то, что предыдущий тест (рисунок X.6) дал правильную оценку оставшейся пропускной способности при наличии конкурирующего трафика. Объединенные потоки точнее соответствуют скорости TBF. Результаты измерения задержки (PDV при передаче в одном направлении), приведенные на рисунке X.7, показывают, что максимальная задержка TBF не наблюдалась (и что задержка может служить полезной входной информацией для алгоритма поиска в целях определения пропускной способности [b-TST 009] в дополнение к числу потерянных пакетов).

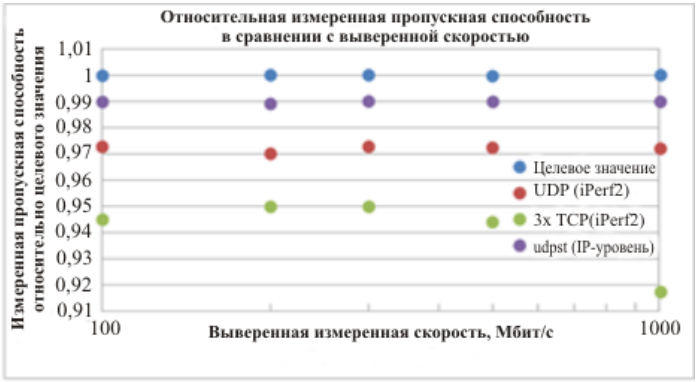
Рисунок X.8 – Измерение PDV с помощью NetProbe в течение 12 с при трех TCP-соединениях

Измерения с помощью инструмента NetProbe демонстрируют задержку, возникающую при достижении скорости фильтра на основе буфера маркеров в течение 12-секундного теста TCP iPerf с тремя соединениями (во время 30-секундного теста NetProbe). В потоке NetProbe не было потеряно ни одного пакета, скорость передачи данных составила 1 156 800 бит/с. Ближе к концу 12-секундного теста TCP три соединения продемонстрировали синхронизацию, и PDV NetProbe указывает на пилообразную задержку в TBF (возможно, в соответствии с моделью AIMD (аддитивное увеличение, мультипликативное уменьшение)) вплоть до максимальной задержки TBF, равной 4 мс.

X.10 Тесты с применением ранней реализации нового инструмента тестирования UDP

Одним из инструментов, которых недостает при тестировании с использованием iPerf2 и 3 UDP, является алгоритм поиска, способный автоматически определять пропускную способность IP-уровня. В ходе предыдущих испытаний с помощью лабораторного теста iPerf 2 определялась максимальная скорость приема пакетов для тестового маршрута (обычно при значительных потерях пакетов), а второй тест на этой максимальной скорости приема пакетов определял, можно ли с этой скоростью передавать пакеты без потерь. В инструменте T-rex применялся алгоритм бинарного поиска с проверкой потерь [b-TST 009], и он успешно определял "истинную" скорость формирователя, но с использованием нескольких испытаний. Было отмечено, что мог бы оказаться полезным более быстрый алгоритм поиска, учитывающий потери и другие нарушения.

				Hack-104
C-Rate, M	Целевое значение	UDP (iPerf 3x	TCP(iPerf2))	udpst (IP-уровень)
100	1	0,973	0,945	0,99
200	1	0,97	0,95	0,9892
300	1	0,973	0,95	0,9899
500	1	0,972	0,944	0,99
1000	1	0,972	0,917	0,99
		2 янв.		



Y.1540(19)_FX.9

Рисунок X.9 – Сравнение с применением инструмента udpst версии 1.4 измеренной с помощью iPerf пропускной способности с выверенными скоростями

udpst – это измерительный инструмент на основе прототипа, созданный Леном Чаваттоне. Алгоритм поиска udpst находит максимальную пропускную способность IP-уровня, регулируя скорость передачи пакетов в соответствии с ответными сообщениями о состоянии, содержащими, в частности, результаты измерения потерь и переупорядочения пакетов, а также информацию о вариации задержки. Получатель udpst отправляет сообщения о состоянии через регулярные промежутки времени (по умолчанию 50 мс). Потеря, переупорядочения или чрезмерная вариация задержки пакетов приводят к уменьшению скорости передачи до тех пор, пока нарушения не прекратятся. Результаты сообщаются на IP-уровне, включая биты заголовка. Это означает, что поправочный коэффициент для служебной информации включает только начальный заголовок ETH (14 октетов). Поправочный коэффициент на служебные данные 1,0112 (1264/1250), примененный к типичному измерению при скорости 990 Мбит/с, дает 1,001 Гбит/с для выверенной скорости формирователя 1 Гбит/с.

X.11 Испытания на влияние низкоуровневой потери пакетов

Одной из переменных при лабораторной оценке первого этапа была потеря пакетов. Первоначально были выбраны коэффициенты потерь 10^-4 и 10^-5, или 0,01% и 0,001% от общего количества пакетов (как указано в **эмуляторе сети**). Распределение потерь не уточнялось, поэтому было выбрано случайное.

На рисунке X.10 показаны результаты испытаний, причем новые результаты с потерями 0,01% или без потерь были получены при разных значениях задержки (22 апреля) и нанесены на график вместе с предыдущими результатами для условий отсутствия потерь.

	Задержка, мс	3x TCP (0.(	UDP (0%)	3x TCP (0%)
22 апр.	0	0,956		
22 апр.	0	0,957		
22 апр.	4			0,954
22 апр.	10	0,888		0,855
22 апр.	10	0,584	0,972	0,87
22 апр.	10	0,844		0,879
22 апр.	10	0,85		
22 апр.	10	0,942		
22 апр.	24			0,564
27 янв.	20		0,972	0,786
27 фев.	20			0,906
27 фев.	10			0,952
27 фев.	10			0,792
27 фев.	5			0,953
27 фев.	5			0,948
11 дек.	0			0,9379
27 фев.	0			0,956

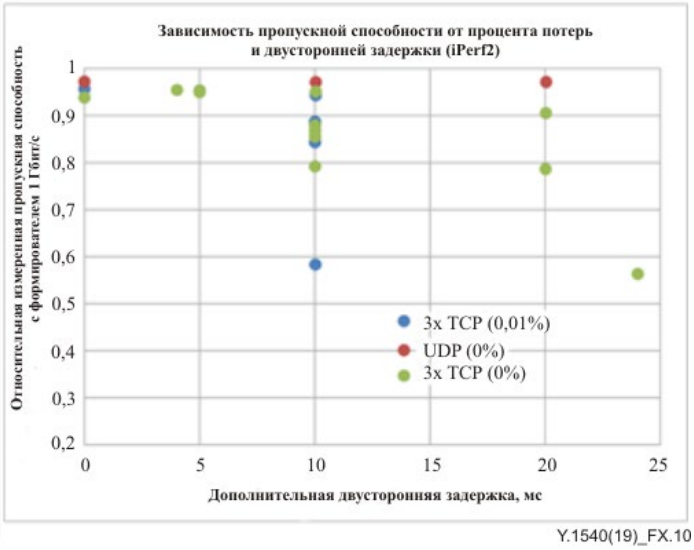


Рисунок X.10 – Сводная информация об измеренной пропускной способности в зависимости от потери и двусторонней задержки при скорости 1 Гбит/с

Во-первых, отметим, что только потери на уровне 0,01% – без дополнительной задержки – мало повлияли на измеренную пропускную способность с TCP на транспортном уровне. Безусловно, более высокий коэффициент потерь (1%) вызвал бы довольно значительное снижение измеренной скорости (примерно в 10 раз). При добавлении двусторонней задержки 10 мс вариация скорости TCP становится существенной с потерями или без них. Один тест с потерями и задержкой 10 мс показал пропускную способность менее 600 Мбит/с, и такой же низкий показатель был получен в ходе недавнего измерения с задержкой 24 мс (возможно, с небольшими потерями). В одном случае с задержкой 10 мс введение потерь 0,01% предположительно привело к повышению скорости TCP, что является своего рода нелинейным изменением пропускной способности, как описано в разделе 4 [IETF RFC 8337].

При тестировании UDP с iPerf2 эмулированные коэффициенты потерь отражаются в результатах (с ожидаемой изменчивостью между 1-секундными сообщениями) и в окончательном итоге.

Вывод состоит в том, что изменчивость результатов измерения TCP вызвана главным образом двусторонней задержкой при низком коэффициенте потерь (0,01%).

X.12 Изучение предельных возможностей передачи инструментов тестирования и платформы

Хотя основное внимание в плане лабораторных испытаний первого этапа было уделено испытаниям при выверенных/истинных скоростях до 1 Гбит/с, полезно также знать верхние пределы возможностей программного инструмента тестирования в сочетании с аппаратным обеспечением, на котором размещаются эти инструменты. Испытания для изучения этих пределов с iPerf2 для транспортных протоколов UDP и TCP проводились несколько раз. Тестовая конфигурация – это просто маршрут, ведущий к vSwitch OVS по каналам 10 Гбит/с, без формирователя трафика TBF и каких-либо нарушений, вносимых эмулятором сети.

Наиболее убедительное тестирование этих пределов было проведено во время хакатона IETF-104. Два теста с тремя соединениями TCP дали 9385 Мбит/с и 9380 Мбит/с, что выгодно отличалось от результатов испытаний, проведенных 11 декабря 2018 года. Тесты с тремя потоками UDP дали 9308 Мбит/с при потерях 1,8%, и около 1500 пакетов оказались переупорядоченными в течение 10-секундного теста (пытались достичь скорости по 3330 Мбит/с в каждом потоке, но это не удалось).

Был сделан вывод о том, что возможностей генерирования и приема пакетов UDP и TCP достаточно для проведения испытаний при скорости 1 Гбит/с и, вероятно, при несколько более высоких скоростях, учитывая приведенные выше измерения при скорости около 10 Гбит/с.

X.13 Изучение тестов с ранними нарушениями на потоках UDP

В ходе нескольких испытаний iPerf 2 для UDP, как сообщалось, в потоке пакетов на первой секунде наблюдались переупорядочение пакетов (обычно менее 40 пакетов) и их небольшая потеря, и эти наблюдения относились к случаям с формирователем TBF 1 Гбит/с. Для выяснения причины ранних нарушений поток UDP перехватывался (с помощью инструмента tshark) в интерфейсе eno4 (непосредственно перед формирователем).

Захват пакетов дополнительно изучался с помощью инструмента Wireshark, особенно время прохождения первых пакетов в потоке UDP. Было обнаружено, что интервал времени между поступлением ранних пакетов нерегулярен для 20 пакетов или более в потоке, после чего достигается номинальный интервал в 12 мкс. Порядковые номера отсутствуют, поэтому отправитель iPerf или тестовый маршрут могли произвести некоторое переупорядочение в уплотненной части потока, а формирователь мог отбросить пакеты, выходящие за пределы его спецификации.

X.14 Изучение параметров формирователя TBF, используемых при испытаниях, и сравнение с фильтром-ограничителем

Была проведена серия испытаний для выявления неблагоприятного влияния на потоки TCP параметров формирователя, используемых в большинстве тестов. Тесты со скоростью формирователя 1 Гбит/с показали, что, когда параметр максимальной задержки TBF был уменьшен с 4 до 0,1 мс, измеренная пропускная способность TCP значительно снизилась (тесты TCP при задержке 4 мс показали максимальную скорость 956 Мбит/с, а при задержке 0,1 мс скорость сильно варьировала и находилась в диапазоне от 763 до 862 Мбит/с). С другой стороны, увеличение параметра максимальной задержки TBF с 4 до 20 мс не обеспечивало каких-либо преимуществ для измеренной пропускной способности TCP. Тесты iPerf 2 для UDP продемонстрировали нечувствительность к этим изменениям.

Когда вместо формирователя был использован фильтр-ограничитель, измеренная пропускная способность TCP снова значительно снизилась, несмотря на попытки повысить ее с помощью настройки параметров (тесты TCP с формирователем показали максимальную скорость 956 Мбит/с, а самая высокая пропускная способность с ограничителем составила 2,02 Мбит/с). Это происходит из-за чрезвычайно ограниченной буферизации, доступной с фильтром-ограничителем. Тесты iPerf 2 для UDP нечувствительны к использованию фильтра-ограничителя ввиду постоянной скорости передачи данных в потоке.

X.15 Сводные результаты лабораторных испытаний первого этапа

Оценки на основе тестов iPerf 2 для TCP, как правило, занижают выверенную пропускную способность и дают результаты:

- менее точные, чем для UDP, при высоких скоростях, таких как 1 Гбит/с (современная служба доступа в интернет);
- более чувствительные к двусторонней задержке, чем для UDP, особенно в отношении изменчивости измерений TCP из-за управления потоком TCP;
- более чувствительные к конкурирующему трафику, что приводит к низкому среднему показателю из-за более длительного времени, необходимого для достижения равновесия.

Измерения iPerf 2 для UDP подтверждают статус "эталонных" для оценки пропускной способности относительно выверенных скоростей ("экспериментальная реальная ситуация") и значимых исследований с использованием более медленных технологий/более низких скоростей доступа.
Задержка может служить полезной входной информацией для алгоритма поиска в целях определения пропускной способности на основе UDP в дополнение к потере пакетов, как предполагается в [b-TST 009]. Прототип инструмента тестирования UDP (udpst ver1.4) обещает удовлетворить эту потребность в автоматическом определении максимально допустимой скорости с использованием UDP.

X.16 Спецификации платформы

См.: https://wiki.opnfv.org/display/pharos/Intel+POD12.

X.17 Сводные результаты полевых испытаний второго этапа

Ниже приведены сводные результаты испытаний (проводившихся в ходе двух кампаний тестирования) с использованием следующих типов доступа:

1. фиксированный: кабельный модем DOCSIS 3.0 с возможностью "тройной услуги" и встроенным коммутатором Wi-Fi и Wired GigE;
2. подвижный: мобильный телефон LTE с модемом категории 12 (нисходящий канал 600 Мбит/с, восходящий канал 50 Мбит/с);
3. фиксированный: пассивная оптическая сеть (PON) "F", услуга 1 Гбит/с;
4. фиксированный: PON "T", услуга 1000 Мбит/с;
5. фиксированный: VDSL, услуги с разными скоростями < 100 Мбит/с;
6. фиксированный: ADSL, 1,5 Мбит/с;
7. подвижный: маршрутизатор с поддержкой LTE и ЛС ETH для хоста (стационарный).

Консенсус по результатам измерений состоит в том, что UDP представляет собой предпочтительный транспортный протокол для оценки пропускной способности:

- UDP дал более последовательные результаты;
- инструменты для UDP могут измерять потери, задержки, вариацию задержки и переупорядочение пакетов;
- при использовании TCP регистрировались более низкие скорости, чем в тестах UDP, и бóльшая изменчивость скорости в различных обстоятельствах;
- измерения TCP с PON 1 Гбит/с демонстрируют значительную недооценку пропускной способности;
- выводы лабораторных испытаний о том, что тесты UDP можно использовать в качестве эталонных, а тесты TCP недооценивают пропускную способность, были подтверждены измерениями в полевых условиях;
- тесты доступа LTE продемонстрировали значительную изменчивость, как и ожидалось для любой беспроводной сети.

Дополнение XI

Краткий обзор исследований QoS и QoE, связанных с доступом в интернет

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

XI.1 Введение

Поставщики услуг, регуляторные органы (и органы защиты прав потребителей), а также поставщики и операторы измерительных систем по разным причинам заинтересованы в измерении скорости доступа в интернет (IAS). Исследования, характеризующие продукты доступа в интернет, предлагаемые поставщиками услуг, хорошо зарекомендовали себя во многих странах. Стандартизация в этой области может заключаться в отслеживании существующих применений. Исследования, содержащие оценку IAS, не требуют высокой точности и часто принимаются конкурирующими поставщиками услуг, если сторона, проводящая опрос, транспарентно предоставляет оцениваемым поставщикам услуг достоверный набор параметров, связанных с измерительной кампанией.

Существует интерес и к стандартизированным точным измерениям IAS. Как и в случае других точных измерений скорости или объема, на которых основаны обязательства или штрафы на коммерческих рынках, для стандартизированных точных измерений IAS требуется определенная точность. Для определения точности измерения требуется контрольный показатель.

Ожидается, что научные публикации позволят коллегам-исследователям воспроизводить опубликованные результаты. В этом вкладе рассмотрен ряд научных публикаций, в которых осуществляется поиск результатов, относящихся к параметрам, измерениям и оценке QoS, связанным с доступом в интернет. Основное внимание уделяется измерениям IAS, но не ограничивается только ими. Научное сообщество в основном интересуется измерением QoE и параметрами QoS, связанными с доступом в интернет. Некоторые подходы, используемые в исследованиях QoE, как представляется, приводят к указанию параметров QoS, более детально характеризующих доступ в интернет и компоненты, связанные со сквозной передачей данных, чем оценка скорости доступа. Кроме того, исследуется новейший набор параметров QoS. Цитаты и ссылки, приведенные в этом вкладе, помогают опираться при обсуждении новых стандартов на аргументы, а не на мнения.

Следует отметить, что по возможности были выбраны исследования, основанные на подходах, подтвержденных более или менее крупномасштабными измерениями с использованием коммерческих услуг доступа. Этому критерию соответствуют работы [2], [4], [6], [7], [8] и [10].

XI.2 Основные выводы

В данном разделе обобщаются опубликованные в рамках исследований показатели QoS, KPI и методы измерения, связанные с доступом в интернет и использованием услуг доступа.

Эталонное измерение максимально достижимой скорости доступа получено путем заполнения канала доступа трафиком UDP [1]. Кроме того, UDP используется в крупномасштабном исследовании для точного измерения скорости доступа [2]. Крупный поставщик услуг OTT включает средства измерения UDP во внутренний спидометр [3].

Как показали результаты параллельных измерений на основе TCP, их можно использовать для оценки пропускной способности доступа в интернет [1]. В некоторых публикациях обсуждаются конкретные факторы, влияющие на точность параллельных измерений на основе TCP, и более подробно рассматриваются отдельные ухудшающие факторы [1], [2], [4]. Параллельные измерения на основе TCP фиксируют эффективную доступную полосу пропускания при наличии фонового трафика [1]. Следует отметить, что доступная пропускная способность идентична скорости доступа в интернет только при отсутствии фонового трафика. Параллельные измерения на основе TCP не позволяют обнаружить наличие фонового трафика. Для обнаружения фонового трафика имеются специальные инструменты и методы [1], [2].

Согласно [14], установлено, что UDP представляет собой конкурентоспособный общий транспортный протокол. Это утверждение основано на тестах, проводившихся в Северной и Южной Америке, Европе, Азии и Океании (примечательно, что не в Африке). Авторы установили, что UDP-трафик блокируется в некоторых портах или – в редких случаях – полностью. Было установлено,

что нарушение работы UDP наблюдается в корпоративных сетях и "сетях географических регионов с затрудненным установлением соединений". В случаях отказа транспортного протокола UDP рекомендуется возврат к транспортному протоколу TCP. Влияние Wi-Fi на QoE приложений можно определять по пассивно собираемой статистике типовых точек доступа, как это предложено в [10]. Авторы сообщают об обычном понижении QoE услуг Wi-Fi при значении TxPhymean ниже 15 Мбит/с.

Во многих приложениях применяется шифрованный транспортный протокол. Это оставляет для оценки QoE сети только информацию о пакетах и IP-потоках. В [11], [12] и [13] предлагаются параметры QoS сети, коррелирующие с QoE потоковых услуг. Предлагаемые там параметры также могут быть полезны и для сравнения и оценки IP-доступа.

Распространение смартфонов повышает интерес OTT, поставщиков услуг и исследователей к QoE, связанной с QoS в сетях подвижной связи. Авторы научных публикаций указывают или прямо заявляют, что параллельные измерения на основе TCP не дают полезных данных для этой цели.

Колебания пропускной способности сетей подвижной связи коррелируют с QoE в обычных условиях работы беспроводной сети (например, при мобильности абонентов). В этих условиях в популярных услугах потокового видео адаптируется качество видеоизображения. В среде с колебаниями пропускной способности корреляция QoE с ключевыми показателями KPI QoS приводит к необходимости ввода дополнительного параметра, помимо средней доступной пропускной способности, такого как средняя максимальная пропускная способность; см. [6], [7], [8]. Как правило, в качестве обязательных KPI упоминаются показатели задержки пользовательского приложения или результаты измерения RTT. В публикациях указывается, что для определения степени удовлетворенности абонентов услугами доступа в интернет LTE на основе измерений QoS требуется учитывать KPI, связанные с интегральным показателем задержки передачи (или количеством битов в пути) либо колебаниями пропускной способности [6], [7], [8].

Пропускная способность остается дешевой на соответствующих рынках, где имеются крупные поставщики услуг OTT. Основным показателем для современных сетевых услуг OTT является воспринимаемое пользователем качество этих услуг. Основным препятствие для повышения QoE на соответствующих рынках услуг OTT является веб-задержка [5]. Дизайн TCP ограничивает возможность дальнейших улучшений с точки зрения OTT. Через некоторое время после опубликования [5] IETF начала работу над QUIC – новым транспортным протоколом на основе UDP.

Согласно выводам одной из публикаций, в среде подвижной связи LTE на многих основных рынках услуг OTT последствия проведенного исследования для конечного пользователя кажутся очевидными: абонентам не нужна подписка на услуги сверхскоростной сотовой связи, если главной областью применения ими услуг подвижного доступа является потоковое видео или просмотр веб-страниц ([7]; следует отметить, что это утверждение справедливо только для места и времени проведения оценки). Аналогичные выводы были сделаны для фиксированного доступа в интернет [5]; на это же, как представляется, указывает [9]. Это не общепризнанные оценки. Эти утверждения указывают на то, что удовлетворенность абонента услугами доступа в интернет может быть больше не связана со скоростью доступа в интернет, если последняя обеспечивает стабильную среднюю пропускную способность, значительно превышающую ту, которая требуется для получения высокой QoE.

XI.3 Анализ научных публикаций, связанных с измерениями QoS и QoE

В период с 2010 по 2012 год в центре внимания некоторых научных публикаций были измерения скорости доступа в интернет. Затем интерес научного сообщества переключился на оценку качества услуг пользователями интернета. Это не означает, что в последующие годы пропускная способность доступа в интернет, ее свойства и измерения QoS были вне поля зрения исследователей. Исследования параметров QoS услуг доступа в интернет и их измерение все еще продолжаются, если эти измерения связаны с QoE.

XI.3.1 Измерение скорости фиксированного доступа в интернет

Гога и Тейшейра [1] исследовали инструменты для оценки скорости доступа в интернет. Для устранения нежелательных помех измерения проводились в часы непиковой нагрузки в фиксированной сети. Целью работы было сравнение доступных инструментов измерения пропускной способности. Для этого определяются точность и измерительная нагрузка этих инструментов путем

измерения параметров коммерческих услуг доступа в интернет на основе ADSL и кабельных сетей с контролируемым перекрестным трафиком.

Авторы оценивают IAS, измеряя пропускную способность доступа UDP, полученную при заполнении канала UDP-трафиком. Затем они оценивают IAS, используя инструменты на основе TCP.

В отсутствие перекрестного трафика по результатам измерений в периоды непиковой нагрузки можно получить следующие относительные ошибки оценки по сравнению с эталоном:

заполнение трафиком TCP ("Speedtest"): в лучшем случае 4,06%, средняя ошибка 5,28%, в худшем случае 6,8%.

В среднем пропускная способность услуг доступа недооценивается.

Заполнение трафиком TCP не позволяет обнаруживать перекрестный трафик. Это подтверждается тестом с одним активным потоком TCP во время выполнения теста скорости на основе TCP. Последний оценивает доступную пропускную способность, но не IAS. Существуют инструменты для обнаружения фонового трафика.

Авторами установлено, что скорость обработки пакетов домашних шлюзов ограниченна, если они действуют как трансляторы сетевых адресов. Следовательно, выбор размера пакета при измерении влияет на точность измерения IAS.

В заключение авторы приводят информацию о нагрузке, необходимой для оценки IAS. Тесты скорости на основе TCP создают самую высокую нагрузку, в то время как другие инструменты оценивают IAS при нагрузке менее чем 10% от нагрузки, создаваемой тестами скорости на основе TCP.

Канупарти [2] также использует измерения на основе UDP для измерения IAS. Он отмечает, что наличие формирователей в "узком месте" канала снижает точность оценок IAS теста скорости на основе TCP. В лучшем случае такой тест показывает значение скорости между скоростью канала и скоростью формирования.

Флах и др. [4] представляют алгоритм, определяющий скорость (и другие свойства) ограничителей, используемых для ограничения пропускной способности доступа в интернет. Оценка IAS напрямую не обсуждается. В среднем в ограниченных TCP-потоках потеря пакетов происходит в шесть раз чаще, чем в неограниченных. Оценки IAS теста скорости на основе TCP без предложенного алгоритма скорее всего будут иметь низкую точность.

Авторы добавляют, что на момент публикации ограничение в некоторой степени все еще применяется в коммерческих услугах доступа в интернет в Азии и Африке.

Основанный на инструментах и измерениях тест для выяснения того, может ли UDP служить конкурентоспособной основой общего транспортного протокола Интернет, показывает, что UDP – действительно конкурентоспособный общий транспортный протокол [14]. Это утверждение основано на тестах, проводившихся в Северной и Южной Америке, Европе, Азии и Океании (примечательно, что не в Африке). Авторы установили, что UDP-трафик блокируется в некоторых портах или – в редких случаях – полностью. В случаях отказа транспортного протокола UDP рекомендуется возврат к транспортному протоколу TCP.

Блокировка UDP отмечалась в 2–4% наземных сетей доступа. Блокировка UDP главным образом связана с сетью доступа. Авторы [14] установили, что нарушение работы UDP особенно часто встречается в корпоративных сетях и сетях тех географических регионов, где установление соединений затруднено. В случаях, когда UDP работал в наземных сетях доступа, каких-либо свидетельств систематического ухудшения трафика с заголовками UDP не было обнаружено.

Чтобы произвести возврат к TCP, узлу не нужно ничего измерять или помнить что-либо о своих парных узлах – нужно помнить только свое интернет-соединение (также в рекомендации, которую дают авторы [14], указывается, что нарушения работы UDP относятся к конкретным каналам доступа, а не к сети).

XI.3.2 Измерение скорости доступа по беспроводной локальной сети

Ранее Канупарти [2] исследовал характеристики доступа WLAN IEEE 802.11. Да-Гора, Ван-Доорселер, Ван-Оост и Тейшейра опубликовали модель для оценки влияния на сети Wi-Fi QoE потребителей [10]. Авторы этой модели основывают свою работу на пассивно собираемых параметрах коммерческих

точек доступа Wi-Fi. Результаты измерительной кампании в сетях поставщиков услуг позволяют сделать вывод о том, что большинство сетей Wi-Fi работают хорошо. Тем не менее более 10% точек доступа (AP) получили среднюю экспертную оценку (MOS) < 3 по крайней мере для 5% всех собранных выборок данных (или более).

Собирались следующие параметры Wi-Fi ([10], таблица II):

Таблица X1.3.2-1 – Показатели Wi-Fi, измеренные в точках доступа (таблица II из [10])

Показатель	Описание	Период
BUSY	Процент времени, когда среда передачи занята	2 с
WiFi	Процент времени занятости трафиком Wi-Fi	2 с
nonWiFi	Процент времени занятости трафиком не-Wi-Fi	2 с
TxPhy	Физическая скорость последнего переданного кадра	1 с
FDR	Количество кадров, переданных/ретранслированных на станцию	1 с
RSSI	Показатель уровня принятого сигнала	1 с

Выборки данных, собранные авторами, содержат среднее значение (mean), стандартное отклонение (std), минимальное (min), максимальное (max) значения и значения 25%-ного и 75%-ного процентилей (соответственно 25%-ile и 75%-ile) для каждого показателя из таблицы X1.3.2-1.

Статистика по выборкам оценивается за период T, зависящий от приложения:

- T = 10 с в экспериментах с аудио- и видеоданными;
- T = 10 с для просмотра веб-страниц;
- T = 120 с для потоковой передачи YouTube (во время испытаний каждое видео воспроизводилось по две минуты).

Исследователи установили, что с QoE потребительских приложений для подмножества функций Wi-Fi лучше всего коррелируют следующие подмножества векторов функций приложений ([10], таблица III):

- видео: TxPhy25%-ile , BUSY25%-ile, BUSYmax, RSSImean, RSSI75%-ile, WiFi25%-ile;
- аудио: TxPhymin, RSSIstd, WiFi25%-ile, WiFimax, nonWiFimax, FDRmean;
- YouTube: TxPhymean, BUSY75%-ile, RSSImean, RSSI25%-ile, WiFi25%-ile, nonWiFimin;
- Web: TxPhymax, BUSYstd, RSSImin, WiFimax, nonWiFimax, FDRmean.

Используемый в [10] подход основан на машинном обучении. В этом вкладе не говорится, применимы ли результаты [10] в общем случае. Предполагается, что указанные параметры QoS коррелируют с QoS приложения. Полную модель и метод подгонки параметров для каждого приложения можно найти в указанном документе. В качестве последнего замечания и цитируемого здесь эмпирического правила авторы [10] ожидают снижения QoE при значениях TxPhymean ниже 15 Мбит/с.

XI.3.3 Измерение QoE и скорости доступа в сети подвижной связи

Публикации Димопоулоса и др. [6] и Касаса и др. ([7] и [8]) относятся к измерениям QoE потокового видео для мобильных терминалов, а в [7] исследуются и другие приложения. Авторы [7] приходят к выводу, что QoE "определенных приложений чрезвычайно чувствительна к колебаниям пропускной способности. Колебания пропускной способности из-за ее изменчивости очень распространены в сотовых сетях, но, к сожалению, их влияние на QoE не фиксируется при современных измерениях характеристик сетей, поскольку обычно учитываются лишь средние значения пропускной способности". Следует отметить, что "современные измерения характеристик сетей" – это измерения, основанные на заполнении трафиком TCP.

Кроме того, в [6] показано, что при наличии изменчивости пропускной способности средняя пропускная способность TCP плохо коррелирует с QoE.

В публикациях QoE коррелирует с измерениями QoS сети по следующим параметрам.

- Согласно [6], следует использовать интегральный показатель задержки передачи, максимальное количество повторных передач пакетов, среднее максимальное количество битов в пути и накопленную сумму значений минимальной пропускной способности.
- В [6] также предлагается "уменьшить шум, создаваемый начальным этапом при обнаружении изменений разрешения", "удалив из набора данных первые 10 секунд всех видеосеансов". Пропускная способность на этом начальном этапе потоковой передачи видео, по-видимому, отличается от пропускной способности и ее колебаний в течение остального времени передачи (средняя продолжительность сеанса составляла 180 секунд).
- В [7] представлены результаты лабораторных измерений колебаний пропускной способности, а в [8] – два показателя QoS для их получения: максимальная пропускная способность нисходящего потока сеанса и средняя пропускная способность нисходящего потока сеанса. Они классифицируются как "наиболее подходящие параметры".
- В [8] дополнительно оцениваются другие ключевые показатели эффективности, а также их корреляция с прогнозом MOS и точность. Оказалось, что помимо средней и максимальной пропускной способности на точность прогноза MOS влияют следующие KPI: средняя мощность сигнала, громкость сеанса и продолжительность сеанса.
- KPI, исследованные в [8], основаны на измерениях в зоне с очень хорошим доступом через сети подвижной связи. В [7] приведены результаты лабораторных испытаний, указывающие на то, что более или менее значительное влияние на QoE могут оказывать дополнительные KPI, такие как RTT и кратковременные перебои в пропускной способности (вызванные передачей обслуживания).
- В качестве актуальной темы в [7] также упоминается сетевой нейтралитет. В одном из изученных приложений пропускная способность была ограничена одним из участвующих поставщиков услуг интернет.

XI.3.4 Измерение QoE приложений с шифрованием данных

Для оценки QoE приложений с шифрованием данных в сети требуется более тщательное изучение соответствующих параметров QoS по сравнению с оценкой QoE приложений без шифрования. Предлагаемые параметры также характеризуют свойства услуг доступа. Параметры для этой цели предлагаются в работах [11], [12] и [13]. Их общей задачей является определение или оптимизация следующих параметров QoE потокового видео путем наблюдения за параметрами QoS сети:

- начальная задержка при пуске (время запуска);
- средняя битовая скорость по фрагментам (сегментам);
- переключения средней битовой скорости потока (вызванные разным уровнем качества видео);
- коэффициент повторной буферизации.

Обычный подход заключается в измерении пропускной способности видеопотока (и аудиопотока [12]). Рекомендуемая продолжительность выборки – типичная длительность фрагмента или сегмента видеопотока (или соответственно аудиопотока). Она находится в интервале от 2 до 15 секунд, при этом для видеопотоков YouTube указано значение 4 с [13].

Скорость в мегабитах в секунду передачи видеоданных в потоке, направляемом в воспроизводящий терминал, рекомендуется вводить отсчетами по одной секунде, которые затем подвергаются статистической обработке в зависимости от длительности фрагментов [11], [13]. Средняя скорость передачи вычисляется по 5-секундным отсчетам простого скользящего среднего [11]. В [13] к этому добавлен ввод данных из 10 последовательных секундных "окон" (что приводит к пяти средним значениям на окно, каждое из которых рассчитывается по пяти 1-секундным отсчетам).

В [13] предлагаются приведенные в следующей таблице параметры QoS и статистические данные для корреляции свойств транспортного уровня (которые могут не обнаруживаться сетью) с параметрами сетевого уровня на этапе обучения.

Таблица X1.3.4-1 – Перечень общих характеристик, рассмотренных в [13], таблица I

	Сетевой уровень	Транспортный уровень
10-секундное окно оценки	Количество байтов Количество пакетов Пропускная способность Время ожидания	Количество флагов TCP (SYN, ACK, FIN, URG, PSH и RST) Количество байтов/пакетов с измененным порядком следования Полезная пропускная способность TCP ‡Коэффициент повторной передачи (значения 0, 1, 2 и > 2) В случае оценки QoE в режиме реального времени: Количество начальных байтов в пути Количество завершающих байтов в пути
Статистика пакетов: среднее, минимальное, максимальное и медианное значения, стандартное отклонение, асимметрия, эксцесс	Время поступления пакетов Количество байтов на пакет	Количество повторных передач на пакет Окно приема транспортного уровня RTT (только для исходящего трафика) Количество байтов в пути

Более подробные определения измерений и указания см. в [13].

Для сопоставления измерений на сетевом и транспортном уровнях предлагается лабораторное обучение в контролируемых условиях сети.

Этап пуска в [13] характеризуется только статистикой, собранной в первом 10-секундном окне оценки.

Чтобы охарактеризовать события повторной передачи и повторной буферизации, в [13] оцениваются и сравниваются свойства в первые пять секунд каждого окна со свойствами во вторые пять секунд.

Авторы [13] установили, что с QoE YouTube коррелируют следующие параметры сети:

- начальная задержка при пуске (медианное количество загруженных байтов, среднее время между поступлением пакетов, медианная пропускная способность в нисходящем направлении – сравнение статистики пакетов через 3,3; 6,6 и 10 секунд);
- события повторной буферизации (минимальное количество загруженных байтов в первой половине окна оценки, пропускная способность нисходящего потока в первой половине окна оценки);
- качество видеоизображения (пропускная способность нисходящего потока, пропускная способность восходящего потока).

Далее в [13] вводится метод машинного обучения для разработки и параметризации модели QoE. В этом вкладе рассматриваются только измерения QoS, коррелирующие с QoE приложения. Полную модель заинтересованные читатели могут найти в [13].

XI.4 Общие тенденции, связанные с качеством доступа в интернет

В двух отчетах также содержатся общие утверждения о требованиях рынка.

Флах и др. [5] отмечают, что в условиях, когда "пропускная способность остается относительно дешевой, основным препятствием для повышения воспринимаемого пользователем качества в настоящее время является веб-задержка". Это относится доступу через фиксированные сети, но в качестве одной из причин данной тенденции называется использование смартфонов в качестве конечных устройств. Следует отметить, что некоторые авторы работают с крупным оператором OTT.

Авторы [9] измерили QoE в соответствии с Рекомендацией МСЭ-Т P.1203 на дисплее с разрешением 1920 × 1080 пикселей, используя контент крупного оператора OTT, получаемый через службу доступа DSL коммерческой фиксированной сети. Между измерительным устройством и DSL-маршрутизатором был помещен формирователь, а пропускная способность нисходящего потока изменялась в 11 шагов от 0,256 до 37,5 Мбит/с. Были получены оценки MOS 4 балла и выше при пропускной способности нисходящего потока 3,073 Мбит/с.

Авторы документа [7], относящегося к подвижным сетям, пришли к выводу, что "при доступе со смартфонов для достижения почти оптимальных результатов с точки зрения общего качества и приемлемости [потокового видео] достаточно пропускной способности в нисходящем направлении 4 Мбит/с. Последствия для конечного пользователя очевидны: …сегодня для оптимальной работы дорогостоящий контракт на услуги LTE не обязателен". Следует отметить, что этот документ был опубликован в 2016 году и авторы для получения своих результатов использовали формат видеоизображения HD720p.

Все три утверждения указывают на то, что при достаточно высокой пропускной способности услуг доступа в интернет удовлетворенность абонентов и поставщиков контента качеством доступа в интернет может не зависеть от максимальной скорости доступа в интернет.

Справочные документы к Дополнению XI

[1] "Speed Measurements of Residential Internet Access", Oana Goga and Renata Teixeira, PAM 2012, 2012.

[2] "End-to-end Inference of Internet Performance Problems", Partha Kanuparthy, PhD Thesis, Georgia Institute of Technology, 2012.

[3] "Diagnosing Path Inflation of Mobile Client Traffic", Kyriakos Zarifis, Tobias Flach, Srikanth Nori, David Choffnes, Ramesh Govindan, Ethan Katz-Bassett, Z. Morley Mao, and Matt Welsh, 2014.

[4] "An Internet-Wide Analysis of Traffic Policing", Tobias Flach, Pavlos Papageorgey, Andreas Terzis, Luis D. Pedrosa, Yuchung Chengy, Tayeb Karimy, Ethan Katz-Bassett, and Ramesh Govindan, IEEE SIGCOMM, 2016.

[5] "Reducing Web Latency: the Virtue of Gentle Aggression" Tobias Flach, Nandita Dukkipati, Andreas Terzis, Barath Raghavan, Neal Cardwell, Yuchung Cheng, Ankur Jain, Shuai Hao, Ethan Katz-Bassett, and Ramesh Govindan, IEEE SIGCOMM 2013.

[6] "Measuring Video QoE from Encrypted Traffic", Giorgos Dimopoulos, Ilias Leontiadis, Pere Barlet-Ros, and Konstantina Papagiannaki, IMC '16, 2016.

[7] "Next to You: Monitoring Quality of Experience in Cellular Networks from the End-devices", Pedro Casas, Michael Seufert, Florian Wamser, Bruno Gardlo, Andreas Sackl, and Raimund Schatz, IEEE Transactions on Network and Service Management Vol 13 issue 2, 2016.

[8] "Predicting QoE in Cellular Networks using Machine Learning and in-Smartphone Measurements", Pedro Casas, Alessandro D'Alconzo, Florian Wamser, Michael Seufert, Bruno Gardlo, Anika Schwind, Phuoc Tran-Gia, Raimund Schatz, QoMEX 2017.

[9] "Measuring YouTube QoE with ITU-T P.1203 under Constrained Bandwidth Conditions", Werner Robitza, Dhananjaya G. Kittur, Alexander M. Dethof, Steve Göring, Bernhard Feiten, Alexander Raake, QoMEX 2018.

[10] "Predicting the effect of home Wi-Fi quality on QoE: Extended Technical Report." Diego Da Hora, Karel Van Doorselaer, Koen Van Oost, Renata Teixeira. [Research Report] INRIA; Technicolor; TelecomParisTech. 2018. <hal-01676921>.

[11] "QoE-based low-delay live streaming using throughput predictions." Konstantin Miller, Abdel-Karim Al-Tamimi, and Adam Wolisz. 2016. ACM Trans. Multimedia Comput. Commun. Appl. 13, 1, Article 4 (October 2016), 24 pages. DOI: http://dx.doi.org/10.1145/2990505.

[12] "eMIMIC: Estimating HTTP-based Video QoE Metrics from Encrypted Network Traffic", Tarun Mangla, Emir Halepovicy, Mostafa Ammar, Ellen Zegura. Georgia Institute of Technology yAT&T Labs – Research.

[13] "Real-time Video Quality of Experience Monitoring for HTTPS and QUIC", M. Hammad Mazhar, Zubair Shafiq, The University of Iowa.

[14] "copycat: Testing Differential Treatment of New Transport Protocols in the Wild", Korian Edeline, Mirja Kühlewind, Brian Trammell, Benoit Donnet, ANRW '17, Prague.

Дополнение XII

Точные измерения скорости передачи данных

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

XII.1 Введение

Каждый измеритель трафика на маршруте связи настроен на измерение или ограничение скорости передачи данных на одном уровне связи (или делает это по умолчанию). Знание уровня связи, на котором ограничивается скорость передачи данных, уменьшает погрешность измерения.

Промежуточные устройства на тракте лабораторных или сетевых измерений могут быть настроены для регулирования трафика, а в их отсутствие скорость передачи данных может ограничивать физический интерфейс. Если используемые системы измеряют скорость передачи данных не на одном и том же уровне связи, то система измерения скорости передачи данных может давать показания выше или ниже значения скорости передачи данных, определяемой ограничивающим звеном.

Для сравнительного тестирования и калибровки особенно необходимо точное знание уровней, на которых эти регуляторы трафика или физические интерфейсы измеряют трафик. Для точного перевода результатов измерения пропускной способности с одного уровня на другой требуется знание размеров заголовков пакетов на разных уровнях. Для точного и понятного представления результатов измерения требуются указание уровня, на котором ограничивается скорость передачи данных, и сопутствующая информация, такая как размер пакетов PDU на этом уровне.

Следует отметить, что ошибки, вызванные игнорированием заголовков пакетов и уровня, на котором ограничивается скорость передачи данных, являются одним из источников погрешности измерения скорости передачи данных, но не единственным таким источником. Измерения с использованием сообщений обратной связи о перегрузке на основе потери пакетов, такие как TCP или QUIC, вводят дополнительные источники ошибок, зависящие от двусторонней задержки и потери пакетов.

В настоящем Дополнении также содержится информация о фильтрах на основе буфера маркеров области, которые являются ключевым компонентом формирователей и ограничителей трафика.

XII.2 Основные выводы

Рабочие характеристики интерфейса и протокола целиком определяются скоростью или пропускной способностью, например количеством мегабит в секунду (Мбит/с). Для общих целей, таких как опросы, приблизительное знание пропускной способности достаточно характеризует результат измерения. Однако это не так, если целью измерения пропускной способности является калибровка или сравнительная оценка рабочих характеристик тестируемого устройства или канала связи. Для того чтобы сравнивать результаты измерения пропускной способности, полученные разными методами или собранные на разных трактах измерения с несколькими пунктами регулирования трафика, требуются точные результаты на основе дополнительной информации. Одним из видов такой информации (но не обязательно единственным) является ошибка, вносимая системой измерения и ограничением скорости передачи данных на разных уровнях.

Рассмотрим простую установку для измерения пропускной способности, показанную на рисунке XII.2-1.

Рисунок XII.2-1 – Простая установка для измерения пропускной способности

Следует отметить, что не утверждается, что показанная конфигурация типична. Ее части могут присутствовать во многих сетях.

Целью испытаний может быть определение максимальной пропускной способности тестовой установки без потерь. Порогом, с которым сравниваются результаты измерения, является пропускная

способность, определяемая скоростью передачи данных, на которую настроены формирователь и ограничитель (допустим, что они оба настроены на одну и ту же скорость передачи данных C_{Access}).

В результате измерения можно получить максимальную пропускную способность без потерь $0{,}95*C_{Access}$. Если целью испытания является калибровка или оценка рабочих характеристик формирователя и ограничителя, то это само по себе не является значимым результатом (даже если он получен в лаборатории в контролируемых условиях).

Предположим, что генератор нагрузки и получатель – это одно и то же устройство. По умолчанию это устройство генерирует и подсчитывает размеры пакетов и результирующие скорости передачи данных, такие как C_{Access}, на уровне 2. Если формирователь и ограничитель настроены на подсчет и планирование или ограничение пропускной способности на уровне 1, то они могут переносить трафик точно с пропускной способностью C_{Access}, если C_{Access} измеряется на уровне 1. Все устройства работают правильно в соответствии с их конструкцией и настройкой. Кажущаяся погрешность в виде отклонения на 5% от ожидаемого результата вызвана уровнем, на котором устройства, используемые при испытании, настроили счетчик трафика.

Теперь допустим, что проводящий испытания персонал вносит небольшое изменение, например уменьшает размер измеряемых пакетов на 50%. В этом случае в результате измерения может быть получена пропускная способность $0{,}93*C_{Access}$. Предположим, что это ограничение не вызвано ограниченной пропускной способностью в пакетах в секунду какого-либо процессора в испытательной установке. Тогда этот результат указывает на несовместимость соответственно уровня или измерения на тестируемом маршруте. Пакеты меньшего размера приводят к меньшей скорости передачи данных на уровне 2, в то время как скорость передачи данных на уровне 1 остается постоянной. Рабочая цепочка функционирует правильно в соответствии с настройкой.

Если пропускная способность тестового потока на регулирующем устройстве неизвестна или не может контролироваться путем настройки отправителя или если неизвестен уровень, на котором регулирующее устройство ограничивает трафик, то калибровка или сравнение такого устройства возможны лишь с ограниченной точностью.

XII.3 Оценка погрешности измерения пропускной способности из-за размера заголовков

Трафик ограничен постоянной скоростью передачи данных только на том уровне связи, на котором работает регулирующий формирователь, ограничитель или физический интерфейс. Не следует ожидать, что формирователи и ограничители будут работать на каком-либо конкретном и четко определенном уровне. В некоторых случаях устройства оператора сети позволяют настроить уровень, на котором работают измерители скорости формирователей и ограничителей.

Для точного сравнения результатов измерения пропускной способности в целях калибровки и сравнительного тестирования требуется следующая информация:

– уровень связи и размер PDU отправителя и получателя;

– размеры всех добавляемых или удаляемых заголовков, если отправитель и получатель измеряют трафик не на одном и том же уровне;

– уровень параметров конфигурации, на которые настраиваются устройства регулирования трафика, подлежащие калибровке или сравнительному тестированию. Если ограничивающим звеном является физический интерфейс, то чаще всего известна пропускная способность интерфейса уровня 1; – точные размеры добавляемых или удаляемых заголовков, если отправитель, получатель и устройства регулирования трафика измеряют пропускную способность не на одном и том же уровне с идентичными размерами PDU;

– уровень порога, с которым сравнивается результат измерения, и размеры всех добавляемых или удаляемых заголовков, если уровень порога не совпадает с уровнем отправителя или получателя.

Если пороговая скорость передачи данных, с которой сравниваются результаты измерения пропускной способности отправителя и получателя, не находится на одном и том же уровне связи, то качество измерения ухудшается. Кроме того, чем больше активных узлов, пунктов регулирования и взаимодействия на маршруте, тем вероятнее наличие дополнительных заголовков, которые могут отсутствовать в передающем и принимающем устройствах, таких как туннельные заголовки между уровнем 2 и уровнем 3 или между уровнем 3 и уровнем 4.

Если при расчетах должны использоваться заголовки Ethernet, то необходимо знать о наличии и количестве тегов VLAN.

В некоторых случаях для правильного формирования кадров требуются управляющие последовательности на уровне 1. Наличие управляющей последовательности может зависеть от структуры битов полезной нагрузки. В этом случае точность измерения ограниченна.

Как правило, скорость передачи данных C_x ограничена (физической или) заданной пропускной способностью на уровне x. На этом уровне x и только на нем справедливо следующее уравнение для скорости передачи данных C_x, измеряемой на уровне x (обобщено из МСЭ-Т Y.1540):

$$C_x\,(t, \Delta t) = N_x(t + \Delta t) / \Delta t, \tag{1}$$

где N_x – общее количество битов уровня x, которое можно передать через базовую секцию с результатом "успешная передача пакета уровня x" в выходном пункте измерения в течение заданного интервала времени $[t, t + \Delta t]$. На уровне связи y, на котором транспортируются пакеты уровня x, к каждому пакету уровня x добавляется заголовок постоянной длины h_y битов. Если известна или измерена только пропускная способность уровня x, то пропускную способность уровня y, используемую измеряемым потоком пакетов, можно определить, только если известны количество пакетов p_x на уровне x и размер заголовков h уровня y:

$$C_y\,(t, \Delta t) = [N_x\,(t + \Delta t) + p_x * h_y] / \Delta t = C_x\,(t, \Delta t) + p_x * h_y / \Delta t. \tag{2}$$

Очевидны два изменения, влияющие на погрешность измерения:

- как и ожидалось, пропускная способность C_y уровня y больше, чем пропускная способность C_x уровня x;
- C_y зависит от количества пакетов p_x на уровне x, а C_x не зависит от количества таких пакетов на уровне x.

Количество пакетов p_x и средний размер пакета s_x связаны уравнением (3):

$$s_x = C_x\,(t, \Delta t) / p_x. \tag{3}$$

Размер пакета s_x уровня x влияет на результирующую скорость передачи данных C_y, измеренную на уровне y.

Определить размер заголовков и максимальный размер пакетов на разных уровнях связи для некоторых рынков позволяют стандарты, общедоступные спецификации и информация о продуктах. Уровень, на котором сеть или устройство поставщика услуг устанавливает заданную скорость передачи данных, следует считать неизвестным.

Наибольшее повышение точности результатов измерения пропускной способности достигается, если во внимание принимается подробная информация о размере пакетов для измерения и указанная информация о формате заголовков в узких местах из как можно большего числа различных уровней.

В отсутствие подробной информации в качестве консервативного допущения следует принять минимальный размер служебных данных, который позволяют принять либо используемая измерительная установка, либо общая информация о доступе, если спецификация формата заголовков ее уровня отсутствует. Это все же позволит уменьшить результирующую погрешность измерения.

Для уменьшения погрешности измерения должны быть известны средние размеры принимаемых измерительных пакетов или количество принятых измерительных пакетов.

Если заголовки уровней и средний размер или количество принятых измерительных пакетов точно не известны, но можно определить их максимальное и минимальное значения, то можно определить и коридор скорректированных результатов измерения.

Формулы (1), (2) и (3) позволяют рассчитать пропускную способность на разных уровнях связи, если известны заголовки этих уровней и средний размер или количество принятых измерительных пакетов либо их максимальное и минимальное значения (в дополнение к результату измерения пропускной способности).

XII.4 Пример расчета служебных данных для проводного интерфейса Ethernet IEEE 802.3

Следует отметить, что все приведенные ниже расчеты действительны только для пакетов, передаваемых в ограничивающем звене по физическому каналу, соответствующему сети Ethernet, как указано в стандартах серии IEEE 802.3.

В рамках этого проекта ИК12 провела лабораторные испытания, направленные на измерение пропускной способности услуг доступа (см. Приложение X). Измерительный инструмент iPerf 2 сообщает результаты измерения скорости по количеству доставленных байтов транспортируемой полезной нагрузки (выше уровня UDP или TCP). Скорость работы фильтра на основе буфера маркеров [ограничивающего формирователя] указывается в "битах в проводе", так что заголовки, добавляемые к транспортируемой полезной нагрузке, включаются в расчеты фильтра на основе буфера маркеров (скорость рассчитывается с учетом битов заголовков ETH, IP и транспортного протокола).

Известно, что полезная нагрузка UDP при первом измерении составила 1470 байтов. Соединение Ethernet – стандартное (без заголовков VLAN).

Вычисления заголовков нижнего уровня:

- заголовок UDP: 8 байтов;
- заголовок IPv4: 20 байтов;
- заголовок Ethernet.

Заголовок

14 байтов (уровень 2 без циклической проверки избыточности (CRC));
18 байтов (уровень 2 с CRC);
26 байтов (уровень 1).

Была получена скорость, составляющая 97,2% от заданной скорости без потери пакетов при разных значениях ограничения скорости. Первоначально предполагалось, что в размер кадра Ethernet уровня 2 включены байты CRC. С заголовком в 46 байтов на пакет был получен поправочный коэффициент 1,0313. Расчет пропускной способности формирователя в "битах в проводе" дал коэффициент 1,00242 к заданной скорости. Погрешность составила 0,24%, что достаточно мало.

Более тщательное исследование показало, что скорость формирователя не учитывает байты CRC. Поправочный коэффициент, основанный на размере заголовка 42 байта, в этом случае составил 1,0286. Расчет пропускной способности формирователя в "битах в проводе" дал коэффициент 0,999799 к заданной скорости. Погрешность составила −0,02%, что еще на порядок ниже. Ошибка измерения в две миллионных доли указывает на то, что лабораторная конфигурация формирователя на уровне 2 Ethernet работает довольно точно (без байтов CRC).

Следует отметить, что оборудование оператора сети также может измерять трафик Ethernet на уровне 2 без CRC. Уровень измерения скорости передачи данных Ethernet по умолчанию пока отсутствует, и аппаратура оператора сети может также измерять Ethernet на уровне 1 или на уровне 2, включая байты CRC.

XII.5 Описание функциональных возможностей фильтра на основе буфера маркеров

Формирователи и ограничители ограничивают скорость передачи трафика. Базовое управление скоростью передачи данных часто основано на использовании фильтра на основе буфера маркеров. Фильтр на основе буфера маркеров обычно работает следующим образом:

- настраивается скорость передачи данных *Rate* в [бит/с];
- настраивается устойчивость к неравномерности трафика *Burst-Tolerance_Byte* в [байтах].

Системы также часто предлагают возможность настройки устойчивости к неравномерности трафика *Burst-Tolerance_ms* в [мс]. Можно ожидать, что в системе будет установлен следующий внутренний буфер:

$$Burst\text{-}Tolerance\_Byte\ [byte] = Rate / 8 / Burst\text{-}Tolerance\_ms * 1000. \quad (4)$$

Ограничитель на основе буфера маркеров каждые *1/Rate* секунды добавляет в буфер однобитовый маркер. Если буфер заполнен маркерами *Burst-Tolerance_Byte*, дополнительные маркеры отбрасываются.

Когда приходит пакет длиной *Packet-Length* байтов, фильтр проверяет, присутствуют ли в буфере маркеры, соответствующие значению *Packet-Length*.

- Если да, то пакет передается и из буфера удаляются *Packet-Length* байтов.
- Если нет, то пакет отбрасывается и буфер остается неизменным (если только не присутствует дополнительный буфер формирователя; см. примечание ниже).

Формирователь на основе буфера маркеров работает как ограничитель, но управляет дополнительным буфером длиной *Buffer_bytes*. Если ограничитель отбрасывает пакет, он сохраняется в буфере до тех пор, пока последний не переполнится. Как только в фильтре на основе буфера маркеров собирается достаточное количество маркеров, первый пакет, хранящийся в буфере, передается (при условии, что установлено обслуживание в порядке очереди).

Если буфер формирователя заполнен поступающими пакетами, любые дополнительные пакеты отбрасываются.

Следует отметить, что у формирователей есть дополнительный буфер, который можно настроить в соответствии со значением *Buffer_ms* в [мс] или с количеством *пакетов*, и когда система выделяет байты для буфера пакетов, обычно предполагается средний размер пакета. Опять же, для расчета глубины внутреннего буфера системы *Buffer_bytes* используется заданное значение скорости передачи данных *Rate*, как показано в формуле (1).

Дополнение XIII

Параметры и методы измерения, связанные с IP-потоком

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

XIII.1 Базовая информация

В марте 2018 года IETF утвердил и опубликовал документ RFC 8337 "Показатели на основе моделей пропускной способности службы транспортировки массивов данных" [IETF RFC 8337]. Работа над показателями на основе моделей (MBM) стала результатом многолетнего изучения проблемы измерения пропускной способности транспортного уровня, прежде всего в рабочей группе IETF по показателям рабочих характеристик IP-услуг (IPPM). В спецификации подробно описаны многие проблемы и трудности, связанные с повторяемостью при тестировании с использованием стандартного TCP (раздел 4), и эти проблемы решаются главным образом путем разработки метода и набора диагностических тестов, в которых управление потоком TCP запрещено. Метод включает в себя оценку рабочих характеристик целевой службы транспортировки с точки зрения скорости передачи и времени передачи в прямом и обратном направлениях (RTT).

Оценка MBM началась еще до публикации RFC. Мортон в статье "Усовершенствованные тесты скорости интернета могут улучшить показатели QoS и QoE" рассматривает несколько методов измерения для оценки структуры модели MBM в контексте выявления многих проблем с точностью существующих методов измерения интернета и начала работы над их решением [MortonPQS].

XIII.2 Почему MBM соответствует требованиям настоящей Рекомендации

В пункте 6.12 представлен набор требований, которым должен соответствовать любой связанный с потоком метод измерения как приемлемый в контексте общих ресурсов интернета. Как описано ниже, MBM соответствует этим требованиям (термины и определения см. в разделе 3 [IETF RFC 8337]).

Все параметры, связанные с потоком или пропускной способностью, должны соответствовать следующим пронумерованным требованиям.

1) Параметр, характеризующий пропускную способность, доступную IP-службе, должен соотносить количество IP-пакетов, успешно переданных IP-сетью или секцией, с количеством IP-пакетов, доставленных в эту сеть или секцию.

Количество отправленных пакетов ("доставленных в эту сеть или секцию") полностью определяется выбором тестового потока. Далее, показатель "успешной передачи" IP-пакетов непосредственно измеряется в рамках метода MBM (для получения коэффициента потерь и измерения длины пути).

2) Параметр, связанный с пропускной способностью, должен применяться к сквозной IP-сети и к IP-транспортировке через EL, NS или NSE.

Показатели и измерения MBM не зависят от места наблюдения и, следовательно, применимы к тестовым маршрутам EL, NS или NSE (как соответствующие нескольким другим ключевым требованиям, см. раздел 4.3 [IETF RFC 8337]).

Ниже перечислены дополнительные требования, предъявляемые в настоящей Рекомендации, с анализом соответствия MBM.

Некоторые параметры, связанные с потоком или пропускной способностью, представляют собой попытку охарактеризовать пропускную способность IP-сети, то есть ее способность поддерживать заданную скорость передачи IP-пакетов. Рекомендуется, чтобы любые такие параметры соответствовали следующим дополнительным требованиям.

1) Следует описать структуру трафика, предлагаемую для IP-сети или секции, поскольку от этой структуры зависит способность IP-сети или секции успешно доставлять эти пакеты.

Структура трафика ("предлагаемая для IP-сети или секции") постоянно контролируется путем выбора тестового потока (в соответствии с заданными параметрами тестирования).

2) Скорость поступления трафика не должна превышать пропускную способность (в битах в секунду) канала, соединяющего тестируемые секции с нетестируемыми секциями назначения.

Предлагаемая структура трафика выбирается и контролируется в соответствии с ограничениями тестового потока и параметром target_rate модели MBM.

3) В любом отдельном заявлении о характеристиках пропускной способности должен быть объявлен тип рассматриваемых IP-пакетов.

Система показателей рабочих характеристик IP-услуг (IPPM) IETF [b-IETF RFC 2330] (которой руководствуются при разработке всех показателей и проведении измерений согласно их спецификациям) устанавливает четкие требования по указанию деталей пакетов; см. раздел 13 "Пакеты типа P". Следует отметить, что в настоящее время этот раздел пересматривается в целях включения в него требований IPv6 и других новейших разработок.

Необходимо отметить, что в Дополнении IX объясняется, почему измерения с использованием стандартного протокола TCP не соответствуют требованиям пункта 6.12.

XIII.3 Роль и статус метода измерения MBM

Роль метода MBM состоит в определении того, имеет ли маршрут или участок маршрута достаточную пропускную способность для поддержки целевой скорости надежной передачи потока байтов отдельного соединения транспортного уровня. Этот метод полезен при оценке того, обеспечивает ли маршрут или участок маршрута, например участок маршрута между сервером доставки контента и головным узлом звена доступа, скорость передачи данных, требуемую конкретным приложением. Однако оценка пропускной способности IP-уровня на гигабитовых скоростях не относится к роли методов MBM.

В остальных разделах данного Дополнения рассматриваются темы, которые в настоящее время подлежат дальнейшему изучению. Необходимы дополнительные исследования в лабораторных и полевых условиях.

XIII.4 Выбор тестового потока

В разделе 6 [IETF RFC 8337] предлагается несколько разных схем тестового потока, которые можно выбрать для целевого комплекса диагностики IP-сети (TIDS).

В разделе 6.1 описана структура потока для **имитации затяжного пуска TCP** (в начале каждого TCP-соединения). Основные параметры потока (отметим, что целевые значения определяются подпиской на услуги и тестируемым маршрутом):

- размер пачки в пакетах (4, но могут использоваться и меньшие размеры);
- target_window_size (размер целевого окна);
- target_RTT (целевое значение RTT);
- target_data_rate (целевая скорость передачи данных).

В [IETF RFC 8337] говорится: "…при масштабах времени, превышающих target_RTT, и при размере пачки, равном target_window_size, средняя скорость равна target_data_rate".

В разделе 6.2 описывается структура **потока с псевдопостоянной битовой скоростью (CBR) с постоянным окном**, а также проблема, заключающаяся в том, что окно размером в целое количество пакетов в сочетании с фиксированным значением RTT может привести к тому, что скорость доставки данных будет точно представлять значение параметра target_data_rate (при работе со скоростью, которая несколько больше или меньше этого значения), например при малых значениях RTT или параметра target_data_rate.

Опять же указаны четыре ключевых параметра потока, имитирующего затяжной пуск TCP.

Отклонение от значения параметра target_data_rate также может происходить при колебании значения RTT из-за использования автосинхронизации в этом потоке (скорость передачи определяется поступлением сообщений ACK TCP, а они зависят от RTT). Изменение RTT (увеличение и уменьшение) может быть вызвано непредусмотренным конкурирующим трафиком.

Как предполагается в [IETF RFC 8337], "в этих условиях более подходящим может быть традиционный измерительный трафик", при котором целевая скорость передачи данных (target_data_rate) не может быть достигнута и не возникают проблемы с RTT/автосинхронизацией. **Трафик с псевдо-CBR** может

содержать неравномерности, но на протяжении всего теста он передается с целевой скоростью передачи данных.

Приведенные выше потоки трафика псевдо-CBR используются при оценках базовой скорости передачи данных, поддерживая, например, тест, описанный в разделе 8.1.2 [IETF RFC 8337].

Следует отметить, что раздел 6.3, в котором описан процесс создания потока псевдо-CBR с окном сканирования, усложняет задачу достижения большего реализма при разных условиях сети и в настоящее время требует дальнейшего изучения.

XIII.5 Пункты измерения

В [b-IETF RFC 7398] определены эталонный маршрут и пункты измерения обычно используемых показателей рабочих характеристик. Описанные здесь расширения для определения местоположения пункта измерения могут использоваться и в других подобных проектах по измерению. Целью [b-IETF RFC 7398] является создание эффективного способа описания местоположения пунктов измерения, используемых для проведения конкретных измерений, особенно указание того, когда в измерение входят управляемые и неуправляемые участки маршрута (частные сети).

Следует отметить, что от маршрута измерения, ограниченного пунктами измерения [b-IETF RFC 7398], зависит применимость параметров подписки, таких как типичные предлагаемые скорости передачи данных, а также влияние параметров подписки на выбор параметров MBM, таких как target_data_rate.

На следующем рисунке показаны две непересекающиеся области измерений: область доступа и область распределения.

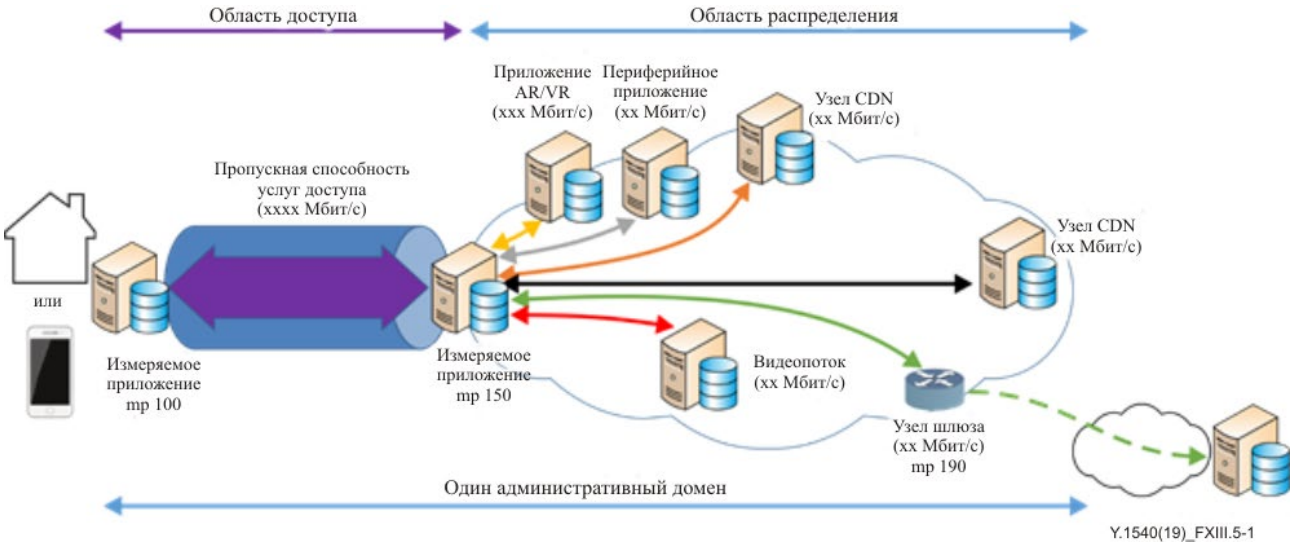


Рисунок XIII.5-1 – Отдельные измерения для областей доступа и распределения

В [b-IETF RFC 7398] область доступа находится между mp100 и mp150, и это предполагаемая область применения показателей пропускной способности IP-уровня на основе UDP и методов из Приложения A.

Область же распределения находится между mp150 и mp190 [b-IETF RFC 7398], и это предполагаемая область применения методов оценки целевой скорости передачи данных (target_data_rate) на основе MBM (между хостами на периферии или внутри области распределения) после их дальнейшего уточнения.

XIII.6 Спецификация целевых параметров модели

См. разделы 5.1 и 5.2 [IETF RFC 8337].

XIII.7 Задание критериев приемлемости и интерпретация результатов

См. разделы 7.1 и 7.2 [IETF RFC 8337].

XIII.8 Методы испытаний

Авторы [b-IETF RFC 6673] и [MortonPQS] отмечают, что следует использовать множество повторяющихся испытаний (тестов). Один тест не даст точной оценки какой-либо абонентской услуги, которую предполагается предоставлять по требованию, но может оказаться достаточным, когда нужно просто убедиться, что результаты соответствуют ожиданиям.

XIII.9 Пример (примеры)

См. раздел 9 [IETF RFC 8337].

Библиография

[b-ITU-T I.353] Рекомендация МСЭ-Т I.353 (1996 г.), *Эталонные события для определения показателей качества ЦСИС и Ш-ЦСИС.*

[b-ITU-T I.356] Recommendation ITU-T I.356 (2000), *B-ISDN ATM layer cell transfer performance.*

[b-ITU-T P.800] Recommendation ITU-T P.800 (1996), *Methods for objective and subjective assessment of quality.*

[b-ITU-T X.25] Recommendation ITU-T X.25 (1996), *Interface between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit.*

[b-ITU-T X.75] Recommendation ITU-T X.75 (1996), *Packet-switched signalling system between public networks providing data transmission services.*

[b-ITU-T X.137] Recommendation ITU-T X.137 (1997), *Availability performance values for public data networks when providing international packet-switched services.*

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

[b-IETF RFC 768] IETF RFC 768 (1980), *User Datagram Protocol*.
<http://www.ietf.org/rfc/rfc768.txt>

[b-IETF RFC 792] IETF RFC 792 (1981), *Internet Control Message Protocol*.
<http://www.ietf.org/rfc/rfc792.txt>

[b-IETF RFC 793] IETF RFC 793 (1981), *Transmission Control Protocol.*
<http://www.ietf.org/rfc/rfc793.txt>

[b-IETF RFC 919] IETF RFC 919 (1984), *Broadcasting Internet Datagrams.*
<http://www.ietf.org/rfc/rfc919.txt>

[b-IETF RFC 922] IETF RFC 922 (1984), *Broadcasting Internet datagrams in the presence of subnets*.
<http://www.ietf.org/rfc/rfc922.txt>

[b-IETF RFC 950] IETF RFC 950 (1985), *Internet Standard Subnetting Procedure.*
<http://www.ietf.org/rfc/rfc950.txt>

[b-IETF RFC 959] IETF RFC 959 (1985), *File Transfer Protocol*.
<http://www.ietf.org/rfc/rfc959.txt>

[b-IETF RFC 1305] IETF RFC 1305 (1992), *Network Time Protocol (Version 3) Specification, Implementation and Analysis.*
<http://www.ietf.org/rfc/rfc1305.txt>

[b-IETF RFC 1786] IETF RFC 1786 (1995), *Representation of IP Routing Policies in a Routing Registry* (*ripe-81++*).
<http://www.ietf.org/rfc/rfc1786.txt>

[b-IETF RFC 1812] IETF RFC 1812 (1995), *Requirements for IP Version 4 Routers.*
<http://www.ietf.org/rfc/rfc1812.txt>

[b-IETF RFC 2018] IETF RFC 2018 (1996), *TCP Selective Acknowledgment Options.*
<http://www.ietf.org/rfc/rfc2018.txt>

[b-IETF RFC 2330] IETF RFC 2330 (1998), *Framework for IP Performance Metrics.*
<http://www.ietf.org/rfc/rfc2330.txt>

[b-IETF RFC 3148] IETF RFC 3148 (2001), *A Framework for Defining Empirical Bulk Transfer Capacity Metrics.*
<http://www.ietf.org/rfc/rfc3148.txt>

[b-IETF RFC 3357] IETF RFC 3357 (2002), *One-way Loss Pattern Sample Metrics.* <http://www.ietf.org/rfc/rfc3357.txt>

[b-IETF RFC 3393] IETF RFC 3393 (2002), *IP Packet Delay Variation Metric for IP Performance Metrics (IPPM).* <http://www.ietf.org/rfc/rfc3393.txt>

[b-IETF RFC 3432] IETF RFC 3432 (2002), *Network performance measurement with periodic streams.* <http://www.ietf.org/rfc/rfc3432.txt>

[b-IETF RFC 3550] IETF RFC 3550 (2003*), RTP: A Transport Protocol for Real-Time Applications.* <http://www.ietf.org/rfc/rfc3550.txt>

[b-IETF RFC 6576] IETF RFC 6576 (2012), *IP Performance Metrics (IPPM) Standard Advancement Testing.* <https://www.rfc-editor.org/rfc/rfc6576.txt>

[b-IETF RFC 6673] IETF RFC 6673 (2012), *Round-Trip Packet Loss Metrics.* <https://www.rfc-editor.org/info/rfc6673>

[b-IETF RFC 7398] IETF RFC 7398 (2015), *A Reference Path and Measurement Points for Large-Scale Measurement of Broadband Performance.* <https://www.rfc-editor.org/info/rfc7398>

[b-BEREC] BoR (18) 32: TENDER SPECIFICATIONS, No BEREC/2018/01/OT Net Neutrality Measurement Tool, March 2018.

[b-C-298] Kotanis, Irina (2015), *Proposals for E.802 Annex: minimum required of samples, statistical significance for benchmarking and quality trends evaluations and minimum required number of mobile agents, (with revisions),* ASCOM, Switzerland.

[b-CVST] Krueger, T. and M. Braun (2012), *R package: Fast Cross – Validation via Sequential Testing, version 0.1.*

[b-Damjanovic] Damjanovic, Welzl et al. (2008), *Extending the TCP Steady-State Throughput Equation for Parallel TCP Flows*, University of Innsbruck, Budapest University of Technology. <http://heim.ifi.uio.no/~michawe/research/publications/mulPadhye-TechnicalReport.pdf>

[b-Ekelin] Ekelin, S., Nilsson, M., Hartikainen, E., Johnsson, A., Mångs, J., Melander, B., Björkman, M. (2006), *Real-time measurement of end-to-end available bandwidth using kalman filtering,* IEEE/IFIP Network Operations and Management Symposium, Vancouver, Canada.

[b-Google-Police] "An Internet-Wide Analysis of Traffic Policing", Flach, Papageorge et al., University of Southern California and Google, 2016.

[b-Lautenschlaeger] Lautenschlaeger, W. (2014), A Deterministic TCP Bandwidth Sharing Model, Bell-Labs Alacatel-Lucent. <https://arxiv.org/abs/1404.4173>

[b-Montgomery] Montgomery, D. (1990), *Introduction to Statistical Quality Control – 2nd edition, ISBN 0-471-51988-X.*

[b-Morton] Morton, Al (2013), *Improved Internet speed tests can enhance QoS and QoE,* Proceedings of the 4th International Workshop on Perceptual Quality of Systems (PQS 2013), Vienna, Austria.

[b-Mou] Mou, M. (2017), *Evaluating a TCP Model-Based Network Performance Measurement Method*, Masters Thesis at MIT, June 2017. <https://dspace.mit.edu/handle/1721.1/113177>

[b-PAM-12] Oana Goga & Renata Teixeira (2012), *Speed Measurements of Residential Internet Access*, Passive and Active Measurements Conference, PAM-12. <https://people.mpi-sws.org/~ogoga/papers/PAM12-speed.pdf>

[b-Pod12] OPNFV Project, Intel POD12.
<https://wiki.opnfv.org/display/pharos/Intel+POD12>

[b-Prasad] Prasad, R.S., Murray, M., Dovrolis, C., Claffy, K.C. (2003), *Bandwidth Estimation: Metrics, Measurement Techniques, and Tools, IEEE Network.*

[b-QUIC] "draft-ietf-quic-recovery-11", Iyengar and Swett. work in progress, IETF 2018.
<https://datatracker.ietf.org/doc/draft-ietf-quic-recovery/>

[b-Rdev] R Development Core Team (2016), R*: A language and environment for statistical computing,* R Foundation for Statistical Computing, Vienna, Austria.
ISBN 3-900051-07-0.
<http://www.r-project.org/>

[b-TST 009] ETSI GS NFV-TST 009 V3.1.1, (2018), *Network Functions Virtualisation (NFV) Release 3; Testing; Specification of Networking Benchmarks and Measurement Methods for NFVI*.
<https://www.etsi.org/deliver/etsi_gs/NFV-TST/001_099/009/03.01.01_60/gs_NFV-TST009v030101p.pdf>
<https://docbox.etsi.org/ISG/NFV/Open/Drafts/TST009_NFVI_Benchmarks>

[b-Wald] Wald, A. (1947), *Sequential Analysis*, Wiley.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ
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	Качество телефонной передачи, телефонные установки, сети местных линий
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 протокола Интернет, сети последующих поколений, интернет вещей и "умные" города**
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2023 г.