УДК 621.935

АНАЛИЗ ФУНКЦИОНИРОВАНИЯ НАЛОЖЕННЫХ СЕТЕЙ В СЕТЯХ ОПЕРАТОРОВ

А. А. Дорт-Гольц, аспирант кафедры сетей связи СПбГУТ им. проф. М. А. Бонч-Бруевича; dortgolts@gmail.com

Проанализированы тенденции роста пользовательского трафика, приведен обзор актуальных (на момент написания статьи) видов наложенных сетей. Процессы генерации трафика оверлеями проиллюстрированы на примере типичных анонимных и файлообменных P2P-сетей. Изложены варианты выхода из сложившейся ситуации для операторов доступа и создателей оверлейных сетей.

***Ключевые слова**: пользовательский трафик, наложенные сети, P2P-сети.*

Прогнозы роста нагрузки в сетях доступа. Каждый год исследовательский отдел компании Cisco Systems, Inc. публикует аналитические материалы, посвященные оценке текущего объема данных, передаваемых в масштабах глобальной сети, а также прогнозу роста на ближайшие годы. Ежегодный отчет носит название Cisco Visual Networking Index (VNI) и находится в открытом доступе. Как показывает время, прогнозы компании довольно точны и отличаются от фактических данных примерно на 2—10%. Очень интересной характеристикой с точки зрения построения сетей доступа является прогнозируемое количество пользовательского трафика. Динамика роста этого показателя, представленная в отчете [1], приведена на рис. 1.

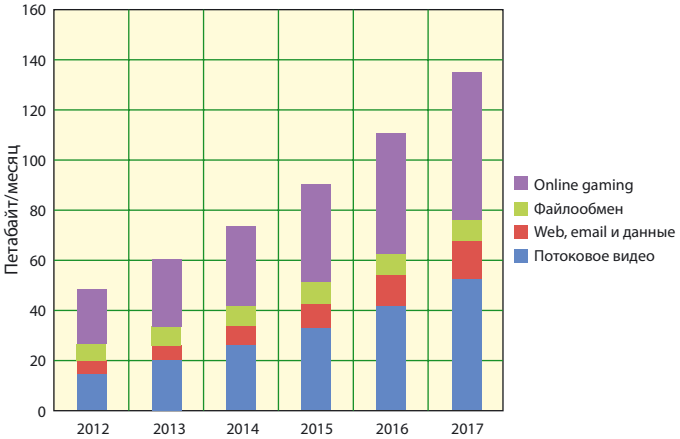


Рис. 1. **Структура пользовательского трафика Интернета**

Как можно заметить из приведенного графика, помимо общего экспоненциального роста объема передаваемых данных, в составе пользовательского трафика меняются количественные соотношения. Например, все более значительным становится вклад трафика онлайн-игр и потокового видео. Данные виды трафика отличаются большей критичностью к таким показателям качества обслуживания (QoS), как задержка и джиттер.

Помимо традиционной, хорошо прогнозируемой клиент-серверной модели организации взаимодействия, использующей для доставки контента традиционные сетевые протоколы, существует другой способ — так называемые наложенные сети. *Наложенная сеть (или оверлей)* в общем случае представляет собой некоторую логическую сеть, организованную поверх существующей физической инфраструктуры и являющуюся надстройкой над стандартными сетевыми протоколами. Рассмотрим подробнее существующее сегодня многообразие наложенных сетей по областям их применения.

Потоковое видео. Согласно уже упомянутому прогнозу Cisco VNI, доля пользовательского видеотрафика к 2017 г. вырастет и будет составлять до 69% всего пользовательского трафика (на данный момент — около 57%). Эта цифра не включает видео, полученное посредством P2P-файлообмена. Если же учесть все виды трафика видео, то к 2017 г. этот тип данных будет доминировать, составляя около 80—90% всего пользовательского трафика.

Доставка больших объемов онлайн-видео до конечных пользователей через Интернет может осуществляться с помощью технологий OTT, CDN или потоковых P2P-приложений. Технология OTT (Over The Top) представляет собой разновидность IPTV, реализующую доставку легального видеоконтента по общему каналу доступа в Интернет без построения собственной сети передачи данных (ПД) или аренды ресурсов у оператора связи. Преимуществом использования P2P-технологий является возможность одновременного просмотра некоторого видеоконтента множеством пользователей. Данное свойство особенно актуально при организации трансляций массовых мероприятий, концертов, спортивных матчей и т.п.

Каждый пользователь, просматривая некоторый видеоролик, становится одним из множества серверов, предоставляющих другим пользователям доступ к уже загруженным частям видео. Указанным способом осуществляется децентрализованное кэширование данных, значительно снижающее нагрузки на сервер-источник и магистральные сети, но вызывающее усиленное использование ресурсов сети доступа. Здесь большее число просматривающих видеоролик означает большее количество узлов наложенной сети, осуществляющих репликацию данных, благодаря чему качество доставки контента улучшается, в отличие от традиционной клиент-серверной архитектуры.

Принцип работы потоковых P2P-приложений близок к широко известным файлообменным P2P-сетям. Иногда в отдельный подвид выделяют системы P2P-TV, представляющие собой описанные потоковые P2P-приложения, предназначенные для просмотра каналов Интернет ТВ. Среди популярных P2P-сетей потокового вещания можно упомянуть BitTorrent Live, TorrentStream, PPLive, UUSee, SopCast и др. Существуют также различные P2P-реализации потоковых аудиоплееров, Интернет-радио

и т.п., однако доля трафика, создаваемого такими приложениями, незначительна на фоне передачи видеопотоков.

Виртуальные операторы услуг связи. Одними из наиболее активных генераторов трафика в сетях доступа являются виртуальные операторы услуг связи. Яркие представители таких операторов — система частично децентрализованной Интернет-телефонии Skype, различные VoIP-сервисы, такие как SIPnet, TeLme, PCTEL и мн. др. Особенность работы виртуального оператора — использование в качестве среды ПД физической инфраструктуры других операторов. При этом работа виртуального оператора никак не согласуется с возможностями конкретных сегментов сети оператора «трубы», не рассчитанных на подобную нагрузку.

Онлайн-игры (MMOG). Под онлайн-играми подразумевается наиболее требовательный к пропускной способности канала подвид MMOG (Massively Multiplayer Online Games). Как можно видеть из рис. 1, уже сейчас данные MMOG составляют значительную долю потребительского трафика, в дальнейшем же ожидается как количественный, так и относительный рост. Делаются попытки организации игровых приложений на базе P2P-платформы (например, Outback Online от компании Yoicks), однако на данный момент подавляющее большинство MMOG организованы по классической клиент/серверной технологии. Одна из особенностей MMOG — высокая критичность приложений к сетевой задержке, даже в большей степени, чем для передачи речи.

Сети распространения контента или CDN (Content Delivery Networks). Они представляют собой географически распределенную сетевую структуру, позволяющую оптимизировать доставку контента конечным пользователям сети Интернет. Прогноз Cisco VNI гласит, что примерно половина всего трафика, потребляемого пользователями к 2017 г., будет доставляться с помощью различных CDN. Среди многообразия возможных реализаций таких сетей в контексте обсуждения уровня доступа наиболее интересными представляются CDN, задействующие машины других пользователей в процессе распространения контента. К ним относятся гибридные CDN, использующие технологии P2P-сетей для оптимизации доставки контента. Например, одна из крупнейших мировых CDN Akamai применяет гибридный подход: данные могут быть переданы с ближайшего кэширующего сервера, либо из P2P-сети, либо обоими перечисленными методами одновременно [2]. Таким образом, задействуются другие клиентские машины, с которых и осуществляется ПД на запрашивающий узел, что создает дополнительную нагрузку на сети доступа оператора, снимая ее с сервера-источника.

Файлообменные P2P-сети. Значительную часть нагрузки, создаваемой на сети доступа, генерируют традиционные приложения P2P-файлообмена. ПД в таких наложенных сетях осуществляется напрямую между узлами-участниками, в роли которых выступают компьютеры пользователей. Все существующие P2P-сети можно классифицировать следующим образом:

- неструктурированные сети — децентрализованные (одноранговые и двухуровневые) и централизованные;
- структурированные сети.

Неструктурированные сети принято относить к первому поколению наложенных сетей, а структурированные, соответственно, ко второму, однако такое разделение основывается лишь на моменте появления соответствующих алгоритмов, и не является показателем их актуальности или распространенности в современном мире [3]. Отличительной особенностью неструктурированных сетей по определению является отсутствие четкой упорядоченности архитектуры сети и размещения хранимых данных. Узлы в структурированных сетях, напротив, организуются строго определенным образом (на прикладном уровне), и точки хранения конкретных данных всегда жестко определены [4]. В некотором смысле традиционные файлообменные P2P-сети можно считать разновидностью CDN, основанной практически полностью на инфраструктуре пользовательских машин и сетей.

Анонимные сети. Среди современных пользователей Интернета постепенно завоевывают популярность так называемые анонимные сети — это сети, в которых невозможно достоверно установить авторство, осуществить цензуру или отследить обмен данными. По своей природе анонимные сети относятся к наложенным сетям различных типов: некоторые позволяют осуществлять только не контролируемый третьими лицами файлообмен, другие же предоставляют платформу для безопасного и анонимного запуска множества разнообразных сетевых сервисов, аналогичных используемым в открытом пространстве Интернета. ПД в анонимных сетях характеризуется большим временем отклика, а также значительным увеличением трафика за счет намеренной протокольной избыточности и ретрансляции данных других участников.

Ботнеты. Одним из редко учитываемых видов нагрузок на сети доступа являются так называемые *ботнеты*. Типичный ботнет (botnet) представляет собой наложенную сеть, состоящую из множества компьютеров, зараженных вредоносным ПО, позволяющим некоторому управляющему узлу скрытно контролировать и координировать их действия. От других типов наложенных сетей ботнеты отличаются тем, что реальные пользователи данных машин не подозревают о своем участии в работе наложенной сети. В основной своей массе ботнеты занимаются различной нежелательной деятельностью, такой как рассылка спама, осуществление DDoS-атак, сканирование портов, уязвимостей и т.п. [5]. Несмотря на то, что подобные наложенные сети способны создавать значительную пиковую нагрузку, генерируемый ими трафик в среднем сравнительно невелик.

M2M. Считается, что действующая на данный момент концепция развития сетей связи общего пользования NGN практически исчерпала себя и нуждается в обновлении. В Рек. МСЭ-Т Y.2060 была предложена новая концепция развития под общим названием Internet of Things (IoT), т.е. *Интернет Вещей*. Под вещами в IoT понимаются объекты физического или информационного мира, которые можно идентифицировать и интегрировать в сети связи [6].

Согласно экспертным оценкам, количество вещей в Интернете к 2017—2020 гг. достигнет 7 триллионов единиц. Ввиду такого огромного числа взаимодействующих объектов должна измениться сама концепция построения глобальной сети — новые сети должны быть самоорганизующимися. Данные предположения позволяют утверждать, что объемы передаваемого M2M-трафика значительно вырастут со временем. Так, по оценкам Cisco VNI доля трафика, потребляемого различными non-PC устройствами, вырастет вдвое и составит 49% против нынешних 26%, причем темпы роста объемов M2M-трафика обещают ускориться на 82%. Частично данная нагрузка ляжет на мобильные

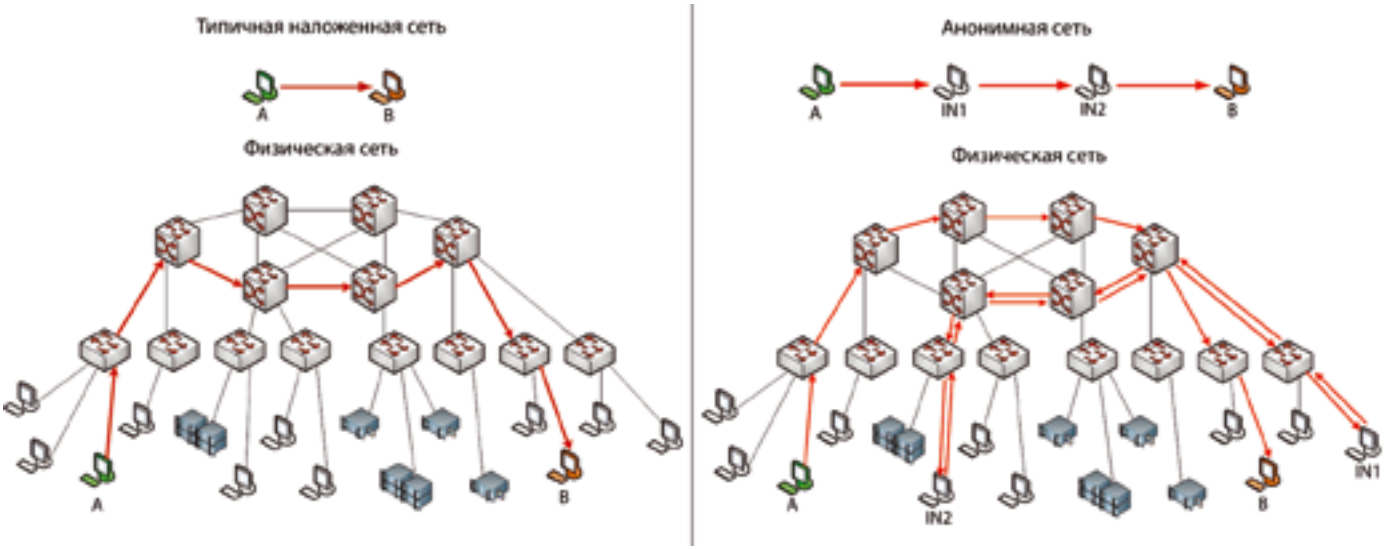


Рис. 2. **Передача данных в наложенных сетях**

сети, однако следует ожидать определенного увеличения объемов передаваемых данных M2M и в фиксированных сетях доступа.

Прочие виды наложенных сетей. Помимо описанных выше категорий, существуют также сравнительно экзотичные и немногочисленные виды наложенных сетей.

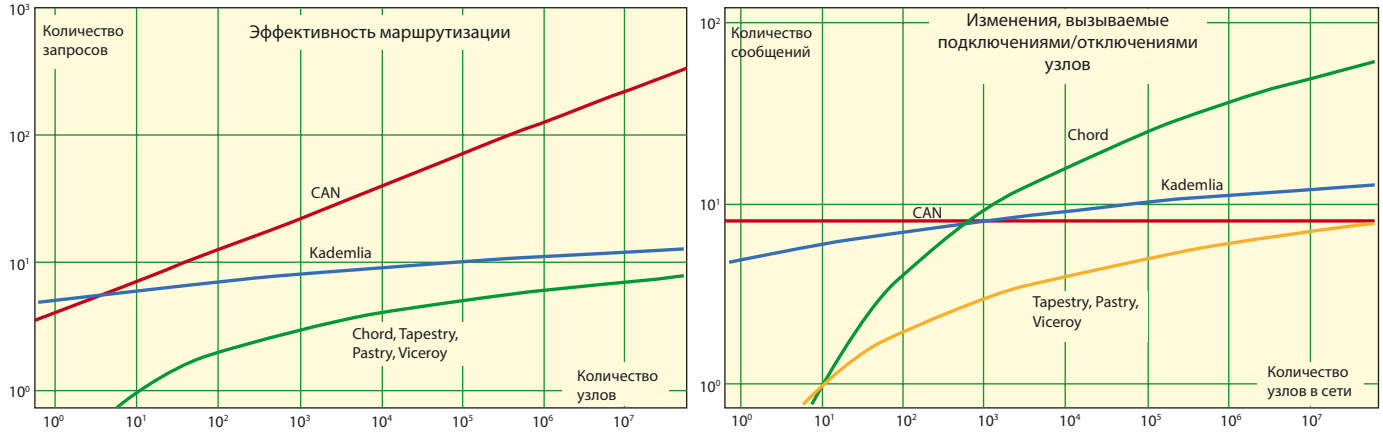
- Различные популярные GRID-проекты. Технология GRID-вычислений представляет собой пространственно распределенную инфраструктуру, позволяющую использовать для решения сложных ресурсоемких задач незадействованные ресурсы пользователей, такие как вычислительные мощности, дисковое пространство и др.
- Персональные P2P-хранилища. В качестве примера можно привести BitTorrent Sync — сервис для синхронизации файлов и резервного копирования данных по протоколу BitTorrent между произвольными устройствами.
- DarkNet или F2F-сети (Friend-to-Friend). Представляют собой разновидности P2P-сетей, использующие нестандартные протоколы и/или не являющиеся публичными. Соединения в таких сетях осуществляются только между доверенными узлами, подлинность которых устанавливается каким-либо сторонним методом.

Перечисленные виды наложенных сетей на данный момент не вносят значительного вклада в трафик сетей доступа.

Генерируемый трафик. Проанализируем генерируемый наложенными сетями трафик на примере двух типичных представителей: анонимных и классических P2P-сетей. Создаваемая такими сетями нагрузка складывается из служебного трафика (поиск данных, информация о подключениях/отключениях узлов и т.п.) и трафика ПД. Так как рассматриваемые сетевые структуры являются наложенными, необходимо ввести специальную нормированную величину, позволяющую оценить эффективности процессов маршрутизации и ПД в таких сетях — *удельное количество сообщений*.

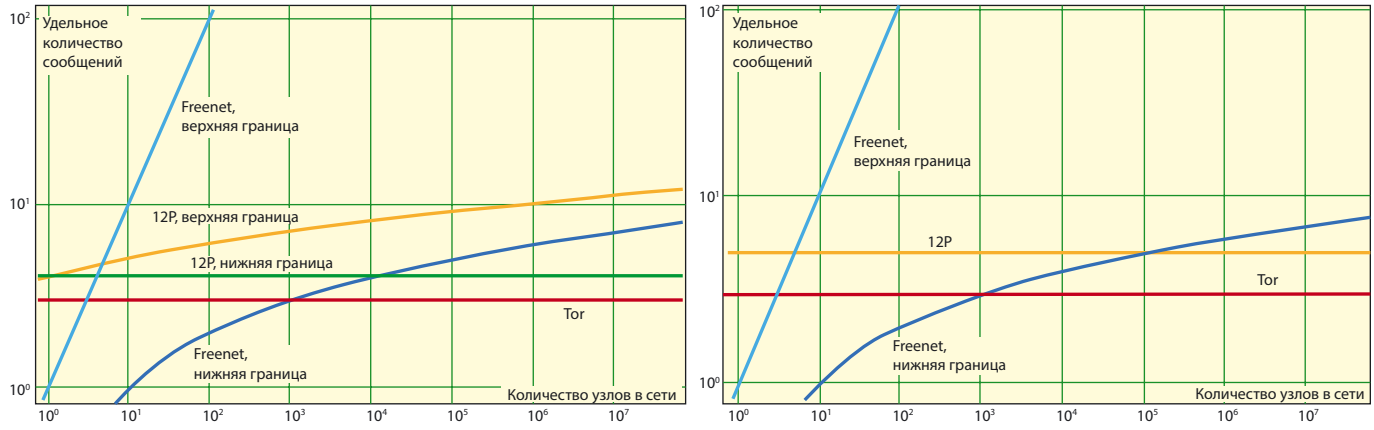
Эта величина выражает условное среднее количество сообщений, которое будет сгенерировано сетью при прохождении по ней одного запроса данных/ресурса (в случае поиска) или передаче некоторого объекта данных. Величина нормируется таким образом, что в идеальном случае, т.е. при наличии прямой связи между узлами (в топологии наложенной сети) для поиска или ПД требуется одно такое сообщение (рис. 2). Эта оценка является вероятностной и может дать представление о характере поведения трафика в сети при масштабировании последней.

Для неструктурированных наложенных сетей трудно получить конкретные границы оценок, так как они могут варьироваться в широких пределах, в зависимости от



а) *б)*

Рис. 3. **Зависимость объема служебного трафика при маршрутизации запросов (*а*) и перестройке сети (*б*)**



а) *б)*

Рис. 4. **Эффективность поиска данных и трафик ПД в анонимных сетях**

расположения узла в сети, популярности запроса и т.д. Поэтому рассмотрим основные зависимости от количества узлов в распространенных структурированных наложенных сетях. На рис. 3, *а* приведено изменение эффективности маршрутизации (т.е. количества запросов, необходимых для нахождения в сети требуемых данных) для различных протоколов. Легко видеть, что наименее ресурсоемкими протоколами являются Chord, Tapestry, Pastry и Viceroy.

Другой важной характеристикой является устойчивость сети к изменениям топологии (перестройка сети). На рис. 3, *б* приведены графики, отражающие зависимость удельного количества сообщений от размера сети при подключении или отключении узлов. Таким образом, наибольшую эффективность с точки зрения минимизации служебного трафика имеют протоколы Tapestry, Pastry и Viceroy [7]. Анализ трафика ПД для структурированных сетей не имеет смысла, поскольку после нахождения объекта данных, обмен между узлами осуществляется напрямую с помощью традиционных протоколов маршрутизации, как показано на рис. 2.

Аналогичным образом рассмотрим три наиболее популярные на данный момент анонимные сети: Freenet, Tor и I2P. Говоря об анонимных сетях, можно выделить следующую особенность, отличающую их от всех других наложенных сетей: для повышения безопасности анонимные сети намеренно выбирают неоптимальные маршруты ПД. Причем, если длина пути передачи уже найденных данных в сетях I2P и Tor имеет мало изменяющееся, почти постоянное значение (длины туннелей/каналов), то при использовании Freenet данные передаются назад тем же путем, который прошел поисковый запрос. Это существенно увеличивает избыточность трафика при большом размере сети, высоких нагрузках, а также при запросах непопулярных данных [8].

Для анализа генерируемого сетью трафика воспользуемся уже известным показателем — удельным количеством сообщений. Вероятностные границы эффективности поиска данных и трафик, генерируемый при ПД в рассматриваемых анонимных сетях, представлены на рис. 4. Анализ приведенных графиков показывает, что при большом количестве узлов в сети (более 1000) наименьшей эффективностью поиска обладает Freenet, генерирующий значительное количество сообщений. Трафик, вызываемый поисковым запросом в I2P, близок к нижней границе оценки среднего количества сообщений в Freenet. В то же время стоимость поиска узла/ресурса в Tor остается на постоянном уровне. Такой результат ожидаем для системы с централизованным поиском.

Как уже упоминалось выше, ПД после их обнаружения в сети происходит неоптимальным образом по цепочке узлов. Однако за счет того, что Tor и I2P используют цепочки приблизительно постоянной длины, рост числа узлов практически не влияет на количество трафика, генерируемого в наложенной сети при передаче запрашиваемых данных. А сеть Freenet показывает значительный рост трафика, так как ПД производится тем же путем, по которому шел поисковый запрос.

Взаимодействие наложенных сетей и операторов. Основной проблемой функционирования наложенных (overlay) сетей, как правило, является их несогласованность с топологией несущей (underlay) сети, не позволяющая последней максимально эффективно использовать собственные ресурсы. Простейшим способом решения подобных проблем, возникающих в результате работы наложенной сети, является блокировка определенного трафика. Однако такое решение нельзя считать приемлемым, так как при этом ущемляются интересы пользователей, ради удовлетворения потребностей которых, в конечном счете, и существует сеть оператора.

Более рациональным подходом является организация взаимодействия оператора сети связи и наложенной сети с целью нахождения некоего компромисса. Как правило, подобную проблему невозможно решить исключительно на уровне доступа. Для получения удовлетворительного результата такое решение должно затрагивать всю сеть оператора. Следовательно, возникают дополнительные проблемы, такие как необходимость выявления трафика определенной наложенной сети в общем потоке и дальнейшая оптимизация взаимодействия физической и виртуальной сетей.

Обсуждение способов детектирования трафика наложенных сетей выходит за рамки данной статьи. Отметим лишь существование широкого спектра подходов к решению данного вопроса, начиная от L7-анализа пакетов и заканчивая сложными статистическими методами, позволяющими выявлять поведенческие паттерны определенных типов трафика.

Основные виды взаимодействия операторов с наложенными сетями можно классифицировать следующим образом [9].

1. Непрямое влияние оператора на наложенную сеть. Оператор использует механизмы управления трафиком и QoS в сети, заложенные в DiffServ, MPLS и т.д.

2. Прямое воздействие на наложенную сеть. Оператор может использовать прозрачные кэширующие серверы, перенаправляющие прокси-серверы и другие методы, позволяющие уменьшить негативные эффекты работы наложенной сети и не затрагивающие ее внутренней логики (т.е. не требующие модификации протоколов самой сети).

3. Односторонняя оптимизация наложенной сети. В этом случае наложенная сеть со своей стороны пытается строить собственную топологию, учитывая параметры физической сети, на базе которой она функционирует: выбор соседних узлов осуществляется с учетом метрики RTT, принадлежности к одной AS и т.д.

4. Двустороннее взаимодействие. Наиболее прогрессивный вариант — и оператор связи, и наложенная сеть пытаются совместно оптимизировать процесс ПД наложенной сети. Алгоритмы наложенной сети строят оптимальную топологию на основании сведений, получаемых от оператора.

Представленные типы взаимодействия призваны по большей части уменьшить негативные эффекты работы наложенных сетей в узких местах: снять часть нагрузки с ядра сети, снизить магистральный трафик между автономными системами и т.д.

Заключение. Говоря о трудностях, возникающих при проектировании и построении сетей доступа, помимо чисто технических моментов можно выделить следующие факторы:

- экспоненциальный рост пользовательского трафика;
- передача разнородного трафика, имеющего различные требования к QoS. Высокая пачечность и самоподобная структура пользовательского трафика вынуждают операторов строить сети с большим запасом ресурса для обеспечения приемлемого QoS;
- нерасчетные пользовательские нагрузки, связанные с работой наложенных сетей и/или операторов услуг.

Основной проблемой работы наложенных сетей является несогласованность физической и наложенной топологий и, как следствие, несоответствие требований и возможностей эффективной передачи такого трафика.

На основании всего вышесказанного можно заключить, что приемлемым решением проблем, создаваемых наложенными сетями (за исключением необходимости блокировки объективно нежелательного трафика, например, ботнетов), является нахождение компромисса между желаниями пользователей и возможностями операторов.

ЛИТЕРАТУРА

1. Cisco Visual Networking Index: Forecast and Methodology, 2012—2017.— Cisco Public, 2013.
2. **Zhi-Hui Lu, Ye Wang, and Yang Richard Yang.** An Analysis and Comparison of CDN-P2P-hybrid Content Delivery System and Model // JCM.— 2012.—7 (3).— 232—245.
3. **Tarkoma S.** Overlay Networks: Toward Information Networking.— CRC Press, 2010.
4. **Crowcroft J., Lua E., Pias M.** A Survey and Comparison of Peer-to-Peer Overlay Network Schemes.— ICST, 2004.
5. **Zeidanloo H., Manaf A.** Botnet Detection by Monitoring Similar Communication Patterns.— IJCSIS, 2010.
6. **Кучерявый А. Е.** Интернет вещей // Электросвязь.— 2013.— № 1.
7. **Дорт-Гольц А. А.** Анализ протоколов наложенных пиринговых сетей / МНТК Актуальные проблемы инфотелекоммуникаций в науке и образовании.— СПбГУТ, 2013.
8. **Дорт-Гольц А. А.** Анализ трафика анонимных сетей. — СПб.: НТОРЭС им. А. С. Попова, 2013.
9. **Dán G., Hoßfeld T., Oechsner S. et al.** Interaction patterns between P2P content distribution systems and ISPs // IEEE Communications Magazine.— 2009.

Получено после доработка 24.02 2014

ИНФОРМАЦИЯ

«ЭКСПРЕСС-АТ 1» И «ЭКСПРЕСС-АТ 2» ВЫВЕДЕНЫ НА ОРБИТУ

16 марта 2014 г. выведены на орбиту российские спутники непосредственного вещания «Экспресс-АТ 1» и «Экспресс-АТ 2».

Новые космические аппараты «Экспресс-АТ 1» и «Экспресс-АТ 2» будут размещены на геостационарной орбите в позиции 56 град.в.д. и 140 град.в.д. соответственно. Они обеспечат услугами непосредственного вещания пользователей на территории России и Казахстана. «Экспресс-АТ 1» будет введен в эксплуатацию после комплекса испытаний в апреле этого года. Коммерческое использование «Экспресс-АТ 2» начнется в мае.

Космические аппараты «Экспресс-АТ 1» и «Экспресс-АТ 2» созданы по заказу подведомственного Федеральному агентству связи ФГУП «Космическая связь» (ГПКС) в рамках Федеральной космической программы России на 2006–2015 гг. Спутники произведены красноярским ОАО «Информационные спутниковые системы» имени академика М. Ф. Решетнёва совместно с французской компанией Thales Alenia Space. Срок активного существования каждого КА составит не менее 15 лет.

«Запуск спутников непосредственного вещания «Экспресс-АТ 1» и «Экспресс-АТ 2» крайне важен для развития рынка отечественного непосредственного вещания. Жители Сибири и Дальнего Востока получат доступ к новым российским и зарубежным телеканалам. После ввода в эксплуатацию этих спутников специалисты ГПКС переведут на них действующие сети с космического аппарата «Бонум-1». Кроме того, будет реализовано много новых интересных проектов в России»,— подчеркнул генеральный директор ФГУП «Космическая связь» (ГПКС) **Ю. В. Прохоров**.

Космический аппарат «Экспресс-АТ 1» создан на платформе «Экспресс-1000Н». Масса КА составляет около 1800 кг. На нем установлено 32 транспондера, работающих в Ku-диапазоне (плюс еще восемь резервных стволов). «Экспресс-АТ 1» обеспечит услугами телевидения западную и центральную Россию, а также западную и центральную Сибирь и практически всю территорию Казахстана.

Телекоммуникационный космический аппарат «Экспресс-АТ 2» создан на платформе «Экспресс-1000К». Его масса составляет около 1250 кг. На КА установлено 16 транспондеров, работающих в Ku-диапазоне. Спутник будет обеспечивать телевизионными услугами восточную часть России.

Заместитель руководителя Федерального агентства связи **И. Н. Чурсин** подчеркнул, что «запуск на орбиту космических аппаратов «Экспресс-АТ 1/-АТ 2» — одно из самых значимых и ожидаемых событий 2014 года не только для организаций, участвующих в создании спутников связи, но и для страны в целом».