УДК 004.042

Шыхалиев Р.Г.
Институт Информационных Технологий НАНА, Баку, Азербайджан
ramiz@science.az

О МЕТОДАХ УПРАВЛЕНИЯ ПРОПУСКНОЙ СПОСОБНОСТЬЮ В КОМПЬЮТЕРНЫХ СЕТЯХ

В статье проанализированы различные методы управления пропускной способностью компьютерных сетей (КС), такие как системы квот, приоритезация трафика, организация очередей, ограничение сервисов, активное управление контентом, пороговое управление, кэширование прокси-серверов, сжатие данных, трансляция сетевых адресов, и определены их преимущества и недостатки, а также возможности использования в управлении трафиком КС.

Ключевые слова: *пропускная способность, управление пропускной способностью, системы квот, приоритезация трафика, ограничение сервисов, управление контентом, пороговое управление.*

1. Введение

В настоящее время, несмотря на высокий уровень развития сетевых технологий, в компьютерных сетях, в особенности в Интернет-подключениях, пропускная способность является дефицитным ресурсом. Инфраструктура КС, в особенности Интернет, растет и меняется очень быстрыми темпами, что приводит к росту объема сетевого трафика, а также возрастает доля нецелевого использования пользователями текущей доступной пропускной способности. Вместе с тем растет популярность так называемых P2P (Peer-to-Peer) приложений, которые используют большую пропускную способность сети [1].

Также в современных сетевых трафиках намного выросла доля мультимедийного, видео- и звукового контента, которые используют большую пропускную способность.

Однако даже выделением большой пропускной способности не всегда удается решить проблемы с обеспечением требуемой производительности трафика пользователей и сетевых приложений, а также сети в целом. Так как при нецелевом использовании большой части текущей доступной пропускной способности одним приложением (например, P2P приложением) или пользователем возникает дефицит пропускной способности для остальных приложений и пользователей, что приводит к нарушению их нормальной работы.

Поэтому для эффективного использования текущей доступной пропускной способности необходимо обеспечить его управление, что является отдельной областью исследований КС.

Пропускная способность КС – это максимальная скорость передачи данных по сети или по каналу связи. Количественно пропускная способность определяется как объем данных, который может передаваться по сети или по каналу связи за единицу времени [2]. Пропускная способность в основном выражается в килобитах в секунду и является одним из параметров, обусловливающим производительность КС. Следовательно, чем эффективнее управляется пропускная способность, тем выше производительность сетей.

Кроме того, общая производительность КС зависит также и от других факторов, таких как латентность, потеря пакетов и т.д.

Управление пропускной способностью – это процесс контроля и измерения пропускной способности сети [3]. Оно является одним из важных элементов

управления КС. Управление пропускной способностью становится особенно важным тогда, когда стоимость необходимой пропускной способности намного превышает стоимость технологий, необходимую для управления пропускной способностью. Эффективное управление пропускной способностью позволит администраторам сети повысить качество сетевых услуг и играет важную роль в обеспечении нормальной работы сетевых приложений и пользователей.

При этом стратегия управления пропускной способностью КС состоит в основном из трех компонент, таких как политика управления, мониторинг и реализация политики управления.

Политика управления пропускной способностью определяет правила использования сети, то есть правила использования сети приложениями, пользователями и т.д. Мониторинг определяет способы и средства мониторинга и анализа сетевого трафика, чтобы выяснить, как используется пропускная способность сети пользователями/приложениями. А реализация политики управления пропускной способностью определяет способы и средства реализации политики.

Существуют различные методы управления пропускной способностью КС, такие как системы квот, приоритезация трафика (traffic shaping), организация (формирование) очередей, ограничение сервисов, активное управление контентом, пороговое управление, кэширование прокси-серверов, сжатие данных, трансляция сетевых адресов и т.д.

Однако управление пропускной способностью КС не заключается в использовании только одного метода или одного средства. Выбор тех или иных методов зависит от таких факторов, как требования к пропускной способности, необходимость приоритезации некоторых типов трафика, реализация стратегии управления пропускной способностью и т.д.

В статье рассматриваются некоторые методы управления пропускной способностью и дается их краткий обзор.

2. Методы управления пропускной способностью

Одной из основных причин перегрузок каналов связи в КС, в особенности в мультисервисных сетях, где используется широкий спектр приложений, таких как видео, голос и данные [4], является недостаточность пропускной способности. Поэтому для обеспечения нормальной работы пользователей, протоколов и приложений необходимо эффективно управлять текущей доступной пропускной способностью сети.

В целях управления пропускной способностью КС были предложены различные методы, такие как:

- системы квот;
- приоритезация трафика;
- организация (формирование) очередей;
- ограничение сервисов;
- активный контроль контента;
- пороговое управление;
- кэширование прокси-серверов;
- сжатие данных;
- трансляция сетевых адресов и т.д.

2.1. Системы квот

Управление пропускной способностью КС на основе системы квот основывается на выделении определенного количества «кредитов» для пользователей в течение определенного периода времени. Эти кредиты могут быть выделены в зависимости от видов трафика или приложения. При этом тип выбранной квоты влияет на их размеры, и в качестве квоты могут быть использованы объем загружаемых данных, значение пропускной способности, количество одновременных соединений и т.д.

Управление пропускной способностью является удачным подходом для достижения справедливости в использовании пропускной способности сети, которая достигается путем ограничения использования отдельными пользователями приложений в течение определенного периода времени [5]. При этом для управления пропускной способностью в качестве простой квоты может быть использован объем данных, который пользователь может загрузить в течение определенного периода времени. Например, пропускная способность может быть ограничена, если объем данных, загружаемых пользователем в сутки, превысит определенный предел. Вместе с тем в системе квот очень важно определение значений оптимальных пределов квот, которые должны минимально влиять на работу большинства пользователей и максимально затруднять деятельность злоумышленников. Поэтому предпочтительными методами определения значений оптимальных пределов квот являются среднесрочный и долгосрочный анализы трафика пользователей, которые позволят определить как неэффективное базовое, так и абсолютно максимальное значения квот.

В системе квот также очень важной является периодичность обновления значений квот, так как со временем меняется профиль пользователей и может увеличиться общая пропускная способность сети. При этом обновление системы квот должно быть полностью автоматизировано и сохранить точность и справедливость квот. Система также должна иметь средства для сброса или корректировки квот. Причем очень важна частота обновления квот, которая в основном определяется скоростью реакции системы на превышение пользователями своих квот, и идеально было бы, чтобы система мгновенно реагировала на превышение квот пользователями. Однако на практике это не всегда получается, так как обработка лог-файлов в режиме реального времени не всегда возможна, ведь они могут находиться на различных серверах.

2.2. Приоритезация трафика

Приоритезация трафика позволяет приоритезировать и управлять трафиками приложений и пользователей в соответствии с заранее определенным предельным значением пропускной способности. Приоритезация трафика, как правило, осуществляется на основе принципа конечной очереди или так называемого принципа «ведра (bucket)», которое заполняется с заданной скоростью по трубе определенного размера и выдает трафик по трубе с меньшим размером [3]. При этом «ведро» используется для обеспечения некоторой задержки трафика, проходящего через него, что определяется максимальной фиксированной скоростью оттока из «ведра». Модификация этого принципа, также известная как принцип «дырявого ведра», показана на рисунке 1.

Другим подходом к приоритезации трафика является так называемый принцип «маркерного ведра (token bucket)», который работает аналогично предыдущему принципу, но вместо фиксированной выходной скорости для ограничения потоков трафика использует набор маркеров.

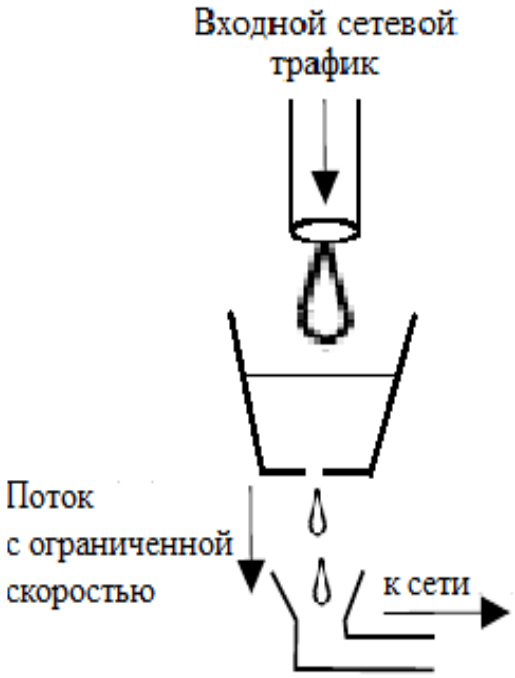

Рис.1. Принцип «дырявого ведра»

Принцип «маркерного ведра» работает следующим образом (рис. 2):

1. Поступающий входной трафик разбивается на части (пакеты), которые помещаются в очередь.

2. Маркеры поступают в «маркерное ведро» с постоянной фиксированной скоростью, и при заполнении маркерами ведра до максимального уровня новые маркеры отбрасываются.

3. Управление пропускной способностью осуществляется удалением из очереди части трафика (пакеты) при наличии соответствующего маркера в «маркерном ведре», например, маркера превышения кредита по объему данных.

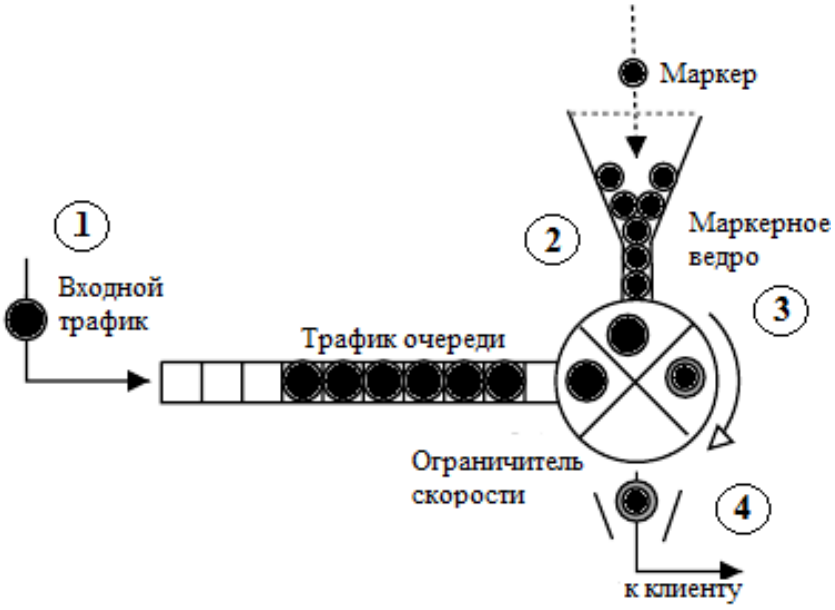

Рис.2. Принцип «маркерного ведра»

4. Выходящий из системы трафик передается клиенту.

Этот принцип имеет преимущество по сравнению с предыдущим в том, что позволяет учитывать «пульсирующий» характер сетевого трафика.

Недостатками же этого принципа являются ограничения размера разбиения трафика, что связано с ограниченностью размера «маркерного ведра», а также ограничения трафика осуществляются с определенной фиксированной скоростью маркирования.

2.3. Организация очередей

При организации очередей передача трафика осуществляется на основе приоритезации трафика по определенным критериям. В этом случае сначала передают трафики с более высоким приоритетом, а трафики с низким приоритетом ожидают в очереди. Поэтому очереди должны иметь достаточно оптимальную длину, чтобы чувствительные к времени приложения не имели задержку.

Организация очередей осуществляется на основе различных методов [6], таких как очереди по принципу «первым вошел, первым вышел» (First-In First-Out, FIFO), приоритетная организация очередей (Priority Queueing, PQ), справедливая организация очередей (Fair Queueing, FQ,), стохастическая организация справедливых очередей (Stochastic Fairness Queueing, SFQ), выборочная организация очередей (Custom Queueing, CQ), взвешенная справедливая организация очередей (Weighted Fair Queueing, WFQ) и организация очередей на основе классов (Class Based Queuing, CBQ).

FIFO-очередь является одним из самых простых и традиционных методов организации очереди при передаче трафика. В этом методе пакеты передаются в порядке их поступления в систему, то есть первый поступающий пакет передается первым. Недостатком этого метода является то, что когда очередь заполняется пакетами, последующие пакеты отбрасываются, так как системы FIFO имеют только одну очередь.

Приоритетная организация очередей является одним из первых методов организации очередей. В этом методе определение приоритетов трафиков основывается на использовании списка контроля доступа (Access Control List, ACL). Метод имеет четыре типа очередей: высокий, средний, нормальный и низкий приоритеты. При этом обслуживание пакетов осуществляется от высокого приоритета к низкому, то есть первыми обслуживаются пакеты с высоким приоритетом и так далее. Пока все пакеты с наивысшим приоритетом не будут обслужены, пакеты с низким приоритетом будут ожидать в очереди. Основной недостаток этого метода заключается в том, что если потоки трафика с высоким приоритетом будут поступать постоянно, то пакеты в очередях с низкими приоритетами никогда не будут обслуживаться и в результате из-за тайм-аутов произойдет потеря пакетов в очередях с низким приоритетом.

Справедливая организация очередей является модификацией метода приоритетной организации очередей, в котором всем очередям выделяется определенная пропускная способность. Это позволяет при большом потоке трафика исключить проблемы с недостатком пропускной способности, что имеет место в методе приоритетной организации очередей. Недостатком этого метода является использование больших системных ресурсов, чем в методе приоритетной организации очередей.

Стохастическая организация справедливых очередей является модификацией метода справедливой организации очередей. В этом методе к множеству FIFO- очередей, организованных для множества потоков пакетов, динамически назначается по одной очереди, и эти очереди обслуживаются циклически. Достоинством этого метода является то, что исключается доминирование одного потока трафика над другим по использованию пропускной способности и используются малые системные ресурсы.

В методе выборочной организации очередей для обработки трафика используется до 17 очередей, причем одна из очередей резервируется для системных трафиков. При

этом выбор трафика происходит так же, как в методе приоритетной организации очередей и из каждой очереди пакеты отправляются циклически. Причем циклический сдвиг к следующей очереди происходит в том случае, если объем трафика, выходящего из текущей очереди, превышает определенное пороговое значение. Однако, если в очереди имеются много пакетов, объем которых превышает порог циклического сдвига, то объем трафика выходящего из очереди может превысить этот порог, но в следующем цикле очередь будет оштрафована на это значение превышения.

Преимуществом этого метода является то, что он может быть использован для относительно справедливого и точного разделения доступной полосы пропускания сети между трафиками. Причем если выделяемая для очереди пропускная способность не используется ею, то она распределяется между остальными очередями.

Взвешенная, справедливая организация очередей обеспечивает автоматизированную классификацию потоков трафиков и справедливо разделяет полосу пропускания сети между множеством потоков. При этом в качестве весов для пакетов входящих потоков трафиков используется время их поступления, и по этим весам они сортируются для дальнейшей их передачи. Кроме этого в методе взвешенной, справедливой организации очередей в качестве весов также используется поле TOS (Type of Service), имеющееся в заголовке протокола IPv4, чтобы определить пару адресов источник/назначение потока. Назначенные веса позволяют управлять потоками трафиков, то есть уменьшить или увеличить их объем в зависимости от приоритета.

Метод организации очередей на основе классов был создан для того, чтобы решить проблему нехватки ресурса при использовании метода с приоритетной организацией очередей. Для этого в каждом из четырех типов очередей определяются по четыре очереди и каждой очереди присваивается приоритет. При этом очереди обслуживаются циклическим образом, а также может быть определен объем трафика, исходящего из каждой очереди, что повышает справедливость метода с приоритетной организацией очередей. Также для определения приоритетов метод позволяет использовать поле TOS-заголовка протокола IPv4. Однако недостатком этого метода является то, что в отличие от метода с приоритетной организацией очередей он не предоставляет строгие приоритеты потокам трафиков реального времени.

2.4. Ограничения сервисов

Известно, что традиционно некоторые приложения и сетевые услуги, такие как FTP, HTTP и NNTP, потребляют большую пропускную способность. Кроме того, также известно, что P2P приложения потребляют больше пропускной способности, чем Web-трафик. Поэтому эффективным подходом к управлению пропускной способностью сети являются ограничения сервисов, используемых в сети. Это, в основном, достигается путем управления потреблением сетевых ресурсов приложениями и сетевыми услугами. Обычно управление пропускной способностью сети осуществляется двумя путями: фильтрацией и приоритезацией трафиков.

При фильтрации трафика на уровне маршрутизаторов и межсетевых экранов на основе определенных правил фильтруются соответствующие приложениям и сетевым услугам порты/IP адреса и принимаются решения об ограничении или запрещении трафиков тех или иных приложений или сетевых услуг.

При приоритезации трафиков сначала устанавливаются правила сопоставления трафиков, и использующие большую пропускную способность трафики могут быть ограничены в определенных пределах с использованием методов приоритезации трафиков.

В работе [7] предложен метод управления полосой пропускания для поддержки дифференцированных сервисов в MPLS-сетях. При этом для управления полосой пропускания авторами используются два механизма – механизмы распределения пропускной способности и приоритетное прерывание обслуживания, в которых управление осуществляется на основе классов и приоритетов.

2.5. Активный контроль контента

В качестве метода управления пропускной способностью КС может быть использовано активное ограничение, манипуляция и управление содержанием поступающих в сеть контентов, которые используют большую пропускную способность [8]. Так как, по сравнению с типичными статическими страницами, которые имели только текст и изображения, сегодня Web имеет очень большой объем контента и сервисов.

Суть метода активного управления контентом заключается в том, что в целях управления пропускной способностью, в основном во время наибольшего спроса к пропускной способности, ограничиваются так называемые «некритические» контенты. В основном это может быть достигнуто активной фильтрацией контента трафика, например, чтобы сэкономить трафик, с помощью активной фильтрации контента трафика можно заблокировать рекламные баннеры имеющиеся на Web-страницах, а также другие «некритическit» контенты.

Активный контроль контента в основном может быть осуществлен на уровне приложений/протоколов и с помощью прокси-серверов, причем наиболее часто это реализуется на уровне HTTP-протокола.

2.6. Пороговое управление

Пороговое управление – это процесс реагирования на превышения заранее установленных пороговых значений использования пропускной способности. В основе этого метода лежит принцип, который заключается в осуществлении определенных политик управления пропускной способностью при превышении установленных пороговых значений. Эти политики управления выполняются до тех пор, пока уровень использования пропускной способности не станет ниже установленных пороговых значений. При этом мониторинг количества, продолжительности и частоты превышения пороговых значений пропускной способности может быть использован для получения профиля сети по использованию пропускной способности. Это позволит точно выбрать соответствующую политику управления пропускной способностью сети.

Кроме этого метод порогового управления пропускной способностью при необходимости может выделить дополнительную пропускную способность тем или иным приложениям или пользователям. При этом если основной канал связи сети загружен, то система для динамического выделения дополнительной пропускной способности предоставляет канал связи по требованию. А также конфигурация маршрутизации может быть изменена динамически, чтобы обеспечить передачу только определенных трафиков, и этот метод поддерживается большинством современных маршрутизаторов.

На основе различных средств могут быть построены системы для определения превышения заранее установленных пороговых значений пропускной способности. Например, используя SNMP [9] и RMON [10], можно построить систему, которая позволит динамически реагировать на перегрузки каналов связи и стабилизировать производительность сети. Это может быть достигнуто путем приоритезации трафика или ограничения определенных сервисов, пока уровень трафика не упадет ниже заранее установленного порога.

2.7. Кэширование прокси-серверов

Кэширование прокси-серверов может быть использовано для управления пропускной способностью КС. Так как принужденное использование прокси-серверов при доступе хостов в Интернет позволит администраторам осуществлять мониторинг и управлять трафиком, проходящим через прокси-серверы.

Как правило, кэширующие прокси-серверы устанавливаются на границах сетей, так, чтобы трафики внутренних пользователей проходили через них. Основной целью использования кэширования прокси-серверов в КС является доставление контента близко к пользователям, чтобы сэкономить пропускную способность и снизить время отклика. Как известно, кэширование прокси-серверов основывается на хранении информации с тем предположением, что большое количество различных пользователей часто обращаются в Интернет за поиском информации с одним и тем же содержанием. Таким образом, если часто запрашиваемая пользователями информация хранится локально в прокси-сервере, то при последующих обращениях эта информация может быть выдана непосредственно из кэша. В результате снижается объем трафика и повышается эффективность использования текущей доступной пропускной способности сети.

Кэширование прокси-серверов работает следующим образом [11]. Кэш прокси-сервер перехватывает HTTP-запросы от пользователей, и если запрашиваемые клиентами объекты имеются в кэше, то он выдает объект пользователям непосредственно из кэша. А если объект не найден в кэше, то прокси-сервер от имени пользователя запрашивает объект из исходного сервера и выдает пользователям, а объект размещается в кэше.

Преимуществом этого метода является то, что прокси-серверы, с использованием алгоритмов замены кэша, могут адаптировать кэширование контента к различным схемам доступа. Однако прокси-серверы не очень хорошо масштабируются для обслуживания больших объемов данных и количества пользователей.

Некоторые виды кэширования прокси-серверов существуют в виде расширений или опций серверов HTTP, таких как общедоступные серверы Apache [12] и Jigsaw [13]. Прокси также доступны в виде автономных систем, таких как общедоступные Squid [14] и коммерческие CacheFlow [15], Cisco Cache Engine [16], а также серверы Microsoft Proxy [17].

2.8. Сжатие данных

Использование методов сжатия данных может привести к заметному росту в производительности сетевых соединений. При этом основным препятствием для реализации этого метода является то, что сжатие является двусторонним процессом и должно быть поддержано в обоих концах соединения.

Одним из простейших методов реализации сжатия данных является сжатие данных на транспортном уровне модели OSI (Open Systems Interconnection), например, сжатие данных при модемном подключении к Интернету происходит на транспортном уровне модели OSI, для которой используется протокол PPP (Point-to-Point Protocol). При этом сжатие данных остается прозрачным для протоколов и приложений более высоких уровней модели OSI.

Однако на более высоких уровнях модели OSI, например на уровне приложений, сжатие данных может стать более сложным. Но, тем не менее, большинство существующих сегодня приложений поддерживает сжатие данных, например, существующие веб-браузеры в основном поддерживают сжатие данных. При этом для уменьшения HTTP-трафика сжатие осуществляется на основе HTTP-спецификаций [18, 19], и экономия полосы пропускания достигается за счет повышения нагрузки

процессора Web-сервера. Однако большинство Web-серверов в состоянии должным образом справляться с этой ситуацией.

Другим подходом к экономии полосы пропускания является использование прокси-серверов на обоих концах сетевого соединения. При этом с помощью специальных протоколов, например, протоколов IPsec, SSH (Secure Shell), L2TP (Layer 2 Tunneling Protocol), Socks [20, 21], между двумя прокси-серверами устанавливается сжатый (или зашифрованный) туннель. Туннель работает следующим образом: сначала клиенты отправляют запросы к локальному прокси-серверу, а локальный прокси-сервер передает эти запросы по туннелю на удаленный прокси-сервер, который находит запрашиваемые веб-страницы и, сжимая, передает их локальному прокси-серверу, а локальный прокси-сервер, в свою очередь, передает эти Web-страницы Web-браузерам клиентов, запрашивающих эти Web-страницы. Основным преимуществом этого подхода является то, что сжатая информация использует меньше пропускной способности.

А также существенно может быть снижено использование пропускной способности путем сжатия вложений сообщений электронной почты, таких как текстовые документы, картинки и т.д. Для этого могут быть использованы такие утилиты сжатия информации, как WinZip и WinRaR.

2.9. Трансляция сетевых адресов

Трансляция сетевых адресов NAT (Network Address Translation) может быть полезной для управления использованием пропускной способности сети конечными пользователями. Обычно NAT реализуется на межсетевых экранах или маршрутизаторах. Причем большинство современных межсетевых экранов и маршрутизаторов поддерживает NAT.

Суть NAT заключается в том, что хосты внутреннего сегмента имеют адреса, указанные в RFC1918 [22], которые не маршрутизируются в Интернете, то есть в Интернете маршрутизируется только адрес межсетевого экрана или маршрутизатора, обеспечивающий доступ внутренних хостов к Интернету. Поэтому при передаче данных между хостами Интернета и внутренними хостами трансляция адресов происходит в межсетевом экране или маршрутизаторе.

Преимуществом этого метода является то, что он позволяет централизованно осуществлять мониторинг, а также приоритезировать трафики. Это возможно из-за того, что при доступе в Интернет внутренние хосты используют межсетевой экран или маршрутизатор.

Заключение

Несмотря на то, что имеется множество методов управления пропускной способностью, которые позволяют реализовывать различные эффективные политики, управление пропускной способностью КС остается сложной задачей. Потому, что управление пропускной способностью состоит не только в непосредственном контроле использования сетевых ресурсов, но также включает в себя процесс разработки сетей и сетевых ресурсов для того, чтобы обеспечить оптимальное предоставление сетевых услуг. Кроме этого для управления пропускной способностью КС очень важным является создание концептуальной структуры для использования методов управления пропускной способностью.

Эта работа может быть полезна для разработчиков и исследователей сетей и может помочь сетевым администраторам выбрать соответствующие методы для оптимального предоставления пользователям сетевых ресурсов и услуг.

Литература

1. Basher N., Mahanti A., Mahanti A., Williamson C., and Arlitt M., A comparative analysis of web and peer-to-peer traffic / Proc. of the 17th international conference on World Wide Web. ACM, 2008, pp. 287–296.
2. Prasad R., Dovrolis C., Murray M., and Claffy K., Bandwidth estimation: metrics, measure ment techniques, and tools // Network, IEEE, 2003, Vol. 17, No. 6, pp. 27–35.
3. Rodrigues P., Snehalatha N., Angeline Julia S., Lenin N., Bandwidth management techniques / I nternational Conference on Computing and Control Engineering (ICCCE 2012), 12 - 13 April, 2012.
4. Kalyanasundaram S., Chong E.K.P., Shroff N.B., Optimal resource allocation in multi-class net works with user-specified utility functions // Computer Networks No 38, 2002.
5. Lin T-C., Sun Y. S., Chang S-C., Chu S-I., Chou Y-T., Li M-W., Management of abusive andun fair Internet access by quota-based priority control // Computer Networks 44 (2004), pp. 441–46 2.
6. Szigeti T. and Hattingh C., End-to-end QoS Network Design: Quality of service in LANs, WANs, and VPNs: Indianapolis, Cisco Press, 2005, 768 p.
7. Shan T., and Yang O. W. W., Bandwidth Management for Supporting Differentiated-Service-A ware Traffic Engineering // IEEE Transactions on Parallel and Distributed Systems, Vol. 18, No. 9, 2007, pp. 1320–1331.
8. Web Content Filtering and Bandwidth Management. http://cipafilter.com/doc/Content%20Fi ltering.pdf
9. RFC 1157 - Simple Network Management Protocol (SNMP) Available at http://ip-doc.com/rfc/rfc1157
10. Waldbusser S., Remote network monitoring management information base. RFC2819/STD0 059, Available at http://www.rfc-editor.org/std/std59.txt
11. Barish G. and Obraczka K., World Wide Web caching: trends and techniques, Communicati ons Magazine, IEEE, Vol. 38, No: 5, 2000, pp. 178–184.
12. Apache Group. Apache HTTP server documentation. Available at http://www.apache.org/
13. World Wide Web Consortium. Jigsaw HTTP server documentation. Available at http://www.w3c.org/Jigsaw/
14. Wessels D., Squid Internet object cache documentation. http://squid.nlanr.net
15. CacheFlow Inc. CacheFlow products web page. http://www.cacheflow.com/products/
16. Cisco Systems, Inc. Cisco cache engine. http://www.cisco.com/web/learning/index.html
17. Microsoft Corporation. Microsoft Proxy Server. Available at http://www.microsoft.com
18. Bernerslee T., Fielding R., and Frystyk H. RFC1945: Hypertext Transport Protocol HTTP/1. 0. Internet RFC, May 1996.
19. Fielding R., Gettys J., Mogul J., Frystyk H., Masinter L., Leach P., and Bernerslee T. RFC2 616: Hypertext Transport Protocol HTTP/1.1. Internet RFC, June 1999.
20. http://ux.brookdalecc.edu/fac/engtech/mqaissaunee/netw125/student%20presentations/SSH %20Tunneling.pdf
21. www.ozeki.hu/attachments/590/ipsec.pdf
22. Rekhter Y., Moskowitz B., Karrenberg D., De Groot, G., and Lear E. RFC1918/BCP5: Address Allocation for Private Internets. Internet RFC, Feb. 1996.

UOT 004.042
Şıxəliyev Ramiz H.
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
ramiz@science.az

Kompüter şəbəkələrinin buraxma qabiliyyətinin idarə edilməsi üsulları haqqında

Məqalədə kompüter şəbəkələrinin (KŞ) buraxma qabiliyyətinin idarə edilməsinin müxtəlif üsulları, o cümlədən kvota sistemi, trafikin prioritetləşdirilməsi, növbələrin təşkili, xidmətlərin məhdudlaşdırılması, kontentin aktiv idarə edilməsi, həddə görə idarəetmə, proksi-serverlərin keşləşdirilməsi, verilənlərin sıxılması, şəbəkə ünvanlarının translyasiyası analiz olunmuşdur və onların üstünlükləri və çatışmazlıqları, həmçinin KŞ trafikinin idarə edilməsi üçün istifadəsi imkanları müəyyən edilmişdir.
***Açar sözləri**: buraxma qabiliyyəti, buraxma qabiliyyətinin idarə edilməsi, kvota sistemi, trafikin prioritetləşdirilməsi, xidmətlərin məhdudlaşdırılması, kontentin idarə edilməsi, həddə görə idarəetmə.*

Ramiz H. Shikhaliyev
Institute of Information Technology of ANAS, Baku, Azerbaijan
ramiz@science.az

Methods of bandwidth management in computer networks

The paper analyzes various methods of bandwidth management of computer networks (CN), such as a quota system, traffic prioritization, queuing, limited service, active content management, threshold control, proxy caching, data compression, network address translation, and determines their advantages and disadvantages, as well as the possibility of their use in the CN traffic management.
***Key words:** bandwidth, bandwidth management, quota systems, traffic shaping, limitation of service, active content control, threshold management.*