УДК 371.687:621.3.037.37

П.А. Дунаев, С.Ю. Рябцунов, М.А. Шукралиев

Сравнительный анализ конфигураций маршрутизатора, влияющих на изменение полосы пропускания сигнала

Рассмотрено влияние протоколов маршрутизации и алгоритмов безопасности на изменение полосы пропускания трафика. При моделировании сети применен комплекс программного обеспечения для проведения полной симуляции изменения сигнала от агрегационного оборудования сервис-провайдера. Смоделирована передача трафика при использовании возможных протоколов маршрутизации в настройках активного сетевого оборудования.

Ключевые слова: полоса пропускания, трафик, конфигурация оборудования, маршрутизатор.
doi: 10.21293/1818-0442-2016-19-1-40-45

При построении проводной IP-сети для передачи видеосигнала по ней возникает ряд вопросов, существенно влияющих на качество изображения у конечного пользователя. Изменение настроек программы маршрутизатора (конфигурация) приводит к изменению полосы пропускания сигнала в зависимости от используемых протоколов маршрутизации [1]. Поскольку каждый клиент за свои деньги желает видеть качественный сигнал, актуальность исследования, приведенного в статье, не вызывает сомнений.

Определение задачи и инструментов моделирования

При передаче данных по сетям связи присутствует множество проблем, влияющих на качество принимаемого сигнала. Некачественная передача таких услуг, как голос, передача данных и HD-видео, занижает так называемый механизм гарантированного качества QoE (Quality of Experience, восприятие качества) и QoS (Quality of Servise, качество обслуживания). Изменение полосы пропускания трафика на программном уровне также негативно сказывается на качестве принимаемого сигнала.

Скорость передачи сигнала, мощность в оптическом канале – параметры, зависящие от технологии подключения абонента к сети (xDSL, PON) и влияющие на качество принимаемого сигнала [2, 3]. Рассмотрим, какую долю вносят в изменение полосы пропускания и средней скорости передачи сигнала элементарные алгоритмы безопасности и протоколы маршрутизации при обработке трафика на уровне его маршрутизации у ISP (Internet Service Provider).

За основу исследования примем типовую схему подключения пользователя к сети Интернет – провайдера [1]. В зависимости от используемого протокола маршрутизации полоса пропускания будет меняться, в настоящее время наиболее часто применяемыми протоколами являются:

– ICMP (Internet Control Message Protocol – протокол межсетевых управляющих сообщений);

– OSPF (Open Shortest Path First – протокол динамической маршрутизации);

– BGP (Border Gateway Protocol – основной протокол динамической маршрутизации);

– ACL (Access Control List – список контроля доступа);

– IPsec (IP security – протокол защищенного канала);

– протокол приоритета трафика.

Скорость сигнала, передаваемого пользователю от провайдера, по свой трассе прохождения изменяется в зависимости от используемого протокола маршрутизации. Трассу условно можно разбить на три логические зоны:

1) зона агрегации – в данном сегменте сети находится агрегирующее оборудование сервис-провайдера;

2) зона передачи или транспортный уровень – на этом участке происходит обработка, кодирование и перекодирование сигналов из одного стандарта в другой. Параметры данного участка в расчет изменений сигнала не учитываются, так как целью исследования является непосредственно конфигурация маршрутизатора сервис-провайдера;

3) зона абонентского доступа – в данном сегменте представлены конечные пользователи, клиенты абонентской сети провайдера (компьютеры, ноутбуки, мобильные телефоны).

Изучение свойств ослабления сигнала на трассе между пользователем и провайдером возможно с помощью модельного эксперимента, что проще и дешевле разработки соответствующих устройств. С помощью модели появляется возможность детального изучения изменения скорости сигнала.

Описание прикладных программ для моделирования

В процессе моделирования задействовано два программных продукта симуляции:

1) Router GNS3 – эмулирует реальное сетевое оборудование в сети от ISP до пользователя [4];

2) LAN Traffic v.2 – эмулирует оконечное оборудование [5].

Программа LAN Traffic v.2 фиксирует изменения трафика, сгенерированного программой Router GNS3.

Для GNS3 в качестве агрегирующего маршрутизатора выберем IOS, принадлежащий к семейству стекового агрегирующего оборудования: cisco7200-

advsecurityk9-mz.124-11.T.bin. Данная операционная система поддерживает расширенные возможности безопасности (Security Agreement), голосовой функционал (Cisco Voice CME) и маршрутизацию граничных шлюзов (BGP Routing).

Исследование влияния протокола маршрутизации ICMP на изменение полосы пропускания

Согласно логике обмена сигналами в IP сети передается стандартный эхо-запрос. При проведении моделирования маршрутизатор находился в стековом состоянии (протокол маршрутизации ICMP), настроенный отсылать весь трафик на маршрутизатор в базовой станции.

Полоса пропускания трафика в стековом состоянии маршрутизатора представлена на рис. 1.

Как видно из графика (см. рис. 1), при протоколе ICMP сигнал колеблется в диапазоне от 60 до 100 Мб/с.

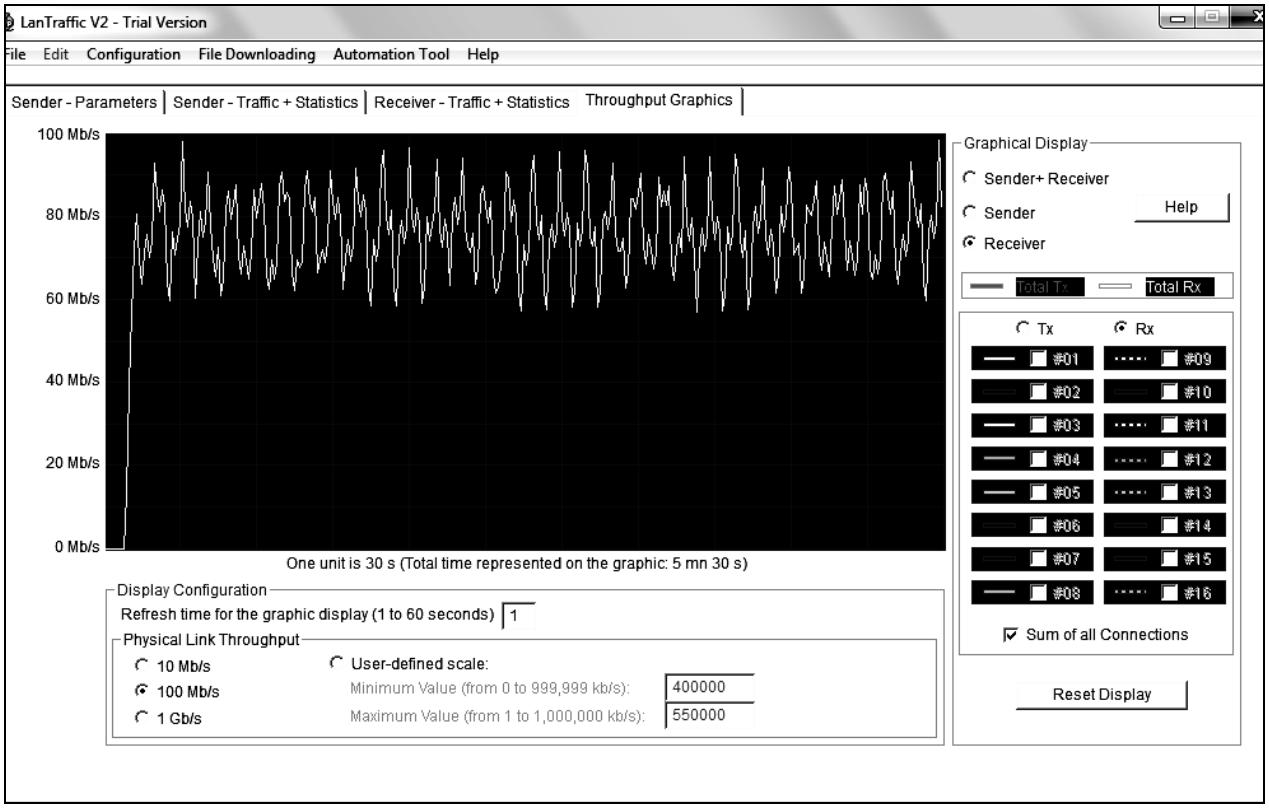

Рис. 1. Изменения скорости сигнала в течение 5 мин 30 с при настройке маршрутизатора по протоколу ICMP

Скорости передачи абонентов являются дискретными и случайными величинами, принимающими значения $b_1^{(k)} = B_p^{(k)}$ с вероятностью $p^{(k)}$ и $b_2^{(k)} = B_{\min}^{(k)}$ с вероятностью $q^{(k)} = 1 - p^{(k)}$, где k – один из вариантов обработки трафика (голос, видео, данные). Тогда плотность распределения скоростей передачи абонентов k-й службы может быть выражена как сумма дельта-функций [6]:

$$f(b^{(k)}) = p^{(k)}\delta(b^{(k)} - B_p^{(k)}) + q^{(k)}\delta(b^{(k)} - B_{\min}^{(k)}), \quad (1)$$

первый начальный момент скоростей передачи имеет вид

$$\beta_1^{(k)} = \int_0^{\infty} b^{(k)}\left[p^{(k)}\delta\left(b^{(k)} - B_p^{(k)}\right) + q^{(k)} + \delta\left(b^{(k)} - B_{\min}^{(k)}\right)\right]db^{(k)} =$$

$$= p^{(k)}B_p^{(k)} + q^{(k)}B_{\min}^{(k)}, \quad (2)$$

где $B_p^{(k)}$ – максимальная (пиковая) битовая скорость передачи абонентов k-й службы; $B_{\min}^{(k)}$ – минимальная битовая скорость передачи абонентов k-й службы.

Соответственно первый начальный момент случайной величины $\beta_1^{(k)}$ характеризует значение средней битовой скорости передачи $B_{\text{mid}}^{(k)}$ [6].

Зададимся вероятностью безотказной работы маршрутизатора $p^{(k)} = 0{,}995$, тогда согласно выражению (2) первый начальный момент, характеризующий среднюю скорость передачи трафика при настройке маршрутизатора по протоколу ICMP, составляет:

$$B_{\text{mid}}^{(k)} = \beta_1{}^{(k)} = 99{,}5 \cdot 100 + (1 - 0{,}995) \cdot 60 = 99{,}8 \text{ Мб/с}.$$

Исследование влияния протокола маршрутизации OSPF на изменение полосы пропускания

Произведем расчет средней пропускной способности трафика при использовании протокола маршрутизации OSPF. OSPF является наиболее распространенным протоколом маршрутизации в сетях сервис-провайдера [7].

Для качественного понимания процесса передачи сигнала при использовании таблиц маршрути-

зации достаточно добавить в схему еще два маршрутизатора Cisco 7200 [7].

Пустим стандартный эхо-запрос на LAN Traffic v.2 и снимем результаты вывода изменения трафика.

При использовании OSPF изменение сигнала осуществляется в диапазоне от 50 до 100 МБ/с. Тем не менее заметны «проседания» трафика через каждые 30 с. Подобное поведение трафика можно охарактеризовать постоянно повторяющимся процессом обмена таблицами маршрутизации между устройствами ядра сети.

Каждый подобный обмен требует не только определенного количества вычислительных ресурсов оборудования, но и определенной полосы пропускания для обмена данными по таблицам маршрутизации. Как известно, данный протокол основывается на технологиях отслеживания состояния каналов, что подразумевает под собой определенное резервирование полосы пропускания для обмена сигнальной информацией. Подобные манипуляции создают большую нагрузку на процессоры маршрутизаторов, вынужденных обрабатывать и отслеживать любое изменение сигнала в сети. Согласно (2) определим среднюю скорость передачи трафика при настройке маршрутизатора по протоколу OSPF:

$$B_{\text{mid}}^{(k)} = \beta_1{}^{(k)} = 99{,}75 \text{ Мб/с}.$$

Отметим, что $B_{\text{mid}}^{(k)}$, рассчитанное для протокола ICMP, незначительно отличается от значения $B_{\text{mid}}^{(k)}$ для протокола OSPF.

Исследование влияния протокола маршрутизации BGP на изменение полосы пропускания

Протокол BGP является основным в сети Internet [8]. Данный протокол предназначен для обмена маршрутной информацией о подсетях между автономными системами (АС), таким образом, группы маршрутизаторов в едином управляемом домене используются протоколом внутри доменной маршрутизации для согласования маршрутов внутри автономных систем и протоколами междоменной маршрутизации для согласования маршрутов передачи пакетов в другие автономные системы. Пересылаемая информация содержит в себе список автономных систем, к которым имеется подключение, через целевую систему. Поиск наилучших маршрутов выполняется по правилам, установленным в сети.

BGP поддерживает бесклассовую IP-адресацию и способен использовать суммирование маршрутов для оптимизации таблиц маршрутизации. На данный момент эксплуатируется четвёртая версия протокола. BGP, как и DNS, является одним из ключевых механизмов, координирующих маршрутизацию трафика в Internet.

BGP работает на прикладном уровне модели OSI и функционирует поверх протокола TCP 4-го уровня. После конвергирования соединения происходит обмен информацией обо всех маршрутах, включенных в домен автономной системы и предназначенных для обмена между этими системами. Впоследствии транслируется только информация об изменениях маршрутов в таблицах маршрутизации. При разрыве соединения удаляются все маршруты.

Рассмотрим процесс передачи сигнала для протокола BGP. Часть конфигурации по BGP позаимствуем с работающего и эксплуатируемого маршрутизатора Cisco 7200, установленного на площадке провайдера ТОО «ЭЛИТКОМ».

Снимем результаты изменения сигнала на выходе со стороны конечного пользователя.

Можно однозначно сказать, что «проседания» сигнала значительно глубже, нежели это было в OSPF маршрутизации, и ослабление достигает 10 Мб/с. Это связано с тем, что BGP обменивается не полными таблицами маршрутизации, а лишь ее частями. Пиковые значения полосы пропускания достигают 100 Мб/сек. Используя выражение (2), определим среднюю скорость передачи трафика при настройке маршрутизатора по протоколу BGP:

$$B_{\text{mid}}^{(k)} = \beta_1{}^{(k)} = 99{,}55 \text{ Мб/с}.$$

Отметим, что $B_{\text{mid}}^{(k)}$, рассчитанное для протокола BGP, отличается от значения $B_{\text{mid}}^{(k)}$ для протокола ICMP и протокола OSPF в меньшую сторону.

Исследование влияния списка контроля доступа ACL на изменение полосы пропускания

ACL – набор правил, которые определяют, кто, куда и как может получать доступ. В конкретном случае это является объект, находящийся в конкретном участке сети или системы.

Access Control List является основой систем безопасности в любых системах. Для данного вида безопасности характерен подход разборчивости к входящим и исходящим соединениям, пытающимся получить доступ к определенным ресурсам или участкам в сети. При создании ACL используется принцип избирательного управления доступом [9].

Этим набором правил ограничим доступ к сети соединениям, не являющимся доверенными для данного участка сети, пропишем правила безопасности для будущих клиентов VPN-подключений, а также опишем простой список сетей, разрешенных для трансляции.

По результатам изменения сигнала можно сказать, что списки доступа не создают серьезных помех для прохода трафика в пределах участка маршрутизатор – базовая станция – конечный пользователь. Наблюдаются определенные всплески и «проседания» в диапазоне от 40 до 100 Мб/с, что говорит об их непосредственном влиянии на сигнал.

На основании этих исследований можно сделать логический вывод: если ACL будет достаточно громоздким, содержать в себе не пару-тройку строк правил, как в нашем случае, а несколько сотен строк, то пропуск трафика в сторону конечных пользователей будет весьма затруднителен. С учетом этого можно однозначно сказать, что ACL больших размеров способен существенно воздействовать на

передаваемые данные и как следствие изменение сигнала в целом.

Используя выражение (2), определим среднюю скорость передачи трафика для ACL:

$$B_{\text{mid}}^{(k)} = \beta_1{}^{(k)} = 99{,}7 \text{ Мб/с}.$$

Отметим, что $B_{\text{mid}}^{(k)}$, рассчитанное для ACL, отличается от средних значений скорости для протоколов BGP, ICMP и OSPF.

Исследование влияния приоритезированного трафика на изменение полосы пропускания

Организовать сеть, которая однозначно пробрасывала бы весь трафик в случае полной сетевой работы всех хостов, практически нереально. Показатели пропускной способности высчитываются по некоторым усредненным значениям с учетом вида использования сети и типа проходящего трафика.

В большей части сетей малых и средних организаций пропускная способность сети задействуется менее чем на 12%, и ограничения в трансляции данных из-за нехватки полосы пропускания, как правило, невозможны или их вероятность крайне мала. Однако не все линии связи имеют подобный запас по полосе пропускания. С увеличением активности использования сетевых ресурсов вероятность закономерной перегрузки сети экспоненциально растет.

В общем случае сама сеть в принципе не гарантирует целостность доставки данных. В случае когда пакет с данными не способен пройти по сети, он уничтожается и пропадает. Подавляющее число приложений адекватно обрабатывает факты утери части пересылаемых данных и передает их вторично. Тем не менее существуют задачи, для которых любая потеря единицы информации крайне критична. К примеру, при передаче видео подобные обстоятельства приведут к возникновению искажений. В таком случае можно разрешить проблему, если обеспечить передаче видео более приоритетные условия, чем, к примеру, протоколу почты и онлайн-сообщений.

Проблемы с приоритезацией трафика разрешаются путем присвоения пересылаемым по сети единицам информации определенного уровня обслуживания и организации для них определенного качества обслуживания [10]. В целом данная проблема является весьма сложной и разрешается различными путями для LAN- и WAN-сетей.

Пропишем в настройках маршрутизатора стандартизированные моменты по приоритезации трафика для передачи данных [1, 10].

Данная конфигурация позволит маршрутизатору терминировать трафик на себе и адекватно его обрабатывать.

По результатам изменения сигнала можно сказать, что трафик ввиду своего приоритета обрабатывается гораздо меньше, чем если бы это были просто данные как единицы информации. Наблюдается характерное для данного вида трафика задержка, вызванная буферами обработки маршрутизатора, который занимается раскладыванием и фильтрацией входящего трафика на приоритетные составляющее.

Колебание полосы пропускания для этого типа трафика составляет 10–40 Мб/с.

Средняя скорость передачи трафика с приоритетом определяется согласно выражению (2):

$$B_{\text{mid}}^{(k)} = \beta_1{}^{(k)} = 39{,}85 \text{ Мб/с}.$$

Значения средних скоростей передачи для ACL, протоколов BGP, ICMP и OSPF отличаются от тех же значений скорости передачи трафика с приоритетом в среднем на 60%.

Исследование влияния протокола защищенного канала IPsec на изменение полосы пропускания

IPsec представляет собой набор протоколов для обеспечения безопасности сетевого соединения.

Говоря о передаче шифрованного трафика, подразумевается создание VPN (Virtual Private Network) – виртуальной приватной сети. Это обобщённое название технологий, которые могут обеспечить одно или *n*-е количество защищенных сетевых соединений поверх недоверенных сетей (например, сети Internet). Соединение происходит по сетям с нулевым, т.е. неизвестным уровнем доверия, уровень доверия к организованной логической сети не зависит от уровня доверия к основным сетям благодаря осуществленным механизмам криптографических средств.

Протокол IPsec предоставляет три вида услуг: аутентификацию (AH), шифрование (ESP) и безопасную пересылку ключей. Обычно желательны обе первые услуги, так как неавторизованный клиент не сможет проникнуть в VPN, а шифрование не позволит злоумышленникам прочитать, исказить или подменить сообщения.

Как правило, VPN организовывается на уровнях не выше 3-го, так как создание криптографических средств на первых уровнях позволяет использовать в каноническом виде транспортные протоколы, что находятся на уровне 4-й принципиальной модели OSI.

Очень часто описывают VPN как одну из видов виртуальной сети – PPTP, между тем используемую не для организации приватной сетей.

Для создания виртуальной приватной сети используют инкапсуляцию протокола PPP в иной протокол, к примеру IP или Ethernet. Технология VPN в настоящее время используется не только для организации частных сетей, но и некоторыми ISP для подключения «последней мили».

При качественном уровне реализации сеть VPN может организовать высокий уровень шифрования трафика. При грамотной настройке технология VPN обеспечивает приватность в сетях общего пользования – Internet.

VPN конфигурация запускает алгоритмы шифрования на маршрутизаторе (MD5 и 3DES). Для начала производится включение в глобальном режиме. После создаются правила по пропусканию протоколов и методы их обработки. VPN-соединение всегда работает в паре, именно поэтому, после организации

подключения генерируется пара 1024-битных ключей для каждого из устройств (клиент, сервер).

Для организации шифрованного подключения создается гостевая подсеть вида x.x.x.x с маской 255.255.255.255. Таким образом, каждый пользователь, инициализирующий соединение извне, получает IP-адрес такого типа.

Оценим результат влияния VPN-шифрования на результирующий выход сигнала.

По результатам исследования видно, что сигнал ведет себя достаточно стабильно. Не наблюдается провалов и задержек. Полоса пропускания используется не на сто процентов. Диапазон колебания полосы пропускания составляет от 20 до 70 Мб/с, что совершенно не отвечает заявленным характеристикам текущей полосы пропускания сигнала (100 Мб/с).

Средняя скорость передачи трафика при использовании протокола защищенного канала IPsec также определяется по выражению (2):

$$B_{\text{mid}}^{(k)} = \beta_1{}^{(k)} = 69{,}75 \text{ Мб/с}.$$

Рассчитанное среднее значение скорости передачи для протокола IPsec отличается от тех же значений: для приоритезированного трафика примерно на 43% больше, а для ACL и протоколов BGP, ICMP, OSPF примерно на 30% меньше.

В таблице представлены зафиксированные параметры по исследованию той или иной настройки маршрутизатора.

Сравнительная таблица по результатам исследования

Тип	Диапазон полосы пропускания, Мб/с		Среднее значение полосы пропускания, Мб/с
	Min	Max	
1	2	3	4
IPsec	20	70	69,75
Приоритезация	10	40	39,85
BGP	10	100	99,55
ACL	40	100	99,7
OSPF	50	100	99,75
ICMP	60	100	99,8

Как видно из таблицы, средние значения полос пропускания сигнала для протоколов ICMP, OSPF, BGP и ACL отличаются незначительно. OSPF и BGP являются основными для определения пути прохождения сигнала между маршрутизаторами, ACL ограничивает доступ указанным адресам, ICMP применяется для диагностики и мониторинга сети. Вследствие этого поддержание пропускной способности сети невозможно без применения вышеуказанных протоколов.

IPsec отвечает за сетевую безопасность канала, следовательно, при передаче сигнала происходит выполнение функции взаимной аутентификации (например, обмен паролями), одновременная передача с сообщением его битовой последовательности, что требует дополнительных ресурсов сети, использование которых негативно сказывается на пропускной способности.

Уменьшение скорости сигнала при использовании протоколов приоритезации говорит о следующем: разным классам трафика отводится гарантированный процент от общей пропускной способности сети, но скорость сигнала может еще уменьшиться, если приход высокоприоритетного пакета совпадает по времени с началом продвижения низкоприоритетного пакета на выходной интерфейс.

Заключение

На основе проведенных исследований возможно сделать следующие выводы:

1. Конфигурация активного сетевого оборудования влияет на изменение полосы пропускания и как следствие на сигнал в целом. Профессиональная настройка оборудования, выбор оптимальных протоколов маршрутизации минимизируют потери сигнала и оптимизируют использование ресурсов канала.

2. Доказана необходимость тестирования сетевого оборудования на предмет выдерживания высоких нагрузок.

3. Необходимо вывести закономерный ряд рекомендаций по настройке и эксплуатации активного сетевого оборудования операторов связи.

4. Определена полоса пропускания канала и средняя скорость передачи трафика при использовании:

– протокола маршрутизации ICMP;
– протокола маршрутизации OSPF;
– протокола маршрутизации BGP;
– мер безопасности ACL;
– протокола защищенного канала IPsec;
– протокола приоритезации трафика.

Литература

1. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов / В.Г. Олифер, Н.А. Олифер. – 4-е изд. – СПб.: Питер, 2010. – 944 с.

2. Дунаев П.А. Экспериментальное исследование мультисервисной IP-сети с целью выявления параметров, влияющих на качество цифрового ТВ-изображения // Вестник СибГУТИ (Новосибирск). – 2013. – № 2. – С. 31–41.

3. Дунаев П.А. Метод оценки качества цифрового ТВ-изображения, передаваемого по мультисервисной сети, использующей технологию подключения GPON // Вестник СибГУТИ (Новосибирск). – 2015. – № 3. – С. 11–22.

4. Your Virtual Network in a Suitcase [Электронный ресурс]. – Режим доступа: https://www.gns3.com/software, свободный (дата обращения: 30.03.2016).

5. LanTraffic V2 [Электронный ресурс]. – Режим доступа: http://www.zti-communica-tions.com/lantrafficv2/, свободный (дата обращения: 30.03.2016).

6. Чутов О.В. Исследование параметров качества обслуживания (QoS), определяющих качество восприятия пользователем (QoE) потокового видео при передаче через Интернет // T-Comm. – 2009. – № 4. – С. 16–18.

7. Томас Т.М. Cisco. Структура и реализация сетей на основе протокола OSPF / Т.М. Томас. – М.: Вильямс, 2004. – 816 с.

8. Хелеби С. Принципы маршрутизации в Internet. / С. Хелеби, Д. Мак-Персон. – М.: Вильямс, 2001. – 448 с.

9. Технологии коммутации и маршрутизации в локальных компьютерных сетях: учеб. пособие / Е.В. Смирнова, А.В. Пролетарский и др.; под общ. ред. А.В. Проле-

тарского. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2013. – 389 с. (Сер. Компьютерные системы и сети).

10. Лапонина О.Р. Основы сетевой безопасности. Ч. 1. Межсетевые экраны: учеб. пособие / О.Р. Лапонина. – М.: Национальный открытый университет «ИНТУИТ», 2014. – 378 с. (Сер. Основы информационных технологий).

Шукралиев Мурат Аяганович
Доцент каф. эксплуатации электрооборудования
КазАТУ, к.т.н.
Тел.: 8-701-350-93-28
Эл. почта: shukraliev.kz@mail.ru

Дунаев Павел Александрович
Ст. преподаватель каф. радиотехники, электроники и телекоммуникаций
АО «Казахский агротехнический университет им. С. Сейфуллина» (КазАТУ), г. Астана
Тел.: 8-707-732-43-66
Эл. почта: dunayev.kz@mail.ru

Рябцунов Сергей Юрьевич, к.т.н.
Гл. специалист ТОО «ЭЛИТКОМ»,
Республика Казахстан, г. Астана
Тел.: 8-705-100-56-56
Эл. почта: ryabtsunov@yandex.kz

Dunayev P. A., Ryabtsunov S. Y., Shukraliev M. A.

Comparative configuration analysis for router influencing change of bandwidth of a signal

Influence of routing protocols and safety algorithms on change of a traffic bandwidth is considered. When modeling a network the software complex is applied to carry out full simulation of a signal change received from the aggregation equipment service – provider. Traffic transfer simulation using possible routing protocols in settings of the active network equipment is performed.

Keywords: bandwidth, traffic, equipment configuration, router.