Средства мониторинга и анализа сетевого трафика, используемые при измерении параметров QoS

Я.С. ЯЗЛОВЕЦКИЙ,
старший научный сотрудник
ОАО «Гипросвязь»,
yazlavetski@giprosvjaz.by

Объективная оценка качества услуг передачи данных может быть определена с помощью специальных аппаратных средств, позволяющих измерить параметры QoS. Результаты измерений параметров QoS зависят от интенсивности существующего трафика в каждом сегменте сети. Рассматривается зависимость точности измерения параметров от характеристик трафика, сравниваются преимущества и недостатки существующих средств мониторинга и анализа сетевого трафика.

Предназначена для специалистов, занимающихся измерением параметров QoS, и для всех, кто интересуется вопросами контроля сетевого трафика.

1. Определение понятия «качество обслуживания (пользователей услуг электросвязи)» (англ. – quality of service (QoS) of telecommunication service users) приводится в пункте 3.4.2 стандарта СТБ 1439 [1]: «Совокупность характеристик процесса и условий обслуживания, обеспечивающих удовлетворение установленных или предполагаемых потребностей пользователя услуг электросвязи».

Как видно, одним из ключевых критериев оценки качества услуг является удовлетворенность пользователя организацией, поставляющей услуги. Существует субъективная оценка степени удовлетворенности пользователя, основанная на его ощущениях, и объективная оценка, основанная на результатах измерения параметров QoS.

В международных стандартах договор между оператором

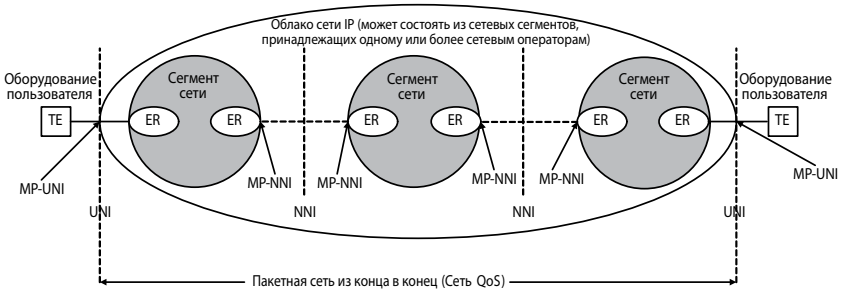

Рисунок 1 – Пакетная сеть из конца в конец
TE – оконечное оборудование; MP – точка измерений; NNI – межсетевой интерфейс; UNI – интерфейс «пользователь – сеть»

и пользователем услуги электросвязи называют Соглашением об уровне обслуживания (англ. – Service Level Agreement (SLA)) [2]. Какие параметры QoS указывать в договоре между оператором и пользователем услуги электросвязи, в основном решает оператор. Особенности выбора конкретных параметров затрагивались автором в статье [3].

Объективная оценка качества услуги может быть определена с помощью специальных аппаратных средств, позволяющих измерить параметры QoS и затем определить, для каких конкретных услуг электросвязи предназначен используемый для услуги канал передачи данных.

В Рекомендации МСЭ-Т Y.1541 определены классы QoS для различных услуг электросвязи между двумя точками интерфейсов UNI (user-network interface) в зависимости от граничных значений следующих сетевых параметров [4]:

- IPTD (Internet Protocol Packet Transfer Delay) – задержка передачи пакета IP;
- IPDV (Internet Protocol Packet Delay Variation) – изменение задержки передачи пакета IP;
- IPLR (Internet Protocol Packet Loss Ratio) – коэффициент потери пакета IP.

Пример такой сети показан на рисунке 1 [4].

Параметры классов QoS приведены в таблице 1 [4].

Результаты измерений параметров QoS зависят от интенсивности существующего трафика в каждом сегменте рассматриваемой сети. Например, в часы интенсивной работы сети, т. е. с увеличением числа соединений, в сегментах сети возрастают параметры IPTD, IPDV и IPLR. Это приводит к ухудшению качества услуг электросвязи. И наоборот, во время отсутствия интенсивной работы услуга может быть более качественной. Таким образом, при измерениях параметров QoS наряду с результатами измерений следует приводить условия, при которых они были произведены, т. е. результаты измерения трафика. Это повысит объективность и достоверность результатов измерения, что позволит сравнивать результаты измерения параметров QoS при одинаковых трафиках работы. Для непрерывного контроля следует производить измерения трафика непрерывно, через определенный период времени.

Таблица 1 [4]

Класс QoS	Использование	Сетевые параметры			Примечание
		IPTD	IPDV	IPLR	
0	VoIP (голос под IP) VNC (видеоконференция)	≤ 100 мс	≤ 50 мс	$\leq 10^{-3}$	PSTN – качество VoIP (или голосовая телефония). Реальное время, чувствительность к джиттеру, высокое взаимодействие
1	VoIP (голос под IP) VNC (видеоконференция)	≤ 400 мс	≤ 50 мс	$\leq 10^{-3}$	Спутниковая связь – качество VoIP. Реальное время, чувствительность к джиттеру, взаимодействие
2	Данные транзакций	≤ 100 мс	Н	$\leq 10^{-3}$	Сигнализация. Высокое взаимодействие
3	Данные транзакций	≤ 400 мс	Н	$\leq 10^{-3}$	Передача данных. Взаимодействие
4	Поток видео	≤ 1 с	Н	$\leq 10^{-3}$	Передача файлов видеопотока. Низкие потери
5	Традиционные приложения IP-сетей	Н	Н	Н	

Примечание. «Н» означает не установлено.

Существует методика измерения качественных характеристик на уровне IP-сетей внутри домена, изложенная в Рекомендации МСЭ-Т Y.1543 [5]. Эта рекомендация определяет ряд параметров работы IP и методы измерения, применяемые для оценки качества передачи пакета в каналах передачи. Методы предполагают многократные системы измерения, которые могут быть использованы для проведения измерений трактов отдельных сегментов и от клиента к клиенту и рекомендуют примеры конфигурации. Методы применяются для известных параметров, указанных в Рекомендации МСЭ-Т Y.1540 [6], охватывают активные и пассивные методики измерения.

Так как входящий и исходящий трафики маршрутизации могут отличаться, все измерения должны быть «односторонними». Пользователи или системные службы могут соединить статистику двух направлений, чтобы оценить работу туда и обратно.

Измерения должны проводиться для каждого из сегментов модели сети и могут быть объединены, чтобы сформировать системы показателей (metrics) для следующих сегментов сети: мультисегмент, от сайта к сайту, от

узла к узлу или от IP-терминала к IP-терминалу. Подмножество этих систем показателей должно использоваться в сообщениях для предлагаемого обслуживания.

Интервал измерений задан равным 5 минутам [5].

Однако некоторые требования, касающиеся условий и результатов измерений, в настоящее время не сформированы. В первую очередь это относится к точности (или неопределенности) измерений. Причиной является нестабильность самого объекта измерения (каналы передачи данных сегментов). Непостоянство характеристик канала передачи может приводить к изменению класса QoS во время оказания услуги.

В общей форме точность измерения (или неопределенность измерения) состоит из двух составляющих [7]:

$$\Delta = \Delta_s + \dot{\lambda}, \qquad (1)$$

где Δ_s – абсолютная систематическая составляющая погрешности измерений;

$\dot{\lambda}$ – абсолютная случайная составляющая погрешности измерения.

Величина Δ_s зависит от характеристик средств измерения (разрешение, точность метода измерений, точность синхронизации и т. д.), значение $\dot{\lambda}$ – от характеристик самого объекта измерения. Рассматривая условия измерения показателей QoS, следует заметить, что обычно $\dot{\lambda}$ намного больше, чем Δ_s. Величину Δ_s можно оценить, так как она является постоянной, а $\dot{\lambda}$ – переменная и зависит от параметров канала соединения, изменяется с течением времени.

Таким образом, чтобы оценить погрешность (1), требуются измерения составляющей $\dot{\lambda}$. Методы измерения параметра $\dot{\lambda}$ пока не разработаны. Эта проблема уже обсуждалась автором в [8]. В этой статье затрагивалась тема оценки границ неопределенности при измерении скорости передачи данных. Но не рассматривался вопрос, каким образом и какими средствами измерений можно оценить случайную погрешность $\dot{\lambda}$. Зависимость оценки величины $\dot{\lambda}$ следует связать с результатами измерений средств мониторинга и анализа сетевого трафика.

Тогда параметр $\dot{\lambda}$ можно представить в виде следующей зависимости:

$$\Delta = f(\gamma, \text{П/Р}, L), \qquad (2)$$

где γ – интенсивность соединений (трафик) за отчетный период;

П/Р – отношение числа данных (пакетов) других соединений (П) и числа данных (пакетов) рассматриваемого соединения (Р) в канале связи;

L – средняя длина пакета данных (фреймов) на физическом уровне.

Из (2) очевидно, что при увеличении интенсивности γ, отношения П/Р и длины L возрастает абсолютная составляющая $\dot{\lambda}$. Численная оценка этой величины является темой будущей статьи.

Объективность и достоверность результатов измерения увеличится, если в сообщениях (или отчетах, протоколах) будет приведен трафик во время измерений параметров Qos. Особенно это важно при пассивных измерениях, когда фиксируют копию трафика, не вводя модификации в оригинальном трафике.

В настоящее время насчитывается не один десяток программных средств, предназначенных для мониторинга [9–11], и программ-анализаторов (снифферов) [12, 13] сетевого трафика. В данной статье приводятся характеристики доступных для пользователей средств контроля.

2. Рассмотрим простейшие программные средства для мониторинга сетевого трафика.

2.1. Программа **BMExtreme** [9], которая является продолжением или, вернее, новым названием известной программы Bandwidth Monitor. Программа отображает IP-адреса, а также LAN и UDP трафики (входящий и исходящий), проходящие через сетевой адаптер, используя программы захвата WinCap [14] и SNMP [15]. Программа BMExtreme самая простая и удобная в пользовании. Она предназначена для контроля трафика интернет-соединений (скорости передачи данных) от коммутируемого доступа до спутниковых высокоскоростных каналов передачи данных.

Окно с примером результатов анализа, отображаемое при мониторинге сетевого трафика за 1 ч и 16 мин, показано на рисунке 2.

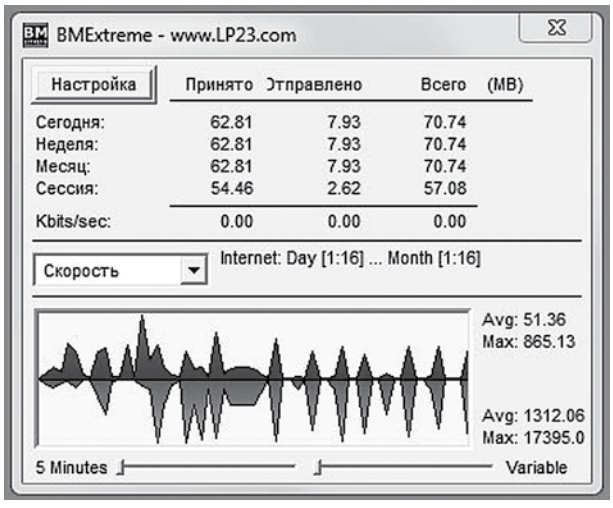

Рисунок 2 – Окно результатов мониторинга программы BVExtreme

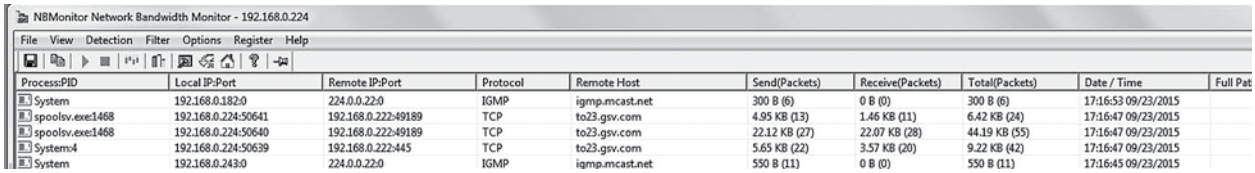

Рисунок 3 – Результаты анализа текущих соединений, произведенных программой NBMonitor

В окне результатов справа от графика скоростей отображены значения скоростей передачи данных исходящего потока, имеющего среднее значение 51,36 Кибит/с и максимальное – 865,13 Кибит/с, а внизу – входящий поток, имеющий среднее значение скорости 1312,06 Кибит/с и максимальное – 17395,0 Кибит/с.

Подробные характеристики программы BMExtreme приведены в таблице 2.

2.2. Программа «**Монитор пропускной способности сети NBMonitor**»[10].

NBMonitor контролирует и анализирует весь сетевой трафик, подсчитывает точное количество данных входящего (down) и исходящего (up) трафиков и выводит на экран статистическую информацию, имеющую отношение к каждой паре: IP-адрес и протокол. Основная цель NBMonitor состоит в том, чтобы собирать статистическую информацию о своем сетевом трафике, который проходит через сетевые адаптеры компьютера. Окно с примером результатов анализа текущей передачи данных программой NBMonitor изображено на рисунке 3.

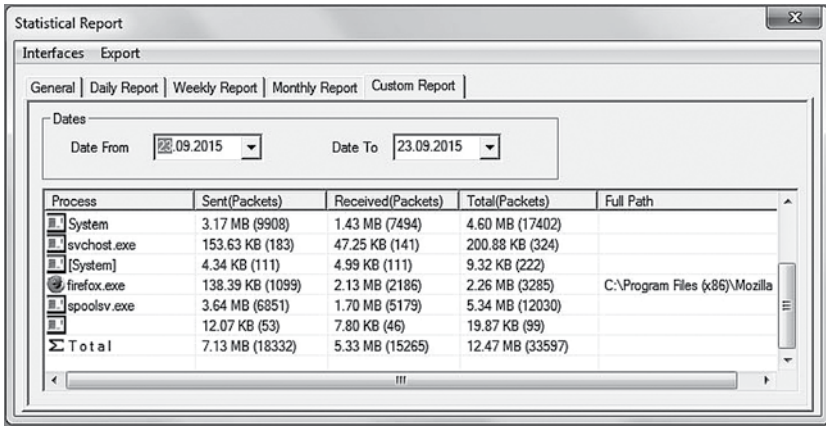

Рисунок 4 – Результат статистического отчета программы NBMonitor

Таблица 2

Наименование характеристики	Наименование программы		
	BMExtreme	NBMonitor	Ethernet Internet Statistic v1.02.404
Язык программы	14 языков, включая русский и английский	Английский	Английский или русский
Запуск мониторинга	При запуске ОС Windows	По кнопке Start	При запуске программы
Отображения IP адресов	Перечень всех IP-адресов, участвующих в обмене	Локальный и удаленный IP-адреса соединений	Нет
Расписание мониторинга	Ежечасно/ежедневно/еженедельно	Ежечасно/ежедневно/еженедельно	Текущее
Отображение накопления данных	Число принятых, отправленных и суммарно данных. В единицах: Гбайт (GB) или Мбайт (MB)	Принятые, отправленные и всего. В единицах: байтах	Получено, отправлено. В единицах: байтах
Отображение скорости передачи в виде графика	Входящего и исходящего потоков в Кибит/с	Нет	Нет
Минимальный временной шаг между отчетами	5 мин	Нет	1 с
Возможность изменения минимального шага между отчетами	От 5 мин до 12 ч	От начала нажатия кнопки Start до нажатии кнопки Stop	Нет
Отображение трафика в виде графика	Нет	Нет	Да
Возможность документирования отчетов	Форматы: .txt, .csv. C:\Users\Пользователь\AppData\Roaming\BMExtreme\Logs	Форматы: xml	Нет
Стоимость	После 14 дней пользования требует оплаты	Лицензия платная	Бесплатно

На рисунке 3 отображена для каждого соединения следующая информация: IP-адреса локального (Local IP:Port) и удаленного (Remote IP:Port) источников данных, протокол взаимодействия, название удаленного узла, число переданных, принятых и суммарно данных в байтах (в пакетах), дата и время соединения. Подробная информация нужна для текущего анализа. Кроме того, в программе есть опция для отображения статистического отчета, пример которого показан на рисунке 4.

В окне статистических результатов (рисунок 4) видно суммарное количество переданных и принятых данных за один день (23.09.2015).

Программа может контролировать в режиме реального времени соединения с интернетом через сеть ISDN, каналы xDSL, кабельный модем, модем коммутируемого доступа или VPN. С помощью программы можно избирательно контролировать сетевую активность соответствующей программы компьютера или сетевую активность выбранного удаленного узла.

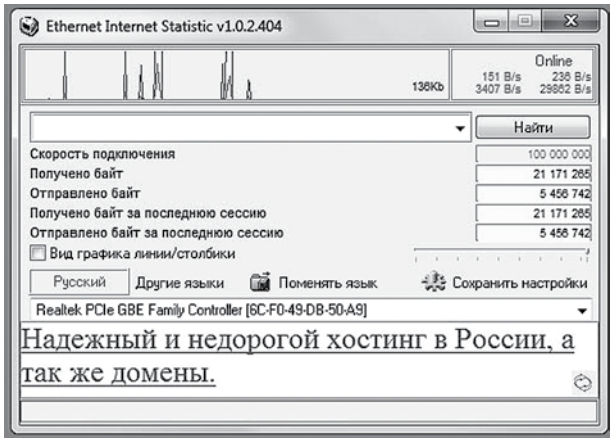

Рисунок 5 – Результаты статистического анализа программой Ethernet Internet Statistic

Конкретные характеристики программы NBMonitor отображены в таблице 2.

2.3. Существует программа **Ethernet Internet traffic Statistic (EIS)** [11], предназначенная для подсчета числа данных интернет-трафика через возможные установленные устройства с технологиями ADSL, LAN, Wi-Fi, Bluetooth.

Программа показывает количество отправленных и принятых данных (в байтах – всего и за последнюю сессию), а также скорость подключения.

Пример результатов текущего анализа для сетевого адаптера LAN модели Realtek PCI GBE Family Controller показан на рисунке 5, где изображены результаты измерения текущей скорости передачи данных (минимальное и максимальное значения) исходящего (соответственно 151 и 236 байт/с) и входящего (соответственно 3407 и 29862 байт/с) потоков. Для наглядности анализируемые данные отображаются в режиме реального времени на графике.

Подробные характеристики программы Ethernet Internet traffic Statistic отображены в таблице 2.

3. Рассмотрим характеристики программ – анализаторов сетевого трафика (снифферы). Существует множество таких программ, например Wireshark [12], Iris Network Traffic Analyzer [13], Ethernet Internet traffic Statistic, CommTraffic, Traffic Inspector, ProxyInspector и т.д. Для отображения сравнительных характеристик остановимся на двух первых.

3.1. Самая известная – это **Ethreal (Wireshark)** [12]. Она относится к программам, которые не только отображают сетевой трафик, но и производят его анализ на различные сетевые протоколы. Программное обеспечение является кроссплатформенным, то есть одинаково корректно работает под управлением различных операционных систем, включая UNIX, Linux, Mac OS, Free BSD, Solaris, Open BSD, Net BSD и

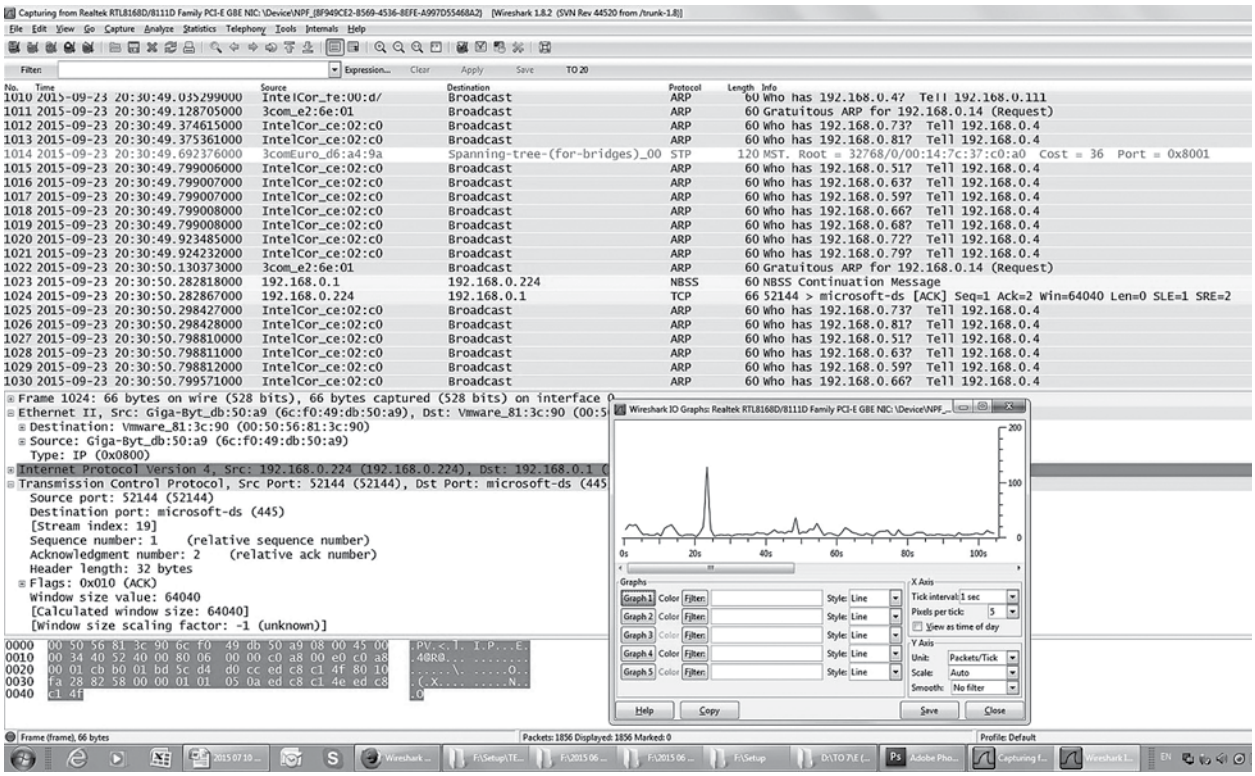

Рисунок 6 – Окно результатов захвата сетевого трафика программой Wireshark

конечно же Windows. Работает с множеством форматов входных данных. На рисунке 6 отображена картина захвата сетевого трафика.

Окно программы Wireshark (рисунок 6) имеет три области просмотра, разделенные на уровни детализации, что дает возможность фильтрации сетевых пакетов по множеству критериев, создавая при этом разнообразную статистику. Отображает значение каждого поля протокола от низкого (физического) до прикладного уровней. Отслеживание информации тем более удобно, что все представление трафика показывается в графическом режиме (рисунок 6). Также программа имеет отличные возможности в поддержке протоколов DNS, FDDI, FTP, HTTP, ICQ, IPV6, IPX, IRC, MAPI, MOUNT, NETBIOS, NFS, NNTP, POP, PPP, TCP, TELNET, X25 и т. д.

Распознавание большого числа различных протоколов делает программу универсальной, поскольку в ней изначально заложена возможность отображения информации сетевого пакета с анализом значения каждого поля протокола любых уровней. Для захвата данных используется собственный протокол программы PCAP. Также стоит отметить, что программа является абсолютно бесплатной и распространяется под свободной лицензией GNU GPL.

Программа эффективна при условии использования в сегменте именно концентраторов (hub), а не коммутаторов (switch). В противном случае метод анализа исходящего трафика малоэффективен, поскольку в программу попадают лишь отдельные пакеты физического уровня (фреймы).

Еще к недостаткам стоит отнести то, что приложение не способно обнаружить какой-либо паразитный, вирусный или закольцованный трафик, да и в системе коммутаторов программа показывает себя неэффективной.

Подробная характеристика программы Wireshark дана в таблице 3.

3.2 Программа **Iris Network Traffic Analyzer** [13] отображает как весь трафик, так и работу отдельных программ.

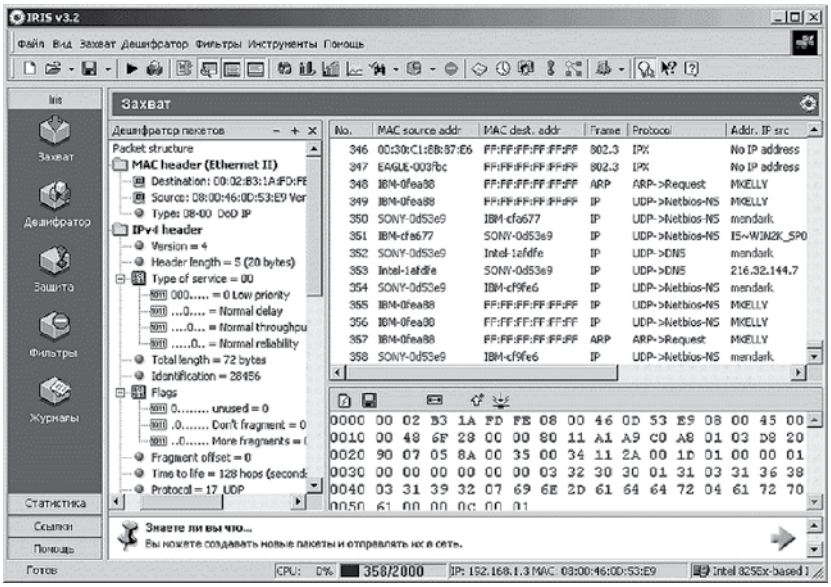

Рисунок 7 – Пример анализа сетевого трафика

Таблица 3

Наименование характеристики	Наименование программы	
	Wireshark	Iris Network Traffic Analyzer
Язык программы	Английский	Английский
Операционная система	UNIX, Linux, Mac OS, Free BSD, Solaris, Open BSD, Net BSD, Windows.	Windows
Формат экспорт/импорт отчета	.bfr, .dmp, .cap, .enc, .erf, .fdc, .libpcap, .ncf, .ntar, .pcap, pcapng, .snoop, .syc, .trc0, . trc1, txt, 5vw	Формат программы Excel Microsoft Office
Возможность изменения минимального шага между отчетами	0,001 с; 0,01 с; 0,1 с; 1 с; 1 мин; 10 мин	1 с
Отображение MAC и IP адресов	Отправителя и получателя	Отправителя и получателя
Отображение типа и операционной системы конечных адресов	Нет	Типы: Host, Router, Broadcast, Switch
Изменение MAC-адресов в журнале адресов	Нет	Название, MAC-адрес, MAC-подмена, IP-адрес
Анализ попыток подключения извне	Нет	Отображения даты и время вторжения, IP-адрес жертвы и хакера, DNS-имя и порт
Использование фильтров	Да	Да
Отображения заголовков пакетов	Заголовки: MAC, IP, ICMP, TCP, UDP	Заголовки: MAC, IP, ICMP, TCP, UDP
Результат измерения скорости передачи на физическом уровне	Среднее значение: байт/с (пакет/с). Меню: Statistics\Summary	Среднее значение: байт/с (пакет/с). MAC
Результат измерения скорости передачи протоколов взаимодействия	Среднее значение: байт/с (пакет/с). Меню: Statistics\Protocol Hierarchy	Среднее значение: байт/с (пакет/с). Только IP, IPX Меню: View\Protocol Distribution
График трафика	Меню: Statistics\IO Graph	Меню: View\Bandwidth
Отображение числа данных по конечным адресам	Меню: Statistics\Endpoints	Нет
Статистическое распределение по длине пакетов	Число; % от числа всех пакетов. Меню: Statistics\Packet Lengths	Нет
Графическое отображение соединений между конечными адресами	Меню: Statistics\Flow Graph…	Нет
Отображение всего трафика сети	Только при отсутствии коммутаторов	Да
Стоимость	Бесплатная	Лицензия платная

В программу встроен качественный анализатор для пакетов, с помощью которого можно отфильтровать, перебрать соответствующие пакеты и сформировать отчет о собранных данных. При помощи программы можно воспроизвести в деталях всю работу пользователей и просмотреть сеансы авторизации с сохраненными паролями.

Программа Iris помогает детально воспроизвести сеансы работы пользователей с различными web-ресурсами. Программа Iris обрабатывает (дешифрирует) собранные данные и предоставляет не только развернутые статистические отчеты, но и наглядную и исчерпывающую картину действий любого пользователя корпоративной сети.

На рисунке 7 показан пример анализа сетевого трафика.

Программный комплекс Iris Network Traffic Analyzer незаменим для сетевых и системных администраторов.

Подробные характеристики программы Iris Network Traffic Analyzer отображены в таблице 3.

Выводы

Приведенный анализ характеристик средств мониторинга и анализа сетевого трафика позволяет сравнить достоинства и недостатки. Системному администратору локальной сети или проектировщику сетей передачи данных полезно иметь информацию о существующих средствах контроля сетевого трафика, чтобы обеспечивать условия измерения параметров QoS, а также сравнивать результаты измерения при одинаковых трафиках сети.

ЛИТЕРАТУРА

1. Государственная система стандартизации Республики Беларусь. Услуги электросвязи. Термины и определения: СТБ 1439–2008. Введ. 01.07.09. – Минск: Госстандарт: Проектный и научно-исследовательский РУП «Гипросвязь» (УП «Гипросвязь»), 2010. – 20 с.
2. International Telecommunication Union. SERIES E: OVERALL NETWORK OPERATION TELEPHONE SERVICE, SERVICE OPERATION AND HUMAN FACTORS. Quality of telecommunication services: concepts, models, objectives and dependability planning – Use of quality of service objectives for planning of telecommunication networks. ITU-T Recommendation E.860 (06/2002): Framework of a service level agreement.
3. **Язловецкий Я.С.** Планирование повышения качества услуг электросвязи / Я.С. Язловецкий // Веснік сувязі. – 2012. – № 6. – С. 32–37.
4. International Telecommunication Union. SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS. Internet protocol aspects – Quality of service and network performance. Recommendation Y.1541 (12/2011): Network performance objectives for IP-based services.
5. International Telecommunication Union. SERIES Y: INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS. Internet protocol aspects – Quality of service and network performance. Recommendation Y.1543 (05/2007): Measurements in IP networks for inter-domain performance assessment.
6. International Telecommunication Union. SERIES Y: INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS. Internet protocol aspects – Quality of service and network performance. Recommendation Y.1540 (11/2007): Internet protocol data communication service – IP packet transfer and availability performance parameters.
7. МИ 1317–2004. Государственная система обеспечения единства измерений. Результаты измерений и характеристики погрешности измерений. Формы представления. Способы использования при испытаниях образцов продукции и контроле их параметров.
8. **Язловецкий Я.С.** Оценка границ интервала неопределенности при измерении скорости передачи данных интернет-соединения / Я.С. Язловецкий // Веснік сувязі. – 2014. – № 4. – С. 40–47.
9. Сайт, отображающий данные программы BMExtreme [Электронный ресурс]. – Режим доступа: http://www.lp23.com/bmextreme. – Дата доступа: 23.09.2015.
10. Описание программы NBMonitor [Электронный ресурс]. – Режим доступа: http://www.nsauditor.com/nbmonitor-network-bandwidth-monitor.html. – Дата доступа: 23.09.2015.
11. Сайт разработчика программы «EIS» [Электронный ресурс]. – Режим доступа: http://nfg.sitebase.ru/news_rus.html?news=6. – Дата доступа: 23.09.2015.
12. Сайт разработчика программы Wireshark [Электронный ресурс]. – Режим доступа: https://www.wireshark.org/#download. – Дата доступа: 23.09.2015.
13. Описание программы Iris Network Traffic Analyzer [Электронный ресурс]. – Режим доступа: http://www.eeye.com/html/Products/Iris/index.html. – Дата доступа 23.09.2015.
14. Сайт разработчика программы захвата на низком уровне доступности WinCap [Электронный ресурс]. – Режим доступа: http://www.winpcap.org. – Дата доступа 23.09.2015.
15. Мониторинг и управления по SNMP [Электронный ресурс]. – Режим доступа: http://aggregate.tibbo.com/ru/solutions/network_management/network_monitoring/snmp_management.html. – Дата доступа: 20.09.2015.