Д11-2001-266

П. М. Васильев[1], В. В. Иванов[2], В. В. Кореньков,
Ю. А. Крюков[1], С. И. Купцов[1]

СИСТЕМА СБОРА, АНАЛИЗА И УПРАВЛЕНИЯ СЕТЕВЫМ ТРАФИКОМ ФРАГМЕНТА СЕТИ **ОИЯИ** НА ПРИМЕРЕ ПОДСЕТИ УНИВЕРСИТЕТА «ДУБНА»

[1]Отдел информатизации, Международный университет природы, общества и человека «Дубна», 141980, Дубна
[2]Объединенный институт ядерных исследований, Дубна, и Международный Сольвеевский институт физики и химии, Брюссель

1. Введение

Современные сети передачи данных сегодня являются одним из динамично развивающихся направлений компьютерной индустрии. Глобализация процессов в сфере обмена информацией, широкое использование мультимедийных приложений, расширение сфер применения компьютерных сетей приводят к экспоненциальному росту объемов передаваемого трафика [1]. На протяжении длительного времени компьютерная индустрия отвечала на запросы потребителей постоянным ростом производительности коммутирующих устройств и локальных сетей [2]. Наметился явно *экстенсивный процесс*, заставляющий производителя отвечать на запросы рынка увеличением скорости коммутации и передачи информации. Производительность предлагаемых к реализации локальных сетей возрастает на порядки, растет также стоимость сетевого оборудования и остаточная стоимость не успевшего амортизироваться оборудования предыдущих поколений.

Такое положение дел выгодно лишь производителям сетевого оборудования [3]. Организации-потребители смирились с необходимостью ежегодно увеличивать расходы на поддержку своих сетевых инфраструктур, а конечный пользователь, как и десять лет назад, находится в постоянном ожидании уменьшения времени реакции системы.

Большинство предприятий пытается минимизировать сетевые затраты административными методами: сокращением времени подключения к глобальным сетям, ограничением круга лиц, имеющих права доступа к ресурсам сети, уменьшением числа используемых сетевых сервисов, тотальным контролем за использованием сети в рамках служебной необходимости. Эти меры достаточно эффективны с точки зрения сокращения расходов, однако они не способны кардинально нормализовать ситуацию на длительную перспективу.

Неудовлетворенность сложившейся ситуацией заставляет различные организации, в том числе и научные, искать пути решения сетевых проблем [4]. Не прекращаются работы по снижению объемов служебного трафика различных сетевых служб (DNS, WINS, DHCP и т.д.) [5], оптимизации работы клиент-серверных приложений, созданию новых и модернизации старых сетевых протоколов и стандартов сетей, разработке новых глобальных кэширующих систем [6]. В то же время движение информационных потоков в сетевых магистралях и коммутаторах подчиняется своим, фундаментальным законам, игнорирование которых нередко приводит к параличу сетевой инфраструктуры.

Еще одной важной проблемой является деятельность сетевых преступников. В условиях явного дефицита высокооплачиваемых рабочих мест в области информационных технологий (особенно в России) становится модной навязчивая демонстрация своих «способностей» путем сетевого хулиганства – хакерства и разработки программ-вирусов [7]. Многие предприятия стоят перед выбором – либо открыть мировому информационному пространству свои достижения и возможности, либо серьезно ограничить доступ извне к своим информационным серверам и сберечь таким образом работоспособность компьютерных систем. Оптимальное решение таких вопросов не лежит на поверхности и требует серьезной работы сетевых администраторов и больших материальных затрат [8].

Упомянутые аспекты явились причиной для создания простой и достаточно гибкой системы сбора, анализа и управления «Трафик» (ССАУ), реализующей задачи захвата сетевых пакетов, сбора нестандартной статистики, проведения анализа основных параметров сетевого трафика, управления логической конфигурацией сети.

Во второй главе обсуждаются задачи ССАУ "Трафик", а также проводится анализ основных программных продуктов, нацеленных на решение таких задач. В третьей главе рассмотрены технические средства, а в четвертой главе - программное обеспечение, позволившие реализовать данную систему. Пятая глава посвящена применению ССАУ "Трафик" в управлении локальной сетью университета "Дубна" и проведении детальных измерений информационного графика на выходном шлюзе сети университета "Дубна".

2. Задачи ССАУ «Трафик»

Главной задачей любой аналитической системы является возможность получения объективной и достоверной информации по любому из рассматриваемых аспектов за достаточно длительный интервал времени.

В настоящее время существует обширный рынок приложений управления сетями [9]. Многочисленные производители сетевого оборудования и соответствующих программных средств предлагают к реализации различные системы управления сетевыми платами, концентраторами, повторителями, мостами, коммутаторами и маршрутизаторами: IBM NetView, AT&T Accumaster Integrator, DECmcc, Novell NetWare Management System, HP OPENVIEW, SOLSTICE SUNNET MANAGER и др. Указанные системы имеют высокую стоимость программного обеспечения, а также требуют больших затрат по развертыванию самих систем. Приложения управления сетями предназначены, в основном, для крупных корпоративных сетей, и хотя включают в свой состав обширный инструментарий, все же имеют узкую направленность – управление разнородными сетевыми элементами.

Такой подход чаще всего неприемлем для сетей среднего размера (как в нашем случае) из-за своей дороговизны, и, кроме того, имеют недостаточный инструментарий для обеспечения поставленной нами задачи – захвата и всестороннего анализа поведения во времени больших объемов сетевого трафика. Вместе с тем, существует большое количество реализаций программ снифферов - программ захвата сетевых пакетов [9]. Многие из них выполнены профессиональными хакерами с достаточно узкой целью – анализа захваченной информации на предмет извлечения действующих имен и, возможно, паролей пользователей, MAC- и IP–адресов функционирующих в сети серверов и рабочих станций, определения задействованных сетевых служб и сервисов, версий операционных систем и т.д.

Корпоративные разработчики подобных программных продуктов преследуют несколько другие цели [8]. В частности, системы Microsoft Network Monitor и EtherBoy от NDG Software Inc. предназначены для детального анализа сбоев в работе сетевых приложений и сервисов, а также для визуализации процессов взаимодействия компьютеров в сети и передаваемого трафика.

Рассмотренные системы в основном предназначены для решения узкого круга задач и не могут быть использованы для захвата и анализа больших объемов сетевого трафика с регистрацией подробной информации, содержащейся в заголовках сетевых пакетов: интервалов времени между отдельными пакетами, размеров поля данных и т.д. Для обеспечения сбора указанной информации необходима реализация системы на основе накопления в базе данных. Такой подход позволяет выполнить детальные

исследования динамики сетевого трафика в течение длительного периода наблюдений. Кроме того, так как в сетях среднего размера регистрируется достаточно большое количество пакетов в единицу времени, то можно надеяться, что данный подход позволит также исследовать и понять проблемы передачи данных в сильно загруженных каналах связи.

Современные сети представляют собой большие, территориально распределенные системы, управление которыми немыслимо без жесткой централизации. Установка новых рабочих мест, компьютерных классов должна быть возможна только после регистрации оборудования в сетевой базе данных, позволяющей осуществлять управление маршрутами каждого из работающих в локальной сети активных устройств, на основе изменения записей в таблице маршрутизации внешнего шлюза.

Быстрое развитие компьютерных систем связи не позволяет заранее оценить необходимые в ближайшем будущем значения некоторых принципиально важных для работы сети величин, таких, как максимально допустимый объем трафика, пиковая пропускная способность сетевой магистрали и т.д. Построение прогнозов развития, а значит и своевременное, обоснованное внесение изменений в топологию и применяемую аппаратуру требуют постоянного сбора детальных данных по мониторингу сети. При этом данные должны быть представлены в виде хорошо структурированных массивов, накапливаемых на основе СУБД. Сбор информации о транзитном трафике позволяет учесть этот аспект при разработке предложений по изменению топологии сети.

Одновременно реализация подобной системы позволяет организовать детальный контроль использования сетевых ресурсов. Учебный процесс в университете «Дубна» требует предоставить возможности для изучения многочисленных сетевых сервисов и в то же время диктует необходимость тщательного контроля целевого использования ресурсов и оборудования. Эти задачи требуют также накапливать информацию о работе каждого из зарегистрированных в системе рабочих мест пользователей. Кроме того, необходимо управлять доступом к десяткам адресов часто посещаемых интернет-сайтов, включая контроль доступа к информации явно развлекательного характера.

Непременным условием стабильной работы локальной сети является анализ пакетов на предмет обнаружения попыток несанкционированного доступа к сетевым элементам, а также выявление источника различного рода сетевых атак. Идентификация и блокировка работы несанкционированных программ-снифферов, является еще одной задачей, решение которой пока не предлагается ни одним из производителей программного обеспечения [9]. Для решения этих вопросов необходимо организовать персонифицированный сбор информации о трафике, связанном со всеми устройствами, генерирующими сетевые пакеты.

В заключение отметим, что для проведения оперативного анализа накопленной информации требуется построение гибких программных средств генерации отчетных форм и передачи информационных блоков в специализированные аналитические системы.

3. Технические средства ССАУ «Трафик»

Проведенный нами анализ позволил придти к выводу о том, что оптимальным решением для создания аналитической системы является реализация программного обеспечения на основе внешнего программного маршрутизатора для сети среднего размера, содержащей 400–600 сетевых элементов: серверов, рабочих станций, ПК, сетевых принтеров и т.д. В этом случае можно получить для анализа значительный по

объему сетевой трафик и в то же время обеспечить его устойчивую маршрутизацию средствами относительно медленного программного шлюза.

В качестве такого устройства был выбран компьютер с процессором Pentium II и тактовой частотой 400 МГц. Маршрутизация осуществляется с использованием двух сетевых интерфейсов Ethernet 10 Mb/s.

В качестве операционной среды для программного маршрутизатора была выбрана Microsoft Windows NT 4.0, которая имеет набор всех операционных средств, необходимых для реализации системы.

4. Программное обеспечение ССАУ «Трафик»

Работа системы основана на реализации программы-драйвера открытого режима. Блок-схема программного обеспечения приведена на рис. 1.

В обычном состоянии сетевой адаптер компьютера находится в режиме обнаружения несущего сигнала (основная гармоника 4 – 6 МГц). После появления в кабеле битов преамбулы пакета сетевой адаптер входит в режим побитовой, а затем и побайтовой синхронизации с передатчиком и начинает прием первых байтов заголовка. Как только из первых принятых адаптером байтов удается выделить MAC-адрес получателя кадра, его числовое значение сравнивается с собственным адресом сетевого адаптера. В случае, если сравнение дает отрицательный результат и MAC-адрес не является широковещательным (FF-FF-FF-FF-FF-FF), сетевой адаптер перестает записывать байты кадра в свой внутренний буфер и очищает его содержимое в ожидании появления следующего пакета.

В целях создания условий для приема и анализа передаваемых по сегменту сети пакетов необходимо перевести аппаратуру адаптера в открытый режим, при котором происходит запись в буфер всех полученных по сети кадров. Эту операцию можно выполнить командами драйвера NDIS.

Драйвер открытого режима записывает принятые пакеты в буфер предварительного захвата (см. рис. 1) и выставляет флаг приема пакета. Далее активизируется модуль приема пакета, производится анализ поля типа пакета для выделения из общего потока лишь пакетов стека TCP/IP (другие протоколы не участвуют в формировании внешнего трафика и работают как «внутрисетевые»).

После идентификации возможно отделение заголовка пакета и уничтожение блока данных, а также запись заголовка в базу данных на основе SQL-сервера. Наряду с данными о переданном объеме информации в запись включается также время приема пакета, измеренное совместно с точностью микросекунды. Хотя запись производится с буферизацией, режим сохранения заголовков пакетов существенно увеличивает нагрузку на механические детали жестких дисков и, соответственно, возрастает вероятность их отказа, т.к. в этом случае происходит постоянная процедура записи информации относительно мелкими порциями. Поэтому указанный режим включается по мере необходимости.

Система обеспечивает также управление внешним трафиком локальной сети на основе контроля записей в таблице маршрутизатора. Исходная информация о разрешенных IP-адресах хранится в базе данных компьютеров локальной сети, откуда происходит загрузка данных о легальных адресах в массив оперативной памяти. Пользователи компьютеров, не участвующие в формировании внешнего трафика, не учитываются при вычислении количества переданных и принятых байтов. Для уменьшения количества сеансов записи информации о внешнем трафике в базу данных в систему введены таймер выгрузки из буфера и таймер смены текущей даты.

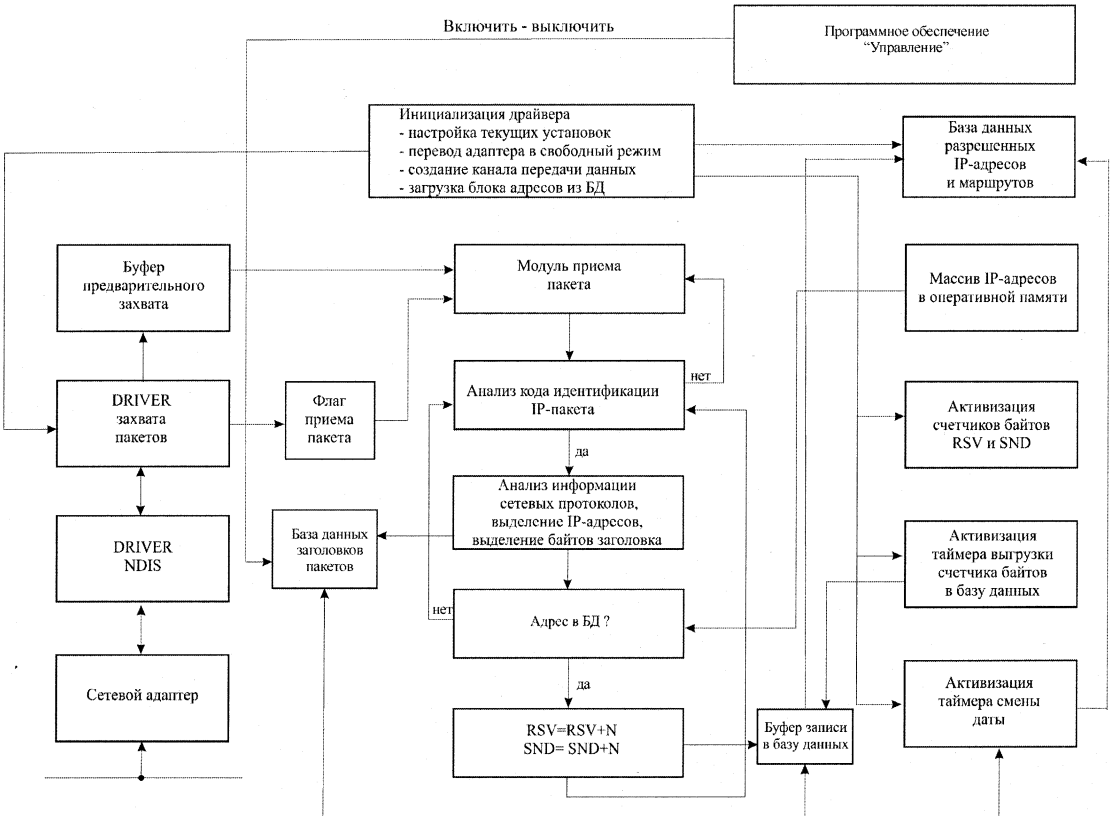

Рис 1. Блок-схема программного обеспечения ССАУ «Трафик»

5. Применения ССАУ «Трафик»

В этой главе представлены первые результаты по применению ССАУ "Трафик" в управлении локальной сетью университета "Дубна" и проведении детальных измерений информационного трафика на внешнем шлюзе сети.

5.1. Управление локальной сетью университета "Дубна"

Университетская сеть накладывает ряд дополнительных, не свойственных корпоративным сетям требований к работе отдельных сетевых групп. С одной стороны, нужно предоставить профессорско-преподавательскому составу и студентам наиболее полный объем существующих Интернет сервисов и приложений. С другой стороны, вследствие ограниченности сетевого ресурса, невозможно не уделять особого внимания административным методам регулирования объемами потребляемого сетевого трафика. С этой точки зрения, актуально деление всех пользователей на соответствующие административно управляемые группы, с возможностью применения к каждой из них специфичной политики регулирования, часто не укладывающейся в стандартные программные решения. Реализация такого подхода на базе аналитической системы позволяет гибко управлять ресурсами для достаточно разнородных групп пользователей.

Так, например, режим работы компьютерных классов требует подключения конкретной учебной аудитории (группы пользователей) к глобальной сети строго на период, определенный учебным расписанием. При этом необходимо закрыть маршруты к «известным» chat-сайтам и другим "развлекательным" ресурсам сети.

Другой пример административной политики можно проиллюстрировать на основе работы электронного читального зала. Здесь основными ресурсами являются внутренние системы (электронный каталог, полнотекстовые базы данных), а доступ к Интернет не ограничен временем. Но в то же время работа с сайтами ограничивается списком ресурсов, рекомендуемых к использованию специалистами отдела комплектования библиотечного комплекса и преподавателями кафедр.

Контроль и управление локальной сетью Университета предусматривает также создание и ведение списка примерно из сотни наиболее часто используемых ресурсов, что позволяет организовывать «зеркализацию» наиболее востребованных из них, сократив тем самым время доступа к интересующей информации, и минимизировать внешний трафик.

На основе вышеизложенного можно оценить, как часто нужно вносить изменения в административную политику той или иной группы пользователей.

Большой объем администрирования требует создания гибкого инструмента управления системой. На рис. 2 показан пользовательский интерфейс для работы с системой "Трафик".

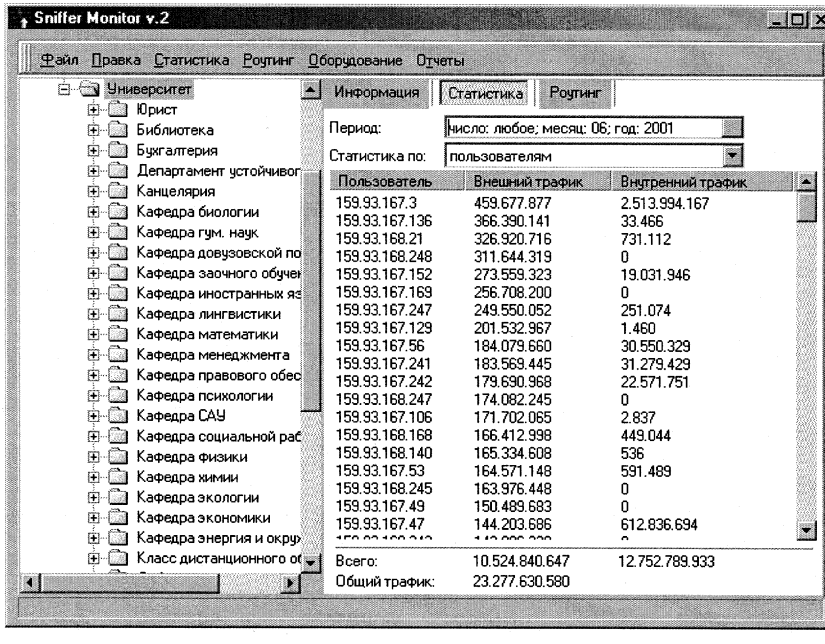

Рис. 2. Пользовательский интерфейс ССАУ «Трафик»

Структуризация сведений о сетевых группах и пользователях позволила создать единую среду для технического сопровождения оборудования. В отдельной таблице базы данных поддерживается подробная техническая информация о комплектации каждой единицы компьютерного оборудования в университете «Дубна» (см. рис. 3).

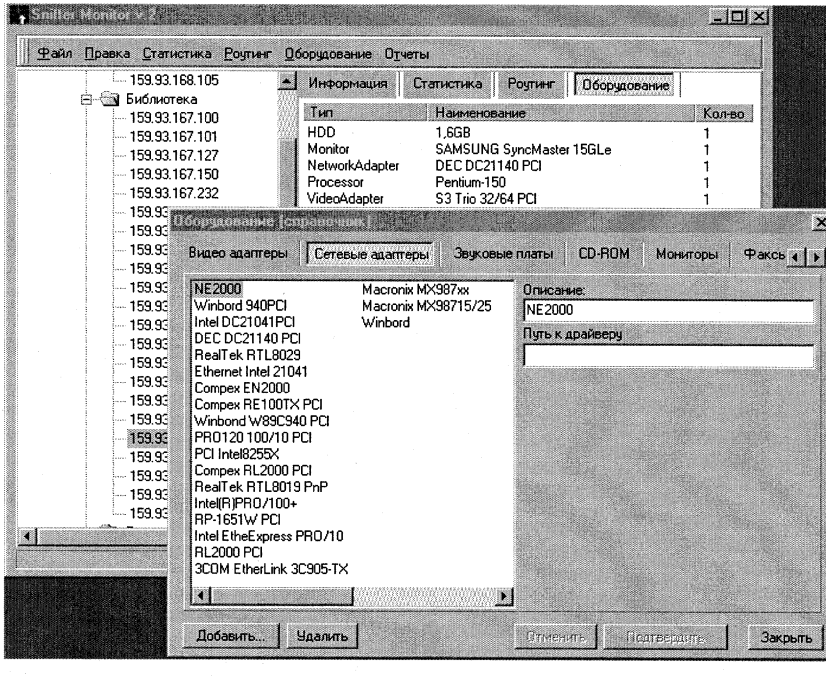

Рис.3. Интерфейс поддержки технического сопровождения оборудования

Данные о соответствии IP- и MAC-адресов из технической базы данных используются для автоматизированного мониторинга присутствия в сети несанкционированных программ-снифферов. Хотя глубокая сегментация сети коммутаторами значительно сужает возможности хакера для прослушивания транзитных пакетов, все же проблема защиты сети является актуальной. Механизм мониторинга основан на известном факте независимости работы сетевых уровней модели OSI. Задача реализации системы «свой-чужой» возложена на канальный уровень модели (аппаратуру сетевого адаптера). Более подробно вопрос о периодическом сниффер-сканировании локальной сети в рамках ССАУ «Трафик» будет рассмотрен нами позднее.

Многие кафедры и подразделения Университета имеют не ограниченные системой «Трафик» возможности доступа к внешним ресурсам. В этом случае задача минимизации объемов внешнего трафика является особенно актуальной. Её решение основано на административном управлении - передаче руководителям подразделений, выбивающихся из среднестатистических объемов потребляемого трафика, данных с информацией (кто, сколько, когда). Такой подход является достаточно эффективным, т.к., не ограничивая возможности преподавателей, обеспечивает их оперативной информацией для самоконтроля. Необходимость приема-передачи больших объемов информации согласовывается дополнительно.

5.2. Детальные измерения информационного трафика

С помощью ССАУ "Трафик" был проведен ряд сеансов по измерению информационных потоков на внешнем шлюзе локальной компьютерной сети университета "Дубна". При этом регистрировались такие характеристики, как время трансляции пакета маршрутизатором, длина передаваемого пакета, адреса источника и приемника и т.п.

На рис. 4, в качестве примера представлена временная серия информационного трафика, отвечающая примерно 1 часу измерений, для данных, агрегированных с шагом 0,1 с.

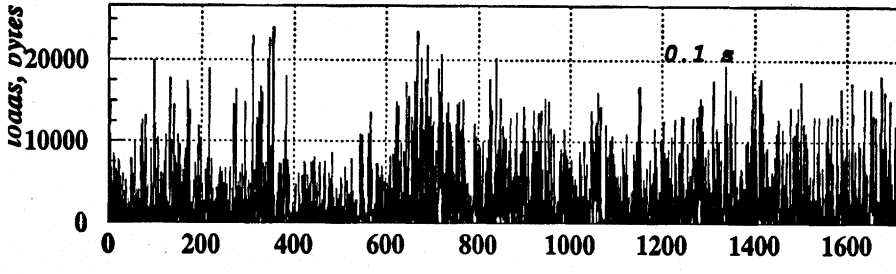

Рис. 4. Измерения информационного трафика, агрегированные с шагом 0,1 с

Возможность проводить измерения информационных потоков с частотой до 10 кГц (что обеспечило регистрацию каждого пакета в отдельности) в совокупности с большим объемом "захваченной" информации позволила провести ряд детальных исследований статистических и динамических характеристик информационного трафика [15, 16, 17, 18].

В работах [15, 16] был выполнен нелинейный анализ информационного трафика, который показал, что эти измерения (см. рис.4) могут быть представлены в виде динамического процесса с размерностью ≤ 15. В работе [17] был получен основной статистический закон информационного трафика и изучены вызывающие его причины. В работе [18] на основе кинетической модели Пригожина - Хэрмана [19] и полученного в [17] статистического закона построена кинетическая модель информационного трафика.

6. Заключение

Разработанная система обеспечивает эффективный и наглядный мониторинг сетевого трафика для локальной сети среднего размера, помогая сетевому администратору в управлении сетью.

Возможность регистрации заголовков сетевых пакетов с фиксацией времени захвата позволяет проводить исследования статистических и динамических характеристик информационного графика, нацеленные на оптимизацию не только

логической структуры сети, но и количественных характеристик информационных потоков.

В идеальном варианте система должна обеспечить не только пассивный режим наблюдения за поведением потока транзитных пакетов в сети, но и активно воздействовать на этот поток путем изменения содержания заголовков, оптимизации размеров пакетов и межпакетных интервалов. Это может значительно сократить непроизводительные издержки всей коммуникационной системы в целом за счет резкого снижения количества потерянных пакетов, исчезающих в моменты перегрузок коммутаторов и маршрутизаторов, увеличить пропускную способность каналов передачи данных и, как следствие, сократить расходы эксплуатирующих организаций и улучшить качество предоставляемых услуг.

Кроме того, ССАУ "Трафик" предоставляет возможности для мониторинга информационного трафика на предмет обнаружения попыток несанкционированного доступа к элементам локальной сети, а также выявления источников различного рода сетевых атак.

Список литературы

[1] Галкин Г. Футурология в IT: Прогноз на 2001 год. // Сетевой, 2000, №11.

[2] Горшков В. Коммутаторы верхних уровней. // Сетевой, 2001, №2.

[3] Круглый стол «Сетевого журнала», посвященный системной интеграции в области электронного бизнеса, с участием представителей компаний Etops, Arrava, «Город-Инфо», Actis, «АйТи» // Сетевой, 2001, №1.

[4] Hillis W.D. The Connection Machine. Cambridge: MIT Press, MA, 1995.

[5] Материалы сайта http://www.microsoft.com

[6] Вершин И. Сетевые шаги MICROSOFT // Сетевой, 2001, №1.

[7] Лукацкий А.В. Адаптивная безопасность сети. // Компьютер Пресс, 1999, №8.

[8] Microsoft Corporation. Microsoft System Management Server 2.0. Учебный курс: Учеб. пособие, - М.: Русская редакция, 2000.

[9] Материалы сайта http://www.hacker.ru

[10] Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 1999.

[11] Андерсон К. Локальные сети: Полное руководство. – Киев: Век, 1999.

[12] Хейвуд Д. TCP/IP Внутренний мир. – Киев: ДиаСофт, 2000.

[13] Теория и практика обеспечения информационной безопасности / Под ред. П.Д. Зегжды. – М.: Яхтсмен, 1996.

[14] Bellovin S. Security Problems in the TCP/IP Protocol Suite. – London, 1996.

[15] Akritas P. et al: **Internet Traffic Dynamics: Local Area Network Study,** "Applied Non-Linear Dynamics: From Semiconductors to Information Technologies", Book of abstracts, Thessaloniki - GREECE, 27-30/8/2001, p. 18 (to appear in "Chaos, Solitons & Fractals").

[16] Akritas P. et al: **Nonlinear Analysis of Network Traffic Measurements,** XVIII JINR Int. Symp. on Nuclear Electronics & Computing, NEC'2001, September 12-18, 2001, Varna, Bulgaria, Book of abstracs, pp. 9-10 (to be published in Proceedings).

[17] Antoniou I. et al: **On the Log-Normal Distribution of Network Traffic,** Physica D (submitted).

[18] Antoniou I. et al: **Kinetic Model of Network Traffic,** Physica A (in press).

[19] I. Prigogine and R. Herman: **Kinetic Theory of Vehicular Traffic,** American Elsevier Publishing Company, Inc., New York 1971.

Рукопись поступила в издательский отдел
19 декабря 2001 года.

Васильев П. М. и др.
Д11-2001-266

Система сбора, анализа
и управления сетевым трафиком фрагмента сети ОИЯИ
на примере подсети университета «Дубна»

Создана система сбора, анализа и управления сетевым трафиком (ССАУ «Трафик») для сегмента компьютерной сети ОИЯИ — локальной сети университета «Дубна». Система разработана на основе PC Pentium II с тактовой частотой 400 МГц и операционной системы Microsoft Windows NT 4.0. ССАУ «Трафик» позволяет проводить on-line-мониторинг параметров сетевого графика, записывать и структурировать в базе данных регистрируемую информацию, обеспечивает наглядную визуализацию результатов анализа трафика и помогает сетевому администратору в принятии решений по управлению локальной сетью.

Работа выполнена в Лаборатории информационных технологий ОИЯИ.

Сообщение Объединенного института ядерных исследований. Дубна, 2001

Перевод авторов

Vasiliev P. M. et al.
D11-2001-266

System for Acquisition, Analysis and Management
of Network Traffic for Segment of the JINR Computer Network —
Local Network of the university «Dubna»

A system for acquisition, analysis and management of network traffic (SAAM «Traffic») for a segment of the JINR computer network — local network of the university «Dubna», has been elaborated. The system is developed on the basis of PC Pentium II with a frequency of 400 MGz and operational system Microsoft Windows NT 4.0. The SAAM «Traffic» permits one to perform the on-line monitoring of the network traffic parameters, to record and structurize into the data base the transferred information, provides the vizualization of results of traffic analysis and helps the network administrator in management of the local network.

The investigation has been performed at the Laboratory of Information Technologies, JINR.

Communication of the Joint Institute for Nuclear Research. Dubna, 2001

Редактор М. И. Зарубина. Макет Н. А. Киселевой

Подписано в печать 04.03.2002
Формат 60 × 90/16. Офсетная печать. Уч.-изд. л. 0,98
Тираж 245. Заказ 53161. Цена 98 к.

Издательский отдел Объединенного института ядерных исследований
Дубна Московской области