А.М. Терентьев

СЕТЕВОЙ МОНИТОРИНГ. МЕТОДЫ И СРЕДСТВА

ТОМ 1

Монография

Чебоксары 2019

Федеральное государственное бюджетное учреждение науки
«Центральный экономико-математический институт РАН»

А.М. ТЕРЕНТЬЕВ

Сетевой мониторинг. Методы и средства. Том 1

Монография

Чебоксары 2019

УДК 004.42
ББК 32.973.5
Т35

Рецензенты:

Хрусталёв Евгений Юрьевич, д-р экон. наук,
г.н.с. ФГБУН «Центральный экономико-математический институт РАН»

Тельнов Юрий Филиппович, д-р экон. наук,
зав. кафедрой прикладной информатики
и информационной безопасности ФГБОУ «Российский экономический университет им. Г.В. Плеханова»

Терентьев, А. М.

Т35 **Сетевой мониторинг. Методы и средства. Т. 1** : монография / А. М. Терентьев. – Чебоксары: ИД «Среда», 2019. – 116 с.

ISBN 978-5-6042304-9-7

В данной работе описана оригинальная технология круглосуточного отслеживания сетевых пакетов, циркулирующих в локальной сети.

Технология базируется на выделенной рабочей станции, работающей в MS-DOS и принимающей все доступные пакеты. Агрегированные данные передаются на соседний Windows-компьютер через serial-соединение. Мониторная программа на этом Windows-ПК способна отследить заражённые ПК и выполнить действия по отключению их от локальной сети. Эта функция исполняется с помощью коммутатора Cisco.

В первом томе даются полные сведения о методах и средствах мониторинга, а также описана пилотная версия программы.

Данная технология реализована в виде пилот-проекта в ЦЭМИ РАН с 2000 г. и успешно эксплуатируется с 2006 г. в профессиональном режиме. Максимальное число пользователей превышало 200 ПК и серверов.

За проведённые исследования по данной тематике в 2003 г. автор удостоен учёного звания “Doctor of Philosophy” Европейской Академии информатизации (Брюссель).

Монография рекомендована к печати Учёным советом Федерального государственного бюджетного учреждения науки ЦЭМИ РАН.

ISBN 978-5-6042304-9-7
DOI 10.31483/a-62

УДК 004.42
ББК 32.973.5

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Использование персональных компьютеров (ПК) практически во всех научных и производственных единицах немыслимо без задействования специальных средств их объединения в единую локальную вычислительную сеть (ЛВС) предприятия. Общение через ЛВС каждого ПК, сервера или иного сетевого устройства требует наличия в нём сетевого адаптера – специальной платы с характеристиками, соответствующими типу сетевых соединений. Сетевое устройство с сетевым адаптером (ПК, сервер, сетевой принтер, каждый сетевой выход коммутатора и т.п.) будем называть нода[1].

Современные средства организации ЛВС могут также включать различные сетевые устройства, организующие ЛВС и выход в Интернет – коммутаторы, маршрутизаторы, хабы, свитчи и др. Эти устройства делают для каждой ноды возможность иметь доступ к другим.

Обмен информацией по ЛВС осуществляется пакетированными данными, организованными в соответствии с протоколами связи. Международными конвенциями предусмотрена семиуровневая модель соглашений ISO-OSI, начиная от физического уровня и завершая прикладным, причём на каждом уровне определены свои соглашения о связях. По умолчанию, сетевые адаптеры настроены так, чтобы принимать либо сетевые пакеты, адресованные «всем» (broadcasting), либо данной ноде-устройству. Для этого, каждый сетевой адаптер имеет свой, уникальный в мире, технологический MAC-адрес (Media Access Control Address), используемый на нижних уровнях ISO-OSI. Для идентификации ноды на верхних уровнях ISO-OSI используется IP-адрес (Internet Protocol Address), уникальный внутри ЛВС или во всём мире.

Крупные организации обычно не ограничены единой ЛВС. Как правило, они имеют собственную систему сетевых сервисов в виде электронной почты, сетевых банков информации, различного рода серверов, удалённого доступа (Dialup) и других, развитую

[1] Этот термин, как и множество других (E-Mail, смайлик и пр.) пришёл в Интернет из самодеятельной международной сети FIDOnet (1985 г.). Вместо IP-адреса там был общемировой аналог, например, автор данной работы известен, в частности, под адресом **2:5020/614.13**.

систему технических средств управления общей вычислительной сетью учреждения (организации). Сама сеть при этом может представлять собой исторически сложившуюся совокупность разнородных фрагментов с разной степенью защиты пользователей, разным уровнем технического обеспечения и даже разной пропускной способностью. Всё это в полной мере относится к ЦЭМИ РАН. Более того, поскольку в помещении института расположены и другие организации, использующие ту же локальную сеть и частично её сетевые сервисы, эксплуатация этих возможностей производится на совместной, корпоративной основе.

По этой причине, совокупность самих сетевых кабелей, обеспечивающих работу локальной сети, технических сетевых устройств (маршрутизаторы, коммутаторы, роутеры, свитчи, хабы и пр.), административных средств управления сетью, включенных в сеть рабочих станций и серверов предложено автором в целом называть корпоративной сетью учреждения (КВС) [1]. Соответственно, единые правила функционирования корпоративной сети и правила работы пользователей в ней естественно назвать корпоративными правилами.

Для различения функционального назначения сетей используются их IP-адреса. Стандартный вариант, до сих пор сохраняющий мировое лидерство, предусматривает кодирование IP-адресов в системе IpV4 как 4 октета (байта). К примеру, основная (глобальная) сеть ЦЭМИ РАН имеет класс **С** и адресацию в виде общемировых адресов 193.232.194.*/24, что означает, что ноды ЦЭМИ РАН могут иметь адреса в пределах 193.232.194.1 – 193.232.194.254 (маска «/24» показывает постоянные 3 * 8 = 24 бита от начала адреса). Некоторые комбинации зарезервированы для сетей других классов, например, внутренние части ЛВС ЦЭМИ РАН имеют адресацию сети класса **В** – 10.0.*.*/16, причём таких сетей в институте существует несколько (конечно, они не взаимопересекаются). Разумеется, внутренняя адресация в Интернет не поступает, для сообщения внутренних ПК с Интернетом существуют специальные службы трансляции внутренних адресов во внешние (NAT), обычно устанавливаемые на ограничителях внутренней сети – роутерах, имеющих связь с общемировым Интернетом.

Физический обмен данными осуществляется с высокой скоростью, от 10Мбит/с до 1ГБ/с. В обычной работе, конечный пользо-

ватель не имеет возможности просмотреть конкретное содержимое пакетов во время обмена и проанализировать все уровни соглашений модели ISO-OSI. Однако, в связи с некоторыми специфическими задачами крайне желательно иметь такую возможность, причём не в реальном режиме времени, а пошагово [2].

Данная работа посвящена обеспечению возможностей наблюдения сетевых пакетов **всех доступных в точке наблюдения нод**. Это открывает набор различных возможностей, от сохранения имеющих хождение в реальном времени сетевых пакетов на жёстком диске (HDD) для последующего пошагового просмотра и анализа до биллинговой агрегации данных и даже ограничения доступа нарушающих правила нод в ЛВС. Процесс наблюдения циркулирующих в сети пакетов называется сетевым мониторингом.

Таким образом, **объектами данного исследования** являлись, с одной стороны, наличествующие на момент создания системы глобальная и локальные вычислительные сети, и, с другой стороны, особенности эксплуатации ПК и других нод в этих сетях.

В процессе исследований, занявшем несколько лет, разумеется, структура ЛВС не была неизменной как в количественном, так и в качественном отношении. Не только увеличивалось число компьютеров и серверов, но также несколько раз кардинально изменилась структура сети. Поэтому ряд результатов, полученных на одной структуре ЛВС, утратил актуальность, скажем, после введения роутера и перевода большинства ПК во внутреннюю сеть. Вследствие этого, достигнутые результаты излагаются в последовательности их получения. В данном томе сосредоточены сведения о начальной структуре ЛВС, типах циркулирующих в ней пакетов, используемых технических и программных средствах, основных получаемых ежедневных и еженедельных результатах. Последующие сведения будут опубликованы позднее.

В процессе работы проводились научные исследования по созданию, развитию и оптимизации технических средств сетевого мониторинга на базе существующей и модифицируемой корпоративной вычислительной сети. **В результате исследований** были выбраны необходимые технические средства, созданы необходимые программные средства и достигнута **цель работы** – создан комплекс программно-технических и организационных решений, обеспечивающий круглосуточное наблюдение и регистрацию

биллинговых параметров исследуемой сети. Достигнута желаемая **степень внедрения** – результаты проведенных исследований нашли практическое применение в институте. **Итоги внедрения** – результаты исследований использовались как для биллинговых статистических исследований, так и для автоматической блокировки нарушающих правила поведения в сети нод, в частности, из-за вирусных заражений.

Возможная **область применения** работы – распространение созданного технического решения на другие организации – достигнута в ходе разработки. Проведены опытные работы по внедрению созданных средств мониторинга в других организациях.

Экономическую **эффективность** работы – не представляется возможным определить вследствие уникальности проведённых исследований и выполненных работ. Сама возможность фиксировать реально протекающие с большой скоростью процессы в локальной сети и впоследствии детально выполнять отложенный их анализ представляла собой к моменту начала работ качественно новый метод исследования сетевых потоков.

Как будет показано в следующем томе, сфера практического применения весьма разнообразна, от выявления некорректно настроенных компьютеров до фиксации сетевых атак и необходимости реорганизации локальной сети.

ГЛАВА 1. АНАЛИЗ И ПОСТАНОВКА ПРОБЛЕМЫ

Выбор и нацеленность средств сетевого мониторинга заявлены в программной работе [3]. К таковым можно отнести следующие.

1. Оптимизация построения корпоративной сети:

- Постоянный замер общего трафика, выявление пиковых нагрузок.
- Выявление наиболее загруженных участков сети, возможно, тормозящих общий трафик.
- Выявление «зацикливаний» при передаче пакетов в сети.

2. Экономические (биллинговые) приложения:

- Учёт трафика интересующей группы ПК.
- Суммарный учёт Интернет-трафика, возможно, по подразделениям организации (института).
- Учёт трафика, специализированного по нужному критерию (SQL-сервер, ресурсные системы Интернета, локальная почта и т. д.).

3. Информационная безопасность:

- Выявление некорректно настроенных ПК и/или серверов.
- Выявление некорректно работающих сетевых устройств.
- Выявление вирусной активности в сети с определением источника.
- Индикация неработоспособности («падения») серверов.
- Отслеживание попыток взлома, нерегламентированных доступов, хакерских атак.

Описанные задачи представляются наиболее интересными и не описывают, разумеется, всех возможностей сетевого мониторинга. Забегая вперёд, скажем, что значительную часть поставленных задач удалось решить в ходе разработки и внедрения сетевого мониторинга. Для корректного решения поставленных задач, представляется, система аудита и мониторинга должна отвечать следующим требованиям.

- Она должна быть способна принимать не только корректные и «логичные», но именно все сетевые пакеты, включая коллизионные и ошибочные. Информация о некорректно настроенных сетевых устройствах крайне важна в практической работе сетевых администраторов.

▪ Задача аудита должна решаться круглосуточно, без перерывов, поставляя периодические отчеты без прекращения своей основной работы.

▪ Технические и программные средства решения задач мониторинга/аудита не должны зависеть от работоспособности прочих сетевых устройств, в том числе серверов. Функциям аудита не должны мешать прочие задачи, исполняемые на тех же технических средствах.

▪ Задача мониторинга не должна быть зависима от текущего состояния сети, и сама не должна использовать внутрисетевые средства передачи информации.

Основываясь на указанных ограничениях, необходимо было построить систему мониторинга корпоративной сети. Вытекающие ограничения как следствия этих условий рассмотрены в соответствующем подразделе ниже.

1.1. Принятая структура данных в сетях

Процессы взаимообмена информацией в сетях носят столь сложный характер, что для точного понимания смысла и сферы действия каждого из них сложилось традиционное представление [4] их в виде семиуровневой модели ISO-OSI (рис. 1), своеобразного международного стандарта. Каждый уровень представления описывается своими стандартами, отвечает за адекватность получаемых данных принимаемым и связан непосредственно лишь с ниже- и вышестоящим.

Данная глава содержит обобщённые сведения о формате и структуре физического и вышестоящих уровней КВС, доступные в работах [5][6][7][8][9].

Такая модель оказалась столь удачной, что обычно соответствует не только структурам данных, но даже реализующим эти уровни программным модулям. Так, протокол Internet Protocol (IP) позволяет приложению «прозрачно» запускаться через существующие сети, «ничего не зная» об оборудовании сети (Ethernet, StarLAN это или Token Ring в локальных или, скажем, X.25 в глобальных сетях); Transmission Control Protocol (TCP) обеспечивает доставку данных и их идентичность, причем при невозможности обеспечить надежную доставку TCP завершает соединение. На самом деле совокупность TCP + IP (обычно обозначается "TCP/IP") является набором более, чем 100 протоколов со своими форматами, предназначенных для

весьма широких целей взаимодействия ПК. Но все они базируются, как мы увидим ниже, на стандартных форматах датаграмм – форматов передаваемых данных канального уровня.

Смысл уровня	Название уровня	Пример уровневого стандарта
Описывает работу базовых служб: пересылки файлов, почты и др.	Прикладной (Application) уровень	SNMP, SMTP
Отвечает за формат данных между разными ОС (Windows, Unix и др.)	Уровень представления данных (Presentation)	DNS
Определяет надежный коммуникационный сеанс связи двух ПК	Сеансовый (Session) уровень	FTP
Задает правила установки надежного соединения между двумя ПК	Транспортный (Transport) уровень	TCP, UDP
Описывается маршрутизация информации при взаимодействии ПК	Сетевой (Network) уровень	IP, ARP
Определение синхронизации коммутаций и управления ошибками	Канальный (Data link) уровень	Формат фреймов Etnernet-II
Описывает надежное соединение ПК с сетью, разъемы, кабели, электрические импульсы и пр.	Физический (Physical) уровень	Соединение «витая пара»

Рис. 1. Модель представления сетевой информации ISO-OSI

В отдельных случаях ряд реализаций протоколов не соблюдает четких границ разделения на описанные уровни модели ISO-OSI (например, Т. Паркер [5] в ряде случаев отмечает отход от стан-

дартов при реализации TCP/IP, путаницу между канальным и физическим уровнем и т.д.). Мы не будем, как правило, фиксироваться на этих частностях.

Естественным способом организации передаваемых данных на каждом уровне являются так называемые «конверты», когда основная информация вышестоящего уровня представления данных обрамляется дополнительными данными в начале и конце пакета – цепочки одновременно передаваемых информационных байтов.

Уже из рассмотренного ясно, что информация какого-либо уровня автоматически исключает служебную информацию «обрамления» нижестоящих уровней. В частности, максимальную информацию о передаваемых в сети данных, в том числе MAC-адрес создавшей пакет ноды, несет только канальный уровень. Это и является основной причиной, по которой средства наблюдения должны быть реализованы именно на этом уровне.

Несколько слов о дисциплине передачи пакетов на канальном уровне. Получив от вышестоящих уровней информацию о необходимости передать пакет, канальный уровень «прослушивает» текущее состояние канала, и, при его готовности, выжидает некоторое время, после чего пытается передать в канал пакет, продолжая «прослушивать» канал. Если одновременно с передачей текущего пакета какая-либо иная нода также пытается передать пакет, такое состояние канала называется коллизией, в текущем пакете начиная с этого момента все передаваемые биты (не менее 60) заменяются на **80**h, и пакет считается непереданным. Через некоторое время попытка передачи повторяется. Все адаптеры воспринимают коллизионный пакет, но обычно не подают его на верхние уровни ISO-OSI.

Время задержки между обнаружением готовности канала и началом передачи у каждого сетевого адаптера разное, оно аппаратно определяется как вероятностный процесс. Этим повышается устойчивость канала к коллизиям.

1.2. Структура сетей ЦЭМИ РАН

Существовавшая к началу разработки (1999 г.) структура сети ЦЭМИ РАН исторически сложилась достаточно сложной. Функционируя на базе популярных ***Ethernet-II/10-100Base-T***, что озна-

чает по стандартным соглашениям принадлежность к классу **01h** (***Etherhet/IEEE802.3***) и типу интерфейса **1Ch** (***D-Link 16 bit***), в ней определён основной стандарт циркулируемых пакетов как мультиплексирование ***Ethernet-II*** и ***IEEE-802.3*** [5]. В структуру сети включены несколько различных сетей класса **C**, имеется ряд выделенных сегментов различного ранга с внутренней адресацией, DialUp. Адресное пространство сети, поддерживаемое в 1999 г. Узлом ЦЭМИ РАН, состояло из трёх сетей класса **C** с различной топологией и нескольких фрагментов сети, выделенных в самостоятельные сегменты. Впоследствии значительное число пользователей было переведено во внутренний сегмент сети.

В основной сети **193.232.194.*/24**, помимо компьютеров ЦЭМИ РАН, присутствовало заметное число ПК других организаций.

Рассмотрим представление данных в сетях ЦЭМИ РАН на **канальном** (Data link) уровне.

В литературе встречаются различные описания стандартного вида фреймов сети ***Ethernet-II*** (традиционный вариант представлен на рис. 2). Ниже описан так называемый стандарт **Novell Frame**, в котором отсутствует контрольная сумма в конце пакета. Именно этот формат свойственен КВС ЦЭМИ. С этим учетом, стандартный вид кадров ***Ethernet-II Novell Frame*** имеет вид, отличающийся от рис. 2, где:

– «преамбулой» являются всегда 8 байтов: 7 байтов со значением **AA**h и последний со значением **AB**h;

– преамбула служит продолжением физического уровня и *не передается* сетевыми адаптерами на вышестоящий, канальный уровень;

– в случае сетевой коллизии, т.е. когда два или более адаптеров пытаются одновременно начать передачу, каждый из них, одновременно с передачей прослушивая сеть и обнаружив коллизию, обязан выдать в канал последовательность из не менее чем 60-ти байт **80**h и прекратить передачу текущего пакета (при этом пакет всё же воспринимается сетевыми адаптерами и может быть как передан, так и не передан на вышестоящий уровень);

– время начала следующей передачи при пустом канале в течение определенного промежутка времени определяется случайным образом по специальному алгоритму, аппаратно «зашитому» в плату сетевого адаптера;

– поле контрольной суммы (КС) в конце пакета отсутствует, а переменная часть кадра может составлять от 50 до 1500 байтов.

8 байтов	6 байтов	6 байтов	2 байта	46 ÷ 1500 байтов	4 байта
Преамбула	MAC-DA	MAC-SA	E-Type	Переменное тело фрейма	КС

Рис. 2. Стандартный вид фрейма Ethernet-II

На рис. 2 применены обозначения:

MAC-DA – MAC-адрес ноды назначения пакета;

MAC-SA – MAC-адрес ноды, испустившей пакет;

E-Type – определенный рядом соглашений код типа пакета как двухбайтовое целое число, позволяющее однозначно интерпретировать переменное тело фрейма или оставшуюся часть пакета;

Переменное тело фрейма – собственно информационная часть пакета, причем в стандарте **Ethernet IEEE082.3** в ее начале присутствует дополнительное специальное поле;

КС (контрольная сумма) – 32-битное целое число, по которому уже на канальном уровне представления данных можно судить о точности воспринятого пакета; отсутствует в варианте ***Novell Frame***.

Если MAC-DA содержит значение **FFFFFFFFFFF**h, то по соглашениям сети это означает, что пакет предназначен всем нодам, которые видят этот пакет. Такой метод передачи информации называется *широковещательным*, или ***broadcasting***. В этом режиме нода обычно информирует всю сеть о своем присутствии в ней и может сообщить, в зависимости от типа пакета, какие-либо индивидуальные характеристики: сетевое имя, описание, является ли нода сервером, имеет ли разделяемые ресурсы и многое другое. Сетевые адаптеры, встретив такие пакеты, обязаны передать их на вышестоящий уровень ISO-OSI.

Без ограничения общности, все прочие значения MAC-DA означают конкретный физический или виртуальный MAC-адрес PC-получателя, и такие пакеты в нормальном режиме работы пропускаются сетевыми адаптерами на вышестоящий уровень только в тех случаях, когда принятый MAC-DA соответствует их собственному MAC-адресу либо специально сообщен вышестоя-

щими уровнями сетевому адаптеру как виртуальный адрес получателя. Такой метод передачи информации называется *unicasting*[2].

Таким образом, стандартный вид наблюдаемого пакета в сетях ЦЭМИ РАН может быть отображён рис. 3.

6 байтов	6 байтов	2 байта	46 ÷ 1500 байтов
MAC-DA	MAC-SA	E-Type / Длина	Переменное тело пакета

Рис. 3. Формат реально наблюдаемых пакетов в сети ЦЭМИ РАН

Разумеется, конкретный вид и набор широковещательных пакетов существенно зависит от установленного на ПК системного математического обеспечения (СМО) – операционной системы, сетевых драйверов, а для сложных современных ОС – и сетевых служб. Для условий ЛВС ЦЭМИ РАН, когда одновременно эксплуатировались и MS-DOS, и файлсерверы Novell Netware 3.12, и практически все релизы Windows 3.1 / 3.11 /95 /OSR2 /98 /98 SE /NTServer /NTWs-2000 /NT /7+, исключая, кажется, только Windows ME, – испускание широковещательных пакетов разными ПК действует в разных стандартах как по периодической частоте испускания, так и по составу.

Помимо указанных, в ЛВС ЦЭМИ присутствует также ряд других типов пакетов, основным из которых является пакет стандарта ***IEEE802.3*** – в этом стандарте, собственно, и работала локальная часть вычислительной сети с файлсерверами Novell Netware 3.12. От рассмотренного выше пакета **Ethernet-II** пакеты **IEEE802.3** отличаются тем, что вместо кода пакета в поле **E-Type** находится длина пакета. Фирма Novell Netware, как и некоторые другие, в свое время поторопилась выпустить на рынок продукты с собственным форматом пакетов **IPX**, попросту проигнорировав международные рекомендации... плоды чего долгое время наблюдались в ЛВС ЦЭМИ РАН, в которой использовались как раз устаревшие пакеты типа **IEEE802.3**, не соответствующие международным рекомендациям, не имеющие контрольных сумм, не объявленные в общедоступной документации и, с появлением версии Nowell Netware 4.x, даже уже не рекомендуемые самой

[2] Посылка пакета по виртуальному IP-адресу часто называется multicasting и предназначена для группы нод, объединённых общей целью. Мы не будем это рассматривать здесь.

фирмой Nowell Netware (!), но более короткие по длине и тем самым более «экономные» в сети.

Таким образом, помимо MAC-адресов, основной проблемой идентификации пакетов, принимаемых на канальном уровне, является интерпретация значения поля типа пакета **E**(thernet)-**Type**. Ряд значений **E-Type** стандартизировано на международном уровне, такие, как **0800**h[3] (**IP**), **0806**h (**ARP**), **8137**h (**Ethernet/IPX**, не путать с **IEEE802.3/IPX**!). Для некоторых пакетов крупных производителей известны их определяющие коды. Однако, в общем случае действует соглашение, по которому если поле **E-Type** содержит значение менее 1500_{10}=**05DC**h, то это поле указывает реальную длину оставшейся части пакета типа **IEEE802.3**, а если более – то это код типа пакета для пакетов **Ethernet-II**.

Обратим особое внимание на то, что отсутствие единого стандарта на принимаемые пакеты уже на канальном уровне приводит к весьма далеко идущим последствиям: все ПК сети **обязаны** иметь, помимо стандартных протоколов, сопровождаемых контрольной суммой уже на канальном уровне, поддержку устаревших типов **Ethernet Novell Frame** и **IEEE802.3**, что приводит к значительным малооправданным расходам компьютерных ресурсов. Вопросы стабильности работы сети и ее перегрузки в этих условиях должны быть исследованы отдельно, что и было сделано в ходе исполнения данной работы.

На **сетевом** уровне происходит интерпретация по типам циркулирующих в сети пакетов. Во всех реализациях выходом именно этого уровня является информация от соответствующих драйверов; стало быть, нужно знать, какому драйверу должен быть передан пакет для его использования. Рассмотрим для примера один из наиболее часто используемых (в том числе, разумеется, один из основных и для ЛВС ЦЭМИ РАН) форматов IP.

На рис. 4 представлен формат IP-заголовка, т. е. первой, а быть может, и единственной совокупности полей, изображенной схематически на рис. 3 под названием **Переменное тело пакета**. Напомним, что для всех протоколов IP в поле **E-Type** стоит значение **0800**h. Да-

[3] Здесь и далее написание многобайтной шестнадцатиричной или десятичной константы дано согласно международному стандарту передачи информации в сетях, когда первым в пакете передается старший байт. Разумеется, это отличается от машинного вида этих констант в памяти компьютера.

лее в пакете следует заголовок переменной, в общем случае, длины, а вслед за ним может следовать, а может и не следовать само тело IP-пакета с данными.

8 бит		8 бит	8 бит	8 бит
Ver	*IHL*	*Type of Service*	*Total Length*	
Identification			*Flags*	*Fragment offset* (13 bits)
TTL		*Protocol*	*Header checksum*	
Source IP-Address				
Destination IP-Address				
Options (Переменная длина!)			*Padding* (Переменная длина!)	

Рис. 4. Формат заголовка IP-пакетов

Поясним значения некоторых из полей заголовка и, попутно, технику обработки пакетов TCP/IP существующими драйверами.

Ver – номер версии семейства протоколов, обычно **4**h, существующие драйверы TCP/IP прочие значение не рассматривают и такие заголовки попросту отбрасывают[4].

IHL – длина заголовка в 32-разрядных словах, т. е. длина каждого заголовка обязана быть кратной 4м байтам; самый короткий заголовок состоит из 20 байт.

Total Length – общая длина IP-датаграммы (то есть без полей канального уровня), включая IP-заголовок. Теоретически возможна длина датаграммы в 65535 байтов, однако в сети, как мы помним, на весь IP-заголовок плюс данные отводится не более 1500 байтов.

Identification – уникальный номер, взятый с верхнего уровня. Именно это число отвечает за то, чтобы данные заполняли нужное из открытых окон при просмотре нескольких www-страниц одновременно.

Fragment offset – смещение данных, прикрепленных в этой датаграмме, от начала фрагмента, максимальная длина которого 65535 байтов. Именно это злосчастное поле, точнее, нечеткость его возможной интерпретации, дало возможность для многочисленных и разнообразных атак на сервера, выводящих из строя драйверы TCP/IP [10].

Protocol – содержит код протокола транспортного уровня. Информационным центром Интернета (InterNIC) предусмотрены около 50 кодов. TCP, к примеру, имеет номер **6**, ICMP – **1**.

[4] В современных сетях встречается новый протокол Ipv6, со значением **6** в этом поле.

Header checksum – контрольная сумма заголовка, дополнительная проверка корректности переданного кадра. При несовпадении кадр отбрасывается драйверами.

Options и **Paddings** – необязательные поля опций (сюда, к примеру, может быть записан маршрут при трассировке узлов пакетом) и заполнителя, который обеспечивает должную общую длину заголовка кратной 4м байтам.

Source IP-Address и **Destination IP-Address** – соответственно, исходный и результирующий IP-адреса в общемировой сети Интернет или локальной сети. Эти адреса однозначно идентифицируют на всех уровнях выше канального как конкретный ПК, так и конкретную организацию, в которой установлен этот ПК. Одни и те же IP-адреса означают одно и то же в любом протоколе или службе на данном ПК. Именно по этому адресу (а не по MAC-адресу!) идентифицируется исходный отправитель пакета в общемировой сети. Разумеется, внутри внутренней локальной сети IP-адреса, как уже было сказано выше, идентифицируют данную ноду среди прочих, а при выходе пакета в Интернет будут заменены IP-адресом роутера.

IP-адрес на конкретном ПК может быть установлен двумя взаимоисключающими способами. Первый из них заключается в конкретной установке значения адреса и ряда вспомогательных значений в момент настройки ПК специалистом или мнящим себя таковым. Второй – предполагает наличие автоматизированной централизованной службы DHCP (*Dynamic Host Configuration Protocol* – протокол динамической настройки узла, обычно устанавливается на одном из серверов), которая в момент включения ПК и подсоединения его к серверу выдает ему IP-адрес, но каждый раз, вообще говоря, разный.

У каждого из вариантов назначения IP-адреса есть как достоинства, так и недостатки. Нетрудно видеть, например, что если сервер с DHCP по каким-либо причинам не работает, то «повиснут» все без исключения ПК локальной сети, даже те, которым этот сервер, вообще-то, больше низачем не нужен, кроме этого самого IP-адреса[5]... С другой стороны, степень квалификации пользователей ЦЭМИ РАН, особенно до 2000 года, такова (см. по этому поводу [11]), что зачастую возникает желание сделать эле-

[5] И ещё нескольких связанных переменных – DNS, маски сети и др.

ментарные вещи централизованно вместо того, чтобы оставлять эту возможность пользователям. (Если что-то и может остановить такую централизацию, то разве только мысль о том, что само по себе введение DHCP все же не исключит возможности пользователям вручную ввести явный IP-адрес, как и прочие сетевые настройки ПК.)

Реальный выход в этой ситуации показало время. В момент написания данной работы на всех ПК, имеющих общемировой IP в сети класса **C**, все значения параметров протоколов TCP/IP устанавливаются вручную. Таких ПК относительно немного. На всех же ПК внутренних локальных сетей роутер между внутренней частью и внешней сетью снабжён службой DHCP, так что выделение IP-адресов находится во власти системного администратора соответствующей внутренней сети.

Несколько слов стоит сказать об устройствах, объединяющих компьютеры и сервера в единую сеть. Проводное соединение «витая пара», вообще говоря, соединяет два сетевых адаптера. Для соединения нескольких рабочих станций между собой необходимо использовать концентраторы.

Хаб – устройство-концентратор, имеющее несколько сетевых портов (5, 8, 16, 24 и т.д.), которое каждый принятый на любом порту сетевой пакет мультиплицирует без изменений на все остальные порты. Используется для объединения всех рабочих станций в единую сеть. Работает на физическом уровне ISO-OSI. Содержимое мультиплицируемых пакетов не анализируется и не видоизменяется.

Сетевой коммутатор, или свитч (англ. Switch) – современный вариант хаба, в котором передача пакета на другие порты исполняется в зависимости от типа пакета: широковещательные (broadcasting) пакеты мультиплицируются на всех портах, unicasting-пакеты транслируются только на тот порт, к которому подсоединено устройство, имеющее MAC-адрес назначения пакета (если таковой неизвестен – трансляция идёт на все порты). Коммутаторы работают на канальном уровне ISO-OSI. «Продвинутые» коммутаторы имеют на прошивке математическое обеспечение, которое позволяет управлять коммутатором по специальному протоколу, позволяя, в частности, разрешать или запрещать подключение того или иного (по MAC-адресу) устройства к тому или ино-

му порту коммутатора. Фактически, такие коммутаторы являются устройствами уже не канального, а сетевого уровня ISO-OSI.

Маршрутизатор (иногда раутер или роутер – англ. router) – специализированный компьютер, который пересылает данные между портами, соединёнными с различными сегментами сети, согласно таблицам и правилам маршрутизации. Маршрутизаторы работают на сетевом уровне модели ISO-OSI. При пересылке пакетов данных между различными сегментами сети всегда меняется MAC-адрес отправителя на MAC-адрес порта маршрутизатора, испускающего пакет, но обычно меняется также и IP-адрес пакета на принятый в принимающей сети. Таблица маршрутизации может быть статической (вводимой вручную администратором сети) или динамической, оформляемой на основе специальных протоколов. В последние годы широко распространены роутеры для домашних сетей, имеющие, кроме порта входа и портов выхода ЛВС, также адаптер для Wi-Fi. Аппарат подмены IP-адресов с внутренних на внешние и обратно называется NAT (Network Address Translation).

Таким образом, с помощью рассмотренных устройств формируется КВС предприятия или группы предприятий, которая может быть весьма сложной, состоя из нескольких сегментов ЛВС.

1.3. Основные измеряемые параметры сети

Легко заметить, что уже в названии сети ***Ethernet-II/10Base-T*** присутствует один из основных параметров этой сети – скорость передачи информации, которую будем определять как число байтов, передающихся по сети в секунду. В вышеупомянутом названии сети значение **10** означает «десять мегабит в секунду» и присутствует как технический параметр. Как мы видели выше, реально в сети всегда присутствуют специальные биты начала пакета, существуют и необходимые технологические интервалы между пакетами, так что реальная предельная скорость передачи информации в 10-мегабитных сетях вовсе не эквивалентна 10Мбит/с = 1.25 МБайт/с, а составляет существенно более низкое значение в переделах 700÷800 МБайт/с.

Однако, и при таких значениях весьма высоко число сетевых коллизий. Принятой нормой 100%-ной загрузки 10Мбит/с-сети считается скорость $\boldsymbol{Vcp}$=600 МБайт/с.

Вторым интересующим параметром сети является ***Ypak*** — число пакетов, переданных за интересующее время. Причем, в это число уже не входят ситуации сетевых коллизий, хотя не каждый прошедший по сети без коллизий пакет аутентичен: может случиться еще несовпадение контрольной суммы из-за искажения отдельных битов при передаче. Соответственно, представляет интерес и абсолютное значение ***Ybytes*** объема переданной информации.

Следующим интересным параметром является число нод ***Ncomp*** в сети в каждый момент, точнее, активных сетевых MAC-адресов.

В целях анализа трафика интересны данные о проходящих пакетах и используемых протоколах как обычных, так и широковещательных.

Наконец, особый интерес представляет возможность получения информации о необработанных станцией наблюдения, «пропущенных» пакетах (далее ***Npak***) и, соответственно, их общем объеме ***Nbytes***, поскольку именно эта возможность залагает основы объективного автоматизированного анализа достоверности проводимых исследований.

Соответственно, коллизионные пакеты будут обозначаться ***Epak*** и ***Ebytes***.

Для биллинга интересны значения объёмов принятого из Интернета ***Internet-From*** и выпущенного в Интернет ***Internet-To*** данных.

1.4. Избранный метод исследования сетевых потоков

В данном разделе будут рассмотрены основные составляющие метода – топология исследуемой сети, средства получения информации обо всех сетевых пакетах и конфигурация технических средств наблюдения.

1.4.1. Топология исследуемой сети

Топология КВС ЦЭМИ РАН в 1999 г. имела неоднородную структуру. Основная часть рабочих станций была соединена по «звезде» через хабы с файл-серверами Novell Netware, серверами обеспечения доступа в Интернет и коммутатором доступа к оптоволоконной сети соединениями «витая пара». Тип пакетов в сети – Ethernet-II. Отдельными сегментами сети существовали маршрутизатор коммутируемых линий доступа и некоторые другие структуры. Без ограничения общности, такая структура может быть подобна рис. 5.

Как отмечено в [12], при такой топологии физически все сетевые адаптеры всех нод основного сегмента сети в адресном поле 193.232.194.*/24 имеют возможность приема любого пакета сети на канальном уровне. Присутствующее математическое обеспечение канального уровня отсортировывает для дальнейшего использования на каждом ПК пакеты общего назначения (broadcasting) и те пакеты, которые предназначены для конкретной ноды. Последующие уровни OSI-модели имеют дело с уже отсортированными указанным образом пакетами, выделяя из них далее пакеты нужных типов (IP, IPX и др.), организуя TCP-стэк, сеансы связи и реализуя все вышестоящие уровни модели ISO-OSI.

Однако, как ряд специальных драйверов сетевых карт в таких ОС, как UNIX BSD, так и некоторые драйверы других операционных систем могут иметь так называемый режим **Promiscuous Mode**, в котором для исследовательских или отладочных целей разрешено прохождение *всех* наблюдаемых пакетов на вышестоящий уровень. Эта функция известна как часть режимов низкоуровневого пакетного PC/TCP FTP-драйвера управления сетевым адаптером в MS-DOS. Эти средства объявлены некоторыми отечественными авторами ([13]) как хорошо известные, а их использование считается крайне опасным для сети.

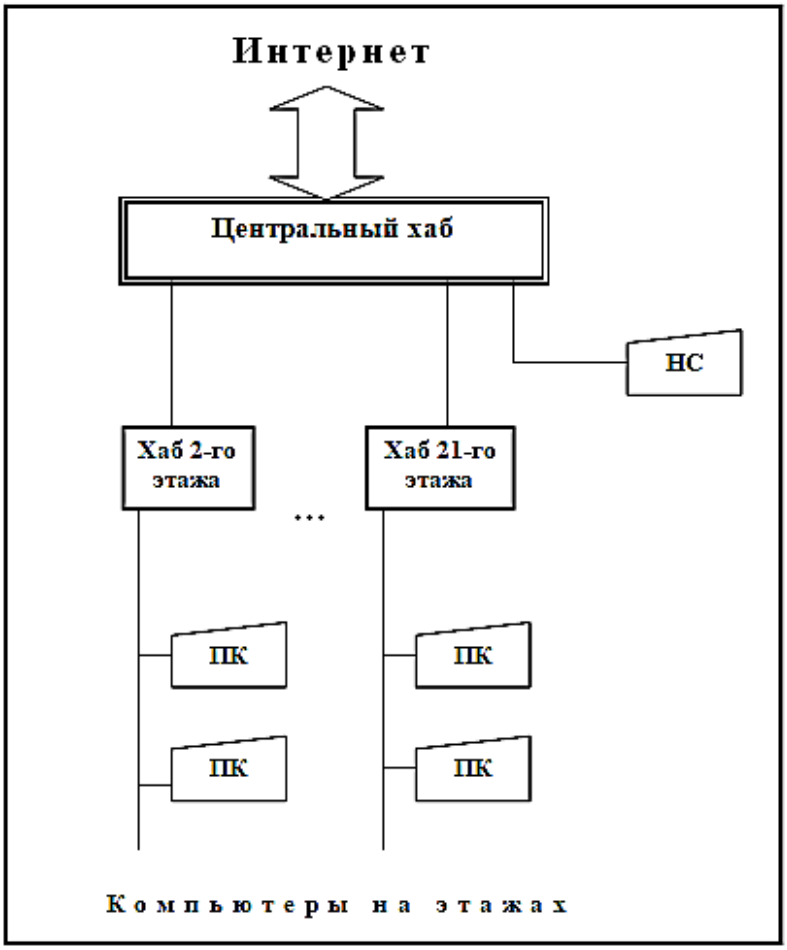

Рис. 5. Начальная схема соединения компьютеров ЦЭМИ РАН

На рис. 5 один из компьютеров выделен справа и помечен символами «НС» (наблюдающая станция) – это именно тот выделенный ПК, на котором установлены средства наблюдения сетевых потоков: MS-DOS 6.22, указанный ниже сетевой адаптер NETGEAR FA310^{TX}, работающий в режиме получения всех пакетов (Promiscuous Mode), и программа сетевого мониторинга.

1.4.2. Известные средства сетевого мониторинга

Среди известных к началу разработок по анализу ЛВС различными примерами решения отдельных задач мониторинга и аудита могут служить целевые пакеты: низкоуровневый и очень дорогой **Spectroum** фирмы Cabeletron (UNIX), весьма сложный **OpenView** фирмы Hewlett-Packard, румынский **PeepNet** и даже отдельные команды UNIX (**snoop**, **atp -a, tcpdump** в BSD и ряд других) или Windows/9x (**NETSTAT.EXE** и др.).

Некоторые средства мониторинга IP-трафика ЛВС присутствуют в маршрутизаторах Cisco [14] (команда **show ip traffic**, а также специфические средства отладки), однако в большинстве случаев эти возможности наиболее пригодны для статистики, ICMP-сообщений и весьма ограниченного по времени и объёму просмотра реальных IP-пакетов.

Известен также неисчислимый ряд популярных хакерских разработок, ориентированных главным образом на вылавливание паролей Dial-Up и Novell NetWare, выведение из действия файл-серверов Novell с присвоением прав супервизора, многотипных атак на серверы Sun, попыток чтения чужой почты и пр.

В последние 10 лет добавился ряд разработок, «вылавливающих» пакеты со средних уровней ISO-OSI. Широко известная утилита **tcpdump** позволяет видеть сетевые пакеты TCP/IP. Получившая в последнее время незаслуженно высокую известность утилита **WireShark**, позиционирующая себя как знаток сотен сетевых протоколов, действительно, отражает многие сетевые пакеты – но, к сожалению, только корректные. В то же время, регулярно наблюдаются случаи, когда из-за некачественной работы или сбоев сетевого адаптера некоторого ПК или сервера в сеть поступают пакеты с «обрезанным» началом, вследствие чего оказываются смещёнными все последующие поля. Такую ситуацию **WireShark** отследить не в состоянии.

Каждое из этих средств либо предоставляет узко специфицированную информацию, либо, являясь сложным и весьма дорогостоящим коммерческим пакетом, ориентировано опять-таки на специфические задачи решения проблем взаимодействия клиент-сервер, устранения физических помех, управление сетью с помощью установленных на каждой ПК агентов (**OpenView**), построение виртуальных сетей (**Spectroum**) и иные задачи.

Вместе с тем, ни одно не дает полного круглосуточного анализа трафика с возможностями дополнительного выделения его компонентов по интересующим подразделениям, лабораториям, отдельным ПК и пользователям, а также выборочной фиксацией на HDD.

1.4.3. Сетевые адаптеры с особыми свойствами

Проведенные в конце 1999 г. десятки экспериментов с разными сетевыми адаптерами из числа используемых в ЦЭМИ РАН позволили подобрать *только один* сетевой адаптер, а именно **Bay Networks Netgear FA310^{TX} 100Base-T Fast Ethernet PCI-Adapter**, и *единственный* драйвер (соответственно, **Packet Driver for NETGEAR FA310TX Fast Ethernet PCI Adapter Ver. 2.08 (970108)**), реально дающий **Promiscuous Mode** в Extended-режиме при использовании в MS-DOS 6.22. Более того, сетевые карты с точно таким же наименованием, но OEM-, а не Retail-поставки, ни с этим, ни с другими драйверами **Promiscuous Mode** не давали (!). Совсем интересно, что среди всех известных модификаций этого драйвера за последние 19 лет только названная (!!) корректно реализует указанный режим. И, как будет показано ниже, реальная эксплуатация этого режима сделана максимально затрудненной. После всего сказанного предоставим судить читателю о степени реальной опасности указанной технологии[6]...

Для лучшей иллюстративности покажем вид Retail-упаковки (рис. 6) и внешний вид (рис. 7) приведённого сетевого адаптера, успешно работающего в Promiscuous Mode в MS-DOS 6.22.

[6] Стоит ли удивляться, что за много лет работы системным программистом при постоянном интересе и долголетнем участии, и даже модераторстве, в конференциях любительской компьютерной сети ФИДО, наполненной хакерами, хотя бы из-за причин ее создания в СССР, реально владеющих описываемым методом не нашлось?

Рис. 6. Общий вид упаковки сетевого адаптера NetGear FA310

Рис. 7. Общий вид сетевого адаптера NetGear FA310 и дискеты с драйверами

Особенностью этого режима, в частности, является то, что он может быть установлен в указанном драйвере только в случае одной нити программных обращений к нему. Другими словами, при установленном режиме приема всех пакетов невозможно одновременное использование стандартных вышестоящих в OSI драйверов IPX, TCP/IP и прочих – все необходимые уровни должны быть запрограммированы заново. К примеру, для реализации интерфейса с другим ПК через UDP, не говоря уже о куда более сложном TCP/IP, необходимо всю процедуру связи программировать вручную, непосредственно.

Естественным следствием является выделение специального ПК под цели наблюдения сети указанным методом.

Следует также отметить, что хотя основной интерфейс с Extended-FTP-драйвером описан в знаменитом ***Interrupt List*** Ральфом Брауном (Ralf Brown) [15] на уровне обращений, процедурного описания корректной последовательности обращений в доступной литературе и на сайтах Интернета в 1999 г найти не удалось. Более того, авторы драйвера предприняли определенные усилия для того, чтобы затруднить его использование в **Promiscuous Mode** непосвящённым в процедурные тонкости. Далее будут изложены детали, которые можно найти в упомянутом ***Interrupt List*** Ральфа Брауна, дополненные собственными исследованиями автора.

Для начала следует найти номер прерывания (IRq) MS-DOS, соответствующего пакетному драйверу, которое может быть в интервале от **60**h до **80**h. Как будет показано на рис. 47, номер прерывания драйвера задаётся при описании драйвера в файле CONFIG.SYS (на этом рисунке задан номер **62**h).

Пакетный драйвер FTP PC/TCP ищется следующим образом. Его обработчик (handler) начинается с 3х-байтной инструкции перехода, непосредственно за которой находится текстовая строка "**PKT DRVR**", заканчивающаяся нулевым байтом (терминатором текстовой строки). Сканируя векторы прерываний в указанном интервале, ищется обработчик с такой характеристикой. При отсутствии такового, драйвер считается отсутствующим.

При дальнейшей работе следует учесть, что один пакетный драйвер может обслуживать на одном адаптере несколько уровней доступа. Поэтому, при начале работы с пакетным драйвером ис-

пользуется специальный числовой указатель (handle), идентифицирующий обращающуюся программу и сетевой адаптер.

В таблице на рис. 8 приведены используемые типы обращений к FTP PC/TCP-драйверу. По всем типам обращений следует отметить, что успешность обращения показывает после выхода сброшенный флаг процессора Carry, а отказ – установленный.

Ряд обращений допускает только драйвер Basic-уровня; некоторые обращения требуют драйвера уровня Extended, и ряд обращений разрешён только в High-performance типе драйвера. Для поставленной задачи требуется драйвер уровня Extended.

При использовании режима Extended Mode, для приёма пакетов внутри программы обработки должна быть создана программная ветвь **UpCall**, вызываемая драйвером асинхронно с обычным процессом. Эта ветвь по каждому пакету вызывается дважды: первый раз (AX = 0) для сообщения длины пакета (CX) и запроса, надо ли его будет сохранять. Второй раз (при первом положительном ответе) – для собственно сохранения полученного пакета (AX = 1). Естественно, при программировании процедуры UpCall следует предусмотреть запоминание всех регистров и переключение текущего стэка с полным их восстановлением перед выходом (эти операции исполняются с предварительным запретом всех прерываний процессора и поэтому должны быть оптимальны).

Теоретически, ветвь UpCall не может быть повторно-входимой, однако на практике автором при реализации блока приёма пакетов в модуле TamINet.OBJ предприняты меры для того, чтобы повторный вход в эту ветвь при уже исполняемой ветви не приводил бы к сбоям работы НС.

Следует отметить, что показанные на рис. 8 обращения далеко не есть полный перечень возможных обращений к PC/TCP FTP драйверу; приведены только реально использованные в реализованной программе наблюдения, точнее, в модуле TamINet.OBJ, входящем в состав программы. В этом же модуле находится асинхронно вызываемая при получении пакета процедура UpCall и ряд других сервисов.

AH	AL	Смысл обращения
7	--	Закрепить Handle перед прочими операциями, сбросить (Reset) интерфейс. BX=handle.
6	--	Принять MAC-address сетевой платы в ES:DI, BX = handle
1	FF	Принять версию драйвера и др. параметры. Имя драйвера в DS:SI, версия в BX, класс в CH, тип в DX, номер в CL, AL показывает поддерживаемые драйвером функции: 6 = basic, extended и high-perfomance.
2	01	Установка Extended Mode; задание адреса Upcall в ES:DI, после возврата в AX – Handle для Promiscuous Mode, CX = 0 для приёма всех пакетов независимо от их типа
14h	00	Уст. Promiscuous Mode, BX = handle, CX = 6
04	00	Посылка пакета из DS:SI длиной CX[7]
03	00	Освободить Handle перед снятием программы

Рис. 8. Использованные обращения к FTP-драйверу

Наличие именно этой процедуры UpCall позволяет отдельно подсчитать число пакетов, отказанных к запоминанию, и их суммарную длину. Иначе говоря, таким образом обеспечена релевантность подсчёта пропущенной информации в средствах мониторинга.

Укажем, что число и общий объем в байтах пакетов, не принятых к обработке вследствие недостаточной мощности обрабатывающих технических средств (т.е. текущей нехватке памяти в буферах для нового пакета), отражается в основных выходных данных программы.

Представляется целесообразным в данном случае не описывать подробно найденный и апробированный алгоритм и процедуры обращений хотя бы из уважения к таинственным и неизвестным силам, предпринявшим столько усилий для засекречивания этой, несомненно, полезной методики. Хотя за время с написания первичной программы на сегодняшний день в Интернете уже появилась информация по этому вопросу от FTP Software [16].

[7] Несмотря на то, что наблюдающая станция никогда не испускает пакетов в стандартном режиме работы, эксперименты с испусканием проводились и были успешными.

1.4.4. Форматы наблюдаемых сетевых пакетов (кадров)

Как уже говорилось, принимаемые в **Promiscuous Mode** пакеты **Ethernet-II**, циркулирующие в реальной КВС ЦЭМИ РАН, оказались имеющими ряд отличий от стандартного вида этих пакетов, описанного в литературе. В частности, позволяется видеть «неполноценные» пакеты канального уровня, передача которых прервана вследствие сетевой коллизии. В то же время, драйвером не видна контрольная сумма канального уровня, что чрезвычайно затрудняет первичную обработку пакетов в смысле отбраковки.

Серией специально поставленных экспериментов на ПК AMD-DX4-100 удалось определить истинную процедуру обращений к указанному драйверу для уверенного приема всех пакетов. Во время этих экспериментов, в частности, было:

– осуществлено написание тестовой программы сплошного дампирования на HDD всех принимаемых в реальном режиме сетевых пакетов;

– написан специальный драйвер, имитирующий работу ЛВС с поэтапной, управляемой оператором ПК по команде с клавиатуры, поочередной подачей с HDD ранее дампированных пакетов для тонкой отладки программы приема и обработки сетевых пакетов с полной имитацией уже «расшифрованных» функций FTP-драйвера в Extended Mode;

– осуществлено с помощью указанных выше вспомогательных средств создание действующего прототипа программы обработки сетевых пакетов, работающего в реальном времени и описываемого ниже в разделе данной работы;

– проведены реальные эксперименты с созданным прототипом программы с целью определения потребных вычислительных мощностей для реально действующей программы подсчета трафика в условиях КВС ЦЭМИ РАН.

Проведенные эксперименты показали:

– принципиальную возможность создания программы наблюдения за сетевым трафиком с использованием выделенного ПК, оснащенного указанными сетевым адаптером и стандартным низкоуровневым пакетным FTP-драйвером в MS-DOS 6.22;

– достаточность малоценной в настоящее время IBM PC/AT-486-DX4-120 для первичной обработки любого сетевого трафика на сетях 10Мбит/с;

– наличие в предложенной технологии средств самоконтроля, учитывающего как число обработанных сетевых пакетов, так и число и объем сетевых пакетов, которым отказано в обработке из-за недостатка вычислительных ресурсов средств мониторинга.

1.4.5. Конфигурация наблюдающей станции

Обсудим выбор операционных средств, на которых должны базироваться средства сетевого мониторинга.

К моменту начала построения средств сетевого мониторинга как законченно оформленные операционные среды существовали:

– MS-DOS 6.22;

– Microsoft Windows'98 и её расширение OSR2;

– различные версии Unix.

Как уже было показано, для MS-DOS было найдено интерфейсное средство приёма всех сетевых пакетов – пакетный PC/TCP FTP драйвер. В то же время, к моменту начала разработки (1999 г), в доступной литературе по Unix автором подобного средства найдено не было[8].

Microsoft Windows является принципиально сетевой операционной системой: работоспособность каждого ПК может зависеть от одного или более серверов, при старте работы даже Windows'98 выдаёт более 200 сетевых пакетов. Принципиальная многозадачность не позволяет сконцентрировать все вычислительные ресурсы на одной задаче. Таким образом, наложенные требования однозначно не допускали построения программных средств мониторинга в Microsoft Windows.

Оптимальным решением представлялось создание наблюдающей станции как выделенного ПК, работающего под MS-DOS или Unix, со стандартными (хотя и отобранными) сетевыми адаптерами и специальными драйверами, позволяющими задаче аудита получать все сетевые пакеты.

Исходя из поставленных задач, ясно, насколько важные функции возлагаются на средства сетевого мониторинга. В 2000 г вышло решение Правительства РФ о построении критически важных программных средств на отечественных вариантах операционных систем. С этой точки зрения, MS-DOS являлась вполне допустимой для построения средств мониторинга хотя бы потому, что

[8] Сейчас такие средства существуют почти для всех версий Unix.

существовал уже PTS-DOS и другие разработки, находящиеся под наблюдением отечественных организаций. Выбор именно DOS предрешал накопленный автором опыт разработок в этой операционной среде, в отличие от Unix, опыта работы с которой у автора не было. К тому же, в литературе присутствовали мнения [17] о том, что MS-DOS рано списывать со счетов.

1.5. Заключительный анализ

Всё сказанное выше свидетельствует об определённом дефиците средств полноценного сетевого мониторинга как на момент начала создания оригинальных средств в ЦЭМИ РАН (2000 г.), так и в настоящее время. Отсутствуют средства, дающие как текущие показатели на экране, так и форматированные отчёты, привязанные к астрономическому времени, исполняющиеся 24 часа в сутки и каждый день в году.

Имеющиеся средства привязаны к сетевой среде и не могут функционировать вне её.

Таким образом, задача построения низкоуровневого средства кругломуточного сетевого мониторинга с Online-показом текущего состояния сети и опциональным выборочным акцентированием пакетов ни до 1999 г., ни до настоящего времени не была решена.

Из изложенного ясно, что создание подобного средства представляет собой актуальную задачу, имеющую десятки различных практических применений.

ГЛАВА 2. СИНТЕЗ ПРОГРАММНОЙ СРЕДЫ МОНИТОРИНГА

Средства наблюдения трафика в локальной сети первоначально представляли собой идею для пробных, экспериментальных исследований. В силу этого ставилась задача создать действующую модель, прототип, который, возможно, не был бы оптимизирован по ряду эксплуатационных параметров для полноценного решения всех задач, но мог бы справляться с действующим потоком и выдавать аутентичные результаты.

По мере получения успешных результатов, ряд параметров написанной программы удалось оптимизировать в процессе эксплуатации. Эти изменения изложены в томе 2. В процессе разработки компоненты постоянно совершенствовались. В данной работе описано состояние разработки на март 2001 г.

Программа наблюдения потоков состоит из двух модулей. Первый, внутренний, написан на языке Макроассемблера, содержит низкоуровневые процедуры инициации, получения очередного пакета из буфера и завершения, а также процедуру помещения принятого от драйвера сетевой карты пакета в буфер, вызов которой исполняется самим драйвером сетевой карты. Объем текста – 570 строк Макроассемблера MASM 5.10 – 1988 г., размер программы вместе со стэком – 1953_{10} байта, предназначение – процессор i80386 в реальном режиме.

Второй модуль написан на алгоритмическом языке высокого уровня PowerBasic for DOS с задействованием высокооптимизирующего компилятора 3.05 [18] [19] [20], содержит 1183 строки. В собранном виде программа TAMCNET.EXE занимает на диске 74Кб, использует только основную память и реальный режим процессора i80x86 и предназначена для исполнения в операционной среде MS-DOS 6.22. Объем буферов для принимаемых пакетов – 128Кб.

Такова начальная структура программы-прототипа.

2.1.Общий алгоритм программы

Программа загружается из командной строки MS-DOS 6.22, принимая необходимые параметры, загружает текущее состояние оперативной БД и определяет номер последнего из ранее сформи-

рованных отчетов. При отсутствии ошибок в БД и нормальном подключении низкоуровневого PC/TCP FTP-драйвера сетевого адаптера программа сразу же входит в бесконечный цикл, исполняя, как показано на рис. 9, этапы:

– проверки текущего состояния буферов, при наличии пакета извлечение его и необходимая обработка (все варианты циклов; если при этом в цикле был обработан пакет, то цикл считается «полезным»);

– при достаточном свободном пространстве в буферах – вывод на экран текущих значений параметров и переменных, а также определение нажатой клавиши и, если нужно, обработка завершенной команды («длинный» цикл).

Таким образом, программа реагирует на интенсивность поступления пакетов из ЛВС, исполняя «короткий» или «длинный» циклы. «Длинный» цикл исполняется в случае, если занятое пакетами в буферах пространство не превышает процента **BufLim** или «коротких» циклов выполнено более, чем **WtCyc** подряд. Оперируя этими параметрами, предполагалось добиться оптимального режима программы как на обработку пакетов, так и на отображение результатов на экране.

На том же рис. 9 вверху справа показана ветвь UpCall низкоуровневой подпрограмы обработки пакетов. Она исполняется асинхронно с основным циклом, при поступлении прерывания по приходу пакета и вызывается PC/TCP FTP-драйвером. К настоящему времени в этот блок добавлена проверка, не исполняется ли уже эта ветвь во время прихода очередного пакета, и в случае положительного ответа исполняется выход с фиксацией типа «Мимо» прерывающего пакета.

Как известно, текстовая экранная видеопамять в MS-DOS начинается с адреса **B000**h и позволяет разместить 8 текстовых экранов по 25 строк или 4 экрана по 50 строк. Для лучшего отображения многочисленной информации, программа сетевого мониторинга использует сжатый экран в 50 строк. Принцип перехода в этот режим взят из популярной программы Norton-Commander. Текущий вывод исполняется одновременно в 4 области экрана – «0», «1», «2» и «3». Какая из областей видеопамяти реально выводится на экран монитора – зависит от параметров вызова программы и/или команд оператора. Для показа нужной области

необходимо нажать соответствующую цифровую клавишу на клавиатуре; программа перейдёт в режим показа соответствующей области видеопамяти без прерывания текущей работы.

В начале работы программы, в видеопамяти формируются макеты всех 4-х областей, далее они корректируются. Для экономии места в основной памяти MS-DOS, форматы всех областей видеопамяти (символы и их атрибуты) подготовлены в виде специального текстового файла в рабочем каталоге программы мониторинга и засылаются в видеопамять при старте программы.

При разработке этого блока неожиданно выяснилось, что все графические адаптеры могут выделять память под видеостраницы не обязательно точно по 4000 байтов. Поэтому, для точного определения размера видеостраницы текущей видеокарты используется засылка символов “--” в её начало через стандартные процедуры BIOS, и определение полученного интервала в видеопамяти.

Во время работы программы допускается сделать скриншот активной области видеопамяти на HDD, для чего достаточно нажать клавишу “**$**”. Именно так были получены все скриншоты, приведённые в данной работе. Разумеется, для получения цветного рисунка используется специальная написанная автором программа, переводящая текстовый формат и атрибуты в графический вид.

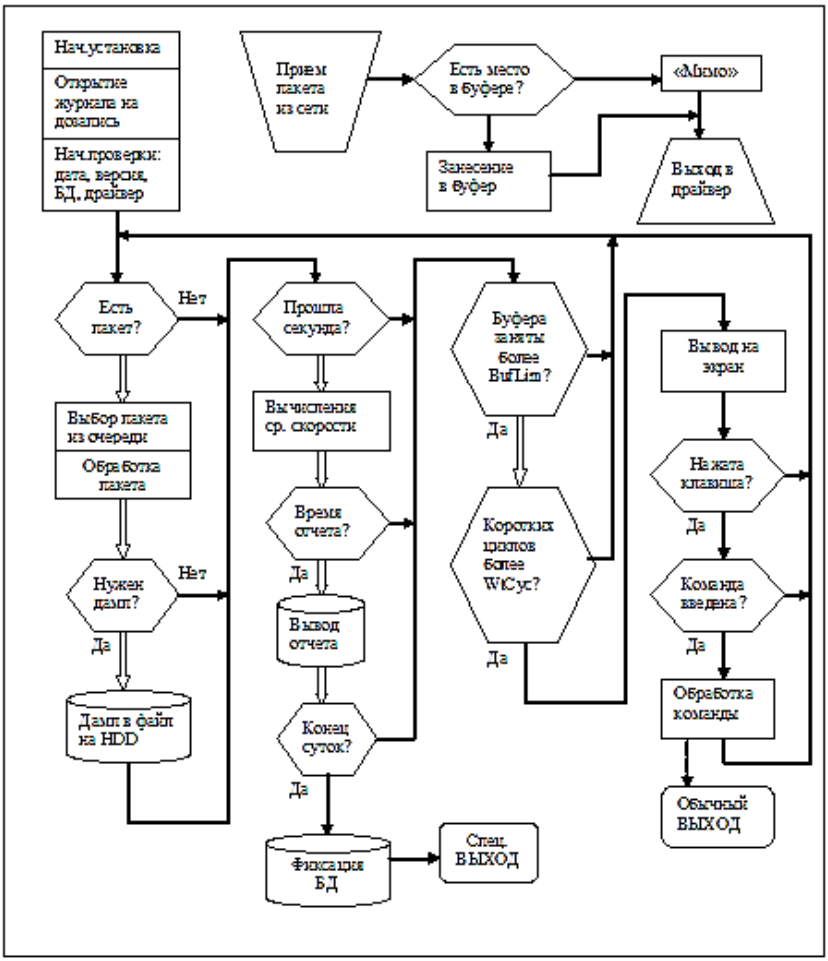

Рис. 9. Схема основных циклов работы программы наблюдения

2.2. Входные данные и управление

Входными данными программы являются:

– параметры командной строки;

– номера ранее созданных отчетов (программа автоматически начнет формировать отчеты со следующего номера, если иное не задано параметром командной строки);

– состояние оперативной БД со списком нод, MAC-адресов и характеристик;

– файл системного журнала (программа автоматически продолжит его вести);

– команды, набираемые на клавиатуре;

– сигналы, поступающие по Com-порту от соседнего ПК, если таковое соединение действует (подробно освещено в последующих Томах).

Оперативное управление программой заключается в подаче управляющих команд с клавиатуры. Можно подать команды, перечисленные на рис. 17, а также некоторые дополнительные.

2.3. Информация на экранах программы

При показе информации программа использует 4 области видеопамяти по 50 строк каждая, нумеруемые от 0 до 3. В данном разделе приведены виды этих экранов и пояснены детали изображений на них.

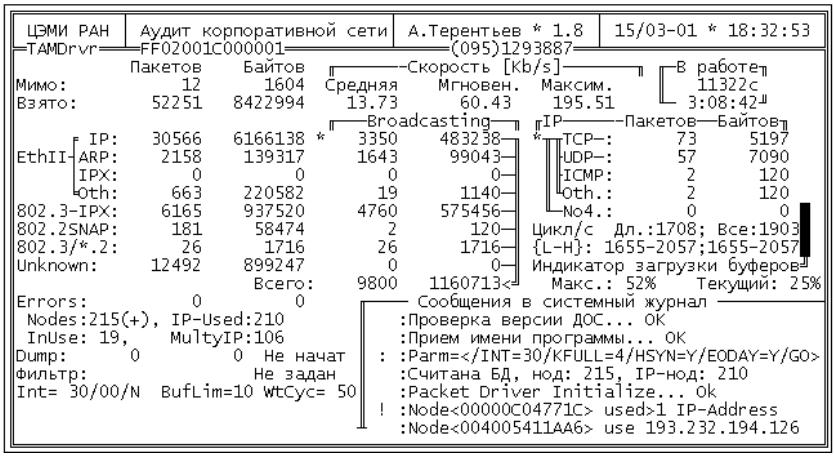

Рис. 10. Верхняя часть основного экрана программы наблюдения

Верхняя половина нулевой, основной страницы экрана изображена на рисунке 10. В её верхней части даются текущие атрибуты (дата, время, версия программы, версия и характеристики драйвера, адрес сетевого адаптера). В нижнем правом углу небольшое окно показывает последние сообщения в системном

журнале (вытесняются снизу вверх). Под заголовками "**Мимо**" и "**Взято**" дается сумма отказанных к обработке и обработанных данных, пораздельно числами пакетов и байтов. Справа в тех же строках дано суммарное время работы программы как числом секунд, так и в привычном виде. В центре показаны значения скоростей: **Мгновенная** (за последнюю целую секунду), **Средняя** и **Максимальная** – с момента начала работы программы в текущем отчетном периоде (с момента выдачи прошлого отчета или запуска программы).

Центральная часть описывает детально обработанные пакеты. С левой стороны дано распределение пакетов по их типам **Ethernet-II, IEEE802.3-IPX, IEEE802.2-SNAP, IEEE802.3** с заголовками **IEEE802.2** и прочие под заголовком **Unknown** (в ЛВС ЦЭМИ туда попадают пакеты Novell Netware), причем пакеты формата **Ethernet-II** подразделены на 4 основных протокола: **IP, ARP, IPX** и **Other** (прочие). Правее для каждого типа пакетов указано, сколько из них широковещательных (broadcasting). Еще правее протокол **IP** как самый употребительный подразделен на несколько ведущих: **TCP, UDP, ICMP, Others** (все прочие) и, отдельно, протоколы версий, отличных от версии **4** IP.

Под детальными данными по IP находятся несколько строк, дающих служебную информацию о работе программы. Прежде всего, это общее количество циклов за истекшую секунду и число «длинных» циклов. Строкой ниже аналогичные пары даны за время отчетного периода своими минимальными и максимальными значениями (эти вопросы подробно освещены при обсуждении валидности результатов программы). Еще ниже даны технологические характеристики загрузки внутренних буферов, а столбец справа дает графическую иллюстрацию занятости буферов за последний цикл.

Слева внизу блок информации содержит числа отмеченных системных ошибок при работе программы и интересную информацию о нодах: общее число зарегистрированных нод в актуальной БД, среди них – количество нод, использовавших хоть раз IP-адрес; число нод, активных за последний отчетный период и число нод, для которых отмечено испускание пакетов с более чем одним IP-адресом.

Еще ниже даются текущие режимы работы программы и, пустая в момент «фотографирования», строка ввода с клавиатуры. В

момент получения рисунка программе было задано выдавать отчет каждые 30 минут, переходить на «короткие» циклы уже при 10% заполненности буферов, однако допускать хотя бы один «длинный» цикл на каждые 50 «коротких». Пакеты на HDD не дампировались.

Вторая половина Основного экрана (показана на рис. 11) содержит в верхней части базовые адреса ряда сегментов программы после загрузки в оперативную память ПК, а также некоторые системные индикаторы и указатели, используемые при пошаговой отладке программы.

В нижней части показаны вытеснением снизу вверх текущие обработанные пакеты, в том числе их MAC-адреса назначения (Destination) и источника (Source). Могут быть показаны индикаторы коллизионных пакетов, некорректные КС и длина. Для корректных TCP-пакетов даются оба IP-адреса, протокол (Prt) и порт назначения (Destination Socket, или DSckt).

```
Errs=0000     Conditions=0000   ByteBufSEG=3F1E   WordBufSEG=3F1A
 Buf1=0000    Pkts=0000   Mrk=0000   Max=3164   RefP=0000   RefB=0000
 Buf2=0000    Pkts=0000   Mrk=0000   Max=3516   Cycles=      806

 Destination      Source  Lngth Fr-Typ IP-To            IP-From        Prt DSckt
00000C04771C 00A0CC3D43FF 0062) E2-IP  212.111.064.170<193.232.194.232:TCP\00080
00A0CC3D43FF 00000C04771C 0060) E2-IP  193.232.194.232<212.111.064.170:TCP\03171
00000C04771C 00A0CC3D43FF 0060) E2-IP  212.111.064.170<193.232.194.232:TCP\00080
00000C04771C 00A0CC3D43FF 0409) E2-IP  212.111.064.170<193.232.194.232:TCP\00080
00A0CC3D43FF 00000C04771C 0060) E2-IP  193.232.194.232<212.111.064.170:TCP\03171
00A0CC3D43FF 00000C04771C 0220) E2-IP  193.232.194.232<212.111.064.170:TCP\03171
00A0CC3D43FF 00000C04771C 0060) E2-IP  193.232.194.232<212.111.064.170:TCP\03171
00000C04771C 00A0CC3D43FF 0060) E2-IP  212.111.064.170<193.232.194.232:TCP\00080
00000C04771C 00A0CC3D43FF 0060) E2-IP  212.111.064.170<193.232.194.232:TCP\00080
00A0CC3D43FF 00000C04771C 0060) E2-IP  193.232.194.232<212.111.064.170:TCP\03171
00A0CC3D43FF 00000C04771C 1514) E2-IP  193.232.194.232<216.032.210.139:TCP\03167
00000C04771C 00A0CC3D43FF 0060) E2-IP  216.032.210.139<193.232.194.232:TCP\00080
01000CCCCCCC 0080242C4470 0326) .3-SAP
0180C2000000 0080242C4452 0060) 0026 4242
00400541319B 00000C04771C 1514) E2-IP  193.232.194.058<195.133.154.002:TCP\04990
00000C04771C 00400541319B 0060) E2-IP  195.133.154.002<193.232.194.058:TCP\08101
0180C2000000 0080242C4452 0060) 0026 4242
00A0CC3D43FF 00000C04771C 1514) E2-IP  193.232.194.232<151.196.092.129:TCP\03170
```

Рис. 11. Нижняя часть основного экрана программы наблюдения

Как можно видеть, по каждому пакету выдаются MAC-DA, MAC-SA, длина в байтах, E-Type в оригинальном или расшифрованном виде, а для ряда протоколов также IP-адреса назначения и источника, тип протокола и порт назначения.

Полный вид Основного экрана (назовём его экраном «0») представлен на рис. 12. Цветная иллюстрация гораздо лучше по-

могает воспринимать насыщенный информацией экран. На этом рисунке видно, что текущий снимок сделан 06 октября 2010 года в 18:25:07, перезагрузок с прошлого полуночного запуска не было, работа исполняется в рабочем (а не отладочном) режиме, за истекшие сутки зарегистрирована максимальная скрость 1146,12 КБ/с, средняя скорость 126,85 КБ/с. Обработано 96862 пакета общим объёмом 79157907 байтов, пропущенных пакетов нет. Из Интернета получено 56885 пакетов, отправлено туда 37548 пакетов, внутрисетевые пересылки составили 2429 пакетов.

MAC-адрес используемой сетевой карты есть 004005407E78, работа исполняется в реальном режиме с драйвером NGRPCI. Нод в текущем периоде зарегистрировано 34, в БД их содержится 219. Текущее задействование буферов программы – 27%, максимально за отчётный период – 29%.

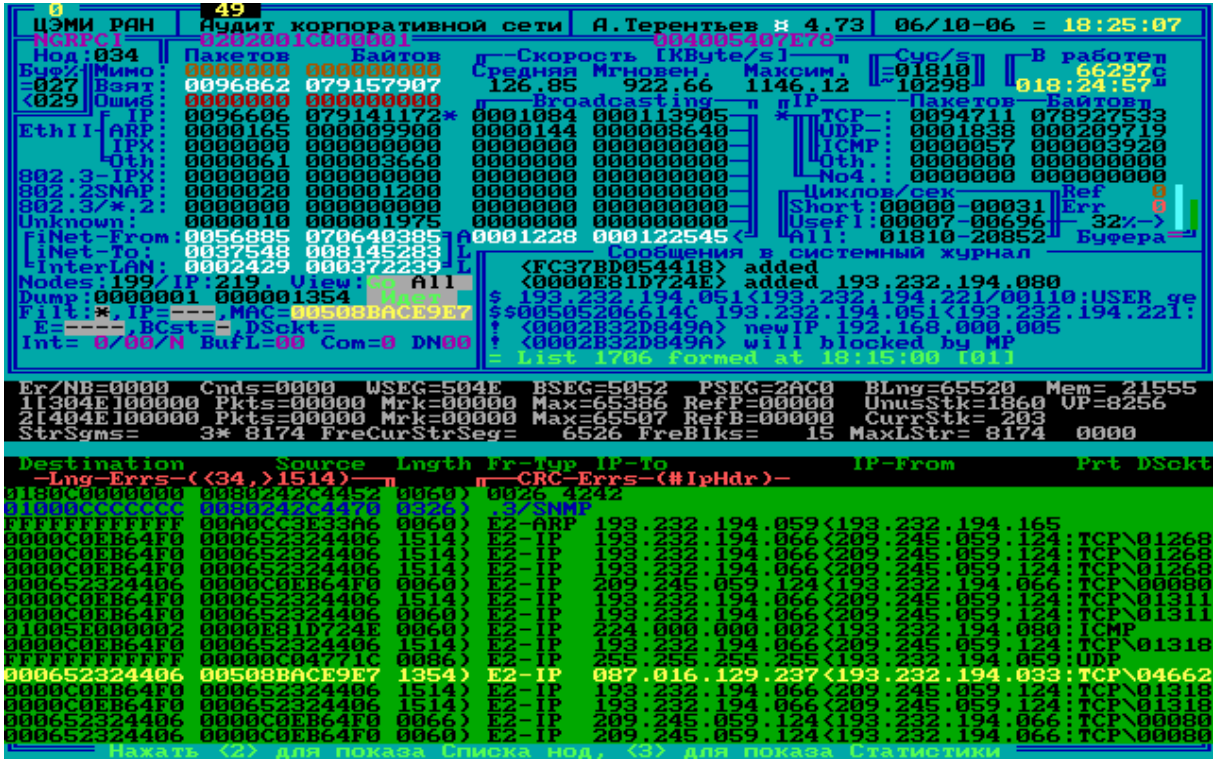

Рис. 12. Полный вид Общего экрана «0»

Голубой столбик в правой части экрана над словом “**Буфера**” показывает текущее задействование буферов на 27%.

За всё время работы программы ситуаций пропуска пакетов не происходило (“**Ref=0**”), сбоев алгоритма также не было (“**Err=0**”).

Из рисунка видно, что задано дампирование по входящему и исходящему MAC-адресу 00508BACE9E7, в нижней части жёлтым цветом показан проходящий пакет, соответствующий этим условиям. Этот пакет пока единственный, записанный на HDD. В этом TCP-пакете нода 193.232.194.33 обратилась к адресу 87.16.129.237 по порту 4662.

По сообщениям в системном журнале, нода 0000E81D724E излучила свой первый IP-адрес 193.232.194.080, нода 0002B32D8490 излучила новый для неё IP-адрес 192.168.0.5 и будет заблокирована Мониторной программой (в этой версии программы мониторинга ещё не вставлен обход блокировки при излучении технологических внутрисетевых адресов 192.168.*.*). Последний отчёт сформирован в кратком виде в 18:15 под номером 1706.

Забегая вперёд, можно сказать, что присутствует активное соединение с Мониторной программой (ярко-белый значок солнышка перед версией программы в строке 1) на соседнем Windows-компьютере.

До окончания показа экрана «0» осталось 49 секунд (в этом режиме вывод на экран очень насыщен, и поэтому время показа ограничено 1 минутой).

В режиме экрана **2** показываются текущие ноды, определившиеся с момента начала 15-минутного (или иного) интервала. Информация берётся из созданной и пополняемой оператором БД нод по их MAC-адресам. Этот режим показа является устанавливаемым по умолчанию, поскольку его информация наиболее интересна в общем случае и минимально нагружает программу мониторинга.

На рисунке 13 видно, что верхние 6 строк эквивалентны соответствующим строкам Основного экрана.

Помимо обработанных за последний отчётный период 77989 пакетов, 71 пакет пропущен. Среднее число циклов – 10294.

На экране показаны в 3 столбца все 92 ноды, определённые за последний отчётный период. По каждой ноде показано подразделение института, фамилия или краткое обозначение ноды, номер

комнаты и 4 последние тетрады IP-адреса в случае, если MAC-адрес ноды есть в БД на момент показа. Если же MAC-адрес отсутствует, он показывается зелёным цветом, и за ним следуют последние тетрады IP-адреса. Так, во втором столбце третьей сверху показана неизвестная нода, имеющая MAC-адрес 000400E41A62 и IP-адрес 193.232.194.238.

Для случаев, когда некоторый MAC-адрес присутствует в БД более одного раза, нода показывается желтым или коричневым цветом. На показанном экране таких нод три – сервер лаборатории Лабренца, господин Бекларян и сервер лаборатории Дыбенко **Exch**. Красная звёздочка слева от имени означает, что сведения о таких нодах переданы Мониторной программе, и предполагается, что такие ноды будут отключены.

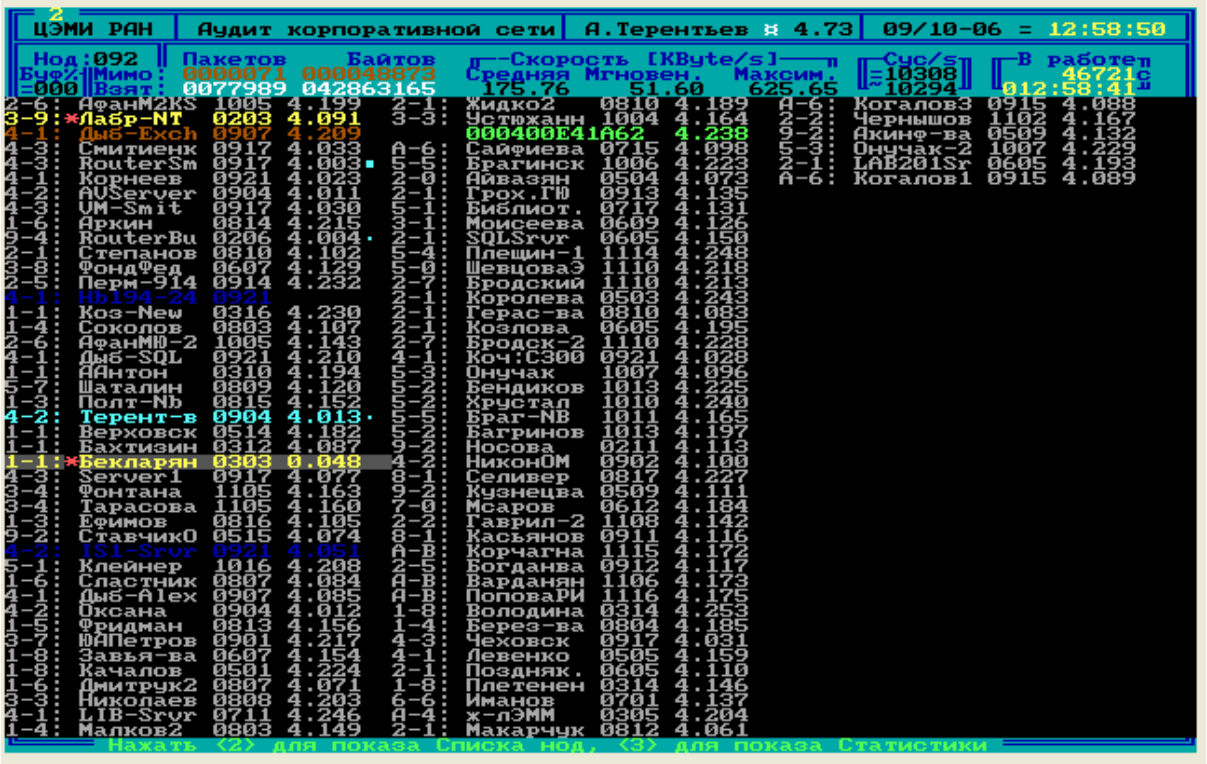

Рис. 13. Экран показа списка нод («2»)

Имеется возможность отслеживать специально заданные флагом в БД компьютеры. Такие строки показываются голубым цветом. На приведённом рисунке 13 такая строка одна, и она отражает компьютер автора данной работы.

Дополнительной информацией можно считать зафиксированные обращения по протоколу POP3 к внутренним и внешним почтовым серверам. Такие ПК дополняются квадратиками после IP-адреса. Мелкий квадратик означает обращение данной ноды по POP3 к внутреннему или внешнему серверу, крупный квадратик – ноду, к которой обращались по протоколу POP3 из Интернета.

Ряд технических нод показан тёмно-синим цветом, напр., IS1-Server (служебный сервер Узла ЦЭМИ РАН) [21].

При создании БД, существует возможность включить до 15 нод в специальную таблицу слежения. Обычно, среди них присутствуют общеинститутские серверы, и, быть может, специальные ПК, состояние включённости которых может воздействовать на общую ЛВС.

На рис. 14 показан режим «**3**» показа состояния выделенных серверов и почты. Показываются 14 выделенных объектов, в том числе маршрутизатор связи с Интернетом Cisco-4000, ПК автора данной работы и 12 общеинститутских серверов.

По каждому объекту выдаются сведения о количестве испущенных и принятых пакетов с начала отчётного периода, а также интервал неактивности в секундах. Так, библиотечный сервер (последняя строка) неактивен в течение 13 секунд, роутер административно-финансового сегмента сети **RouterBu** и ряд других вообще не обнаружил активности за последние 7 минут.

Такие сведения могут быть полезны при частичном нефункционировании сети для определения места возникновения проблемы. Уже отмечалось, что работа наблюдающей станции сетевого мониторинга не зависит от текущего состояния сети; именно это и даёт возможность получения подобных данных.

Нижняя часть экрана «**3**» даёт возможность отследить обращения по сеансам POP3 и FTP. В обычном, сокращённом режиме, как на показанном рисунке, приводятся только строки обращений с интересуемыми атрибутами (точное время до секунды, исходящий IP, IP почтового сервера и порт обращения) пользователей, идентифицируемыми их никами на соответствующих почтовых серверах. В расширенном режиме приводятся также пароли пользователей, например, у первого из указанных пользователей пароль “**zebra**”.

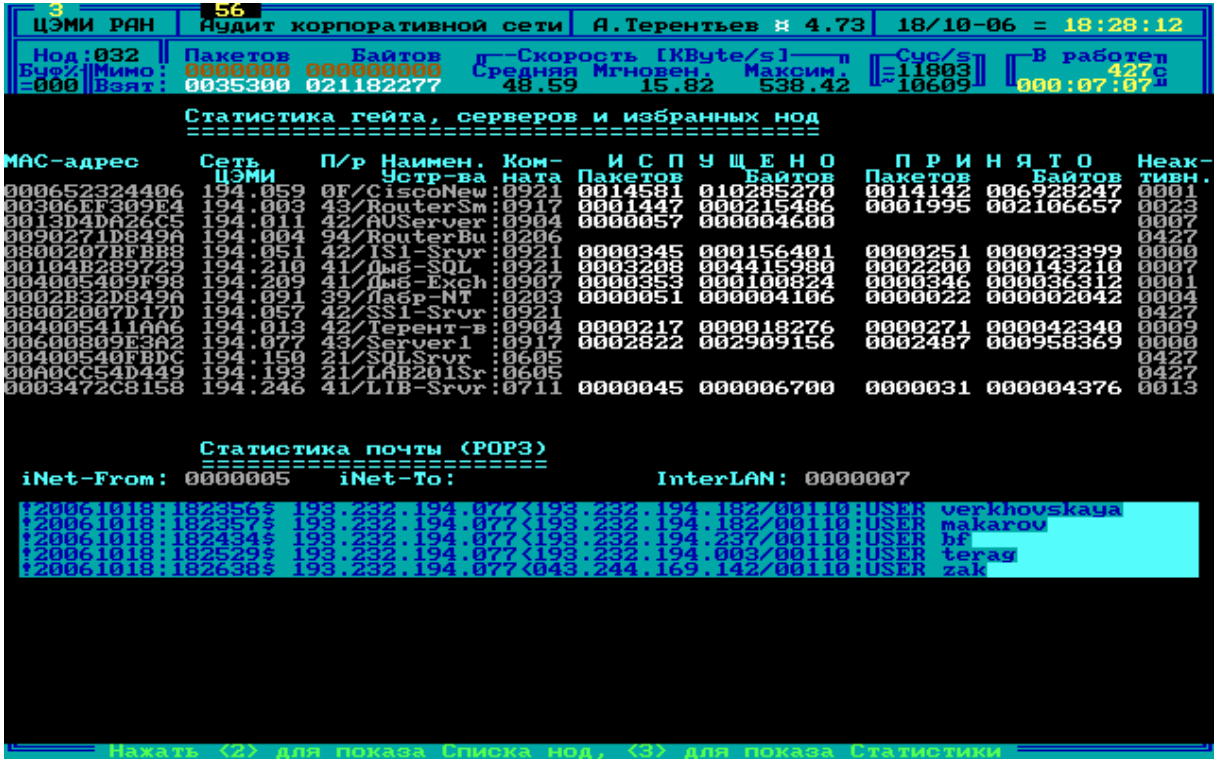

Рис. 14. Экран показа статистики выделенных серверов и почты «3»

```
!20021204:000419$  Аудит корпоративной сети * 4.19 = А.Терентьев
!20021231:090413  Проверка даты и времени...
!20021231:090413  Проверка идентификации...
!20021231:090413  Проверка версии ДОС...
!20021231:090413  Прием имени программы...
!20021231:090413: CNF=<C:\NETWORK\TAMCNET.CFG>
!20021231:090413  Прием параметров ком.строки
!20021231:090413: Parm=</INT=15 /KFULL=4 /HSYN /EODAY /GO /CNDS /3 /PPASS /STMRK>
!20021231:090413  Сводки Краткие, АБСОЛЮТНЫЕ
!20021231:090413  Dump начат
!20021231:090413  Считана БД, нод: 239, IP-нод: 221
!20021231:090413: Макс. известный <TAMC5837.LST>
!20021231:090413  Packet Driver Initialize...
!20021231:090441$ 193.232.194.239<194.067.023.103/00110:USER danilov
!20021231:090441$ 000652324406 193.232.194.239<194.067.023.103:PASS 777777
!20021231:090605$ 193.232.194.209<213.033.180.026/00110:USER march
!20021231:090605$ 000652324406 193.232.194.209<213.033.180.026:PASS MichaeL
!20021231:090811$ 193.232.194.239<194.067.023.103/00110:USER koshevoy
!20021231:090811$ 000652324406 193.232.194.239<194.067.023.103:PASS larisa
!20021231:090900$ 193.232.194.239<194.067.023.103/00110:USER danilov
!20021231:090900$ 000652324406 193.232.194.239<194.067.023.103:PASS 777777
!20021231:090916$ 193.232.194.239<194.067.023.103/00110:USER spivak
!20021231:090916$ 000652324406 193.232.194.239<194.067.023.103:PASS gbvtyjdf[9]
```

Рис. 15. Протокол работы с данными почтовых сеансов

[9] Комбинация латинских букв, соответствующая слову “пименова” на русской раскладке.

На рис. 15 представлен фрагмент протокола сетевого мониторинга, включающего почтовых пользователей, адреса почтовых серверов и пароли. Сведения достаточно давние (декабрь 2002 года), так что опасений скомпрометировать пользователей у автора нет.

IP-адрес **193.232.194.239** в то время соответствовал внутреннему почтовому серверу института. Все обращения были выполнены к этому серверу по стандартному порту **110**.

Приведём здесь ещё один пример Основного экрана (рис. 16). На этом рисунке показана реакция программы сетевого мониторинга на некоторые пакеты.

В этом примере из сети (на самом деле с HDD с помощью программы TAMDRVR) считано и отображено 6 пакетов. Первые два из них представляют собой ARP-запрос и ARP-ответ, и являются копией изображённых ниже на рис. 26, вторые два – обычные TCP-пакеты. Два последних пакета являются некорректными. В пятом нарушена контрольная сумма, что показывает знак "**#**", стоящий в поле с заголовком "**CRC Err (#IpHdr)**", шестой пакет с нарушением длины пакета (значок "**<**" в поле под заголовком "**Lng Errs**"); на самом деле он коллизионный, хоть и не соблюдено правило фиксации коллизионных пакетов – не менее 60 символов.

Ошибочные пакеты, как легко видеть, выделены красным цветом.

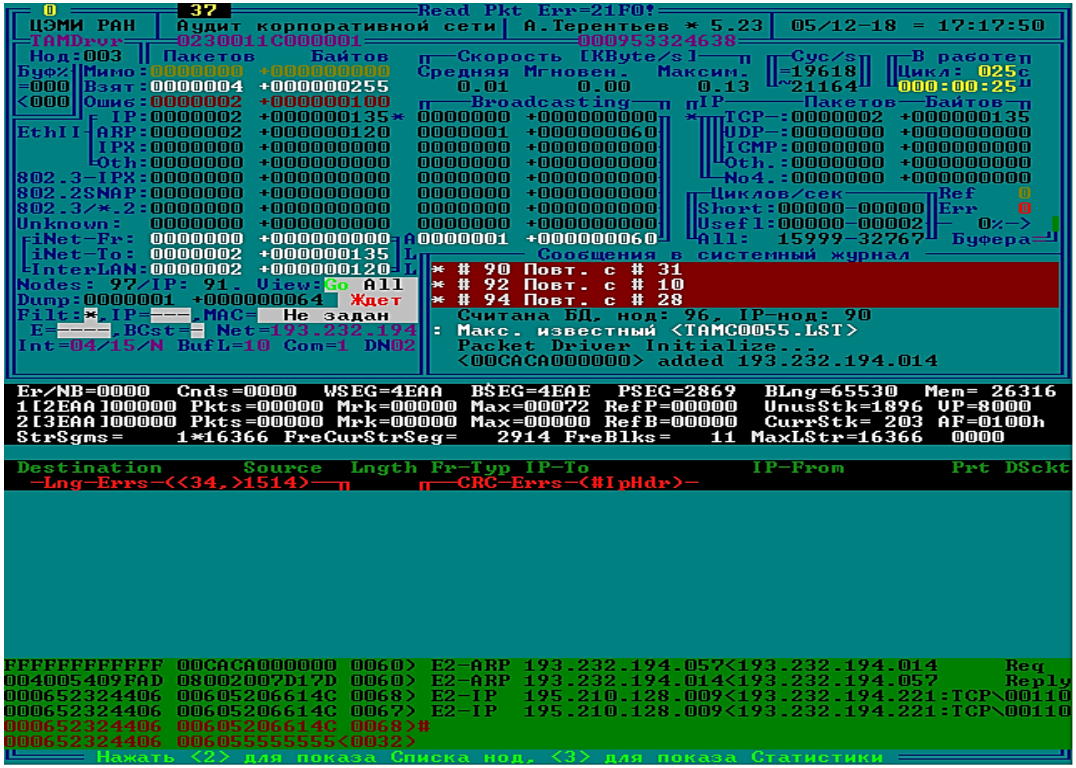

Рис. 16. Пример экрана «0» для некоторых пакетов

Последний из описываемых есть экран вида «**1**» (рис. 17). Эта область видеопамяти, помимо обязательной верхней части, содержит краткий Help по командам, допустимым для ввода с клавиатуры, а также справочник по цветовому выделению нод на экране «**2**».

В справочнике не учтена команда “**$**”, формирующая скриншот текущего экрана в специальном формате **.SAV**, а также команда “**!**”, имитирующая ошибку вычислений для отладки блока обработки аварийных ситуаций.

Значительная часть команд разрешена к подаче только в режиме экрана «**0**». Команда “**$**” может быть подана в любом из экранов.

Рис. 17. Справочный экран по командам оператора «1»

2.4. BAT-файлы и возможные коды завершения программы

Возможные **коды завершения** программы показаны на рис. 18.

```
001 = Конец дня, выход без ожидания для спецветви BAT-файла
      Выходы из цикла
000 = Нажатие Esc, выход с прерыванием BAT-файла
002 = Отключение ПК
010 = Сбой вычислителя, нужен повторный вход
020 = ErrOnErr, сб.вычислений в процессе обработки сб.выч.
101 = Сбой КС авторизации
102 = Неверна область Env
103 = Неверно имя программы
105 = Невозможно открытие LOG-файла
106 = Невозможно открытие DMP-файла
110 = Общая ошибка параметров
112 = Нераспознанная конструкция параметра
113 = Нет пробела в конце строки параметров
118 = Недостаточно памяти для динамических массивов
120 = Ошибки в БД
130 = Ошибка пакетного драйвера сетевого адаптера
```

Рис. 18. Возможные коды завершения программы TAMCNET

BAT-файл запуска программы может быть организован, например, так, как показано на рис. 19.

```
@ECHO OFF
SET NAM=
IF .%1.==.. GOTO Cycle
IF NOT .%1.==.N. GOTO Help
IF .%2.==.. GOTO Help
SET NAM=%2
:Cycle
IF .%NAM%.==.. GOTO First
:Next
tamcnet /INT=15 /KFULL=4 /HSYN /EODAY /LST1=%NAM% /GO /2 /COM=1
/DNODES=2 /STMRK /NET=193.232.194
GOTO Result
:First
tamcnet /INT=15 /KFULL=4 /HSYN /EODAY /GO /2 /COM=1 /DNODES=2 /STMRK
rem /DNODES=14 /NET=193.232.194
:Result
IF ERRORLEVEL 99 GOTO Her
IF ERRORLEVEL 21 GOTO TFirst
IF ERRORLEVEL 20 GOTO ErOnEr
IF ERRORLEVEL 3 GOTO TFirst
IF ERRORLEVEL 2 GOTO OK
IF ERRORLEVEL 1 GOTO EoDay
GOTO Zero
:ErOnEr
tamdate ErOnEr >>TAMCNET.LER
:TFirst
IF EXIST TAMCNET.DBN GOTO NoRstDB1
IF EXIST TAMCNET.BAK GOTO RstDB1
ECHO === БД отсутствует. Из копии восстановить НЕВОЗМОЖНО ===
GOTO OK
:RstDB1
COPY TAMCNET.BAK TAMCNET.DBN
:NoRstDB1
GOTO First
:EoDay
IF EXIST TAMCNET.DBN GOTO NoRstDB2
IF EXIST TAMCNET.BAK GOTO RstDB2
ECHO =*= БД отсутствует. Из копии восстановить НЕВОЗМОЖНО =*=
GOTO OK
:RstDB2
COPY TAMCNET.BAK TAMCNET.DBN
:NoRstDB2
call tambneu.bat C:\REPORTS
GOTO Cycle
:Help
ECHO = Для вызова используйте один из вариантов:
ECHO = tambne {без параметров} - стартует исходя из текущих условий
ECHO = tambne N xxxxx - стартует начиная отчет с номером xxxxx
GOTO OK
:Her
ECHO =**= Внимание! Неустранимая ошибка.
:OK
```

Рис. 19. Основной BAT-файл TAMBNE2 для программы TAMCNET

Вспомогательный BAT-файл показан на рис. 20. Поясним, что переменная TMP должна указывать на любой временный пустой каталог на компьютере.

```
@ECHO OFF
copy tambn.ba/a + tamclast.num/a %TMP%\tambr.bat
call %TMP%\tambr.bat
REM Теперь переменная NAM приобрела значение
REM из 4х цифр - номер последнего TAMCnnnn.LST
arj m %TMP%\A%NAM% tamcnet.bak tamcnet.log
arj a %TMP%\A%NAM% tamcnet.dbn
arj m %TMP%\A%NAM% tamc????.lst
copy /b %TMP%\A%NAM%.ARJ %1
del %TMP%\A%NAM%.ARJ
```

Рис. 20. Вспомогательный BAT-файл TAMBNEU.BAT

```
@ECHO OFF
SET NAM=
```

Рис. 21. Вспомогательный файл TAMBN.BA

Обратим особое внимание на то, что в файле TAMBN.BA вторая строка заканчивается равенством, т.е. **отсутствует символ перевода строки**! Поскольку файл TAMCLAST.NUM всегда содержит в текстовом виде номер последнего сделанного отчёта, результат первых двух строк рис. 20 будет в том, что переменная NAM приобретёт значение последнего номера отчёта, и таким образом архив будет сформирован с именем "**A*nnnn*.ARJ**", где nnnn – номер последнего отчёта за этот день.

2.5. Оперативная БД

Этот файл является как входным в начале работы программы, так и выходным по ее завершении. Файл содержит в текстовом виде перечень MAC-адресов, IP-адресов, восьми букв условного текстового наименования ноды и одного байта ее технологических характеристик. Фрагмент этого файла можно видеть на рис. 22, расшифровка характеристик почти соответствует соответствующему байту в отчетах, рассматриваемых чуть ниже.

Безусловно, этот файл является самым важным для работы программы наблюдения, поскольку по каждому поступившему пакету просматривается вся база от начала до нахождения или ненахождения строки соответствия пакету. При нахождении фиксируется наличие пакета, при отсутствии соответствия в БД до-

бавляется строка. Ноды, чаще других испускающие пакеты, время от времени приходится перемещать в начало БД для сокращения времени обработки; ряд случайных строк, соответствующих коллизионным пакетам, исключается.

Периодически также исключаются строки, несущие устарелую информацию (например, о ранее существовавшей комбинации MAC-SA и IP-адреса, если достоверно известно, что такая комбинация уже неактуальна).

```
00000C04771C 07 255.255.255.255 Cisco-4K
00104B289729 01 193.232.194.210 П:WEBSQL
00400540FBC8 03 193.232.194.211 П:NTSrvr
0000C0F347F8 03 193.232.194.074 П:SergeP
0000C0F347F8 03 193.232.194.090 П:SergeP
0000E8EC1A5D 03 193.232.194.069 П:Ego-va
00400540FBCD 03 193.232.194.107 GOLSHTN
0020AFF61A62 21 193.232.194.033 Server2.
0080242C4470 41 193.232.194.035 Switch35
00A0CC3E9A70 03 193.232.194.247 П:DevSrv
00A0CC3E9A70 01 193.232.194.085
08002007D17D 01 193.232.194.057 SS1.
0800207BFBB8 01 193.232.194.051 IS1.
00A0CC3E269E 01 193.232.194.010 Аносова
008048AE590D 03 193.232.194.011
008048AE590D 03 193.232.194.012 Недзвецк
00A0CC3D43F8 01 193.232.194.014 Яркин
52544C17FD43 01 193.232.194.017 ИСЭСП-Нb
00400540FBE5 03 193.232.194.034 S:Горш-н
0000C06365F0 01 193.232.194.039 Малкова
0000C0EB64F0 03 193.232.194.066 Греб-604
0000C0CE4BF8 03 193.232.194.068 Б:ganna
004005407E78 03 193.232.194.073 Айвазян
00600809E3A2 01 193.232.194.077 Server1.
00A0CC3E33A9 23 193.232.194.075 Перминов
00A0CC3E33A9 03 193.232.193.003 Перминов
```

Рис. 22. Фрагмент оперативной БД (первые 4 позиции)

В приведенном примере можно видеть, что уже 4-я и 5-я строки имеют одинаковый MAC-SA, но разные IP-адреса (правильный адрес первый, второй – следствие сетевой коллизии). В последних приведенных строках также одинаковый MAC-SA, но разные IP-адреса. Обе строки верны: сеть **193.232.194.*** – общеинститутская ЛВС, сеть **193.232.193.*** – строящаяся сеть АТМ. ПК с указанным MAC-адресом участвует в обеих сетях. Первым в списке стоит

безусловный лидер по пакетам – маршрутизатор Cisco-4000, который внутри ЛВС испускает все пакеты, приходящие из Интернета.

2.6. Выходные отчеты

Программа наблюдения способна периодически выдавать текстовые отчеты о наблюденной информации. Период выдачи определяется параметром вызова, по умолчанию – 15 минут. Краткий формат отчета содержит только общую часть, полный – еще и подробный перечень (согласно нормативной БД) нод с их активностью за отчетный период и списком характеристик. Программа способна формировать отчеты с заранее заданным интервалом, причем возможно указать периодичность выдачи полных отчетов.

На рис. 23 можно видеть пример реального полного отчета за 12 октября 2000 г. по состоянию на 17 часов, причем предыдущий отчет был 900 секунд (15 минут) назад. Строки с **#00** по **#50** включительно присутствуют как в кратком, так и в полном отчетах, и содержат информацию исключительно за отчетный период; последующие строки присутствуют только в полных отчетах и включают информацию от одного полного отчета до другого.

Как легко видеть, обязательная часть отчета по сути фиксирует информацию, отображаемую на экране и рассмотренную выше. Вторая часть отчета представляет детальную информацию об активности нод за интервал между полными отчетами и содержит два стобца чисел – число переданных байт всего и нешироковещательных пакетов в частности, – а также бинарные признаки того, какие типы пакетов испускались нодой под указанным IP-адресом. Так, строки **001** и **012** второй части указанного отчета свидетельствуют о том, что маршрутизатор Cisco-4000 и Ethernet-Switch обмениваются информацией по протоколу **SNAP** (более ни у одной ноды такого протокола не встречается), что вызвало явный интерес у руководителей лабораторий, отвечающих за работу этих устройств.

Другим интересным фактом даже этого одного отчета является то, что существуют несколько нод (строки **045** и **048**), использующих один и тот же IP-адрес, правда, в отчетный период указанного дня активность второй из отмеченных нод не выявлена.

Особый интерес представляют строки **208** и **209**, явно соответствующие коллизионным ситуациям в сети. Строка **210** является примером плохо настроенной ноды, испускающей IP-пакеты с нулевым IP-адресом (что является грубым нарушением сетевых правил).

Эти отчеты являются базовой информацией, используемой в последующем анализе событий. Введенная с лета 2000 года принудительная выдача полного отчета в 00 минут 00 секунд наблюдающей программой по сути автоматически синхронизирует появление очередного полного отчета точно в ближайший час. При правильной установке параметров **/Int** периодичности выдачи отчетов и **/Kfull** кратности выдачи очередного полного отчета, например, **/Int=15 /Kfull=4**, гарантируется автоматическое получение полного отчета каждый час и 3 кратких отчета в 15, 30 и 45 минут каждого часа.

```
#00 ЦЭМИ РАН *  Аудит корпоративной сети * 1.8 = А.Терентьев
#02 Полный, поясняющий файл отчета <TAMC4678.LST>, серия начата с 4611
#04 Программа запущена 12/10-00 в 00:00:28
#05 Текущее время      12/10-00 = 17:00:00, работает     61172с
#06 В цикле     900сек.; всего    16ч59м32с
#07 Отчет сформирован  по признаку   8
#10 Взято пакетов:  50554,        Байтов: 21855509
#11 Мимо пакетов:      69,        Байтов:    64116
#12 Скорость максимальная:  196.40 Kb/s;   Средняя:  23.72 Kb/s
#14 ВД:  213,  ПК в работе:   88
#17 Циклов в секунду минимально:     219;     максимально:     313
#18 Ситуаций пропуска пакетов:      42
#20                  К О М П О Н Е Н Т Ы   Т Р А Ф И К А
#20              По типу трафика        В т.ч. широковещательные
#20             Пакетов   Байтов         Пакетов   Байтов
#21 EtherII-IP:    48269 21552395             340    52981
#22 EtherII-ARP:      279    16740             202    12120
#23 EtherII-IPX:       0        0               0        0
#24 EtherII-ост:       91     5477               0        0
#25 IEEE802.3IPX:     912   203397             565    70497
#26 IEEE802.2SNAP      29     9319               0        0
#27 802.3/802.2:       15      900              15      900
#28 Не опознаны:      959    67281               0        0
#40  =  Компоненты IP-трафика
#41 IPv4/TCP:     45675 21211439
#42 IPv4/UDP:      2359   318008
#43 IPv4/ICMP:      235    22948
#44 IPv4/Other:       0        0
#45 IPvers.#4:        0        0
#50 - - - - - - - - - -
#80            Сведения о нодах (MAC-адресах) и их трафике
001.00000C04771C *255.255.255.255 Cisco-4K  56521734 56461709 ++ -+-- ++++
...
012.0080242C4470  193.232.194.035 Switch35     19256      434 ++ -+-- ---+
...
045.0020AF3F67AF *193.232.194.089 Лей6-NT       1248        0 ++ --+- --++
046.0020AF3F67AF *193.232.194.090                  0        0 -- ---- --++
047.0020AF3F67AF *193.232.194.091 Лей6-NT       2602     2602 -+ ---- --++
048.00E098161DEE  193.232.194.089 Макаров          0        0 -- ---- ---+
...
208.0000E8EB76A4  170.170.170.170                  0        0 -- ---- ---+
209.004005413184  193.168.170.170                  0        0 -- ---- ---+
210.525400DB01DA  000.000.000.000              11716     1368 -+ --+- ---+
211.0000C0DA64F0   No IP-traffic                  0        0 -- ---- ----
212.0060B0718111   No IP-traffic                  0        0 -- ---- ----
213.525400DB008A   No IP-traffic               2312        0 -+ +-+- +---
------ Признаки в битовой карте (слева направо) ----
 + Присутствие трафика EthernetII/ARP   - - - - - - - - - - +| |||| ||||
 + Наличие исход. пакетов сейчас        - - - - - - - - - - -+ |||| ||||
 + Присутствие трафика IEEE802.3/802.2  - - - - - - - - - - - +||| ||||
 + Присутствие трафика IEEE802/SNAP     - - - - - - - - - - - +|| ||||
 + Присутствие трафика IEEE802.3/IPX    - - - - - - - - - - - -+| ||||
 + Присутствие трафика EthernetII/IPX   - - - - - - - - - - - - + ||||
 + Присутствие трафика EthernetII/Oth.  - - - - - - - - - - - - +|||
 + Признак сервера (задается вручную)   - - - - - - - - - - - - -+||
 + Наличие более 1 IP-адреса в пакетах  - - - - - - - - - - - - +|
 + Присутствие трафика EthernetII/IP    - - - - - - - - - - - - -+
Конец отчета <TAMC4678.LST>
```

Рис. 23. Формат и основные части отчета программы наблюдения

2.7. Просмотр дампированных пакетов

Дампированные на HDD пакеты при работе программы мониторинга записываются в единый дамп-файл с именем TAMCNET.DMP. Для разграничения пакетов принято, что перед информацией пакета дописываются 4 байта, **55AA**h в первых из

них и последующая информационная длина пакета в двух последующих байтах.

Разумеется, поскольку принятая система кодирования сетевых пакетов, в отличие от машинного представления чисел, предполагает последовательное указание байтов, то длина пакета оказывается инвертированной. Так, на рис. 24 изображен результат программы просмотра пакетов TamView.EXE, в котором показано 2 пакета с длиной каждого 74 байта, что соответствует шестнадцатиричному значению **004A**h, в то время как на диск будет записана последовательность байтов **4A00**h.

При показе пакетов отдельной строкой выводится заголовок пакета, в котором даны идентификационный признак **55AA**h, длина в инвертированной форме (в данном случае **4A00**h), десятичный и шестнадцатиричный виды смещения начала пакета относительно начала файла, последовательный номер пакета и его десятичная длина. Далее идут байты дампированного пакета, сначала **MAC-DA** и **MAC-SA**, затем два байта типа протокола, если можно, его расшифровка, и для TCP/IP-пакетов результирующий и исходный IP-адреса. В конце для некоторых типов пакетов (TCP, ICMP и т.п.) присутствует расшифровка типа пакета. Далее строчками идут остальные символы пакета, по 16 байт в строке, в шестнадцатиричном виде, и справа эти же символы в текстовом виде. При подготовке данных к печати выбран специальный режим, когда в текстовой части служебные символы заменяются точками, чтобы не сбивался формат изображения при распечатке.

На рис. 24 показано два пакета, исходный и обратный, образующиеся в сети при выдаче команды пингования интересуемой ноды. В изображённом случае нода 193.232.194.126 посылает пинг на ноду 193.232.194.97 и получает обратно результат.

```
:  55AA 4A00   Offs= 0 (00000000h)   Pkt= 1   L= 74
   0060088D88D3 004005411AA6 0800=E2-IP  193.232.194.097<193.232.194.126:ICMP
   45 00 00 3C 8A 00 00 00 20 01 08 10 C1 E8 C2 7E   E..<Љ... ...БиВ~
   C1 E8 C2 61 08 00 47 5C 01 00 05 00 61 62 63 64   БиВa..G\....abcd
   65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74   efghijklmnopqrst
   75 76 77 61 62 63 64 65 66 67 68 69               uvwabcdefghi
 : 55AA 4A00   Offs= 78 (0000004Eh)   Pkt= 2   L= 74
   004005411AA6 0060088D88D3 0800=E2-IP  193.232.194.126<193.232.194.097:ICMP
   45 00 00 3C EC 4F 00 00 80 01 45 C0 C1 E8 C2 61   E..<мO..Ъ.ЕАБиВa
   C1 E8 C2 7E 00 00 4F 5C 01 00 05 00 61 62 63 64   БиВ~..O\....abcd
   65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74   efghijklmnopqrst
   75 76 77 61 62 63 64 65 66 67 68 69               uvwabcdefghi
```

Рис. 24. Показ дампированных на диск пакетов команды PING

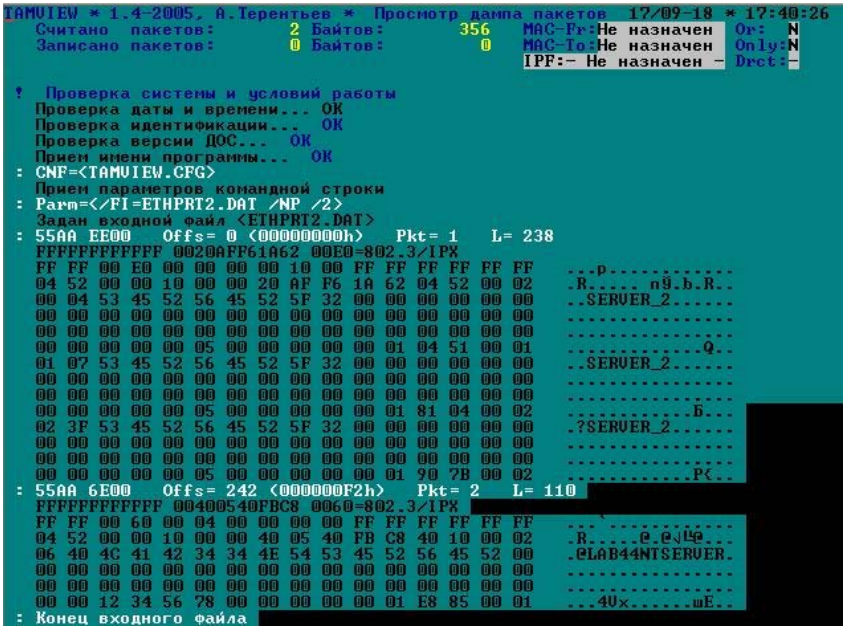

Рис. 25. Показ дампированных broadcasting-пакетов

На рис. 25 изображён показ broadcasting-пакетов, излучаемых двумя серверами общего доступа на всю ЛВС. Формат пакетов – IEEE802.3/IPX.

На рис. 26 изображён показ ARP-пакета и ответный пакет. Ноутбук с адреса 193.232.194.14 (**C1 E8 C2 0E**), имеющий MAC-адрес **00 40 05 40 9F AD**, запрашивает у всех (**FF FF FF FF FF FF**) сетевых адресов MAC-адрес, соответствующий IP-адресу 193.232.194.57 (**C1 E8 C2 39**) в первом пакете. В ответном пакете сообщается требуемый MAC-адрес (**08 00 20 07 D1 7D**).

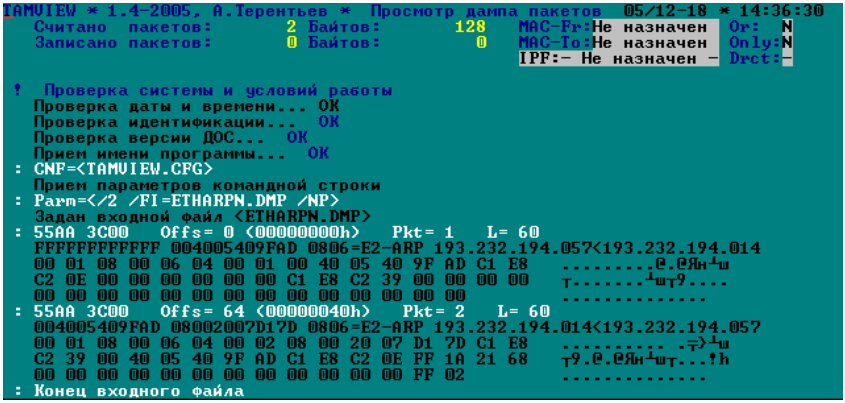

Рис. 26. Показ ARP-запроса и ответа

Приведём для иллюстрации также пакеты, организуемые по протоколу POP3 общения с почтовым сервером. На рис. 27 показаны информационные пакеты такого сеанса (служебные пропущены), в которых видны текстовые сообщения (подчёркнуты) между сервером POP.LIST.RU на адресе 193.232.193.52 и пользователем **tam** на компьютере 193.232.194.13 с паролем **tam-PSW**.

Видно, как устанавливается связь с сервером, запрашивается пользователь (USER), сообщается имя пользователя, запрашивается пароль, выдаётся пароль, сообщается, что на сервере текущих писем **0**, запрашивается статистика, сообщается о нулевой статистике и, наконец, заканчивается сеанс связи.

Из 17 пакетов показаны 11, в которых имеется содержательная часть. Остальные пакеты, являясь техническими подтверждениями связи, смысловой нагрузки не несут.

```
TAMVIEW * 1.4-2005, А.Терентьев *  Просмотр дампа пакетов  * 08/12-1419:10:56
 !  Проверка системы и условий работы
   Проверка даты и времени...
   Проверка идентификации...
   Проверка версии ДОС...
   Прием имени программы...
 : CNF=<TAMVIEW.CFG>
   Прием параметров командной строки
 : Parm=</2 /FI=ETHPOP3D.DAT /LOG=EthPop3D.LOG>
   Задан входной файл <ETHPOP3D.DAT>
   Задан файл протокола <ETHPOP3D.LOG>
   55AA 4700   Offs= 128 (00000080h)   Pkt= 3   L= 71
   000652324406 00508BACF971 0800=E2-IP  193.232.193.052<193.232.194.013:UDP
   45 00 00 39 00 41 00 00 80 11 33 60 C1 E8 C2 0D  E..9.A..A◀3`┴ш┬
   C1 E8 C1 34 FD 8A 00 35 00 25 C4 50 6C 47 01 00  ┴ш┴4¤K.5.%─PlG .
   00 01 00 00 00 00 00 00 03 70 6F 70 04 6C 69 73  . ......└pop┘lis
   74 02 72 75 00 00 01 00 01                       t┐ru.. .
 : 55AA 5700   Offs= 203 (000000CBh)   Pkt= 4   L= 87
   00508BACF971 000652324406 0800=E2-IP  193.232.194.013<193.232.193.052:UDP
   45 00 00 49 20 84 40 00 FF 11 54 0C C1 E8 C1 34  E..I Д@..◀T.┴ш┴4
   C1 E8 C2 0D 00 35 FD 8A 00 35 5C 8A 6C 47 85 80  ┴ш┬..5¤K.5\КlGEA
   00 01 00 01 00 00 00 00 03 70 6F 70 04 6C 69 73  . . ....└pop┘lis
   74 02 72 75 00 00 01 00 01 C0 0C 00 01 00 01 00  t┐ru.. . └.. . . .
   00 00 3C 00 04 D9 45 8B 4E                       ..<.┘┘EЛN
: 55AA 7300   Offs= 490 (000001EAh)   Pkt= 8   L= 115
   00508BACF971 000652324406 0800=E2-IP  193.232.194.013<193.232.193.052:TCP
   45 00 00 65 20 94 40 00 40 06 12 EC C1 E8 C1 34  E..e Ф@.@─↕ь┴ш┴4
   C1 E8 C2 0D 00 6E 04 A4 28 D5 F1 FE 8B F5 29 16  ┴ш┬..n┘д(┌ёЛї)┬
   50 18 61 08 B6 C6 00 00 2B 4F 4B 20 51 70 6F 70  P↑a◘╢╞..+OK Qpop
   70 65 72 20 28 76 65 72 73 69 6F 6E 20 34 2E 31  per (version 4.1
   2E 30 29 20 61 74 20 76 73 31 2E 63 65 6D 69 2E  .0) at vs1.cemi.
   72 73 73 69 2E 72 75 20 73 74 61 72 74 69 6E 67  rssi.ru starting
   2E 20 20 0D 0A                                   .  ..
 : 55AA 4000   Offs= 609 (00000261h)   Pkt= 9   L= 64
   000652324406 00508BACF971 0800=E2-IP  193.232.193.052<193.232.194.013:TCP
```

```
   45 00 00 32 08 21 40 00 80 06 EB 91 C1 E8 C2 0D   |E..2◘!@.A─ыC┴ш┬
   C1 E8 C1 34 04 A4 00 6E 8B F5 29 16 28 D5 F2 3B   |┴ш┴4┘д.nЛї)┬(╒Є;
   50 18 FF C2 AA 2C 00 00 55 53 45 52 20 74 61 6D   |P↑.┬к,..USER tam
   0D 0A                                             |..
: 55AA 5600   Offs= 741 (000002E5h)   Pkt= 11   L= 86
   00508BACF971 000652324406 0800=E2-IP  193.232.194.013<193.232.193.052:TCP
   45 00 00 48 20 96 40 00 40 06 13 07 C1 E8 C1 34   |E..H Ц@.@.─‼●┴ш┴4
   C1 E8 C2 0D 00 6E 04 A4 28 D5 F2 3B 8B F5 29 20   |┴ш┬..n┘д(╒Є;Лї)
   50 18 61 08 B5 43 00 00 2B 4F 4B 20 50 61 73 73   |P↑a◘╡C..+OK Pass
   77 6F 72 64 20 72 65 71 75 69 72 65 64 20 66 6F   |word required fo
   72 20 74 61 6D 2E 0D 0A                           |r tam...
 : 55AA 4400   Offs= 831 (0000033Fh)   Pkt= 12   L= 68
   000652324406 00508BACF971 0800=E2-IP  193.232.193.052<193.232.194.013:TCP
   45 00 00 36 08 22 40 00 80 06 EB 8C C1 E8 C2 0D   |E..6◘"@.A─ыМ┴ш┬
   C1 E8 C1 34 04 A4 00 6E 8B F5 29 20 28 D5 F2 5B   |┴ш┴4┘д.nЛї) (╒Є[
   50 18 FF A2 12 4E 00 00 50 41 53 53 20 74 61 6D   |P↑.в↕N..PASS tam
   2D 50 53 57 0D 0A                                 |-PSW..
 : 55AA 6E00   Offs= 903 (00000387h)   Pkt= 13   L= 110
   00508BACF971 000652324406 0800=E2-IP  193.232.194.013<193.232.193.052:TCP
   45 00 00 60 20 97 40 00 40 06 12 EE C1 E8 C1 34   |E..` Ч@.@.─↕ю┴ш┴4
   C1 E8 C2 0D 00 6E 04 A4 28 D5 F2 5B 8B F5 29 2E   |┴ш┬..n┘д(╒Є[Лї).
   50 18 61 08 16 98 00 00 2B 4F 4B 20 74 61 6D 20   |P↑a◘┬Ш..+OK tam
   68 61 73 20 30 20 76 69 73 69 62 6C 65 20 6D 65   |has 0 visible me
   73 73 61 67 65 73 20 28 30 20 68 69 64 64 65 6E   |ssages (0 hidden
   29 20 69 6E 20 30 20 6F 63 74 65 74 73 2E 0D 0A   |) in 0 octets....
 : 55AA 3C00   Offs= 1017 (000003F9h)   Pkt= 14   L= 60
   000652324406 00508BACF971 0800=E2-IP  193.232.193.052<193.232.194.013:TCP
   45 00 00 2E 08 23 40 00 80 06 EB 93 C1 E8 C2 0D   |E...◘#@.A─ыУ┴ш┬.
   C1 E8 C1 34 04 A4 00 6E 8B F5 29 2E 28 D5 F2 93   |┴ш┴4┘д.nЛї).(╒ЄУ
   50 18 FF 6A 31 F7 00 00 53 54 41 54 0D 0A         |P↑.j1ў..STAT..
 : 55AA 3F00   Offs= 1081 (00000439h)   Pkt= 15   L= 63
   00508BACF971 000652324406 0800=E2-IP  193.232.194.013<193.232.193.052:TCP
   45 00 00 31 20 98 40 00 40 06 13 1C C1 E8 C1 34   |E..1 Ш@.@.─‼ ┴ш┴4
   C1 E8 C2 0D 00 6E 04 A4 28 D5 F2 93 8B F5 29 34   |┴ш┬..n┘д(╒ЄУЛї)4
   50 18 61 08 91 66 00 00 2B 4F 4B 20 30 20 30 0D   |P↑a◘Cf..+OK 0 0.
```

```
   0A                                                    |.
 : 55AA 3C00   Offs= 1148 (0000047Ch)   Pkt= 16   L= 60
   000652324406 00508BACF971 0800=E2-IP  193.232.193.052<193.232.194.013:TCP
   45 00 00 2E 08 24 40 00 80 06 EB 92 C1 E8 C2 0D   |E...◘$@.А─ыТ┴ш┬.
   C1 E8 C1 34 04 A4 00 6E 8B F5 29 34 28 D5 F2 9C   |┴ш┴4┘д.nЛї)4(╒ЄЬ
   50 18 FF 61 2B F0 00 00 51 55 49 54 0D 0A         |P↑.a+Ё..QUIT..
 : 55AA 6700   Offs= 1212 (000004BCh)   Pkt= 17   L= 103
   00508BACF971 000652324406 0800=E2-IP  193.232.194.013<193.232.193.052:TCP
   45 00 00 59 20 99 40 00 40 06 12 F3 C1 E8 C1 34   |E..Y Щ@.@─↕е┴ш┴4
   C1 E8 C2 0D 00 6E 04 A4 28 D5 F2 9C 8B F5 29 3A   |┴ш┬..n┘д(╒ЄЬЛї):
   50 18 61 08 3F 75 00 00 2B 4F 4B 20 50 6F 70 20   |P↑a◘?u..+OK Pop
   73 65 72 76 65 72 20 61 74 20 76 73 31 2E 63 65   |server at vs1.ce
   6D 69 2E 72 73 73 69 2E 72 75 20 73 69 67 6E 69   |mi.rssi.ru signi
   6E 67 20 6F 66 66 2E 0D 0A                        |ng off...
: Конец входного файла
```

Рис. 27. Показ части дампированных на диск пакетов сеанса POP3

Как видим из показанного, передача паролей в сеансе POP3 ничем не защищена. Программа сетевого мониторинга в специальном режиме показывает не только адреса обращения, как на рис. 14, но и пароли. В данном примере использован, разумеется, временный пароль.

Аналогичная структура пакетов используется в сеансах FTP.

Все возможности программы просмотра TamView.exe описаны отдельно ниже.

2.8. Средства организации круглосуточной работы

Выше было указано, что программа наблюдения имеет возможность завершать свой рабочий цикл немедленно после формирования отчета в 00:00 очередных суток. При этом она формирует код завершения **1** в отличие от других кодов в других ситуациях. Это дает возможность использовать программу наблюдения в круглосуточном цикле работы с перерывом в 00:00:00 для автоматического оформления конца рабочего дня.

Методами BAT-файлов MS-DOS в конце дня организуется формирование ежедневного ARJ-архива со всеми отчетами, протоколом работы и копией текущего состояния оперативной БД, очистка текущего каталога от протокола и отчетов и продолжение работы прерванного цикла наблюдения. Можно отметить по строке **#04** рис. 23, что все эти операции занимают весьма немного времени (в приведенном примере – 28 секунд). За целые сутки формируется, таким образом, 96 отчетов, из которых 24 полных.

Разумеется, архивный банк отчётов хранится на другом ПК. Еженедельная информация наблюдающей станции занимает 7 ARJ-архивов и переписывается на 1 дискету примерно за 3 минуты, что минимизирует период отключения наблюдающей станции от основного режима работы для переписи архивов.

Созданная технология позволяет иметь подробные данные о всем состоянии сети, в том числе копию любой информации, поступающей от любого ПК сети. Поэтому при формировании рабочей наблюдающей станции общего доступа предпринят ряд мер для санцкионирования доступа к ней, а именно:

– рабочий экземпляр программы мониторинга формируется защищенным от копирования, для использования исключительно на данном экземпляре наблюдающей станции;

– в рабочем экземпляре программы мониторинга отсутствуют все команды, кроме <**Esc**>;

– операционная среда наблюдающей РС содержит основанные на разработанной ранее автором методике ([11], [22]) средства разграничения доступа к MS-DOS, исключающие доступ к целой РС или даже снятому с нее HDD лиц, которым неизвестен пароль.

2.9. Средства получения суточных и недельных отчетов

Суточные отчеты дают весьма интересную информацию, являясь первичной базой, однако в ряде случаев агрегация этих данных способствует полноценному их раскрытию. В этих целях был написан ряд дополнительных программных средств для обобщения различных основных характеристик и их графической интерпретации.

Поскольку в процессе эксплуатации круглосуточной системы наблюдения выяснилось, что ежедневно получается уникальная информация по контролю за качеством настройки ПК на рабочих местах сотрудников института, оказалось веьма целесообразным предпринять шаги по формированию автоматизированной базы данных рабочий станций (БДРС) ЦЭМИ РАН.

Наконец, ряд основных показателей принимает особую выразительность при интерпретации их в течение более длинного, чем сутки, периода. В связи с этим, разработано программное обеспечение автоматизированной агрегации основных показателей за неделю и получения соответствующих графиков.

Указанные средства отнюдь не исчерпывают возможностей агрегации. Выходной отчет основной программы специально выполнен в форматированной форме с кодированием информационных строк именно для того, чтобы обеспечить возможность быстрого создания программ, обеспечивающих необходимую обработку в случае возникновения интереса к любым отчетным показателям.

Общая схема информационных потоков при обработке отчетов представлена на рис. 28. Двойными линиями показана информация о нодах и ip-адресах. Пунктирными лниями выделены ручные операции. Утолщением показана обработка агрегированной информации.

Блок **Ежедневная обработка** на самом деле выполняется после снятия отчетов, как и было сказано, один раз в неделю, сразу для всех дней обработки. Сразу же после этого делается и **Еженедельная обработка** с получением необходимых графиков и (не

показан на рисунке, но, конечно же, существует) интегрирующего файла данных.

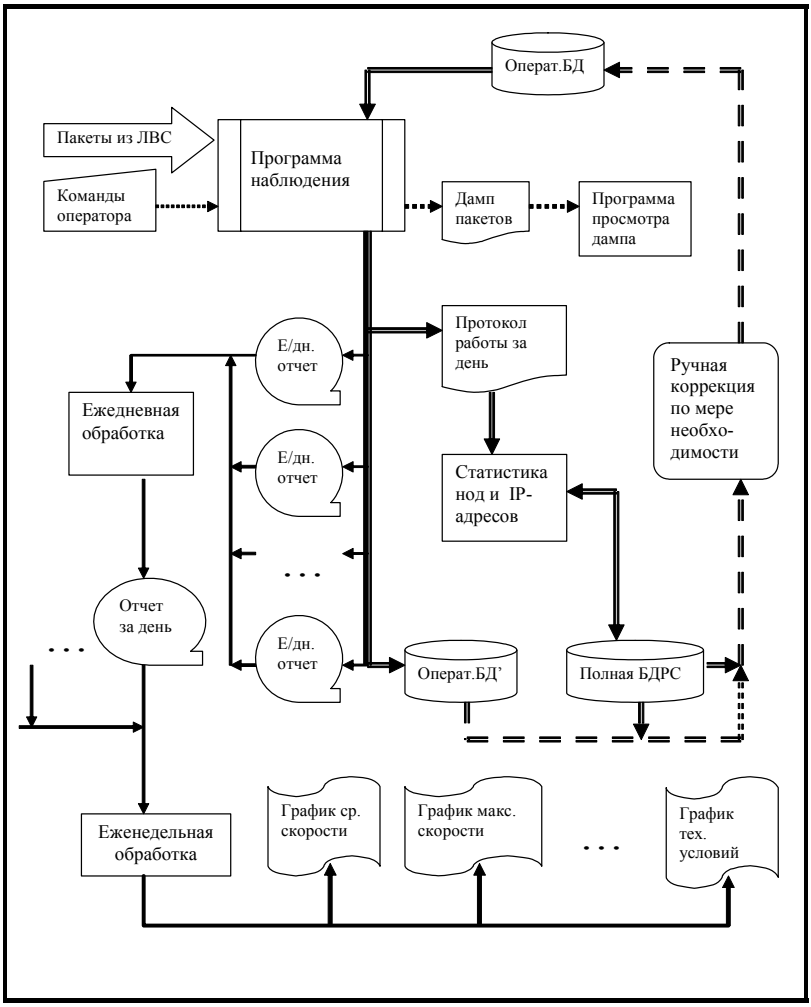

Рис. 28. Основные информационные потоки при агрегации отчетов

2.10. Сводные ежедневные данные

Как было указано выше, совокупность суточных отчетов составляет 72 кратких и 24 полных отчета. Пример ежечасного отчета приведен выше на рис. 23. Фрагмент первичной агрегации суточных отчетов по основным параметрам за то же самое число представлен на рис. 29 ниже.

```
10D001012
        96Vcp      Vmax Nref  YPak   YBytes NPak  NBytes Cmps  Sec CYCs
         2.43     56.47    1  6642  2235236    4    2580   23  900  153
         1.25     44.86    1  4848  1149655    1    1514   23  900  225
         2.66    210.2    58  6355  2450053  103   67634   23  900  234
01:00    4.62        52    1 10016  4119501    1    1514   25  872  235
.....................................
16:00   32.99    144.12   28 61850 30406522   47   27721   89  900  216
        18.97    322.64  170 40528 17514109  665  167558   75  900  108
         20.9    295.97   25 46250 19259007   37   46192   80  900  190
        31.78    216.48   33 57862 29287472   56   42143   83  900  220
17:00   23.72     196.4   42 50554 21855509   69   64116   88  900  219
        23.26    121.47    1 49908 21439110    1     446   71  900  121
        25.39    110.95   16 49096 23396115   22   18200   76  900  224
        32.11    181.42   13 63970 29598805   15   19109   77  900  218
18:00   23.16    100.27    6 59625 21346800   10    6842   79  900  211
.....................................
         5.38    110.46    9 11817  4951886   14   18189   26  900  118
         5.61     67.76    0 10851  5169136    0       0   27  900  235
         3.67      63.5    3 10464  3383487    4    6056   28  900  242
00:00    6.16     73.61    0 12967  5687308    0       0   28  900  232
```

Рис. 29. Фрагмент первичной агрегации суточной сводки за 12.10.2000

Как видим, общий суточный отчет содержит 10 числовых столбцов, среди которых:

Sec – промежуток измерения в секундах (обратите внимание, из строки 6 отчета следует, что в 01:00 выяснилось, что процедура архивации отчетов за предыдущие сутки, исполнявшаяся в 00:00:00, заняла 28 секунд, что согласуется со строкой **#04** рис. 23);

Ypak и **Ybytes** – соответственно принятое число пакетов и байтов за интервал **Sec**;

NPak и **Nbytes** – соответственно, необработанные пакеты и байты («**Мимо**») за то же время;

Nref – число ситуаций отказа в приеме (1 ситуация есть все отказы за 1 рабочий цикл программы от отчёта до отчёта);

Cmps – число активных компьютеров (точнее, MAC-адресов) за то же время;

Cycs – минимальное число рабочих циклов программы в секунду за время **Sec**;

Vmax – зафиксированная за тот же промежуток **Sec** максимальная скорость;

Vcp – вычисленная как **(YBytes+NBytes)/Sec** средняя скорость.

Рис. 30. Пример данных о ср. скорости ЛВС ЦЭМИ РАН за сутки

Необходимо обратить внимание на то, что минимальной измеряемой единицей времени в системе мониторинга является секунда, поэтому все понятия средних величин приводятся именно к секундному интервалу. Поэтому, разумеется, **Vcp** может резко отличаться от соответствующих значений, измеренных другими способами (например, на маршрутизаторе Cisco Catalyst). С другой стороны, говоря о средней скорости за день, конечно же, мы имеем в виду отношение числа обработанных байтов за день к длительности дня в секундах.

Приведённый на рис. 30 пример средней скорости, вообще говоря, показывает весьма невысокий уровень загрузки ЛВС. Уже через несколько лет данные **Vcp** свидетельствовали о более чем 5-кратном превышении приведённых за 2000 г значений. Об этом будет сказано в разделе тома 2, посвящённом модифицированной локальной сети.

Графики, основой которых служат перечисленные выше данные, представлены на рисунках с 30 по 33.

Обращаем внимание, что согласно рис. 32, максимальное число включённых ПК за сутки достигается примерно в 16 часов дня, что вполне согласуется с данными психологов об излюбленных часах труда научных работников. Примерно в это же время достигают пиков средняя и максимальная скорости в ЛВС.

Рис. 31. Пример данных макс. скорости ЛВС ЦЭМИ РАН за сутки

Рис. 32. Пример данных о числе ПК в ЛВС ЦЭМИ РАН за сутки

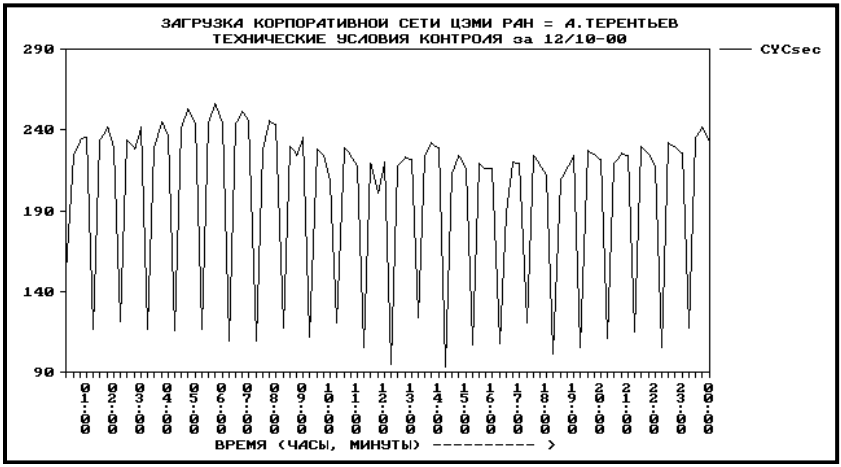

Рис. 33. Пример данных об условиях наблюдения за сутки

Особо следует сказать о технических условиях контроля. На рис. 33 приведены данные о минимальном числе «коротких» рабочих циклов программы за каждые 15 минут. Легко видеть, что своеобразные «максимумы» совпадают с моментами, когда число минут равно нулю. Это вполне объяснимо: в эти моменты весьма значительная доля процессорного времени обработки в рабочем цикле тратится на формирование символьного вида текущего времени на экране, поэтому для вывода остальной информации ресурсов не хватает, за исключением, конечно, «обязательных» «длинных» циклов.

Уже по первым данным представленных графиков можно сделать ряд интересных выводов. Поскольку день 12 октября был взят с определенным умыслом – это не начало недели, не день зарплаты, в этот день не было катастрофических зависаний серверов и т.п. – можно считать представленные графики типичными для ЦЭМИ РАН. Сразу же видно, насколько средний трафик в сети (не более 38 КБ/с согласно рис. 30) отличается от практически нормальной (600 КБ/с) загрузки. Даже пиковые значения, достигнутые, быть может, всего на одну-две секунды, едва превышают 300 КБ/с. Сеть, очевидно, недогружена и обладает значительным запасом пропускной способности.

2.11. Сводные еженедельные данные

Одновременно с получением ежедневных данных по форме, представленной на рис. 29, та же программа агрегирует результаты, обобщая их до одного показателя в час. На рис. 34 представлены те же показатели за то же самое число в агрегированном виде.

Для показателей максимальной скорости **Vmax** и числа рабочих станций **Comps** попросту выбирается максимальное из четырех значений четырех отчетов, полученных за час. Прочие показатели, кроме средней скорости, попросту суммируются, а средняя скорость пересчитывается как **Vcp=(YBytes/Sec/1024)** с округлением до двух десятичных цифр.

Получаемые сводные графики за неделю куда более интересны, чем ежедневные. На рис. 35 показаны сводные данные о средней скорости. Именно эти данные являются основой выводов о загрузке сети в разное время недели (для читабельности по оси абсцисс оставлена подпись только под каждой четвертой отметкой текущего времени). Поскольку график линеен по оси ординат, легко сравнивать интегрированную загрузку сети в разные дни и разные периоды рабочего времени.

10E001012

	24Vcp	Vmax	Nref	YPak	YBytes	NPak	NBytes	Comps	Sec	CYCs
01:00	2.72	210.2	61	27861	9954445	109	73242	25	3572	153
02:00	3.75	110.24	8	34187	13819299	12	11139	27	3600	117
03:00	1.26	59.35	5	15680	4661004	7	10598	25	3600	122
04:00	1.01	75.85	9	14887	3717705	14	15380	28	3600	117
05:00	.94	78.33	3	14150	3479940	4	6056	25	3600	116
06:00	.55	63.56	9	10303	2031827	13	10412	25	3600	117
07:00	.95	47.82	10	11682	3503737	18	13641	26	3600	110
08:00	.94	72.4	0	13673	3450168	0	0	26	3600	110
09:00	1.78	110.04	21	19460	6579654	34	51476	27	3600	118
10:00	14.88	314	440	114159	54837597	800	528846	45	3600	112
11:00	22.92	233.7	117	176985	84478732	189	128081	67	3600	121
12:00	19.58	295.11	550	170616	72187686	893	495634	76	3600	106
13:00	23.28	310.14	532	190163	85811889	1522	1148458	88	3600	95
14:00	12.14	127.66	39	105071	44741355	138	51390	75	3600	124
15:00	19.73	241.98	102	182992	72750822	222	151821	96	3600	94
16:00	30.1	243.38	114	235518	1.1096e8	201	192219	89	3600	107
17:00	23.85	322.64	270	195194	87916097	827	320009	88	3600	108
18:00	25.98	181.42	36	222599	95780830	48	44597	79	3600	121
19:00	17.31	125.96	36	160779	63793421	64	49614	67	3600	102
20:00	14.57	156.88	3	121851	53717444	12	728	56	3600	106
21:00	17.87	160.8	54	148023	65868166	352	56513	47	3600	111
22:00	18.49	313.68	551	173092	68169860	1307	1261875	43	3600	115
23:00	9.71	159.33	46	73294	35808347	94	97134	33	3600	106
00:00	5.21	110.46	12	46099	19191817	18	24245	28	3600	118

Рис. 34. Агрегированная суточная сводка за 12.10.2000

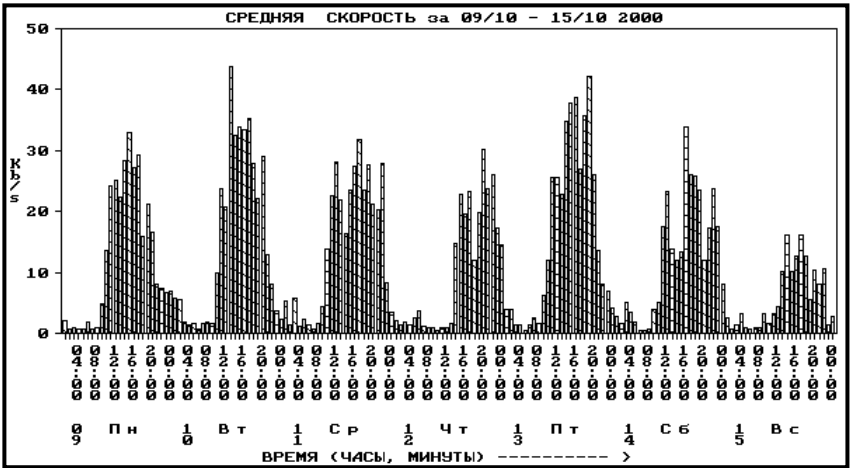

Рис. 35. Еженедельные данные по средней скорости

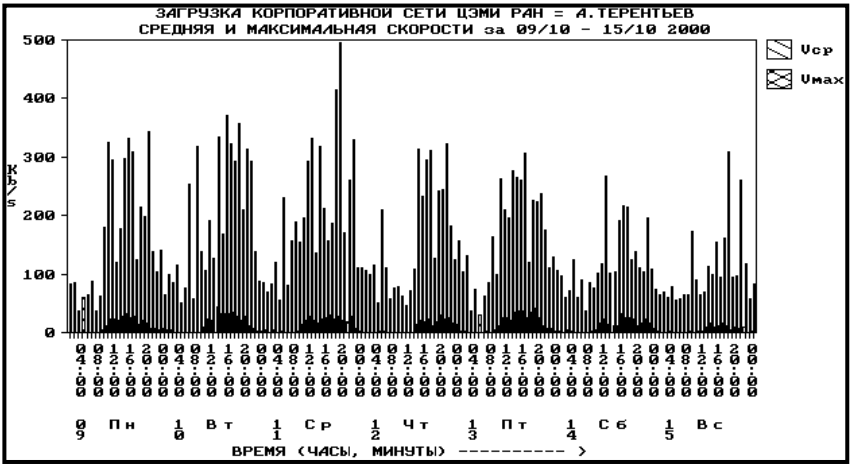

Рис. 36. Еженедельные данные по ср. и макс. скоростям (2000 г.)

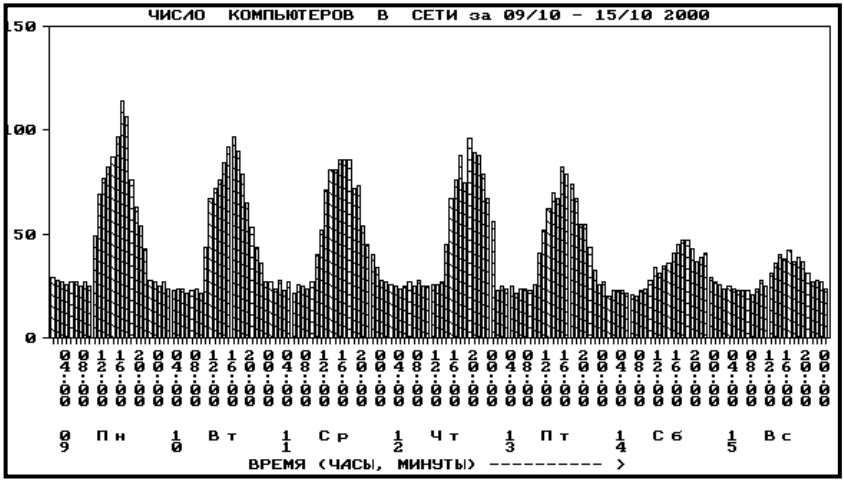

Рис. 37. Еженедельные данные по числу рабочих станций в сети

Пик на графике **Vmax** рис. 36, относящийся примерно к 19 часам среды, соответствует файлсерверным операциям (в это время исполнялась установка антивирусных средств с файлсервера ЦЭМИ на одну из РС).

Интересен график рис. 37, по которому можно видеть число реально включенных РС сети в разные моменты времени за неделю. В понедельник в сети присутствует максимальное число РС (забегая вперед, скажем, что этот результат характерен для любой недели). Не менее интересен и тот результат, что никогда, даже ночью, число подключенных РС не бывает менее 22 – это и есть общее число постоянно включенных серверов и ПК как общеинститутского, так и лабораторного значения.

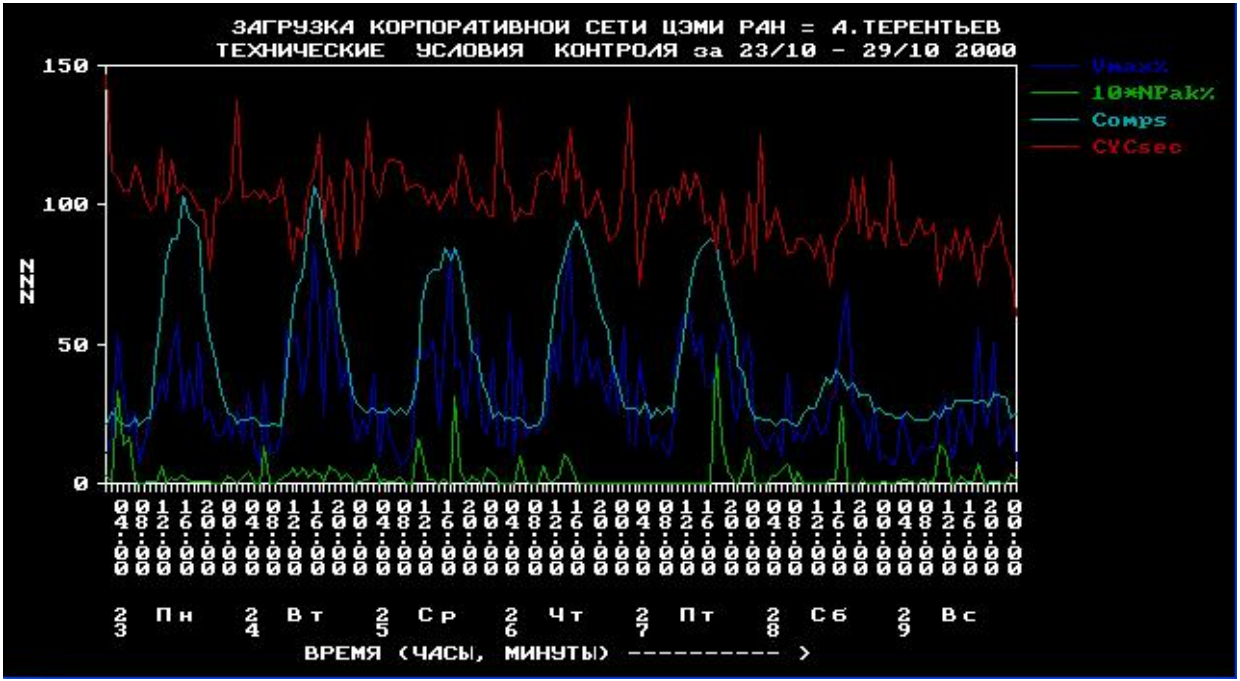

Рис. 38. Сводка технических условий контроля за неделю

Следует особо пояснить графики на рис. 38, для наглядности выбранные за последнюю неделю октября 2010 г. На него спроецированы как уже знакомые **Vmax** тёмно-синим цветом (в данном случае отсчитываемое в процентах от максимального, за 100% принят уровень 600 КБ/с) и **Comps** голубым цветом, так и две дополнительные важные характеристики. **CYCsec** (коричневый цвет) дает минимальное число «коротких» циклов в секунду и представляет собой, таким образом, нижнюю огибающую серии ежедневных графиков типа приведенных на рис. 33. **10*Npak%** пояснён чуть ниже.

Исходя из того, что за 1 рабочий цикл программа наблюдения может обработать 1 пакет, длина которого не превышает 1514 байт, максимальный объем сетевой информации, который может переработать программа наблюдения, при 100 циклах составит 1514*100/1024 = 148КБ. Теперь понятен смысл наблюдения переменной CYCsec: нужно следить, чтобы эти значения не были бы слишком малы.

Переменная **CYCsec** на рис. 38 имеет еще одну отчетливую тенденцию: к снижению своих средних значений от понедельника к 19 часам среды (время снятия отчетов) и далее к концу воскресенья. Дело в том, что, как сказано выше, оперативная БД периодически – естественно, во время снятия отчетов, – корректируется с удалением из нее строк, соответствующих коллизиям, временной настройке компьютеров и т.п. С течением времени между коррекциями эта БД, однако, растет в объеме, что снижает число рабочих циклов программы наблюдения, поскольку каждую последующую проверку пакета приходится исполнять уже по увеличенной БД.

Последний из показателей рис. 38, обозначенный как **10*Npak%**, соответствует самой нижней, светло-зелёной ломаной на рисунке и показывает процент отказанных к обработке пакетов от общего числа пакетов. Для лучшей наглядности при графическом показе показатель умножается на 10, чтобы сделать более заметными выбросы. Видно, что по крайней мере 1 раз на рис. 38 (27 октября около 18 часов) этот показатель поднялся до 50, т.е. до 5% отказанных к обработке пакетов, что является довольно высоким значением.

Покажем теперь другие возможности агрегации. На рис. 39 показан список компьютеров Лаборатории 4.04 по состоянию на 12 октября 2000 г[10]. На рис. 40 даны сводные данные за 12 октября 2000 г по всем этим компьютерам.

```
1. Egorova  IP=69
 2. SergeP   IP=74
 3. Polak    IP=78
 4. Alex     IP=85
 5. 802      IP=94
 6. 905      IP=98
 7. MMX      IP=99
 8. PII-907  IP=167
 9. PII-905  IP=168
10. Exch     IP=209
11. WEB SQL  IP=210
12. NTSrvr   IP=211
13. Y905     IP=245
14. EMS      IP=246
15. DevSrv   IP=247
16. Y907     IP=252
```

Рис. 39. Список компьютеров Лаборатории 4.04 на 12.10.2000

[10] В настоящее время такой Лаборатории в ЦЭМИ РАН не существует.

	Обм_др	Cisco-4K	802.3IPX	ПРОЧИЙ	IP-Bx%	IPX-%	ПРОЧИЙ %	Egorova IP=69	SergeP IP=74	Polak IP=78	Alex IP=85	802 IP=94	905 IP=98	MMX IP=99
01:00	9955445	1964738	95160	7895547	20	1	79	0	0	0	6015492	0	0	0
	13819199	3552888	129830	10136481	26	1	73	0	0	0	9138369	0	0	0
	4661004	625532	129382	3906090	13	3	84	0	0	0	3206469	0	0	0
04:00	3717705	742564	130480	2844661	20	4	76	0	0	0	2179740	0	0	0
	3479940	491284	128374	2860282	14	4	82	0	0	0	2115050	0	0	0
	2031827	317026	128540	1586261	16	6	78	0	0	0	995709	0	0	0
	3503737	435036	129252	2939449	12	4	84	0	0	0	2440054	0	0	0
08:00	3450168	704432	129124	2616612	20	4	76	0	0	0	1952658	0	0	0
	6579654	2061230	129372	4389052	31	2	67	0	0	0	3461246	0	0	0
	54837597	33411796	880939	20544862	61	2	37	0	0	0	14239781	0	0	0
	84478732	54902300	243138	29333294	65	0	35	0	136207	0	16565697	85448	99192	0
12:00	72187686	53680823	266552	18240311	74	0	26	23990	303847	289443	7976046	6100	392079	0
	85811889	52875937	1304364	31631588	62	2	36	7087	213140	916117	20954418	5528	302218	0
	44741355	27922216	542554	16276585	62	1	37	2288	32985	15167	11515313	2384	308459	0
	72750822	51994628	339400	20416794	71	0	29	11118	231270	553830	8145559	80452	421856	0
16:00	1.1096e8	76139115	254894	34569036	69	0	31	7311	287182	403402	13024510	108236	265263	0
	87916097	56521734	387752	31006611	64	0	36	3919	496462	270991	14975993	0	423045	0
	95780830	58408128	207498	37165204	61	0	39	3368	373790	801210	24622481	0	0	0
	63793421	40045110	184179	23564132	63	0	37	4417	177599	192127	13619372	53691	0	0
20:00	53717444	31888218	177804	21651422	59	0	41	0	403563	214890	14401864	0	0	0
	65868166	45829321	190460	19848385	70	0	30	0	473785	6863	9101712	0	0	0
	68169860	39693908	1157394	27318558	58	2	40	0	504065	0	18802527	0	0	0
	35808347	25279586	165384	10363377	71	0	29	0	48261	0	6206273	0	0	0
24:00	19191817	9232403	151408	9808006	48	1	51	0	0	0	7985409	0	0	0

	PII -907 IP=167	PII-905 IP=168	Exch IP=209	WEB SQL IP=210	NTSrvr IP=211	Y905 IP=245	EMS IP=246	DevSrv IP=247	Y907 IP=252	ВСЕГО LAB. 4.04
01:00	0	0	14430	1027686	34218	0	5008	0	0	7096834
	0	0	41170	18703	33690	0	4811	0	0	9236743
	0	0	10319	202125	28725	0	4278	0	0	3451916
04:00	0	0	18561	64112	35669	0	4916	0	0	2302998
	0	0	12955	249952	34532	0	5798	0	0	2418287
	0	0	23168	102224	29233	0	4535	0	0	1154869
	0	0	13004	101095	33934	0	4627	0	0	2592714
08:00	0	0	13033	178682	33878	0	4535	0	0	2182786
	0	0	9788	242105	29413	0	4824	0	0	3747376
	0	0	2699	669558	330502	0	4475	0	0	15247015
	0	0	531941	1410431	736005	0	4895	0	0	19569816
12:00	228857	0	818888	754073	796479	0	4535	0	242525	11836862
	246014	0	380440	572042	441738	18057	4895	41655	618452	24721801
	3240	0	533078	235135	166257	97525	5315	473046	288333	13678525
	1140	0	2007607	754535	1093228	149225	59594	260222	304135	14073771
16:00	1560	0	866867	2293202	351368	532438	193307	203585	200735	18738966
	114153	0	213701	1949246	1780049	21126	38810	28777	0	20316272
	26920	0	29493	988256	468343	19259	51861	992765	0	28377746
	378859	0	105896	2059411	434553	464088	46015	0	0	17536028
20:00	19276	0	9815	1165262	955656	289978	41797	0	0	17502101
	29787	0	3016500	233340	573399	855320	34855	0	0	14325561
	17625	0	10967	734817	807805	1422333	31220	0	0	22331359
	0	0	7266	772095	73941	86093	252675	0	0	7446604
24:00	0	0	12047	143876	30211	0	168917	0	0	8340460
						ИТОГО УЗЛЫ ЛАБОРАТОРИИ 4.04			- - - >	288227446

Рис. 40. Сводные данные по ПК лаборатории 4.04 за 12.10.2000

Из полученных данных можно сгенерировать следующие рисунки: трафики различных сетевых пакетов (рис. 41 и 42), входящий и исходящий трафики (рис. 43), соотношение суммарного трафика Лаборатории 4.04 с общеинститутским (рис. 44) и соотношение трафиков по различным ПК Лаборатории (рис. 45).

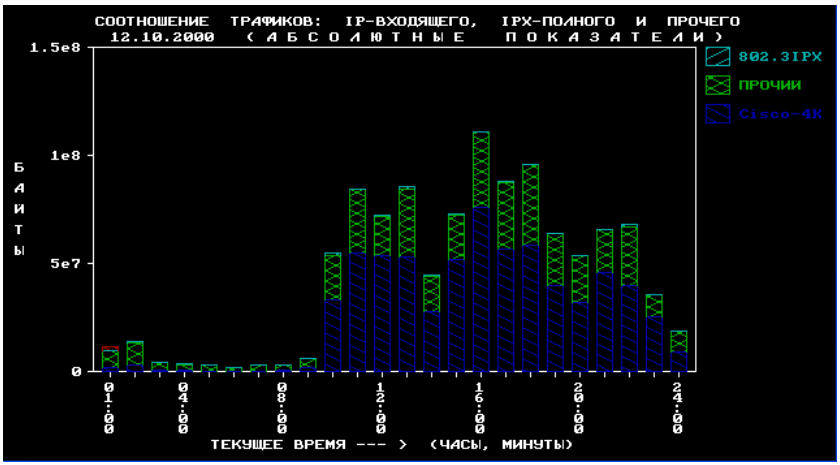

Рис. 41. Трафики по ПК лаборатории 4.04 за 12.10.2000

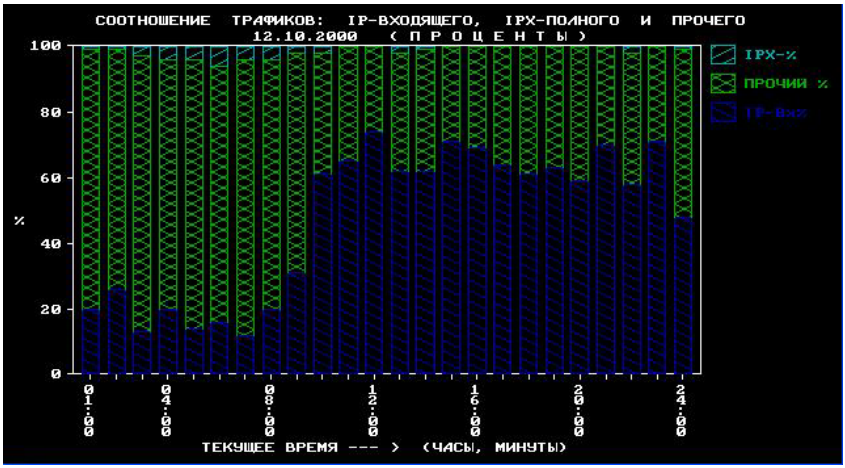

Рис. 42. Трафики IPX, Other и IP по лаборатории 4.04 за 12.10.2000

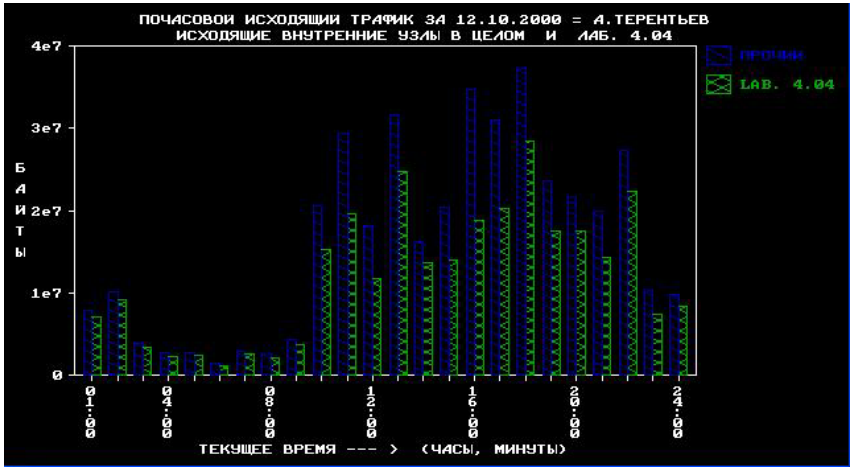

Рис. 43. Исходящий трафик лаборатории 4.04 за 12.10.2000

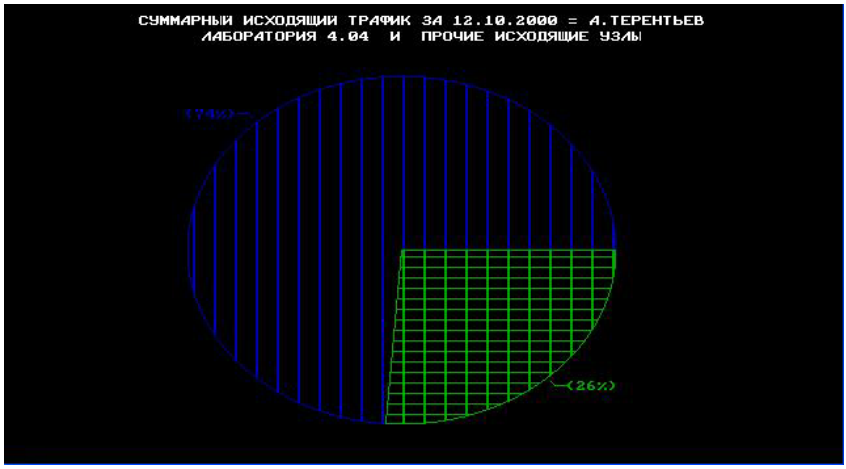

Рис. 44. Суммарный трафик лаборатории 4.04 за 12.10.2000

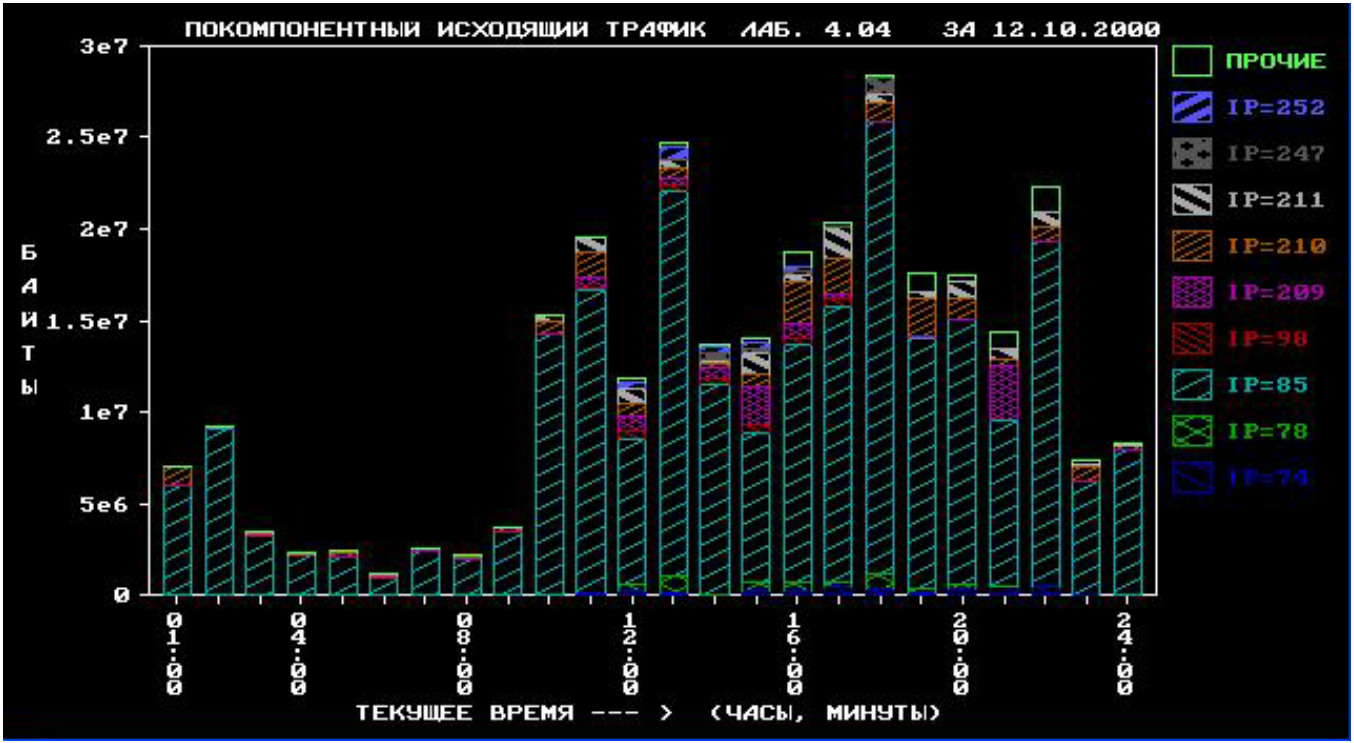

Рис. 45. Покомпонентный трафик лаборатории 4.04 за 12.10.2000

Легко видеть, к примеру, что среди всех ПК Лаборатории 4.04 основной трафик давал ПК с IP 193.232.194.85 “**Alex**” пользователя А. Дыбенко.

Таким образом, с помощью агрегированных отчётов сетевого мониторинга возможно получение различных «срезов» по различным группам компьютеров, в том числе в составе подразделений института, для сравнительной оценки биллинговых показателей.

Аналогичные данные позднее были неоднократно использованы для анализа трафиков различных групп PC в сети при серьёзном превышении средних значений до пороговых показателей для уточнения конкретных нод, «забивающих» своим трафиком сеть. Подробнее этот вопрос будет рассмотрен в последующих томах данной работы.

ГЛАВА 3. ПРОГРАММНАЯ РЕАЛИЗАЦИЯ МОНИТОРИНГА

В ЦЭМИ РАН автором велась разработка сетевого мониторинга в течение 19 лет. Фактически, в течение всех лет эксплуатации постоянно исполнялась та или иная доработка программ, BAT-файлов, инструкций пользователю, а также внешнего вида веб-сайта и его контента [23].

В процессе разработки был опробован ряд технических конфигураций различных ПК, от Pentium-I-90 до современных. Итоговой конфигурацией основной наблюдающей станции, сохранённой на долгие годы, стал Intel Core Duo E7300 2,66 GHz с кэшем 3Mb. Конечно, в MS-DOS работало только одно ядро.

В качестве web-сервера был выбран сервер на основе Pentium-III/600GHz, Microsoft Windows Server'2000 и Apache 1.3.23. Впоследствии эта конфигурация была обновлена до Intel Pentium4 / 3,0 GHz / 2Gb / Raid1:2*80Gb \ Microsoft Windows Server 2003 R2 Service Pack 2, что оказалось вполне достаточным для раздачи антивирусных обновлений [24] [25], поддержки Антивирусного сайта и выполнения ряда других операций реального времени, в том числе связанных с отображением на сайте в реальном времени основных характеристик загрузки сети (подробно рассматриваются во втором томе данной работы).

3.1. Создание программной среды мониторинга

С учётом особенностей выбранной операционной среды как MS-DOS 6.22, создание программной среды разработки приобретает самостоятельное значение. Особенно важно это для современных компьютеров, не рассчитанных на эксплуатацию в MS-DOS. Поэтому, представляется важным описать подробно создание программной среды сетевого мониторинга на современных ПК, не теряя их возможного функционального назначения как Windows-ориентированной среды разработок.

Собственно, этапы создания, начиная с полностью освобождённого от данных HDD, перечислены ниже.

- Отключить через BIOS встроенный сетевой адаптер, если таковой имеется на материнской плате.
- Установить в слот PCI – Fast Ethernet PCI Adapter FA 310^{TX}, рассмотренный выше как сетевой адаптер, позволяющий выпол-

нять Promiscuous Mode в режиме принятия сетевых пакетов пакетным драйвером MS-DOS.

- Загрузиться с поставочной дискеты MS-DOS 6.22[11] и вызвать программу обслуживания дисков **fdisk.exe**.
- Удалить все существующие разделы HDD, если они есть.
- Образовать новый раздел Primary FAT16 (отказаться от использования всего дискового пространства для этого раздела!) объёмом 2047Мб. Этот раздел будет виден под буквой **C:** как в MS-DOS, так и в Windows.
- Образовать ещё один раздел Primary FAT16 с теми же параметрами. Этот раздел будет виден как **D:** в MS-DOS и как **F:** в Windows. Этот диск предназначен для оперативных данных сетевого мониторинга. Конечно, можно было бы их хранить также на диске C:, но тогда невозможно сохранение оперативных данных без переустановки MS-DOS. Вообще, разделение томов под программы и данные является хорошим тоном при любой ОС.
- Перезагрузиться с дискеты.
- Форматировать раздел **C:** с переносом операционной системы MS-DOS (параметр **/S** команды **format**) с дискеты на HDD.
- Форматировать раздел **D:** без переноса MS-DOS.
- Определить диск **C:** как загрузочный раздел в MBR (программа **fdisk.exe**).
- Перезагрузиться в MS-DOS с HDD; будут видны диски **C:** и **D:**.
- На диске **C:** создать каталог \DOS и перенести туда все файлы с дистрибутивных дискет MS-DOS 6.22.
- На диске **C:** создать необходимые каталоги и перенести туда необходимые вспомогательные средства (например, Нортон-Коммандер или, лучше, Волков-Коммандер v.5.0), а также в каталоге, к примеру, \UTIL, необходимые программные средства для работы, в частности, архиватор ARJ.EXE, и другие (я использую собственный драйвер клавиатуры TAMKB.COM). Не забыть в каталоге, например, \NETWORK записать драйвер NGRPCI.SYS с поставочной дискеты для адаптера FA 310^{TX}.

[11] В моём варианте поставочной дискеты MS-DOS 6.22 присутствуют также ряд вспомогательных утилит, например, Волков-Коммандер VC.COM с необходимыми файлами, а также ряд программ из Norton Utilities 4.50.

• Создать файлы CONFIG.SYS и AUTOEXEC.BAT в корне диска **C:**, например, в виде, показанном на рисунках 47 и 48.

• Создать на диске **D:** каталог \NETWORK и записать туда необходимые для работы сетевого анализатора основные и вспомогательные файлы TAMCNET.EXE, TAMCNET.SCR, TAMCNET.HLP, TAMDRVR.EXE, TAMVIEW.EXE и пакетные файлы TAMBNE2.BAT, TAMBNEU.BAT и прочие. Создать в этом же каталоге начальный вариант TAMCNET.DBN хотя бы с одной строкой, описывающей гейт Интернета (в моём случае Cisco-4000).

• Перезагрузиться и убедиться в том, что сетевой анализатор подключается нормально и принимает пакеты. В случае необходимости, исправить в файле CONFIG.SYS параметры драйвера NGRPCI.SYS и/или драйвера EMM386.EXE.

• Загрузиться с поставочного CD-ROM Windows и создать новый первичный системный раздел для Windows, отведя ему примерно 20-30Гб. Форматировать его как FAT32 и установить туда Windows. Этот раздел не будет виден в MS-DOS, но будет определяться как **D:** в Windows.

• Доступными средствами Windows создать вторичный (extension) раздел, отведя ему весь остаток HDD и отформатировать его как NTFS. Этот раздел также не будет виден в MS-DOS, но виден как диск **E:** в Windows. При желании, можно вместо одного создать несколько разделов в блоке extension (при этом, разумеется, буквы в Windows будут другие). Диск **E:**, в отличие от **D:**, предназначен для данных в Windows, чтобы при сбоях Windows можно было бы легко переустановить систему Windows на диске **D:**, не затрагивая данных.

Таким образом, все разделы HDD можно представить в виде таблицы на рис. 46, приняв объём HDD за 120 Gb.

Существуют и другие, более сложные варианты распределения HDD. На ПК автора используются 3 тома в разделе Extension и ещё один Windows Primary для второй операционной системы Windows'XP SP3 (первая является Windows'2000 SP4 Update Rollup 1, и ей недоступен второй раздел Windows Primary, начинающийся выше 120 Gb). Зачем и почему на рабочем ПК используются две Windows, а также распределение HDD в этом случае подробно пояснено в [26] [27].

Тип тома	Объём раздела	Формат раздела	Буквенное наименование	
			MS-DOS	Windows
HDD, Primary, MBR	2047 Mb	FAT-16	C:	C:
HDD, 2й Primary	2047 Mb	FAT-16	D:	F:
Windows Primary	30 Gb	NTFS/FAT32	–	D:
Windows Extension	85 Gb	NTFS	–	E:
CD/DVD-ROM			E:	G:
Flash			–	H:

Рис. 46. Наименования томов одного и того же ПК в различных ОС

При установке Windows после MS-DOS, Windows «видит» уже установленную MS-DOS и автоматически формирует BOOT.INI, включающий обе операционные системы. На этапе загрузки пользователю предлагается список из обеих систем с вопросом, какую из них загрузить.

При работе в Windows, рекомендуется диски **C:** и **F:** исключить из отслеживания изменений системы, поскольку информация на них производится только в MS-DOS. Обслуживание этих дисков (проверки ошибок, сбоев, каталогов, проверка пересечений файлов по кластерным цепочкам и мн.др.) рекомендуется также исполнять в MS-DOS. Правда, придётся смириться с тем, что Windows всюду «суёт» свои файлы с длинными именами, в том числе и на эти тома.

Следует также отметить, что при использовании внешних CD-ROM различных производителей для проверки на антивирусы при блокировке Windows на дисках **C:** или **E:** могут быть образованы сторонние файлы до 500 Мб, подлежащие удалению после восстановления системы Windows от вирусов [26] [27].

На ПК автора в целях усиления безопасности установлен также BOOT-Wizard от ФизтехСофт, в котором можно сохранять критические для той или иной ОС файлы и автоматически восстанавливать их перед загрузкой. Нужно признаться, что этот функционал несколько раз спасал автора при ошибках в установке различных экземпляров Windows.

Описанная конструкция HDD компьютера позволяет использовать его постоянно как рабочий ПК в Windows, но при желании перезагрузкой он может быть превращён в мощную наблюдаю-

щую станцию. Разумеется, наблюдать пакеты в этом случае придётся из точки подключения ПК к КВС.

```
[MENU]
menuitem=Game, Max Conventional
menuitem=Work, Possible Working
menuitem=Net, Network Operations
menudefault=Net,5
menucolor=14,1
[Game]
FILES=40
BUFFERS=45,0
STACKS=4,512
LASTDRIVE=Z
DEVICE=C:\DOS\himem.sys /V /NUMHANDLES=64 /TESTMEM:OFF
DEVICE=C:\DOS\emm386.exe NOEMS HIGHSCAN D=64 X=D400-
DFFF V
DOS=HIGH,UMB
SHELL C:\command.com C:\ /E:512 /P
[Work]
FILES=50
BUFFERS=40,0
FCBS=4,0
STACKS=9,512
COUNTRY=007,866,C:\DOS\country.sys
DEVICE=C:\DOS\himem.sys /V /NUMHANDLES=64 /TESTMEM:OFF
DEVICE=C:\DOS\emm386.exe NOEMS HIGHSCAN D=64 X=D400-
DFFF V
DEVICEGIGH=C:\DOS\display.sys CON=(EGA,866,3)
DEVICEGIGH=C:\UTIL\vide-cdd.sys /D:ECSCD001
LASTDRIVE=M
DOS=HIGH,UMB
SHELL C:\command.com C:\ /E:512 /P
[Net]
FILES=50
BUFFERS=45,0
FCBS=4,0
STACKS=4,512
LASTDRIVE=Z
DEVICE=C:\DOS\himem.sys /V /NUMHANDLES=64 /TESTMEM:OFF
DEVICE=C:\DOS\emm386.exe NOEMS HIGHSCAN D=64 X=D400-
DFFF V
DEVICE=D:\NETWORK\ngrpci.sys 0x62 /w
DOS=HIGH,UMB
SHELL C:\command.com C:\ /E:512 /P
```

Рис. 47. Файл CONFIG.SYS на 3 варианта загрузки

```
@ECHO OFF
PROMPT $p$g
MODE CON CP PREPARE=((866) C:\DOS\ega3.cpi)
MODE CON CP SELECT=866
PATH=C:\DOS;C:\UTIL;C:\
SET TEMP=C:\TEMP
SET TMP=C:\TEMP
tamkb /i=0,31
IF .%CONFIG%.==.Net. GOTO Net
LH C:\GMOUSE\gmouse /P2
LH C:\UTIL\mscdex.exe /V /D:ECSCD001 /M:10
GOTO Ok
:Net
D:
CD NETWORK
REM Далее вызов наблюдающей станции
tambne2.bat
:Ok
```

Рис. 48. Файл AUTOEXEC.BAT на 3 варианта загрузки

3.2. Специфические программные средства

Программные средства сетевого мониторинга включают в себя несколько групп программных компонентов. Одна из них является собственно программой сетевого мониторинга и написана на языке высокого уровня PowerBASIC for DOS 3.0 (впоследствии 3.5).

Вторая служит для оптимизации ряда вычислений, включая приём и первичную обработку принятых сетевых пакетов, и написана на Макроассемблере MS-DOS MASM версии 5.10 − 1988 г.

Третья группа является вспомогательной и исполняет операции агрегации данных, написана на макроязыке программного пакета SuperCalc-4.

3.2.1. Программа сетевого мониторинга TamCNet.exe

Эта программа является собранным с рядом подпрограмм модулем, исполняющим все функции сетевого мониторинга. Подключаемые модули – библиотека конвертации данных TamCnv.OBJ и подпрограмма низкоуровневого приёма пакетов TamINet.OBJ.

Программа допускает управление указанием параметров вызова в командной строке. Параметры предваряются слэшами и отделяются пробелами. Иными словами, командная строка имеет вид:

TAMCNET.EXE [***ключ***[=***значение***]] …

Таковыми параметрами (по последней версии) могут быть следующие.

LST1=*nnnn* (0<nnnn<9900) – задаёт начальный номер первого отчёта TAMCnnnn.LST, иначе берётся максимально присутствующий в каталоге и к нему прибавляется **1**. Номер свыше **9000** меняется на **2**. Поскольку результирующий архив содержит 96 отчётов, а имя архива содержит последний номер отчёта, в каталоге хранения отчётов будут имена A0096, A0192, A0288 и т.д. Если каталог не опустошить до момента, когда номер отчёта превысит 9900, новая последовательность начнётся с A0097, A0193 и т.д. Такой приём позволяет хранить в каталоге архивов НС отчёты за 5–6 месяцев.

INT=*tt* (0<***tt***<61, по умолчанию **15**) – задаёт интервал в минутах между отчётами.

KFULL=*ll* – приказ в каждом ***ll***-м отчёте выводить статистику нод. По умолчанию, **4**.

KEEP – приказ после каждого отчёта НЕ обнулять текущие показатели, иначе они принудительно обнуляются. Используется для сравнительно кратковременного (несколько дней) анализа сторонних сетей. Подробнее см. Том 2.

BUFLIM=*kk* (19<***kk***<81, по умолчанию **10**) – процент заполнения буферов, при котором обновление основных показателей на экране сокращается до 1 раза в секунду (ранее было исчисление по **WtCyc**).

STMRK – вести и выдавать статистику по маркированным в БД нодам.

HSYN – синхронизировать сводки с нулём минут часов на ПК.

NET=*aaaa.bbbb*[***.cccc***] – внутренняя текущая сеть. Параметр введён сравнительно недавно после перевода большинства нод во внутреннюю сеть 10.0.*.*/16 (для срабатывания параметра CNDS).

CNDS – после каждого полного отчёта сжать БД, исключив IP-адреса вне текущей сети. Дополнительно параметр **CNOISE** – для исключения добавленных неIPшных нод (т.е. MAC-адресов без IP).

EODAY – осуществить выход из программы с кодом завершения 1 в 00:00:00 после отчёта.

PPASS – показывать и фиксировать пароли почты.

2, **3** – указать видеостраницу, переход на которую будет осуществлён принудительно через 60 секунд после показа иной страницы.

NOUT – запрет любого вывода на HDD, кроме журнала .LOG. Используется при показе внутренней сети (подробнее см. Том 2).

GO – приказ начать работу, без этого параметра выдаётся короткая справка о возможных параметрах и работа заканчивается.

DEMO – деморежим, поочерёдно показываются страницы 1, 2, 3.

COM=*x* – указание COM-порта для связи с мониторной программой.

DNODES=*yy* – указание, какие пакеты дампировать на диск: **16** – длинные, **8** – NoDestination, **4** – NewMAC, **2** – NewIP, **1** – те, которые имеют признак **+4** в БДРС. Число ***yy*** может быть арифметической суммой указанных составляющих.

Программа написана на алгоритмическом языке высокого уровня для трансляции компилятором PowerBASIC for DOS 3.5. Последняя стабильная версия программы – 5.23. Версия программы 5.13 зарегистрирована в ФИПС 14.07.2014 г под N2014617164.

3.2.2. Клавиатурный драйвер TamKb.com

Строго говоря, этот драйвер русской клавиатуры был написан ещё до эксплуатации сетевого мониторинга в 1988 г. и эксплуатировался на разных ПК вплоть до Windows 3.x.

После первой загрузки драйвер остаётся резидентным в оперативной памяти (TSR – Terminate and Stay Resident), занимая менее 1 КБ. Объём загруженной программы менее 4 КБ. Драйвер перехватывает прерывание **09**. Для показа русских символов на экране предварительно необходимо загрузить соответствующие шрифты в знакогенератор ПК.

Отличительные особенности драйвера следующие.

- Возможность переключать язык с русского на латынь и обратно однократным нажатием и отпусканием нефункциональной правой клавиши Shift, так что переключение языка не влияет на ввод управляющих символов.
- Возможность при вызове драйвера указать на экране место (строку и столбец) подсветки «РУС/LAT» при переключении языка.
- Возможность оперативно менять место (строку и столбец) подсветки «РУС/LAT» во время эксплуатации драйвера вызовом второй его копии с нужными параметрами (настройки меняются в первой копии программы).
- Возможность принудительно при первом или последующем вызове установить интерпретацию русской или латинской клавиатуры.
- Возможность временно дезавуировать драйвер, не выгружая его из памяти компьютера, и при необходимости вновь включить его действие.

• Возможность снять драйвер (с восстановлением Int**09**h) без перезагрузки MS-DOS вызовом второй копии драйвера с соответствующим параметром (обе копии перестают функционировать, Int**09**h восстанавливается). Разумеется, для обеспечения этого вектор прерывания **09**h не должен быть перекрыт посторонней программой.

• Выдача трели на динамик ПК при залипании клавиш или переполнении внутреннего буфера.

• Выдача звукового сигнала на динамик ПК при переключении языка – высокого тона при переключении на русский и низкого при обратном переключении на латынь.

Программа, помимо обычного вызова, может быть инсталлирована через CONFIG.SYS оператором INSTALL, в том числе в HMA. В этом случае она невыгружаема.

Программа написана на языке Макроассемблер MS-DOS 5.10, последняя версия – 1.5-98.

3.2.3. Драйвер имитации приёма пакетов из локальной сети TamDrvr.EXE

Данная программа полностью имитирует получение пакетов из сети стандартным PC/TCP FTP драйвером. После загрузки становится резидентной в памяти и по команде оператора берёт по одному сетевые пакеты из предварительно созданного на HDD файла ETHERX.DAT и подаёт на верхний уровень, как если бы исполнялись процедуры UpCall стандартного FTP драйвера при получении пакетов из сети. Реализует или имитирует процедуры FTP драйвера, поименованные в табл. рис. 8; опознаётся стандартными процедурами поиска как обычный пакетный PC/TCP FTP драйвер.

Получение пакетов исполняется при нажатии и отпускании регистровой клавиши LShift. По достижении конца файла при нажатой клавише ScrollLock осуществляется автоматический переход к началу файла.

Программа написана на Макроассемблере MS-DOS 5.10 – 1988 г., занимая менее 7 КБ. Текущая версия – 1.4 2013.

Версия 14.06.13 зарегистрирована в ФИПС под N2014617165.

3.2.4. Библиотека конвертации данных TamCnv.OBJ

Данная утилита исполняет преобразование различных данных в символьный вид. Необходимость создания библиотеки опреде-

лена тем, что стандартные средства форматирования (**USING$()** и др.) языка PowerBASIC for DOS весьма неоптимальны по сравнению с элементами созданной библиотеки (подробнее это показано в томе 2). Библиотека написана на Макроассемблере MS-DOS 5.10 и имеет следующие входы, описанные ниже.

TAMCWH4 (Word, Flex) – преобразование переменной типа WORD в текстовую FLEX-переменную длиной 4 байта в 16-ном виде.

TAMCBH2 (Byte, Flex) – преобразование переменной типа BYTE в текстовую Flex-переменную длиной 2 байта в 16-ном виде.

TAMCID4 (Integer, Flex) – преобразование целочисленной положительной переменной INTEGER во FLEX-переменную длиной 4 знака (десятичный вид). Допустимо для значений от 0 до 9999.

TAMCBD3 (Byte, Flex) – в настоящее время не используется.

TAMCID3 (Integer, Flex) – преобразование целочисленной положительной переменной INTEGER во FLEX-переменную длиной 3 днака (десятичный вид). Допустимо для значений от 0 до 999.

TAMCBD2 (Byte, Flex) – преобразование байтовой переменной во Flex-переменную в десятичном виде (2 знака). Для значений от 0 до 63h.

TAMCID2 (Integer, Flex) – преобразование целочисленной положительной переменной INTEGER во FLEX-переменную длиной 2 знака (десятичный вид). Допустимо для значений от 0 до 99.

TAMCWD5 (Word, Flex) – преобразование переменной типа WORD во Flex-переменную длиной 5 знаков. Допустимо для значений от 0 до 1869Fh.

TAMCID5 (Integer, Flex) – преобразование целочисленной положительной переменной INTEGER во FLEX-переменную длиной 5 знака (десятичный вид). Допустимо для значений от 0 до 99999.

TAMCLD9 (Long, Flex) – преобразование целочисленной положительной переменной LONG INTEGER во FLEX-переменную длиной 9 знаков (десятичный вид). Допустимо для значений от 0 до 999999999.

TAMCDD9 (Double Word, Flex) – преобразование целочисленной положительной переменной DOUBLE WORD во FLEX-переменную длиной 9 знаков (десятичный вид). Допустимо для значений от 0 до 999999999.

TAMCLDA (Long, Flex) – преобразование целочисленной положительной переменной LONG INTEGER во FLEX-переменную

длиной 10 знаков (десятичный вид). Допустимо для значений от 0 до 9999999999.

TAMCDDA (Double Word, Flex) – преобразование целочисленной положительной переменной DOUBLE WORD во FLEX-переменную длиной 10 знаков (десятичный вид). Допустимо для значений от 0 до 999999999.

TAMCLD7 (Long, Flex) – преобразование целочисленной положительной переменной LONG INTEGER во FLEX-переменную длиной 7 знаков (десятичный вид). Допустимо для значений от 0 до 9999999.

TAMCDD7 (Double Word, Flex) – преобразование целочисленной положительной переменной DOUBLE WORD во FLEX-переменную длиной 7 знаков (десятичный вид). Допустимо для значений от 0 до 9999999.

TAMCXH2 (Byte, Flex) – в настоящее время не используется.

TAMCXH4 (Byte, Flex) – преобразование байтовой переменной или элемента байтового массива в текстовый 16-ричный вид длиной 4 байта.

TAMCXHC (Byte, Flex) – в настоящее время не используется.

TAMCMH6 (Flex, Flex) – преобразование MAC-адреса из 6 символов в сжатом виде в 12 символов Hex-кода без разделителей.

TAMCMIP (Flex, Flex) – преобразование текстового IP-адреса в сжатом виде (6 байтов) в 15-символьный вид (xxx.xxx.xxx.xxx).

TAMCNV3S (BYVAL WORD) – формирование сегментного адреса страницы видеопамяти в оперативной памяти программы конвертации.

TAMWLDS (FLEX, INTEGER, BYVAL INTEGER, BYVAL INTEGER) – перенос текстовой Flex-строки в видеопамять (NPage, NPos, NStr). Число переносимых символов определяется длиной Flex-переменной.

TAMWLDA (DWORD, INTEGER, BYVAL INTEGER, BYVAL INTEGER) – преобразование целочисленной переменной DOUBLE WORD в десятичное значение длиной 10 знаков непосредственно в видеопамять (NPage, NPos, NStr).

TAMWLD7 (DWORD, INTEGER, BYVAL INTEGER, BYVAL INTEGER) – преобразование целочисленной переменной DOUBLE WORD в десятичное значение длиной 10 знаков непосредственно в видеопамять (NPage, NPos, NStr).

TAMWDD7 (DWORD, INTEGER, BYVAL INTEGER, BYVAL INTEGER) – преобразование целочисленной переменной DOUBLE WORD в десятичное значение длиной 7 знаков непосредственно в видеопамять (NPage, NPos, NStr).

Программа написана на языке Макроассемблера MASM 5.10 – 1988 г.

Длина библиотеки – 1167 байтов, последняя версия от 13.06.2013.

Версия программы 13.06.13 зарегистрирована в ФИПС под N2014617400.

3.2.5. Низкоуровневый приём сетевых пакетов TamINet.OBJ

Как уже было сказано, интерфейс с пакетным PC/TCP FTP-драйвером должен быть выполнен на Ассемблере. Данная процедура исполняет весь интерфейс с этим драйвером и дополнительно включает ряд процедур, для которых требуется исполнение на Ассемблере, в частности, переключение экрана со стандартного режима в 25 строк на режим в 50 строк и обратно.

Подпрограмма написана на Макроассемблере MS-DOS 5.10 – 1988 г.

Длина подпрограммы 2716 байтов, последняя версия – 23.06.2013.

Версия программы 23.06.13 зарегистрирована в ФИПС под N2014617161.

3.2.6. Программа просмотра дампированных сетевых пакетов TamView.EXE

Эта программа позволяет последовательно от начала дампа к концу просматривать записанные сетевые пакеты. Информацию о методе показа пакетов можно получить из рис. 25.

Однако программа позволяет выполнить и более сложные операции. В частности, можно задать *выходной* дамп-файл, в который переносить или не переносить очередной просматриваемый пакет, выделяя, таким образом, нужную цепь пакетов. Более того, если специальными параметрами программы задать MAC-адреса источника и/или получателя, можно автоматизированно создать результирующий дамп-файл только из заданных таким образом пакетов. Результирующий дамп-файл будет построен по тому же принципу, что и исходный.

Команда вызова программы имеет вид:

TAMVIEW.EXE /FI=*ВходнойФайл* [/***имя***[**=*значение***]] …

Параметры вызова программы следующие.

FO – задание имени выходного файла для выборки.

LOG – задание имени выходного ASCII-файла для отчёта.

MF – MAC-адрес <From> при выборке.

MT – MAC-адрес <To> При выборке.

ONLY – приказ отбирать пакеты только по обоим MAC-адресам (И).

OR – приказ отбирать пакеты по обоим MAC-адресам (ИЛИ)

IF или **NIF** – задание IP-From или IP-No-From.

NP – приказ не показывать непечатные символы в правых полях.

GO – автоматический режим работы без управления с клавиатуры.

При управлении с клавиатуры в неавтоматическом режиме при указании **FO** действуют клавиши: <Esc> – немедленный выход с закрытием всех файлов, <Space> – пропуск пакета без копирования, <Enter> – копирование пакета в результирующий файл.

Программа написана на языке PowerBASIC for DOS 3.5.

3.2.7. Программа просмотра сделанных скриншотов TamVPcx.EXE

Структура страницы текстовой видеопамяти предполагает использование двух байтов под каждый символ – сначала указывается код символа, а вслед за ним – код атрибута, с которым данный символ показывается на экране. Скриншот программой сетевого мониторинга записывает подряд нужную страницу видеопамяти на диск как 8000 байтов. Разумеется, в таком виде показать что-либо на экране, да ещё в операционной системе Windows, не получится.

Специально для просмотра сделанных скриншотов сделана данная программа, которая имеет две функции:

– подготовка из сделанного скриншота на диске страницы в видеопамяти и показ её в окне Windows;

– формирование чёрно-белого варианта скриншота специально для иллюстраций в статьях, сборниках и т.д. с записью в виде TXT-файла.

Те рисунки, где важен цвет, в данной работе сделаны с использованием описываемой программы. Показываемый в окне цветной рисунок копируется в формат BMP или PCX и вставляется в текст работы.

Прочие рисунки получены из текстового чёрно-белого варианта скриншота, подготовленного данной программой. Принцип

подготовки: все атрибуты всех символов заменяются на атрибут «чёрный цвет на белом фоне».

Программа написана на алгоритмическом языке PowerBASIC for DOS 3.5.

3.2.8. Программа фиксации даты в логе TamDate.COM

В BAT-файле на рис. 19 есть ссылка на давно разработанную автором программу TamDate. Эта программа используется для занесения в какой-либо протокол нужного текста, снабжённого текущей датой и временем. При вызове

TAMDATE *Text* > PROT.LOG,

в файл PROT.LOG будет добавлена строка наподобие

! 2018.12.03(1) 17:40:56 *Text*,

а также сформирован код завершения согласно порядковому номеру дня недели.

Последний вариант программы – от 28.08.1991. Язык – Макроассемблер для MS-DOS версии 5.10 – 1988 г.

3.2.9. Программы агрегации отчётов

Для конвертации ежедневного отчета или группы отчетов за день в формат CSV разработана программа TAMSNET2.EXE. Поскольку за время эксплуатации программы сетевого мониторинга формат выходного отчёта несколько раз менялся, последующие программы имели возрастающие имена. Последний вариант – TAMSNET5.EXE.

Результат работы программы – CSV-файл, читаемый пакетом SuperCalc-4, содержащий данные всех отчётов за нужные сутки. На рис. 49 представлен такой файл за 03 декабря 2000 г. Он содержит данные 96 отчётов за этот день.

Параметры программы следующие.

LST1=*nnnn* – указывает первый из отчётов, хранящихся в общем каталоге.

KLST=*kkkk* – количество отчетов; если не указано, берутся до конца или до номера 9000. Обычно за день образуется 96 отчётов, однако если были выходы из программы (при этом формируются дополнительные отчёты), число другое.

GO – приказ начать работу. Без этого параметра выдаётся Help.

Последний вариант программы TAMSNET5.EXE – версия 5.3 от 29.10.06.

```
10, "03/12-00",
 96,"Vcp","Vmax","Nref","YPak","YBytes","NPak","NBytes","Comps","Sec","CYCmin",
00:15,   6.07,  44.24,      1,  13244,  5594375,      3,     3164,  22,    900, 118,
00:30,   5.81,  48.10,     13,  10511,  5350988,     15,    17666,  22,    900, 223,
00:45,   6.51, 101.50,      6,  11092,  6002355,      8,     9487,  23,    900, 240,
01:00,   7.61, 100.40,      3,  14329,  6782772,      5,     7570,  24,    871, 235,
01:15,   5.24, 112.62,      0,   8660,  4828068,      0,        0,  21,    900, 105,
01:30,   4.88,  28.43,      0,   8346,  4500408,      0,        0,  21,    900, 231,
01:45,   4.66,  21.57,      0,   7532,  4298714,      0,        0,  21,    900, 239,
02:00,   5.15, 298.16,     52,   8260,  4745613,     98,    93796,  22,    900, 239,
02:15,   4.56,   9.67,      0,   7636,  4205351,      0,        0,  20,    900,  91,
02:30,   4.68,  62.50,     21,   7923,  4313865,     35,    27149,  20,    900, 235,
02:45,   4.57,  17.06,      0,   7459,  4211021,      0,        0,  20,    900, 230,
03:00,   4.49,  10.33,      0,   7133,  4141170,      0,        0,  22,    900, 237,
03:15,   5.07,  43.90,      0,   8702,  4669348,      0,        0,  20,    900,  86,
03:30,   4.72,  14.07,      0,   7819,  4350601,      0,        0,  20,    900, 233,
03:45,   4.42,  59.06,      0,   8047,  4068413,      0,        0,  21,    900, 221,
04:00,   0.36,  24.87,      0,   2599,   329793,      0,        0,  21,    900, 244,
04:15,   0.29,  29.61,      0,   2333,   263314,      0,        0,  19,    900,  84,
04:30,   0.33,  19.34,      0,   2475,   308543,      0,        0,  20,    900, 224,
04:45,   0.33,  14.05,      0,   2443,   299843,      0,        0,  20,    900, 232,
05:00,   0.32,  32.31,      0,   2292,   297695,      0,        0,  21,    900, 234,
05:15,   3.62,  37.50,      8,   5477,  3329766,     12,    10898,  19,    900,  96,
05:30,   0.44,  70.70,      0,   2436,   405235,      0,        0,  19,    900, 246,
05:45,   0.37,  21.24,      0,   2375,   342888,      0,        0,  19,    900, 239,
06:00,   0.76,  53.63,      1,   2715,   699027,      1,     1514,  19,    900, 234,
06:15,   0.27,  19.27,      0,   2200,   252630,      0,        0,  20,    900,  93,
06:30,   0.44,  70.44,      0,   2320,   409523,      0,        0,  20,    900, 249,
06:45,   0.39,  33.21,      0,   2273,   356280,      0,        0,  20,    900, 243,
07:00,   0.21,   3.50,      0,   1955,   197782,      0,        0,  21,    900, 247,
07:15,   0.25,  25.12,      0,   2020,   226991,      0,        0,  18,    900, 104,
07:30,   0.28,  44.69,      0,   2022,   259380,      0,        0,  18,    900, 247,
07:45,   0.24,  42.24,      8,   2033,   224882,     15,    11964,  20,    900, 242,
```

```
08:00,   0.22,  12.94,      0,   2038,   206147,      0,        0,  20,    900, 221,
08:15,   0.17,   1.40,      0,   1773,   159747,      0,        0,  19,    900,  97,
08:30,   0.24,  10.38,      0,   2153,   219777,      0,        0,  20,    900, 253,
08:45,   0.53,  93.20,      1,   2981,   488107,      1,     1514,  20,    900, 256,
09:00,   0.91,  64.08,      0,   4336,   836934,      0,        0,  22,    900, 238,
09:15,   0.42,   9.04,      0,   3831,   388758,      0,        0,  18,    900, 100,
09:30,   0.35,  65.32,      0,   2351,   322634,      0,        0,  18,    900, 247,
09:45,   0.26,  18.25,      0,   2097,   240077,      0,        0,  18,    900, 239,
10:00,   0.39,  18.50,      0,   2787,   360433,      0,        0,  22,    900, 234,
10:15,   0.26,  12.39,      0,   2109,   236535,      0,        0,  22,    900,  94,
10:30,   0.72,  50.33,      0,   6497,   662000,      0,        0,  23,    900, 251,
10:45,   0.27,  21.79,      0,   2245,   248335,      0,        0,  23,    900, 244,
11:00,   0.98,  57.40,      3,   4124,   907062,      8,     7750,  23,    900, 240,
11:15,   6.44,  87.14,      9,  17724,  5934003,     23,    15641,  21,    900,  85,
11:30,   4.24,  98.18,      7,   8684,  3905418,      8,     8928,  22,    900, 241,
11:45,   1.32,  51.58,      0,   4436,  1221027,      0,        0,  22,    900, 249,
12:00,   2.20,  83.84,      8,   7438,  2020171,     16,    10570,  23,    900, 248,
12:15,   2.43,  73.74,      0,   5453,  2239911,      0,        0,  23,    900, 101,
12:30,   4.85,  74.24,      2,  10679,  4468792,      2,     3028,  23,    900, 247,
12:45,   1.15,  82.29,      0,   4212,  1061182,      0,        0,  24,    900, 231,
13:00,   4.55,  94.80,      0,  10202,  4191445,      0,        0,  26,    900, 230,
13:15,   3.50, 144.49,      6,   9337,  3228244,     12,    13238,  22,    900,  97,
13:30,   2.55,  69.94,      0,   9288,  2345998,      0,        0,  23,    900, 245,
13:45,   2.04,  80.98,      2,   6546,  1889297,      4,     1713,  25,    900, 237,
14:00,   5.44, 118.46,     11,  12111,  5014091,     26,    11105,  28,    900, 231,
14:15,  13.04, 270.20,     22,  23983, 12015294,     58,    38885,  23,    900,  83,
14:30,   9.02,  72.43,      0,  16708,  8306964,      0,        0,  24,    900, 238,
14:45,   8.61, 107.57,      5,  17956,  7932169,     12,     5855,  26,    900, 241,
15:00,  10.86, 123.79,     11,  21589, 10017105,     22,    15439,  26,    900, 208,
15:15,  12.82, 183.12,     25,  26346, 11781240,     47,    31838,  26,    900,  97,
15:30,  20.05, 285.42,     11,  36351, 18466141,     21,    19183,  28,    900, 220,
15:45,  16.55, 330.51,     79,  29542, 15250378,    148,    86032,  30,    900, 211,
16:00,  18.24, 272.17,     33,  32714, 16813083,     60,    45597,  30,    900, 232,
```

```
16:15,  25.18, 283.76,     64,  48946, 23184293,    275,   104668,  27,    900,  91,
16:30,  25.37, 208.39,    124,  42650, 23538384,    378,   152422,  30,    900, 233,
16:45,  14.94, 135.75,     14,  27896, 13769733,     23,    19460,  30,    900, 231,
17:00,  20.33, 136.90,     44,  37163, 18728150,     85,    41062,  34,    900, 232,
17:15,  39.67, 194.51,    100,  52374, 36559851,    243,   157980,  31,    900,  97,
17:30,  16.95, 150.67,      2,  27813, 15617087,      4,     1634,  33,    900, 235,
17:45,  15.67, 323.51,     31,  29544, 14434480,     71,    41246,  34,    900, 230,
18:00,   8.64, 324.00,    255,  20756,  7962287,    406,   250915,  35,    900, 230,
18:15,  10.58, 314.57,    137,  24812,  9749382,    290,   136977,  30,    900,  84,
18:30,  11.28, 173.44,      4,  26992, 10388017,      7,     2147,  31,    900, 216,
18:45,  10.19, 126.88,      0,  20971,  9392354,      0,        0,  32,    900, 224,
19:00,  10.26, 154.70,      1,  21701,  9456548,      3,     1634,  32,    900, 237,
19:15,   9.11, 103.45,      2,  18493,  8473582,      2,     1159,  27,    900,  84,
19:30,  13.22, 203.90,     53,  24007, 12181244,    104,    70498,  28,    900, 221,
19:45,  14.66, 143.88,     84,  30146, 13480614,    149,   108804,  28,    900, 240,
20:00,   3.60,  60.66,      1,   9070,  3315354,      3,      905,  29,    900, 238,
20:15,   2.25, 130.51,      0,   6483,  2073122,      0,        0,  24,    900,  83,
20:30,   4.85, 301.50,    389,  15741,  4468989,    889,  1131902,  25,    900, 221,
20:45,   7.58,  86.24,     10,  21850,  6978534,     27,     6539,  25,    900, 226,
21:00,   1.74, 126.68,     23,   5276,  1605823,     50,    43984,  26,    900, 224,
21:15,   0.41,  30.07,      1,   3184,   377157,      2,     1006,  25,    900,  85,
21:30,   0.42,  12.30,      0,   2816,   388731,      0,        0,  25,    900, 243,
21:45,   1.20,  21.71,      4,   4979,  1101718,      4,     5812,  25,    900, 247,
22:00,   0.57,  12.47,      0,   3739,   528988,      0,        0,  28,    900, 244,
22:15,   0.71,  41.90,      0,   3342,   652195,      0,        0,  23,    900,  84,
22:30,   0.44,  17.00,      0,   3314,   405414,      0,        0,  23,    900, 244,
22:45,   0.35,  19.31,      0,   2713,   326752,      0,        0,  23,    900, 239,
23:00,   0.51,  15.03,      0,   3184,   470235,      0,        0,  23,    900, 235,
23:15,   0.96,  61.54,     11,   4185,   886424,     19,    15112,  19,    900,  83,
23:30,   0.23,   5.22,      0,   2284,   215284,      0,        0,  19,    900, 243,
23:45,   0.50,   9.51,      0,   2879,   458615,      0,        0,  19,    900, 232,
00:00,   0.82,  22.35,      0,   4702,   751995,      0,        0,  20,    900, 239,
```

Рис. 49. CSV-файл, интегрирующий отчёты за 03.12.2000 г.

Программа написана на языке PowerBASIC for DOS 3.5, последняя версия 1.2 от 30.08.2000.

Полученные CSV-файлы именуются как **D*yymmdd*.CSV** и служат входом для макропрограммы на языке SuperCalc-4, которая исполняет дальнейшую интеграцию в вид, показанный на рис. 50. Эти файлы именуются **E*yymmdd*.CSV**.

```
10,"E001203",,,,,,,,,
24,"Vcp","Vmax","Nref","YPak","YBytes","NPak","NBytes","Comps","Sec","CYCmin"
"01:00",6.49,101.5,23,49176,23730490,31,37887,24,3571,118
"02:00",4.98,298.16,52,32798,18372803,98,93796,22,3600,105
"03:00",4.58,62.5,21,30151,16871407,35,27149,22,3600,91
"04:00",3.64,59.06,0,27167,13418155,0,0,21,3600,86
"05:00",.32,32.31,0,9543,1169395,0,0,21,3600,84
"06:00",1.3,70.7,9,13003,4776916,13,12412,19,3600,96
"07:00",.33,70.44,0,8748,1216215,0,0,21,3600,93
"08:00",.25,44.69,8,8113,917400,15,11964,20,3600,104
"09:00",.46,93.2,1,11243,1704565,1,1514,22,3600,97
"10:00",.36,65.32,0,11066,1311902,0,0,22,3600,100
"11:00",.56,57.4,3,14975,2053932,8,7750,23,3600,94
"12:00",3.55,98.18,24,38282,13080619,47,35139,23,3600,85
"13:00",3.24,94.8,2,30546,11961330,2,3028,26,3600,101
"14:00",3.38,144.49,19,37282,12477630,42,26056,28,3600,97
"15:00",10.38,270.2,38,80236,38271532,92,60179,26,3600,83
"16:00",16.9,330.51,148,124953,62310842,276,182650,30,3600,97
"17:00",21.49,283.76,246,156655,79220560,761,317612,34,3600,91
"18:00",20.23,324,388,130487,74573705,724,451775,35,3600,97
"19:00",10.58,314.57,142,94476,38986301,300,140758,32,3600,84
"20:00",10.16,203.9,140,81716,37450794,258,181366,29,3600,84
"21:00",4.1,301.5,422,49350,15126468,966,1182425,26,3600,83
"22:00",.65,30.07,5,14718,2396594,6,6818,28,3600,85
"23:00",.5,41.9,0,12553,1854596,0,0,23,3600,84
"00:00",.63,61.54,11,14050,2312318,19,15112,20,3600,83
```

Рис. 50. CSV-файл вторичной интеграции за 03.12.2000 г.

Следует отметить, что независимо от того, сколько было отчётов за интегрируемый день, и в какие точно часы и минуты они были, в файлах вторичной интеграции всегда присутствуют точные 24 часа с нулевыми минутами.

В файлах вторичной интеграции автоматически строится ряд графиков, наподобие указанных на рис. 30, 31, 32 и 33.

Возможна также дальнейшая интеграция собранных данных для получения недельных и месячных файлов. Примеры результатов такой интеграции приведены выше на рис. 36, 37.

При необходимости можно провести интеграцию по «срезам» – группам компьютеров, как это показано на рис. 40–45.

3.3. Отладка мониторной программы

Проектируя столь сложные комплексы программ, невозможно было не задуматься о способах их отладки. Программа сетевого мониторинга, вместе со своими компонентами, включала несколько

сегментов, часть на PowerBASIC, часть на Макроассемблере, и занимала почти всю основную память MS-DOS. Вместе с ней легко умещался драйвер эмуляции сети TamDrvr.EXE и клавиатурный драйвер TamKb.COM, но места для отладчика уже не было.

Выход из положения был найден следующий. Стандартный вариант программы мониторинга включал два больших буфера для приёма сетевых пакетов, определяемые как "**DIM STATIC A1(0:%BufSize), A2(0:%BufSize)**". Переменная %BufSize в начале программы имела максимальный размер для словных массивов A1 и A2, т.е. длина каждого массива определялась как 32768 элементов, или 65536 байтов (132Кб для обоих). Однако, помня, что максимальный размер сетевого пакета составлял 1560 байтов, перед началом отладки программа перекомпилировалась со значением %BufSize в 1580, что давало 3160 байтов в каждом массиве. Общая экономия памяти оказывалась таковой, что позволяла загружать и использовать отладчик AFD (Advanced Full-Screen Debugger), который отнимал примерно 97 Кб оперативной памяти.

Драйверы HIMEM.SYS и EMM386.EXE, как показано на рис. 47, присутствовали, но реально верхняя память не использовалась иначе, как для размещения там части MS-DOS (см. рис. 51).

```
Memory Type         Total  =   Used  +   Free
----------------  -------   -------   -------
Conventional          640K       87K       553K
Upper                 107K       18K        89K
Reserved              384K      384K         0K
Extended (XMS)     15,253K      265K    14,988K
----------------  -------   -------   -------
Total memory       16,384K      753K    15,631K

Total under 1 MB      747K      104K       643K

Largest executable program size       553K (566,576 bytes)
Largest free upper memory block        46K  (47,440 bytes)
MS-DOS is resident in the high memory area.
```

Рис. 51. Распределение оперативной памяти после загрузки MS-DOS

Таким образом, в момент начала отладки сначала загружался отладчик AFD, который после команды "**Q**{UIT} **R**" оставался резидентным в памяти. Затем грузились клавиатурный дайвер и драйвер эмуляции локальной сети (файл с необходимыми для от-

ладки пакетами был заранее подготовлен), а последним загружалась собранная программа сетевого мониторинга с «уменьшенными» буферами, разумеется, поставленная в режим отладки, когда время показа страницы «0» не ограничено.

Для быстрейшего отыскания в оперативной памяти необходимых блоков, на экране «0» показываются сегментные адреса подпрограммы TamCnv.OBJ, подпрограммы TamInet.OBJ, обоих буферов для считывания пакетов и разнообразная отладочная информация (см. рис. 12), такая, как индикация заполнения буферов, плавающие смещения текущей загрузки буферов и многое другое.

Сами подпрограммы TamCnv.OBJ и TamInet.OBJ устроены таким образом, что все важные точки начала алгоритмических блоков начинались с оператора NOP (**90**h), который на время отладки мог заменяться вручную на INT3 (**CC**h), что давало прерывание и переход к отладчику AFD, всегда находящемуся в ждущем режиме.

Пошаговый приём сетевых пакетов осуществляется после нажатия и отпускания регистровой клавиши Left Shift. Если необходимо, используются специальные режимы пошагового продвижения сетевых пакетов в буферах с помощью клавиш отладки “[” и “]”, показанных на рис. 17.

Следует отметить, что, к сожалению, исполнение отладки в окне Windows неудобно, поскольку вызов отладчика AFD из ждущего режима исполняется сочетанием клавиш <**Ctrl+Esc**>, что является стандартной комбинацией Windows для аналога активации Главного меню.

При желании смены файла с дампированными пакетами необходимо снять отлаживаемую программу и драйвер эмуляции, сделать необходимые переименования файлов и вновь запустить драйвер эмуляции и отлаживаемую программу.

3.4. Мониторинг при изменившейся схеме ЛВС

Как уже было сказано, тематика сетевого мониторинга разрабатывается автором с 1999 г. За это время несколько раз существенно изменилась структура ЛВС, формат некоторых экранов программы мониторинга. И сама программа мониторинга претерпела ряд существенных изменений в сторону оптимизации своей работы.

В данном томе автор сознательно ограничился первичными сведениями о структуре ЛВС и работе программы сетевого мониторинга. Практические приложения и развитие программы сете-

вого мониторинга будут рассмотрены во втором томе данной работы, планируемом к отдельной публикации.

Как уже отмечалось, по условиям гранта 04-07-90260в РФФИ, результаты промышленной разработки обязаны были быть размещены в Интернете, что и было исполнено в 2004 г. специальным разделом Антивирусного сайта. На рис. 52 показана принципиальная схема потоков информации при сетевом мониторинге к моменту завершения промышленной разработки (2006 г.).

Как можно видеть из рис. 52, персональный компьютер с мониторной программой (МП), регулярно получая данные от наблюдающей станции (НС) по serial-кабелю, исполняет агрегацию данных и посылает через локальную сеть результаты на АВ-сервер [28] [29] [30] [31]. Этот случай является примером функционала, работающего на АВ-сервере помимо антивирусных дополнений. Одновременно используется функция отсечения заражённых ПК с помощью коммутатора Cisco Catalyst.

Подробнее все эти связи [32] [33] [34] [35] [36] [37] [38] будут описаны в последующих томах работы.

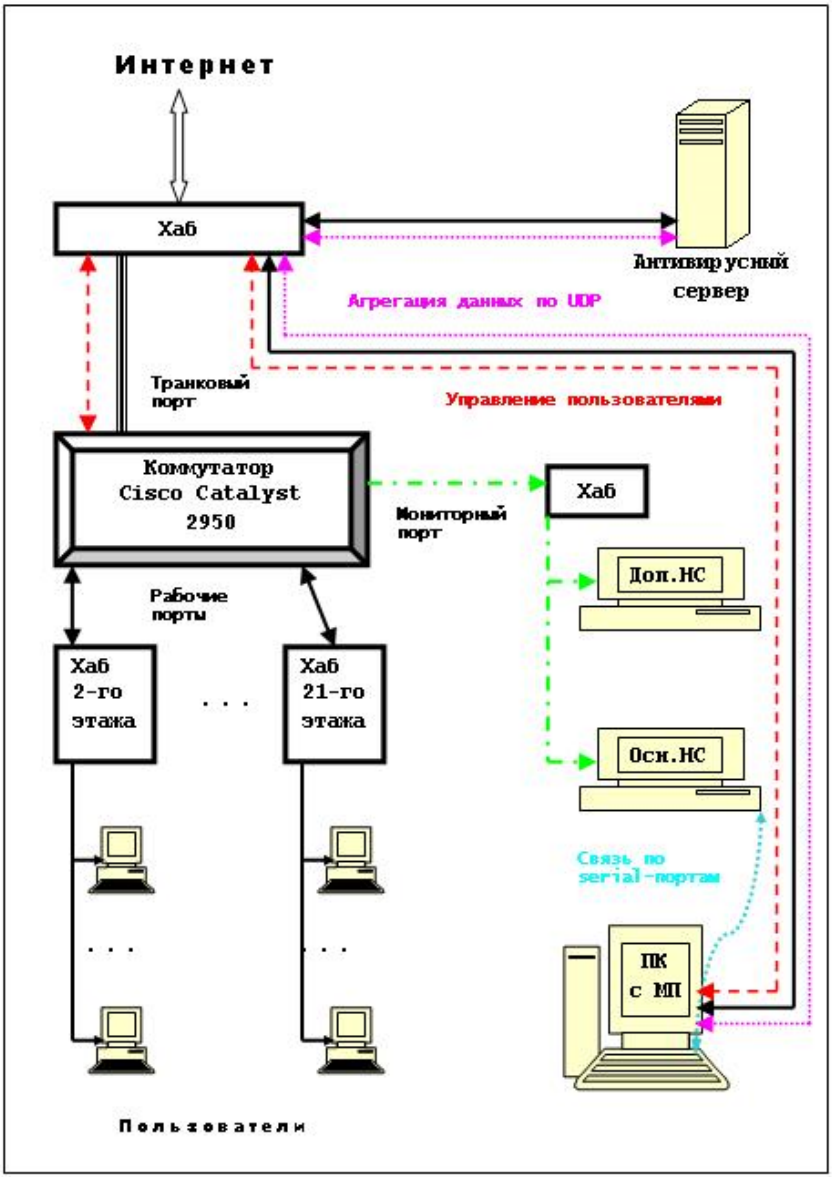

Рис. 52. Схема сетевого мониторинга в 2006 г.

ЗАКЛЮЧЕНИЕ

Том 1 данной работы посвящён созданию прототипа сетевого анализатора, основанного на обычном ПК и имеющемся в продаже сетевом адаптере. Работая в круглосуточном режиме и наблюдая все имеющие хождение пакеты в интересуемом участке локальной вычислительной сети, снабжённый процедурами, организующими круглосуточную работу, сетевой анализатор канального уровня превращён в средство постоянного сетевого мониторинга объектов ЛВС.

Исследованы особенности физического строения и канального уровня передачи сетевых данных в ЦЭМИ РАН. Определена связь между канальным уровнем пакетов и вышестоящими по модели ISO-OSI уровнями передачи сетевых данных.

Определён метод и найдены технические средства получения всех сетевых пакетов канального уровня ISO-OSI на выделенном ПК, работающем под управлением операционной системы MS-DOS 6.22. Показано, что избранная ОС адекватна поставленной задаче реального времени.

Синтезированы программные средства сетевого мониторинга. Для отладки указанных средств разработан эмулятор приёма сетевых пакетов (драйвер локальной сети).

Создание описанного средства позволило решить принципиальный вопрос о детальном отложенном рассмотрении сетевых пакетов. Уже сама по себе эта возможность представляет основу для многих исследований, таких, как определение точного алгоритма межпрограммной связи HyperTerminal с коммутаторами Cisco Catalyst, отслеживание процессов получения файлов с серверов Apache по протоколу HTTP 1.1 и многими другими.

Внедрение сетевого мониторинга сразу же решает ряд биллинговых задач, таких, как отслеживание средней и максимальной скоростей в сети, распределение нагрузки по принимаемым из Интернета, посылаемым в Интернет и внутрисетевым пакетам. Эти результаты фиксируются как в Online-режиме с помощью экранов Наблюдающей станции, так и в форме долговременных протоколов, сохраняемых в архиве на другом компьютере.

Одной из частных решённых задач является отслеживание почтовой активности пользователей.

Другой решённой частной задачей является слежение за активностью набора выделенных сетевых устройств – обычно, серверов общего назначения. При этом отказ любого из серверов, и, в частности, общего маршрутизатора не влияет на получение результатов сетевым мониторингом по другим отслеживаемым устройствам.

Поскольку сами технические средства предложенного варианта сетевого мониторинга не испускают никаких пакетов и даже не имеют ни IP-адреса в сети, ни MAC-адреса, фиксация наличия наблюдения принципиально невозможна. По тем же причинам, какое бы то ни было управление или злонамеренное вмешательство в средства предложенного варианта сетевого мониторинга через сеть неисполнимо.

Показано, что с помощью синтезированных средств на ПЭВМ невысокой мощности возможно устойчивое наблюдение сетевых пакетов канального уровня, в том числе коллизионных.

Успешное внедрение предложенной технологии позволило решить ряд различных задач, подробно описываемых в других томах данной монографии.

К их числу, в частности, относятся:

– выявление атак сетевых вирусов на ЛВС;

– оптимизация структуры сети ЛВС с выделением сегментов, содержащих ПК с большими объёмами пересылаемых данных, для исключения влияния на остальные участки сети;

– определение нарушающих правила работы в сети персональных компьютеров или серверов:

– автоматическое отключение от ЛВС устройств, нарушающих правила работы в сети, при использовании централизованного коммутатора Cisco Catalyst;

– создание переносной наблюдающей станции, пригодной для экспресс-анализа сторонних сетей.

Предложенная технология работы с сетевым мониторингом опробована в ЦЭМИ РАН и ряде сторонних организаций.

Все созданные автором утилиты спроектированы с поддержкой обращения с набором управляющих параметров, что позволяет их быстро перенастраивать на нужный режим работы и требуемые объекты информационного пространства. Все утилиты являются 16-битными приложениями MS-DOS.

Автору к моменту публикации данной работы, несмотря на почти 20 лет эксплуатации разработанных средств, неизвестны полные аналоги описанных программно-технических средств сетевого мониторинга.

Представленные средства сравнительно легко могут быть тиражированы для использования в других организациях. Необходимые материальные ресурсы для этого гораздо меньшие, чем покупка специализированных пакетов.

ПЕРЕЧЕНЬ РИСУНКОВ

ПЕРЕЧЕНЬ ТЕРМИНОВ

ПЕРЕЧЕНЬ ССЫЛОЧНЫХ ДОКУМЕНТОВ

1. Терентьев А.М. Методы и средства наблюдения загрузки локальных вычислительных сетей на примере ЦЭМИ РАН / Препринт #WP/2001/110 – М., ЦЭМИ РАН, 2001, – 74 с. – ISBN 5-8211-0141-7.

2. Терентьев А.М. Информационная безопасность в крупных локальных сетях // Концепции. – 2002. – №1 (9). – С. 25–30. – Свидетельство Роскомпечати 014305.

3. Терентьев А.М. Задачи полноценного аудита корпоративных сетей // Концепции. – 2003. – №1 (11). – С. 94–95. – Свидетельство Роскомпечати 014305.

4. Хейвуд Д. Внутренний мир Microsoft TCP/IP / Д. Хейвуд; пер. с англ. – К.: ДиаСофт, 2000. – 496 с.

5. Паркер Т. TCP/IP. Освой самостоятельно. – М.: Бином, 1997. – 448 с.

6. Компьютерные сети+. Учебный курс: Официальное пособие Microsoft для самостоятельной подготовки / Пер. с. англ. – 2-е изд., испр. – М.: Русская Редакция, 2000. – 552 с. – ISBN 5-7502-0134-1.

7. Найк Д. Стандарты и протоколы Интернета / Пер. с англ. – М.: Русская редакция; ТОО «Channel Traiding Ltd», 1999. – 384 с.

8. Крейг Х. Персональные компьютеры в сетях TCP/IP / Пер. с англ. – К.: Издательская группа BHV, 1997. – 384 с. – ISBN 5-7733-0019-2.

9. Microsoft TCP/IP. Учебный курс: Официальное пособие Microsoft для самостоятельной подготовки / Пер. с. англ. – 2-е изд., испр. – М.: Русская Редакция, 1999. – 344 с. – ISBN 5-7502-0112-0.

10. Медведовский И.Д. Атака на Интернет / И.Д. Медведовский [и др.]. – 3-е изд., стер. – М.: ДМК, 2000 – 336 с.

11. Терентьев А.М. Многопользовательский режим работы на персональных ЭВМ. Средства системной поддержки / Препринт #WP/99/071 – М., ЦЭМИ РАН, 1998. – 79 с. (рус.) – ISBN 5-8211-0035-6.

12. Терентьев А.М. Методы аудита локальных сетей в MS-DOS / А.М. Терентьев, А.Е. Винокуров // Вопросы информационной безопасности узла Интернет в научных организациях: Сборник трудов / Под ред. М.Д. Ильменского – М: ЦЭМИ РАН, 2001, С. 60–63. – ISSN 5-8211-0134-4.

13. Анин Б. Защита компьютерной информации. – СПб.: БХВ-Петербург, 2000. – 384 с.

14. Кочетова Н.А. Методы и средства защиты маршрутизаторов и серверов удалённого доступа производства Cisco Systems / Н.А. Кочетова, Н.Г. Ляпичева // Вопросы информационной безопасности узла Интернет в научных организациях: Сб. трудов / под ред. М.Д. Ильменского. – М: ЦЭМИ РАН, 2001. – С. 10–42. – ISBN 5-8211-0134-4.

15. Ralf Brown's Interrupt List. Indexed HTML Version – Release 61 [Электронный ресурс]. – Режим доступа: http://www.ctyme.com/rbrown.htm

16. PC/TCP Packet Driver Specification [Электронный ресурс]. – Режим доступа: http://www.crynwr.com/packet_driver.html

17. Ломов А. ДОС и теперь живее всех живых // Hard'n'Soft. – 1998. – №2. – С. 50.

18. Zale, R.S. PowerBASIC Compiler, version 3. User's Guide. – PowerBASIC, Inc. 316 Mid Valley Center. Carmel, CA 93923. – 335 с.

19. Zale, R.S. PowerBASIC Compiler, version 3. Reference Guide. – PowerBASIC Inc. 316 Mid Valley Center. Carmel, CA 93923. – 335 с.

20. PowerBASIC [Электронный ресурс]. – Режим доступа: https://www.powerbasic.com

21. Ляпичева Н.Г. Информационные сервисы и обеспечение их защиты от несанкционированного доступа из сети Интернет / Использование и развитие современных информационных технологий в научных исследованиях: Сб. статей / Под ред. М.Д. Ильменского. – М: ЦЭМИ РАН, 2003. – С. 32–63.

22. Терентьев А.М. Индивидуальная парольная защита рабочих станций // Вопросы информационной безопасности узла Интернет в научных организациях: Сборник статей / Под ред. М.Д. Ильменского. – М: ЦЭМИ РАН, 2001. – С. 84–89.

23. Антивирусный сайт ЦЭМИ РАН [Электронный ресурс]. – Режим доступа: http://av.cemi.rssi.ru

24. Терентьев А.М. Технология антивирусной защиты сетевых ПК с использованием специализированного сервера и ПК-сателлита / А.М. Терентьев, А.С. Львова // Развитие и использование средств сетевого мониторинга и аудита: Сб. статей / Под ред. А.М. Терентьева. – М., ЦЭМИ РАН, 2004. – Вып. 1. – С. 47–59. – ISBN 5-8211-0317-7.

25. Терентьев А.М. Корпоративный вариант технологии использования антивирусных пакетов DrWeb в научных учреждениях: монография / А.М. Терентьев. – Чебоксары. ИД «Среда», 2018. – 100 с. – ISBN 978-5-6040294-5-9. – DOI 10/31483/в-15, DOI 10.31483/r-11245.

26. Терентьев А.М. Лечение компьютерных вирусов на ПК с помощью подключения внешних операционных систем / А.М. Терентьев, П.В. Григорьев // Развитие технологий и инструментальных средств информационной безопасности: Сб. статей / Под ред. А.М. Терентьева. – М., ЦЭМИ РАН, 2012. – Вып. 2. – С. 6–21. – ISBN 978-5-8211-0615-5.

27. Терентьев А.М. Антивирусное обеззараживание персональных компьютеров с помощью подключения сторонних операционных систем // Национальные интересы: приоритеты и безопасность. – М.: Финансы и кредит. – 2012. – №37 (178). – С. 45-51. – ISSN 2073-2872.

28. Терентьев А.М. Технология представления результатов сетевого мониторинга в Интернете. Системная служба // Стратегии устойчивого развития мировой науки: XXVII Международная научная конференция. – М.: Евразийское научное объединение, 2017. – №5 (27). – Т. 1. – С. 41–46. – ISSN 2411-1899.

29. Терентьев А.М. Технология представления результатов сетевого мониторинга в Интернете. Управление системной службой // Интеграция науки в современном мире: XXVIII Международная научная конференция. – М.: Евразийское научное объединение, 2017. – №6 (28). – Т. 1. – С. 28–33. – ISSN 2411-1899.

30. Терентьев А.М. Технология представления результатов сетевого мониторинга в Интернете. Результаты // Теоретические и практические вопросы современной науки: XXIX Международная научная конференция. – М.: Евразийское научное объединение, 2017. – №7 (29). – Т. 1. – С. 27–31. – ISSN 2411-1899.

31. Терентьев А.М. Технология представления результатов сетевого мониторинга в Интернете. Дополнительные сведения // Научные аспекты современных исследований: XXX Международная научная конференция. – М.: Евразийское научное объединение, 2017. – №8 (30). – Т. 1. – С. 37–41. – ISSN 2411-1899.

32. Терентьев А.М. Построение и развитие системы сетевого мониторинга // Развитие и использование средств сетевого мониторинга и аудита: Сб. статей / Под ред. А.М. Терентьева. – М., ЦЭМИ РАН, 2004. – Вып. 1. – С. 5–23. – ISBN 5-8211-0317-7.

33. Терентьев А.М. Мониторинг корпоративной сети ЦЭМИ РАН в условиях использования коммутатора Cisco Catalyst / А.М. Терентьев, Н.Г. Ляпичева, Н.А. Кочетова // Развитие и использование средств сетевого мониторинга и аудита: Сб. статей / под ред. А.М. Терентьева. – М., ЦЭМИ РАН, 2004. – Вып. 1. – С. 75–87. – ISBN 5-8211-0317-7.

34. Терентьев А.М. Мониторная программа как средство интеграции данных наблюдающей станции в локальной сети // Развитие и использование средств сетевого мониторинга и аудита: Сб. статей / под ред. М.Д. Ильменского. – М., ЦЭМИ РАН, 2005. – Вып. 2. – С. 6–13. – ISBN 5-8211-0365-7.

35. Ляпичева Н.Г. Коррекция ошибок HTTP-соединения в локальной сети ЦЭМИ РАН / Н.Г. Ляпичева, А.А. Акиншин, А.М. Терентьев, П.В. Григорьев / Развитие технологий и инструментальных средств информационной безопасности: Сб. статей / Под ред. А.М. Терентьева. – М., ЦЭМИ РАН, 2012. – Вып. 2. – С. 49–58. – ISBN 978-5-8211-0615-5.

36. Терентьев А.М. Поддержание доступности HTTP-соединения с помощью периодического пингования // Современные концепции научных исследований: XXIV Международная научная конференция. – М.: Евразийское научное объединение, 2017. – №2 (24). – Т. 1. – С. 37–39. – ISSN 2411-1899.

37. Вегнер В.А. Разработка и реализация типового проекта выделенного сегмента ЛВС на примере ПК административно-финансовой группы ЦЭМИ РАН / В.А. Вегнер, Н.Г. Ляпичева, А.С. Львова, А.М. Терентьев / Развитие и использование средств сетевого мониторинга и аудита: Сб. статей / Под ред. А.М. Терентьева. – М., ЦЭМИ РАН, 2004. – Вып. 1. – С. 88–101. – ISBN 5-8211-0317-7.

38. Терентьев А.М. HTTP-атаки на web-сервер // Актуальные вопросы развития науки в мире: XXVI Международная научная конференция. – М.: Евразийское научное объединение, 2017. – №4 (26). – Т. 1. – С. 58–62. – ISSN 2411-1899.

Для заметок

Для заметок

Научное издание

Терентьев Александр Макарович

СЕТЕВОЙ МОНИТОРИНГ.
МЕТОДЫ И СРЕДСТВА.
ТОМ 1

Монография
Чебоксары, 2019 г.

Редактор *А.М. Терентьев*
Компьютерная верстка и правка *Н.К. Толкушкина*
Дизайн обложки *Н.В. Фирсова*

Подписано в печать 03.04.2019 г.
Дата выхода издания в свет 10.04.2019 г.
Формат 70×100/16. Бумага офсетная. Печать офсетная.
Гарнитура Times. Усл. печ. л. 6,7425. Заказ 591. Тираж 500 экз.
Издательский дом «Среда»
428005, Чебоксары, Гражданская, 75, офис 12
+7 (8352) 655-731
info@phsreda.com
https://phsreda.com

Отпечатано в ООО «Типография «Перфектум»
428000, Чебоксары, ул. К. Маркса, 52