– методы теории массового обслуживания;
– методы проектирования (планирование сетей, масштабирование сетей);
– методы анализа данных и математической статистики.

В настоящем сборнике публикуется ряд работ, подготовленных в рамках исследований этой школы авторами Саенко В.И., Клименко А.В., Панченко А.В., Макрушан И.А.

Поступила в редколлегию 14.06.98

УДК 519.687.5:681.324

АНАЛИЗ ТРАНСПОРТНЫХ ПРОЦЕССОВ В ЛОКАЛЬНЫХ СЕТЯХ

САЕНКО В.И., ПАНЧЕНКО А.В.

Приводится классификация возможных сбоев в сети, способствующих частичной или полной потере функциональности. Проявление сбоев рассматривается с позиции семиуровневой модели. Предлагаются процедуры оценки появления ошибок в сети, причины их возникновения, а также варианты принятия решений по их устранению. Процедуры включаются в специализированный программный комплекс анализатора транспортных процессов в локальной сети, анализатор предназначен для использования при мониторинге и администрировании сети.

1. Актуальность

Современная информационная система с множественным доступом – это сетевая система, функционирование которой обеспечивается несколькими слоями сетей [1]. Механизмы переноса и передачи данных между ресурсами и пользователями сети обеспечиваются транспортной сетью, образующей основной сетевой слой. Построение информационных сетей основано на использовании сетевых технологий. Современные сетевые технологии – это технологии корпоративных сетей с открытой или закрытой intra-extranet-транспортной средой передачи. Такие сети характеризуются большим разнообразием аппаратных и операционных платформ (не принадлежащих семейству Wintel-платформ), разнообразием протоколов (существует более 140 типов) и высокой распределенностью общих ресурсов. Представляется актуальным решение задачи поддержания полной (стопроцентной) функциональности информационной системы и обеспечения восстановления ее функциональности за минимально

возможный интервал времени. Задача решается в рамках администрирования и мониторинга транспортной сети. Наиболее целесообразным является автоматический анализ ситуации в сети и выдача пользователю рекомендаций о вероятных причинах и источниках неполадок.

2. Описание проблемы

Функциональность системы будем рассматривать как обеспеченность решения заданного набора задач **X**. Каждой задаче Xj∈**X** ставим в соответствие вектор некоторых показателей **Wj** , характеризующих степень ее решаемости. Стопроцентная возможность решения каждой задачи определяет стопроцентную возможность функционирования всей системы, т.е. полную ее функциональность. Отказ в выполнении какой-либо задачи связан с возникновением в системе различных сбоев. Таким образом, сбои будем понимать именно как отказ системы в обеспечении функциональности решения какой-либо задачи.

При анализе работы сети необходимо принимать во внимание множество важных факторов, касающихся аппаратных и программных платформ, системы кабельных соединений, взаимодействия отдельных компонентов сети посредством разнообразных протоколов. Анализ перечисленных факторов осуществляется при использовании специальных программно-аппаратных средств-анализаторов протоколов.

Анализатор протоколов предоставляет возможность исследовать большинство протоколов, используемых в современных сетях. Современному состоянию информационных систем соответствует разнообразие стеков протоколов, стандартизированных в рамках семиуровневой модели взаимодействия открытых систем (OSI). Это разнообразие тем выше, чем более разветвлена сеть и чем больше разнородных программных платформ используется в ней. Такое положение отражает ситуацию в большинстве современных корпоративных сетей. Анализ взаимодействия процессов в сети для оценки производительности и поиска неполадок сводится к анализу всего множества стеков протоколов, используемых в данной сети.

Корпоративная сеть представляет собой географически распределенную структуру с определенным нестандартизированным набором разнообразных сетевых устройств, установленных в узлах сети. Тенденция увеличения количества устройств в сети обуславливает повышение вероятности отказа какого-либо из ее элементов в текущий момент времени, а значит, и возможность временной потери стопроцентной функциональности сети. С ростом размеров сети увеличивается интервал времени на поиск и устранение ло-

кальной неисправности, т.е. увеличивается период частичной потери функциональности сети. В данной ситуации наиболее целесообразным является автоматический анализ ситуации в сети и выдача пользователю рекомендаций о наиболее вероятных причинах и источниках неполадок, т.е. разработка таких процедур и средств, которые обеспечат полный мониторинг задач и администрирование с поддержкой процедур принятия решений.

3. Анализ сетевых сбоев

Сбои сети рассматриваются на каждом из уровней семиуровневой модели сети. Для физического и канального уровня это искажения сигнала, потеря бит, искажения в полях кадра. Для сетевого и транспортного уровней это повышение загруженности полосы пропускания сети, ошибки пакетов и дейтаграмм.

Для канального уровня эти сбои проявляются прежде всего в виде различных ошибок кадров: коллизии (локальные, удаленные, поздние); ошибки контрольной последовательности; ошибки длины кадра. Результаты анализа возникающих ошибок сведены в таблице. Анализ показал, что в случае возникновения локальных или удаленных коллизий длина принятого кадра меньше 64 байт и данный кадр имеет неверную контрольную последовательность. Локальные коллизии регистрируются схемой обнаружения коллизий, входящей в состав сетевого адаптера. Возможной причиной возникновения большого числа коллизий может быть перегруженный сегмент или слишком большая его длина. В качестве рекомендаций пользователю предлагается сравнить текущую загруженность сети с измеренной ранее и проверить реальную длину сегмента.

Возникновение поздних коллизий связано с неисправностью оборудования сети или кабельной системы. Данная ситуация определяется схемой обнаружения коллизий сетевого адаптера, при этом длина пакета не менее 64 байт, а контрольная последовательность неверна. Причиной является неисправность сетевого адаптера или слишком большая длина сегмента.

Ошибки контрольной последовательности могут быть вызваны неисправностью сетевого адаптера или кабельной системы. Неисправный компонент сети искажает передаваемый пакет и передает ошибочные сигналы в линию.

Ошибка длины кадра определяется по выходу длины пакета за пределы диапазона 64–1518 байт. Данная ошибка возникает по вине сетевого драйвера, файл которого может иметь устаревшую версию либо может быть искажен.

Выявление данных ошибок и вероятных причин их появления возможно только в случае непосредственного подключения анализатора к сегменту, где произошла ошибка.

Ошибка	Способ определения			Возможные причины
	Длина пакета	Ошибка контрольной последовательности	Определение схемой обнаружения коллизий сетевого адаптера	
Канальный уровень				
Локальная коллизия	Менее 64 байт	+	+	Перегруженный сегмент, слишком длинный сегмент
Удаленная коллизия	Менее 64 байт	+	-	Перегруженный сегмент, слишком длинный удаленный сегмент
Поздняя коллизия	Не менее 64 байт	+	+	Слишком длинный сегмент, неисправность сетевого адаптера
Ошибка контрольной последовательности (выравнивания)	Не менее 64 байт	+	-	Неисправный кабель, неисправность сетевого адаптера
Ошибка длины кадра	Менее 64 байт или более 1518 байт	–	–	Неисправный сетевой адаптер

Оценка загруженности полосы пропускания сети производится в результате анализа группы показателей:

- средний и пиковый уровень загруженности полосы пропускания;
- пиковое значение числа пакетов в секунду;
- пиковое значение числа ошибок в секунду.

Для Ethernet средний уровень загруженности полосы пропускания не должен превышать 30%, пиковый – 55% от пропускной способности канала. Пиковое значение числа ошибок – не более 1-2% от общего числа пакетов. Пиковое значение числа пакетов зависит от средней длины пакета в сети и не превышает 4000 при средней длине пакета 64 байта.

4. Реализация функций анализа процессов в сетях NetWare

Анализ процессов в сети сводится к реализации специальных процедур в системе мониторинга. Он необходим прежде всего, чтобы снизить суммарное время потерь функциональности сети. Реальный режим функционирования транспортной сети характерен тем, что весь временной интервал может быть разбит на участки T_{1i},

на которых сеть находилась в состоянии полной функциональности, на участки T_{2i}, на которых сеть находилась в состоянии частичной потери функциональности, и на участки T_{3i}, соответствующие полной потере функциональности. В большинстве случаев, как показано в [2,3], участки T_{3i} трудно прогнозируемы, характеризуются поломками аппаратных или программных систем и в хорошо отлаженной системе очень редки. Наибольший интерес представляют участки T_{2i}, которые довольно часто проявляются в сети, трудно устранимы и часто имеют "блуждающий" характер. Анализ процессов позволяет выявить источники и причины возникновения T_{2i} и свести к минимуму суммарную величину этих участков. При этом за основу принимается концепция, заключающаяся в том, что причиной сбоев является скрытое (неисправное) локальное устройство, которое необходимо выявить. Неисправности в сети приводят прежде всего к перегруженности сетевого трафика и сервера. Перегруженность может произойти из-за сбоев в функционировании какой-либо станции (тогда эта станция будет создавать большую нагрузку на сеть), из-за неправильной обработки запроса-пакета, из-за появления станции, работающей в широковещательном режиме; из-за файловых запросов, из-за операций печати. Рассмотрим процедуры решения каждой из задач.

Процедура обнаружения устройства, вызывающего сбои, строится таким образом, что в случае превышения одного из пороговых значений загруженности сети производятся следующие действия:

– собирается статистическая информация обо всем сетевом трафике;

– сортируются все имена рабочих станций по объему переданных данных;

– в результате сортировки определяются рабочие станции, которые больше других загружают полосу пропускания сети.

Механизм управления потоком сервера NetWare позволяет серверу сообщить рабочей станции о своей перегруженности. Если рабочая станция отправила запрос на сервер и не получила ответ в течение времени таймаута, то она посылает запрос повторно. В случае длительной обработки сервер посылает NCP-пакет типа 9999–"запрос обрабатывается". Данный пакет свидетельствует о перегруженности сервера. Причиной перегруженности сервера может быть не та рабочая станция, которая получила пакет "запрос обрабатывается". При получении пакета "запрос обрабатывается" рабочая станция сбрасывает свой счетчик таймаута и продолжает ожидать ответ. Не получая ответа, рабочая станция может повторять запрос то количество раз, которое указано в параметре IPX RETRY в файле NET.CFG. Когда счетчик повторов будет исчерпан, пользователь получит сообщение "Error receiving from server server_name".

Процедура по выявлению типов пакетов, приводящих к возникновению сбоев, основана на анализе статистических выборок, объединяющих однородные типы пакетов, появляющиеся в заданном интервале времени. Введем параметр $\mathbf{e_i}$, характеризующий количество пакетов определенного типа на заданном интервале времени. В общем случае $\mathbf{e_i}$ рассматривается как временной процесс, описываемый некоторой функцией $\mathbf{e_i(t)}$, $\mathbf{i=1...n}$, где $\mathbf{n}$ – количество возможных типов пакетов. Для анализа в заданный период времени отбирается множество всех зарегистрированных пакетов в сети $\mathbf{S=S\{Q_1,Q_2,...,Q_n\}}$, где $\mathbf{Q_i}$ – множество пакетов i-го типа, необходимое для решения проблемы перегруженности сервера. Пакеты представляют собой различные типы запросов к серверу и соответствуют определенному протоколу. Поскольку непрерывное накопление информации об отобранных протоколах в течение длительного времени является избыточным и требующим значительных ресурсов, осуществляется сбор статистики обо всех передаваемых на сервер пакетах в течение времени перегруженности сервера с периодом выборки 20-30 с.

Накопленную анализатором статистику можно представить в виде матрицы **E**, строкам которой соответствуют типы пакетов $\mathbf{t_n}$ (всего **n** типов пакетов), а столбцам – номера выборок пакетов (всего **m** выборок). В каждой выборке может быть произвольное суммарное число пакетов $\mathbf{k_i}$, где $\mathbf{i=1....n}$, элемент матрицы **E** – $\mathbf{e_{ij}}$ есть число пакетов i-го типа в j-й выборке (рис. 1).

Тип пакета		1	2	...	...	N
N1 – запрос обрабатывается	E=	e_{11}	e_{12}	...	...	e_{1n}
N2 – запрос на чтение файла		e_{21}	e_{22}	...	...	e_{2n}
N3 – запрос на запись файла		...	...	...	...	...
...		...	...	...	...	...
Nm – запрос		e_{m1}	e_{m2}	...	...	e_{mn}

Рис.1. Типы пакетов и статистические выборки

Каждая строка матрицы представляет таблично заданную функцию $\mathbf{e_i(t)}$ количества пакетов соответствующего типа. Для определения типа пакетов, являющихся причиной перегруженности сервера, производится обработка по всем типам запросов и сравнение их

количества с количеством пакетов задержки. Анализ корреляции между типами пакетов позволяет определить тип пакетов, являющихся причиной перегруженности.

Для каждого типа запросов вычисляется коэффициент корреляции r_{ij} между ним и типом пакета 9999 – "запрос обрабатывается":

$$r_{ij} = \frac{Cov(e_i, e_j)}{\delta_i \delta_j},$$

где $\mathbf{e}_i$,$\mathbf{e}_j$ – функции распределения количества пакетов определенного типа; d_i, d_j – средние квадратичные отклонения значений количества пакетов от их математического ожидания.

В данном случае для всех вычислений $\mathbf{e}_i$ соответствует типу пакетов NCP-9999 "запрос обрабатывается", а $\mathbf{e}_j$ – выборка для любого другого типа пакетов. Максимальный коэффициент корреляции r_{ij} указывает на тип пакетов $\mathbf{e}_j$, являющихся причиной перегруженности.

Данную ситуацию можно представить в виде графиков каждой функции количества типа пакетов $\mathbf{e}_j$ *(t)* (рис.2). Между типом запроса N2 "запрос на чтение файла" и пакетами NCP-9999 "запрос обрабатывается" наблюдается очевидная зависимость. Анализ адресов источников пакетов, перегружающих сервер, позволяет определить станцию-источник перегрузки.

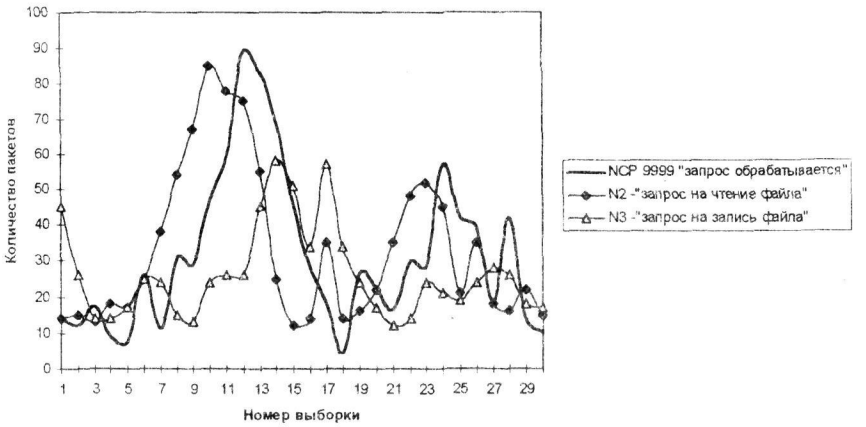

Рис. 2. Функции распределения количества типа пакетов

Процедура обнаружения станции, функционирующей в широковещательном режиме, сводится к выявлению конфигурации уст-

ройства источника данных пакетов, при которой количество широковещательных пакетов будет сокращено до минимума.

При перегрузке из-за файловых запросов причиной может быть перегрузка кэш-памяти, используемой при выполнении файловых запросов.

В случае перегруженности из-за операций печати необходимо осуществить перераспределение очередей на сервере или перевести наиболее активных пользователей на менее загруженный сервер.

5. Структура анализатора протоколов

Процедуры контроля состояния каналов и транспортной сети в целом целесообразно возложить на специальный комплекс программ, включаемый в состав процедур мониторинга и администрирования сети. Такой комплекс может быть представлен анализатором протоколов. На рис. 3 предлагается структура анализатора.

Каждый модуль в составе анализатора протоколов (рис.3) осуществляет выполнение строго определенных функций. Модуль получения пакетов производит прием всех передаваемых пакетов из физической среды передачи. При этом устанавливается специальный режим работы сетевой платы, исключающий анализ физического адреса пакета.

Фильтр отбора пакетов настраивается аналитиком для сбора информации об определенных типах пакетов или протоколов. Весь объем принятых пакетов записывается в буфер для их хранения, откуда осуществляются выборки для дальнейшего анализа. Блок декодирования пакетов выполняет преобразование информации из принятых пакетов в форму, удобную для просмотра и анализа. Фильтр отображения пакетов позволяет оперативно осуществлять выборки по заданным критериям из накопленного объема статистических данных. Модуль анализа текущего состояния сети ситуаций производит обработку накопленных статистических данных и анализирует их на возможность появления стандартной ошибочной ситуации (неверное значение контрольной суммы CRC, укороченные либо слишком длинные пакеты, длительное время реакции сервера на запрос и т.п.). Модуль принятия решений по результатам анализа предоставляет эксперту информацию из баз данных стандартных ситуаций о возможных причинах и путях устранения неисправности: адрес узла источника ошибочных пакетов, возможные неисправности кабельной системы и т.д. Анализатор структур пакетов обеспечивает группирование протоколов по принадлежности к определенной группе и позволяет просматривать вложенные протоколы (UDP, SNMP являются вложенными протоколами для TCP/IP и т.п.). При появлении ошибочного пакета в списке принятых пакетов аналитику предоставляется возможность проанализи-

ровать выборку пакетов на предмет появления стандартной ошибочной ситуации и получения рекомендаций по ее устранению.

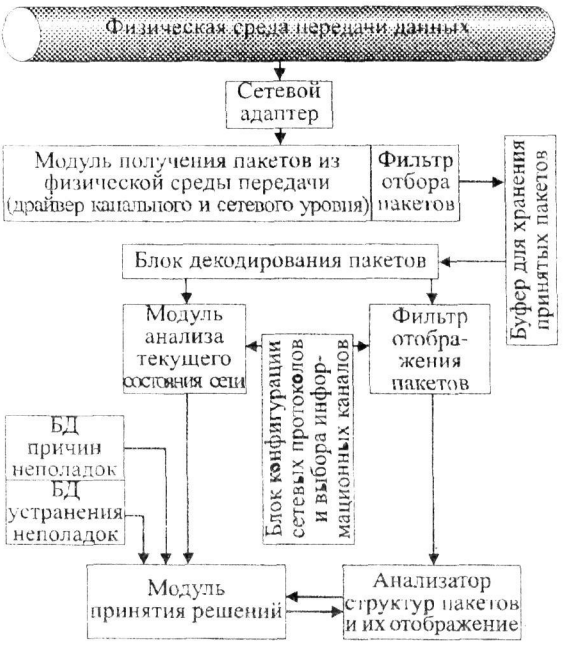

Рис. 3. Структура взаимосвязей между модулями анализатора протоколов

6. Выводы

Предложенные процедуры оценки появления ошибок в сети и процедуры принятия решений по их устранению расширяют функции стандартных процедур мониторинга сетей и в итоге обеспечивают повышение функциональности контролируемой сети, сводя к минимуму интервал ее потери.

Литература: 1. *Саенко В.И.* Администрирование, управление и мониторинг в компьютерных сетях// АСУ и приборы автоматики. 1998. № 108. С.251-258. 2. *Чаппелл Л., Хейкс Д.* Анализ локальных сетей NetWare. М.: Лори. 1995. 596 с. 3. *Рули Д. и др.* Сети Windows NT. К.:BHV. 1997. 798 с.

Поступила в редколлегию 19.05.98