КОМПЬЮТЕРНАЯ ИНЖЕНЕРИЯ И ТЕХНИЧЕСКАЯ ДИАГНОСТИКА

УДК 681.326

МОДЕЛИ НЕИСПРАВНОСТЕЙ КОРПОРАТИВНЫХ СЕТЕЙ И ФОРМУЛИРОВКА ЗАДАЧ ИХ ДИАГНОСТИРОВАНИЯ

ХАХАНОВ В.И., ХАНЬКО В.В., АБУ ЗАНУНЕХ И.М. ХАЛИЛЬ

Сформулированы основные задачи диагностирования сети, связанные с возникновением и устранением неисправностей на стадиях проектирования и эксплуатации современных компьютерных локальных и корпоративных сетей. Представлены классификация сетевых дефектов и их влияние на функционирование, а также средства, пути поиска и локализации неисправностей.

1. Введение

Компьютерные сети крупных предприятий не являются однородными по структуре и топологии. В их состав входит большое количество подсетей различных типов с различной топологией, в которых используются разнообразные протоколы обмена, что значительно усложняет архитектуру корпоративной сети в целом. Крупная корпоративная сеть со сложной инфраструктурой, как правило, образуется путем объединения нескольких локальных сетей или добавлением новых к уже существующим. Этот процесс сопровождается внесением изменений в архитектуру корпоративной сети, что, наряду с возрастающей сложностью сети, отсутствием дорогостоящего оборудования для тестирования и диагностики (анализаторы протоколов, кабельные сканеры) значительно усложняет процесс ее обслуживания. В этих условиях часто бывает трудно проанализировать работу сети в целом, а также предсказать – какие последствия будет иметь то или иное изменение, внесенное в ее архитектуру. В результате при ее работе часто возникают проблемы, связанные как с ошибками, допущенными при проектировании, так и с ошибками, возникающими в результате внесения в архитектуру сети изменений, а также с неисправностями, которые появляются во время эксплуатации. Кроме того, задача усложняется еще и тем, что в большинстве случаев даже при наличии сервисного оборудования ни предварительное тестирование (стрессовое тестирование, цель которого – определение пороговых значений для параметров сети, обычно предшествует вводу сети в эксплуатацию или проводится после изменения ее архитектуры), ни упреждающая диагностика (диагностика сети при ее нормальной работе, которая проводится в целях выявления возможных причин возникновения ошибок в будущем) сети, как правило, не проводится. Работы по выявлению и устранению ошибок традиционно сводятся к проведению реактивной диагностики (когда ошибки уже присутствуют в сети, но необходимо выявить и устранить причину их появления за минимальное время), которая при отсутствии накопленной ранее статистической информации малоэффективна, требует больших временных затрат. К тому же работы приходится вести во время штатного функционирования сети (выполнение различного рода кабельных переключений, внесение изменений в таблицы маршрутизации серверов), что в конечном итоге приводит к неэффективной работе пользователей и сети в целом.

2. Постановка задачи

Как проектировщику, так и пользователю целесообразно иметь возможность прогнозировать поведение сети с учетом выбранных архитектурных решений на ранних стадиях ее разработки, а также при внесении изменений в архитектуру сети во время эксплуатации, на основании данных, полученных при проведении стрессового тестирования и упреждающей диагностики. Это значительно сокращает временные и материальные затраты на поиск ошибок в сети при ее развертывании и эксплуатации. Поставленную задачу можно решить путем моделирования работы сети заданной архитектуры с требуемым уровнем абстракции.

Цель моделирования состоит в выработке оптимальных с точки зрения производительности и надежности технических решений путем оптимизации архитектуры сети, выявления и устранения возможных причин и мест возникновения дефектов как на стадии проектирования сети, так и при ее наладке и эксплуатации (обслуживании).

В зависимости от класса решаемых задач технической диагностики обобщенная модель корпоративной сети может быть представлена в виде:

$$M_N=\{S, t, F, N\},$$

где каждый компонент определяет уровни или слои описания существенных для решения каждой конкретной задачи атрибутов модели:

1) S – структурный (логический) уровень, когда для пользователя интерес представляет структура логических взаимосвязей компонентов сети – возможные пути передачи информации. В данном случае модель представлена парой $S=<V,E>$, где V – множество вершин-станций графа; E – множество дуг, задающих отношения приема-передачи информации между компьютерами.

2) t – временной уровень, когда для пользователя существенным представляется параметр времени при использовании сети для приема или передачи информации. Здесь речь идет о двух характеристиках: $t=<t_D,t_S>$, где t_D – номинальная задержка линии связи или других пассивных компонентов; t_S – параметр быстродействия (Мбит/с), относящийся к активным компонентам сети.

3) F – функциональный уровень, когда для пользователя существенной является информация о функциях, которые могут быть выполнены сетью или ее компонентами. Уровень представлен двумя подмножествами $F=<F_K,F_N>$, где F_K – функции компонентов, представленных номенклатурой: компьютеры, сетевые карты, коммутаторы, репитеры, маршрутизаторы, коннекторы, терминаторы, кабели; F_N – функции сети или сегмента: а) хранение информации (распределенная база данных); б) обмен информацией (прием – передача); в) обработка информации (распараллеливание или рассредоточение вычислительного процесса по компьютерам сети); г) управление рассредоточенной базой данных; д) управление приемом – передачей информации; е) управление рассредоточенным вычислительным процессом.

4) N – топологический уровень, когда элементами сети являются физические компоненты, связанные между собой в соответствии с техническими условиями. В данном случае имеет место классификация $N=<N_E,N_T,N_S>$, где N_E – примитивная топология типа EtherNet; N_T – примитивная топология типа TokenRing; N_S – примитивная топология типа ArcNet. В общем случае реальная локальная или корпоративная сеть представлена сочетаниями из упомянутых примитивов.

Локальная сеть и/или ее компоненты, заданные на любом из упомянутых уровней, могут быть представлены на языках высокого уровня описания аппаратуры (VHDL, Verylog). Однако адекватно описать реальную сеть в виде полной модели M_N практически невозможно. Поэтому для решения конкретной задачи технической диагностики следует определять минимально необходимое множество уровней из M_N. Для этого нужно сформулировать практически значимые задачи технической диагностики локальных сетей в терминах компонентов тетрады <M,D,T,R>: <модель, дефекты, стимулы, реакция>.

Обобщенное уравнение анализа модели сети при наличии или отсутствии неисправностей

$$M = R \vee DR \vee TR \vee DTR = R(1 \vee D \vee T \vee DT)$$

формализует постановку следующих наиболее существенных и практически значимых задач:

1. Создание модели устройства в виде входных тестовых наборов и соответствующих им реакций при наличии заданных неисправностей – таблица функций неисправностей:

$$M = f^{1,4}(T,D,R).$$

2. Определение множества потенциальных, фактических или проверяемых дефектов в сети:

$$D=M \vee MT \vee MR \vee MTR = M(1 \vee T \vee R \vee TR).$$

2.1. Генерация списков неисправностей сети по ее модели в виде физических или функциональных дефектов:

$$D = f^{2,1}(M,T,R)|_{T=\varnothing;\ R=\varnothing}.$$

2.2. Моделирование заданных неисправностей сети на функциональных режимах в целях определения качества теста:

$$D = f^{2,2}(M,T,R)|_{R=\varnothing}.$$

2.3. Определение фактических неисправностей сети на функциональных режимах по экспериментальным реакциям – обратное прослеживание дефектов:

$$D = f^{2,3}(M,T,R)|_{T=\varnothing}.$$

2.4. Определение фактических неисправностей сети на тестовых режимах по экспериментальным реакциям – безусловное диагностирование:

$$D = f^{2,4}(M,T,R).$$

3. Создание теста верификации модели сети, проверки ее исправности, обнаружения заданных неисправностей:

$$T=M \vee MD \vee MR \vee MDR = M(1 \vee D \vee R \vee DR).$$

3.1. Проектирование теста (проверки исправности) сети по ее модели:

$$T = f^{3,1}(M,D,R)|_{D=\varnothing;\ R=\varnothing}.$$

3.2. Проектирование теста (проверяющего, диагностирования) сети по ее модели и заданным неисправностям:

$$T = f^{3,2}(M,D,R)|_{R=\varnothing}.$$

3.3. Проектирование теста (проверки исправности) сети по ее модели исправного поведения и заданным реакциям – обратная импликация:

$$T = f^{3,3}(M,D,R)|_{D=\varnothing}.$$

3.4. Проектирование теста (проверяющего, диагностирования) – определение режимов функционирования терминальных станций по его модели, заданным дефектам и реакциям – обратная импликация:

$$T = f^{3,4}(M,D,R).$$

4. Определение реакции сети – прямая импликация:

$$R=M \vee MD \vee MT \vee MDT = M(1 \vee D \vee T \vee DT).$$

4.1. Определение состояний компонетов сети как реакции модели на функциональные режимы:

$$R = f^{4,1}(M,D,T)|_{D=\varnothing;\ T=\varnothing}.$$

4.2. Определение состояний компонетов сети как реакции модели на входные последовательности при наличии заданных неисправностей:

$$R = f^{4,2}(M,D,T)|_{T=\varnothing}.$$

4.3. Определение состояний компонетов сети как реакции модели на ее тестовые режимы:

$$R = f^{4,3}(M,D,T)|_{D=\varnothing}.$$

4.4. Определение состояний компонетов сети как реакции модели на ее тестовые режимы при наличии заданных дефектов – моделирование неисправностей заданного класса:

$$R = f^{4,4}(M,D,T)|.$$

В формулировках проблем $f^{i,j}$ (i=1,4; j=1,4) есть система логических преобразований (методы и алгоритмы), предназначенная для рационального решения конкретной задачи анализа или проектирования.

3. Средства моделирования сетей

Для построения модели сети требуемой архитектуры можно использовать один из множества коммерческих пакетов, особенности которых подробно освещены в [1]. Пакет NetMaker XA (компания Make Systems) является лидером в области программного обеспечения (ПО), предназначенного для моделирования сетей. Данный пакет в базовой конфигурации позволяет с помощью встроенных SNMP-модулей автоматически распознавать сетевые устройства и создавать соответствующие им объекты. Кроме того, пользователь имеет возможность самостоятельно добавлять в модель сети новые объекты (а также самостоятельно создавать их, дополняя базовую библиотеку) из объемной библиотеки сетевых устройств, поставляемой вместе с пакетом. Это позволяет прогнозировать результат, который может быть получен при изменении архитектуры сети. Благодаря таким возможностям пакет позволяет легко и быстро строить модели сетей и анализировать альтернативные варианты. При установке дополнительных модулей к указанным ранее возможностям добавляются контроль сетевого трафика и возможность выработки сценариев быстрого восстановления сети после отказов. NetMaker XA работает только на Sun SPARCstation. Стоимость пакета NetMaker XA в базовой конфигурации – 37 тыс. долларов США. Кроме того, отдельно оплачивается обучение по обслуживанию пакета, а также приобретение дополнительных модулей, что в совокупности составляет еще 30 тыс. долларов.

COMNET Predictor компании CACI – пакет для моделирования сетей. Его возможности позволяют импортировать информацию об архитектуре сети из популярных средств мониторинга, контролировать объемы трафика, который генерирует то или иное приложение, анализировать поведение сети при возможном увеличении трафика, генерируемого приложениями, учитывать возможности ее развития, прогнозировать возникновение проблем при развитии сети и выявлять их причины. COMNET Predictor может работать как под UNIX, так и под Windows95/NT. Стоимость пакета COMNET [1] составляет – 29 тыс. долларов.

Очевидно, что наряду с большими возможностями в области моделирования сетей рассмотренные пакеты имеют существенный недостаток в виде их высокой стоимости. Тем не менее в большинстве случаев администратору сети приходится решать возникающие проблемы собственными силами, не прибегая к помощи системных интеграторов. В этих условиях, если есть необходимость в моделировании сети, но нет средств на приобретение дорогих высокоинтеллектуальных пакетов, стоит обратить внимание на приемлемые по стоимости программные продукты [1]. При желании можно смоделировать интересующие процессы в сети (речь не идет о модели всей сети, здесь не обойтись без специализированного пакета с соответствующими возможностями), используя, например, возможности VHDL, Perl [2,3].

В последнее время появилось большое количество средств для создания VHDL-моделей объектов как коммерческих (например, Active-HDL от Aldec Inc.,Windows95/NT), так и свободно распространяемых (например, FreeHDL под Linux). Для того чтобы эффективно использовать недорогие средства моделирования, а также средства диагностики сети (тем более использовать возможности VHDL), обслуживающему персоналу необходимо иметь представление об особенностях работы сетевой среды, ошибках, которые могут быть допущены на стадии разработки сети; о дефектах и причинах их возникновения; о методах их поиска и устранения на стадии эксплуатации; о способах тестирования и диагностики сетей; о минимальном и достаточном для проведения диагностики наборе оборудования, его возможностях; о том, как правильно собрать, интерпретировать и использовать информацию, полученную во время тестирования и диагностики сети.

4. Классификация сетевых дефектов

Все ошибки, за исключением тех, что связаны с исчезновением информации, выявляются путем перехвата и анализа кадров канального уровня. Ошибки из-за неисправности сетевой платы связаны с конкретными MAC-адресами. Исчезновение информации в активном оборудовании на канальном уровне определить невозможно. Косвенным признаком этой ошибки является большое число повторных передач по конкретному MAC-адресу. В данном случае необходимо проанализировать информацию, инкапсулированную протоколами верхних уровней в кадр канального уровня.

Учитывая сказанное ранее, прежде чем перейти к анализу методов выявления и устранения ошибок в среде Ethernet, уместно обозначить их типы, характерные для данной среды, и указать возможные причины возникновения. Отметим, что метод доступа к среде CSMA/CD, принятый в среде Ethernet, предполагает в сети некоторый процент ошибок, называемых коллизиями. Напомним, что существуют коллизии трех типов [3,7].

1. Локальная или местная (local collision) – это коллизия, фиксируемая в домене, где подключено измерительное устройство, в пределах передачи преамбулы или первых 64 байт кадра, когда устройство наблюдения и источники сигнала находятся в одном домене. Проявляется в виде коротких, неправильно оформленных кадров длиной менее 64 байт с неверной контрольной последовательностью CRC. В сетях 10BASE-2 сопровождается удвоением уровня напряжения в кабеле, в сетях 10BASE-T – присутствием сигнала на линиях приема передающей кадр станции.

Причины: А. *Высокая утилизация канала.* Уменьшение допустимой полосы пропускания канала вследствие чрезмерной нагрузки, создаваемой прикладным ПО на сеть. (Нехватка полосы пропускания канала). **Б.** *Неисправная сетевая плата.* В данном случае ошибка может быть связана с некорректной работой схемы обнаружения коллизий, с уменьшением допустимой полосы пропускания канала вследствие частых повторных передач из-за неисправно-

сти приемопередающей части платы, схемы вычисления CRC. В. *Дефектный драйвер.* Некорректно реализуется back off алгоритм. Г. *Коммутатор.* Перегрузка порта (эффект back pressure) с уменьшением полосы пропускания канала вследствие частых повторных передач. Д. *Неправильное заземление.* Уменьшение допустимой полосы пропускания канала вследствие частых повторных передач из-за искажения информации в кабеле вследствие эффекта inter ground noise. Е. *Дефекты кабельной системы.* Уменьшение допустимой полосы пропускания канала вследствие частых повторных передач из-за искажения передаваемой информации вследствие отражений сигнала в местах перегиба кабеля, плохого контакта в разъемах RJ45, BNC, Т-коннекторах, терминаторах. Ж. *Источник электромагнитных помех.* Уменьшение допустимой полосы пропускания канала вследствие частых повторных передач из-за искажения информации, связанного с воздействием на сигнал электромагнитных помех.

2. Удаленная коллизия (remote collision) – это та, которая возникает в другом физическом сегменте сети (за повторителем). *У*стройство наблюдения и источники сигнала находятся в разных доменах. Характеризуется правильно переданным кадром с неверной контрольной суммой и нормальным уровнем напряжения в сетях 10BASE-2, либо отсутствием сигнала на линиях приема передающей кадр станции в сетях 10BASE-T. Станция узнает, что произошла удаленная коллизия, если она получает неправильно оформленный короткий кадр с неверной контрольной последовательностью CRC, и при этом уровень напряжения в канале связи остается в установленных пределах (для сетей 10Base-2). Для сетей 10Base-T/100Base-T показателем является отсутствие одновременной активности на приемной и передающей парах (Tx и Rx).

Причины: Аналогичны причинам возникновения локальных коллизий, с той лишь разницей, что источник ошибок расположен в соседнем, по отношению к наблюдаемому, сегменте.

3. Поздняя коллизия (late collision) – это местная коллизия, которая фиксируется уже после того, как станция передала в канал связи первые 64 байта кадра. В отличие от местных и удаленных является верным признаком наличия проблем в сети. В сетях 10Base-T поздние коллизии часто фиксируются измерительными устройствами как ошибки CRC.

Причины: А. *Неисправная сетевая плата.* В данном случае ошибка может быть связана с некорректной работой схемы обнаружения коллизий. Б. *Чрезмерная длина сегмента (нарушение правила четырех концентраторов).* В данном случае станция, расположенная на большом расстоянии от передающей станции, слишком поздно обнаруживает факт возникновения коллизи в сети из-за большой задержки распространения сигнала в кабеле. В результате этого информация может быть потеряна. В. *Дефекты кабельной системы.* Искажение передаваемой информации вследствие отражений сигнала в местах перегиба кабеля, плохого контакта в разъемах RJ45, BNC, Т-коннекторах, терминаторах. Г. *Источник электромагнитных помех.* Искажение кадра после передачи 64 байт информации, связанное с воздействием на нее электромагнитных помех.

4. Короткий кадр определяется длиной меньше 64 байт (после 8-байтной преамбулы), с правильной контрольной последовательностью (CRC). Возможная причина возникновения ошибок этого типа – неисправная сетевая плата или некорректно работающий драйвер.

Причины: А. *Неисправная сетевая плата.* В данном случае ошибка может быть связана с некорректной работой блока формирования кадра. Б. *Дефектный драйвер.* Некорректно реализуется алгоритм формирования кадра.

5. Длинный кадр – кадр, длиной более 1518 байт с правильной либо неправильной CRC.

Причины: А. *Неисправная сетевая плата.* В данном случае ошибка может быть связана с некорректной работой блока формирования кадра. Б. *Дефектный драйвер.* Некорректно реализуется алгоритм формирования кадра.

6. Jabber – кадр более 1518 байт с неправильной CRC.

Причины: **А.** *Неисправная сетевая плата.* Ошибка может быть связана с некорректной реализацией алгоритма CSMA/CD (не выдерживаются паузы 9,6 мкс между кадрами). Б. *Дефектный драйвер.* Аналогично. В. *Коммутатор.* Аналогично. Г. *Неправильное заземление.* Искажение информации в кабеле вследствие эффекта inter ground noise. Д. *Дефекты кабельной системы.* Искажение передаваемой информации из-за отражений сигнала в местах перегиба кабеля, плохого контакта в разъемах RJ45, BNC, Т-коннекторах, терминаторах. Е. *Источник электромагнитных помех.* Искажение информации при электромагнитном воздействии.

7. Ошибка CRC-правильно оформленный кадр допустимой длины (64 -1518 байт) с неправильной CRC.

Причины**:** А. *Неисправная сетевая плата.* Длина ошибочного кадра, как правило, меньше длины корректного кадра из той же серии. В данном случае ошибка может быть связана с некорректной работой схемы вычисления CRC, схемы кодирования/декодирования информации (код Манчестер 2), приемопередатчика платы. Б. *Дефектный драйвер.* Некорректно реализуется алгоритм обработки передаваемых / принимаемых данных. В. *Коммутатор.* Длина ошибочного кадра, как правило, больше длины корректного кадра из той же серии. В данном случае ошибка связана с добавлением в конец кадра нескольких пустых байтов в результате некорректной работы порта коммутатора. Г. *Чрезмерная длина сегмента.* Для сетей 10BASE-T ошибка CRC в данном случае является по сути поздней коллизией. Д. *Неправильное заземление.* Искажение информации в кабеле вследствие эффекта inter ground noise. Е. *Дефекты кабельной системы.* Искажение передаваемой информации вследствие отражений сигнала в

местах перегиба кабеля, плохого контакта в разъемах RJ45, BNC, T-коннекторах, терминаторах. Ж. *Источник электромагнитных помех.* Искажение информации, связанное с воздействием на нее электромагнитных помех.

8. Потеря информации. Проявляется в виде частых повторных передач, не вызванных ошибками канального уровня (пакеты IP, IPX) либо отключением порта концентратора.

Причины**:** А. *Неисправная сетевая плата.* Б. *Коммутатор.* Ошибка связана с отсутствием или неправильной работой в ряде коммутаторов (например, Ethernet- FDDI) обратной связи быстрого порта с медленным, с эффектом back pressure (слишком большое число эмулируемых коммутатором коллизий при перегрузке порта, в результате чего после 16 последовательных коллизий рабочая станция прекращает передачу кадра), с несоблюдением стандарта CSMA/CD на минимальный межкадровый интервал (9.6 us), в результате чего возможен захват канала одной станцией (jabber), с перегрузкой порта коммутатора. Ошибка выявляется путем отслеживания кадра распределенным анализатором протокола до прохождения порта коммутатора и после него, а также при помощи стрессового тестирования сети. В. *Чрезмерная длина сегмента* (см. поздние коллизии).

9. Блики (ghosts) – последовательность сигналов, отличных по формату от кадров Ethernet, не содержащая разделителя (SFD) и длиной более 72 байт. Выявляются на стадии стрессового тестирования.

Причины: **А.** *Неправильное заземление.* Искажение информации в кабеле вследствие эффекта inter ground noise. Б. *Дефекты кабельной системы.* Искажение передаваемой информации вследствие отражений сигнала в местах перегиба кабеля, плохого контакта в разъемах RJ45, BNC, T- коннекторах, терминаторах. В. *Источник электромагнитных помех.* Искажение информации, связанной с воздействием на сигнал электромагнитных помех.

Большинство проблем в Ethernet может проявляться как на канальном, так и на более высоких уровнях протоколов обменов данными в виде присутствия также и других типов ошибок [3,7]:

а) ошибки выравнивания – число бит в кадре не кратно числу байт, а возможная причина возникновения ошибок этого типа – неисправное активное оборудование;

б) искажение информации в активном оборудовании (на транспортном уровне, протоколы IP, IPX), не обнаруживаемое на канальном уровне, возможная причина – несогласованность в работе буферов в активном оборудовании;

в) блокировка канала – захват активным оборудованием передающей среды, а возможные причины возникновения – неисправность активного оборудования, несоблюдение оборудованием стандарта CSMA/CD (оборудование не выдерживает паузы 9,6 мкс перед отправкой очередного кадра);

г) "широковещательные штормы" – чрезмерно высокий уровень широковещательных передач в сети, занимающий полосу пропускания среды; может быть вызван, например, неисправными мостами, некорректно работающим программным обеспечением;

д) ошибки маршрутизации, например, дубликатные адреса (протоколы верхних уровней), приводят к прямым конфликтам в сети, вызваны ошибками в конфигурации ПО рабочих станций, маршрутизаторов, брандмауэров, серверов.

5. Ошибки проектирования сети

Характерными для стадии проектирования локальной или корпоративной сети могут быть следующие просчеты или неточности, обусловленные неполнотой информации, связанной с будущей эволюцией:

1. Проектирование сегмента чрезмерной длины может привести либо к его неработоспособности вообще, либо к снижению допустимой утилизации канала за счет увеличения накладных расходов, связанных с обработкой поздних коллизий.

2. Проектирование прокладки кабеля без учета влияния на него внешних источников шума (особенно чувствительны к внешним шумам сегменты 10BASE-T) в дальнейшем может привести к большому количеству коллизий, к ошибкам типа "длинный кадр", "ошибка CRC", "блики".

3. Большое число перегибов кабеля в сегменте, предполагающееся при проектировании, также может привести к возникновению помех в кабеле и как следствие – к большому числу коллизий из-за многократных отражений сигнала.

4. Отсутствие в проекте или неверная топология заземления может также вызвать большое число коллизий и ошибок в сети из-за появления тока в кабеле вследствие разности потенциалов между корпусами рабочих станций.

5. Выбор некачественного активного оборудования может привести, например, к возникновению ошибок типа "короткий кадр", "длинный кадр", "ошибка CRC", "ошибка выравнивания", а также к исчезновению информации в сетевых платах, коммутаторах. Кроме того, использование некачественного активного оборудования может затруднить диагностику сети ввиду ограниченных возможностей последнего (отсутствие поддержки оборудованием групп RMON MIB).

6. Некорректная установка, конфигурирование и использование программного обеспечения серверов, маршрутизаторов, рабочих станций и другого оборудования (например, назначение дубликатных IP-адресов).

Еще на стадии проектирования возможных вариантов топологии сети Ethernet полезно рассчитать для каждого из них значения PVV и PDV, что в дальнейшем сразу исключит ошибки, связанные с несоблюдением ограничений, накладываемых на физическую среду в Ethernet [4]:

$$PVV = SVV_1 + SVV_2 + ... + SVV_n, \qquad (1)$$

где PVV – суммарная величина уменьшения межкадрового интервала при прохождении сигналом всех повторителей; SVV_1, SVV_2, SVV_n – величины уменьшения межкадрового расстояния при прохождении сигнала между соседними сегментами;

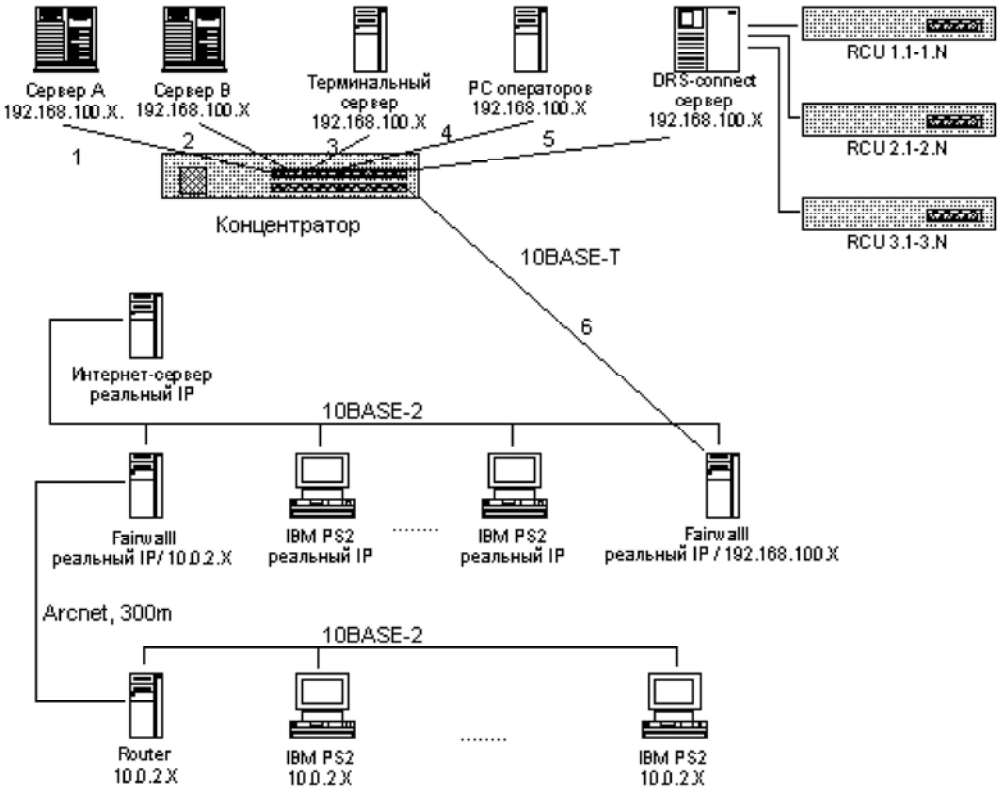
$$PDV=(BASE_1+t_1\times L_1)+(BASE_2+t_2\times L_2)+...+$$
$$+(BASE_n+t_n\times L_n), \qquad (2)$$

здесь PDV – величина максимально возможной задержки оборота сигнала; $BASE_1$, $BASE_2$, $BASE_n$ – базовые задержки (определяются типом сегмента); t_1, t_2, t_n – погонные задержки сигнала в кабеле (определяются типом среды); L_1, L_2 , L_n – длины сегментов. Необходимые данные для расчета PVV и PDV для всех физических стандартов Ethernet приведены в [4]. Полученные значения PVV и PDV для данной топологии сети должны удовлетворять требованиям Ethernet к максимальной величине уменьшения межкадрового интервала (не более 49 битовых интервалов) и величине максимально возможной задержки оборота сигнала в сети (не более 575 битовых интервалов).

Кроме того, при проектировании схемы проводки коммуникаций внутри здания следует стремиться обеспечить минимальное число перегибов кабеля, а также исключить возможное влияние на него источников электромагнитного излучения (близость силовых кабелей). Разработка правильной топологии линий заземления также позволит избежать проблем при эксплуатации сети. При разработке топологии заземления необходимо обеспечить наличие его общей точки для всех рабочих станций и исключить возможность заземления сегмента коаксиального кабеля более чем в одной точке. Подробные рекомендации по этому вопросу можно найти в [5].

Желательно, чтобы приобретаемое для проектируемой сети активное оборудование имело подробную документацию, поддерживало большинство групп RMON MIB, имело возможность вывода полной информации об ошибках в сети. Все это в дальнейшем позволит организовать диагностику в сети с наибольшей эффективностью и минимальными материальными затратами. Подробнее этот вопрос будет освещен ниже. Следует иметь четкое представление об архитектуре проектируемой сети, а именно, подсети каких типов будут входить в состав сети, какие сетевые протоколы будут использоваться, сколько и какие рабочие станции будут входить в состав подсетей, какое программное обеспечение и какие прикладные пакеты предполагается использовать в той или иной подсети, как правильно их установить и сконфигурировать, каким образом и посредством чего будет осуществляться взаимодействие между подсетями.

Перед вводом сети в эксплуатацию, при наличии кабельного сканера, следует протестировать кабельную систему на соответствие стандарту и отсутствие шумов. Затем необходимо провести стрессовое тестирование сети, цель которого состоит в определении реальных значений параметров сетевого оборудования (как правило, производители сетевого оборудования указывают для своих изделий параметры, полученные при работе в наивыгоднейших режимах) для конкретных условий эксплуатации (тип трафика, длина пакетов), а также в определении границ применимости выбранной архитектуры сети. На этом этапе возможно определить причину появления некоторых ошибок (например, “блики”, искажение информации в активном оборудовании), локализация которых затруднена в процессе реактивной диагностики. Кроме того, результаты стрессового тестирования часто используются в качестве пороговых значений при проведении упреждающей диагностики сети. Они являются ключом к построению адекватных моделей единиц сетевого оборудования при моделировании сети конкретной архитектуры. Подробные рекомендации по проведению стрессового тестирования даны в [6]. Интегральным показателем нормальной работы устройства при заданных условиях в данном методе тестирования принято считать отсутствие потери кадров тестируемым устройством на транспортном уровне.



Тестирование проводят в два этапа. На первом следует оценить, какой из

элементов сети является наиболее ответственным с точки зрения работоспособности сети в целом. Для примера корпоративной сети, показанной на рисунке, таким элементом является концентратор, поскольку почти весь трафик в сети, за исключением интернет-трафика, направлен через него. Далее следует выяснить характеристику трафика и тестирование проводить, ориентируясь на конкретный тип пакетов. В данном случае для тестирования лучше всего подойдет распределенный анализатор протокола (например, программный распределенный анализатор протоколов Distributed Observer фирмы Network Instruments). Центральный анализатор, инсталлированный на рабочую станцию, следует подключить к зеркальному порту концентратора. Поскольку в данном случае тестированию подвергается только концентратор, то из эксперимента целесообразно исключить основной сервер в сегменте 1, а агенты анализатора протокола инсталлировать на однотипные рабочие станции, подключенные к каждому сегменту. Затем агенты, размещенные в сегментах 2,3,4,5,6, настраиваются на генерацию выбранного типа трафика по MAC-адресу агента, размещенного в сегменте 1, последний в свою очередь настраивается на генерацию трафика по MAC-адресам агентов, размещенных в сегментах 2,3,4,5,6. Длину пакета можно выбрать минимальной с тем, чтобы увеличить нагрузку, что повысит достоверность полученных результатов. В процессе эксперимента центральный анализатор поочередно подключается к каждому из портов концентратора для сбора информации, которая затем обрабатывается. При обнаружении факта потери кадров (увеличения количества повторных передач) выясняется причина, повлекшая за собой потерю кадров. Это может быть перегрузка коммутатора, дефект линии связи (например, плохой контакт в разъеме RJ45, который иногда не выявляется кабельным сканером), чрезмерное количество генерируемых концентратором коллизий. Трафик необходимо проанализировать как на транспортном, так и на канальном уровнях, чтобы убедиться, что потеря кадров происходит именно на транспортном уровне. Изменяя параметры тестового трафика в процессе эксперимента, можно выяснить, при каких параметрах трафика и значениях утилизации портов возникает повторная передача кадров на транспортном уровне.

На втором этапе проводится стрессовое тестирование серверов и рабочих станций. На них, одновременно с работой приложений, запускается какой-либо стрессовый тест, например FTest компании "ПроЛАН", а агенты анализатора протокола настраивают на сбор данных. В данном случае значение стрессовой нагрузки необходимо выбрать на 10-15% ниже полученного на первом этапе порогового значения, что позволит говорить о потере кадров, которая никак не связана с концентратором. Полученные с помощью распределенного анализатора протокола данные обрабатываются, и с учетом данных, полученных на первом этапе тестирования, выводится общее пороговое значение утилизации для каждого компонента сети.

6. Заключение

При проведении реактивной диагностики использование встроенных в активное оборудование SNMP-агентов зачастую приводит к искажению результатов диагностики, что связано с их некорректной работой в случае неисправного оборудования. В связи с этим для проведения реактивной диагностики целесообразно использовать специализированное диагностическое оборудование, например, аппаратные анализаторы протокола. Во многих источниках подчеркивается, что использование распределенных анализаторов протокола предпочтительнее, так как они позволяют сопоставлять события, происходящие в одно и то же время, но в разных точках сети, что часто бывает нужно на практике [6]. При использовании программного анализатора протокола следует выяснить, насколько полна и корректна будет собранная информация при использовании программного анализатора протокола с конкретным типом сетевой карты и драйвера. По данным, опубликованным в [8], полную информацию об ошибках выдают лишь сетевые карты NE2000, а также карты компаний D-Link и Kingstone.

7. Выводы

1. На этапе проектирования архитектуры сети следует убедиться, соответствует ли выбранный вариант топологии сети физическим ограничениям среды.

2. Следует использовать активное оборудование, поддерживающее наибольшее число групп RMON MIB.

3. При прокладке кабеля необходимо избегать большого числа его перегибов и воздействия на кабель внешних помех.

4. После разводки кабельной системы целесообразно протестировать ее с помощью кабельного сканера.

5. Перед вводом сети в эксплуатацию необходимо провести ее стрессовое тестирование для определения максимально допустимых параметров активного оборудования и применимости выбранной архитектуры сети для данных условий.

6. Во время эксплуатации сети нежелательно пренебрегать упреждающей диагностикой; данные, полученные на этом этапе, позволят более эффективно организовать реактивную диагностику сети.

7. Необходимым и достаточным условием для организации диагностики сети является наличие анализатора протокола (желательно распределенного, с возможностью генерации трафика).

8. При использовании программного анализатора протокола необходимо убедиться в том, что применяемая совместно с ним сетевая карта и драйвер способны предоставить информацию об ошибках в сети в нужном объеме.

9. Использование в своей работе средств моделирования может значительно облегчить диагностику сети, а также прогнозировать ее возможное поведение при внесении в сеть изменений.

10. Данные, полученные на этапах проектирования, стрессового тестирования и упреждающей диагностики сети, могут с успехом быть использованы при создании модели сети.

11. Высокий уровень утилизации канала не всегда является причиной проблем в сети.

12. При поиске причин появления ошибок в сети прежде всего следует проверить корректность заземления аппаратуры и качество напряжения.

13. Передаваемые данные могут искажаться на верхних протокольных уровнях, без сообщения об ошибках на канальном уровне (протоколы IP, IPX).

Литература: 1. *Стернс Том.* Учимся моделировать. Сети, 1998. №5. С.35-39. 2. *Baldi M., Corno F., Rebaudengo M., Prinetto P., Sonza Reorda M., Squillero G.* Simulation-Based Verification of Network Protocols Performance CHARME'97: Advanced Research Working Conference on Correct Hardware Design and Verification Methods. Montreal, Quebec, Canada, October 1997. P.156-159. 3. *Baldi M., Corno F., Rebaudengo M., Squillero G.* GA-based Performance Analysis of Network Protocols ICTAI'97: 9th IEEE International Conference on Tools with Artificial Intelligence, Newport Beach, CA (USA), November, 1997. P.186-189. 4. *Юдицкий С., Подлазов В., Борисенко В.* Искусство диагностики локальных сетей: LAN. Журнал сетевых решений. 1998. № 07. Открытые системы. С.156-159. 5. *Олифер Н., Олифер В.* Базовые технологии локальных сетей. Центр Информационных Технологий. С.18-24. 6. *Барнс Дж.* Электронное конструирование: Методы борьбы с помехами: Пер. с англ. М.: Мир, 1990. 234с. 7. *Юдицкий С., Борисенко В., Овчинников С.* Основы диагностики сети: LAN. Журнал сетевых решений. 1998, №12. С.56-59. 8. *Нессер Д. Дж.* Оптимизация и поиск неисправностей в сетях. К.: Диалектика, 1996. 646с.

Поступила в редколлегию 12.10.99

Рецензент: д-р техн. наук, проф. Кривуля Г.Ф.

Хаханов Владимир Иванович, д-р техн. наук, профессор кафедры автоматизации проектирования вычислительной техники ХТУРЭ. Научные интересы: техническая диагностика вычислительных устройств, систем, сетей и программных продуктов. Увлечения: баскетбол, футбол, горные лыжи. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. 40-93-26.

Ханько Вадим Викторович, аспирант кафедры автоматизации проектирования вычислительной техники ХТУРЭ. Научные интересы: техническая диагностика компьютерных систем и сетей. Увлечения: иностранные языки. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. 40-93-26.

Абу Занунех Халиль И.М., аспирант кафедры автоматизации проектирования вычислительной техники ХТУРЭ. Научные интересы: техническая диагностика вычислительных устройств и сетей. Хобби: шахматы, футбол, теннис. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. 40-93-26.

УДК 620.179.13

ОСОБЕННОСТИ ПОСТРОЕНИЯ АЛГОРИТМА ТОМОГРАФИИ В ТЕПЛОВЫХ МЕТОДАХ КОНТРОЛЯ

МЕЛЬНИК С.И., ОРЕЛ Р.П.

Рассматриваются особенности построения алгоритма томографии в тепловых методах контроля. Проводится анализ существующих методов тепловой томографии. Указываются причины, не позволяющие осуществлять тепловую томографию в полной мере. Предлагается комплекс алгоритмов теплового контроля, позволяющих реализовать выявленные закономерности.

1. Введение

Неразрушающий контроль (НК) качества промышленной продукции является неотъемлемой частью современного производственного процесса. В настоящее время томография промышленных изделий как метод НК широко применяется в промышленной диагностике и контроле. Существуют гостированные методы проведения томографии, например, рентгеновский и ультразвуковой. Однако первый из них связан с опасностью для персонала, а второй применяется только в узком диапазоне промышленных изделий и требует в каждом случае разработки специального оборудования.

В отличие от указанных методов тепловой обладает рядом неоспоримых преимуществ: простота, безопасность, быстродействие, универсальность. Стремление расширить сферу применимости тепловых методов повлекло за собой создание во всем мире нового поколения тепловизионных компьютерных комплексов, технические возможности которых позволяют решать практически любые задачи фильтрации и обработки наблюдаемого теплового отклика.

К числу наиболее эффективных следует отнести алгоритмы динамической [1] и адаптивной [2] тепловой томографии (ТТ). Однако эти методы обладают рядом недостатков, не позволяющих их широко использовать. Во-первых, применяется одномерная модель, которая не учитывает растекание тепла в направлениях, параллельных поверхности объекта контроля (ОК). Это приводит к возникновению артефактов при анализе термограмм. Во-вторых, при послойной расшифровке температурного поля объекта удается восстановить лишь несколько верхних слоев, причем толщина последующего слоя вдвое больше предыдущего. Таким образом, до сих пор не удалось построить технологический процесс промышленной ТТ в полном объеме.

2. Цель исследований

Кардинальное отличие теплового метода контроля от альтернативных (рентгеновский, ультразвуковой и т.д.) заключается в диффузионном характере распространения тепла. Эта особенность является главной причиной затухания тепловых волн (носителя информации) в объекте контроля, что влечет за собой потерю информации о внутренней структуре ОК. Более того, информация о неоднородностях необратимо теряется не только с течением времени, но и по мере удаления от них.

Геометрические особенности ОК (дефекта) характеризуются размером l – его длиной (шириной). Так