**Содержание**

ВВЕДЕНИЕ 3

1 Диагностика локальных сетей 5

1.1 Актуальность создания и использования средств и систем 5

1.2 Инструменты диагностики 14

2 Техническое и информационное обеспечение технологий и средств диагностики 19

2.1.1 Сетевые анализаторы 19

2.2.2 Кабельные сканеры 19

2.2.3 Тестеры кабельных систем 20

2.3 Анализаторы протоколов 28

2.4 Общая характеристика протоколов мониторинга 32

2.4.1 Протокол SNMP 32

2.3.2 Агенты RMON 35

2.5 Обзор популярных системы управления сетями 41

3 Организация диагностики компьютерной сети 46

3.1 Документирование сети 49

3.2 Методика упреждающей диагностики 57

3.2 Организация процесса диагностики 58

4 Экономическая часть 79

4.1 Расчет капитальных затрат на создание технико-программного обеспечения 79

4.1.1 Расчёт затрат на оборудование 80

4.1.2 Расчёт затрат на создание ТПО 81

4.2 Расчет годовой экономии от автоматизации управленческой 86

деятельности 86

4.2.1 Расчет годовой экономии 86

4.2.2 Расчет себестоимости выполнения управленческих операций в ручном варианте 87

4.2.3 Расчет себестоимости выполнения управленческих операций в автоматизированном варианте 89

4.3 Расчет годового экономического эффекта применительно к 94

источнику получения экономии 94

4.4 Расчет коэффициента экономической эффективности и срока окупаемости капиталовложений 94

5 Охрана труда 96

5.1 Обеспечение электробезопасности 96

5.2 Анализ опасных и вредных производственных факторов 99

5.3 Требования к организации рабочего места и режима труда. 101

ЗАКЛЮЧЕНИЕ 104

Список ссылок 106

# ВВЕДЕНИЕ

Информационная инфраструктура современного предприятия представляет собой сложнейший конгломерат разномасштабных и разнородных сетей и систем. Чтобы обеспечить их слаженную и эффективную работу, необходима управляющая платформа корпоративного масштаба с интегрированными инструментальными средствами. Однако до недавнего времени сама структура индустрии сетевого управления препятствовала созданию таких систем – «игроки» этого рынка стремились к лидерству, выпуская продукты ограниченной области действия, использующие средства и технологии, не совместимые с системами других поставщиков.

Сегодня ситуация меняется к лучшему - появляются продукты, претендующие на универсальность управления всем разнообразием корпоративных информационных ресурсов, от настольных систем до мэйнфреймов и от локальных сетей до ресурсов Сети. Одновременно приходит осознание того, что управляющие приложения должны быть открыты для решений всех поставщиков [1].

Актуальность данной работы обусловлена тем, что в связи с распространением персональных компьютеров и созданием на их основе автоматизированных рабочих мест (АРМ) возросло значение локальных вычислительных сетей (ЛВС), диагностика которых, является объектом нашего исследования. Предметом исследования являются основные методы организации и проведения диагностики современных компьютерных сетей.

"Диагностика локальной сети" - процесс (непрерывного) анализа состояния информационной сети. При возникновении неисправности сетевых устройств фиксируется факт неисправности, определяется ее место и вид. Сообщение о неисправности передается, устройство отключается и заменяется резервным.

Сетевой администратор, на которого чаще всего ложатся функции по проведению диагностики, должен начинать изучать особенности своей сети уже на фазе ее формирования т.е. знать схему сети и подробное описание конфигурации программного обеспечения с указанием всех параметров и интерфейсов. Для оформления и хранения этой информации подойдут специальные системы документирования сети. Используя их, системный администратор, будет заранее знать все возможные «скрытые дефекты» и «узкие места» своей системы, для того, чтобы в случае возникновения нештатной ситуации знать, с чем связана проблема с оборудованием или программным обеспечением, повреждена программа или к ошибке привели действия оператора.

Сетевому администратору следует помнить, что с точки зрения пользователей качество работы прикладного программного обеспечения в сети оказывается определяющим. Все прочие критерии, такие как число ошибок передачи данных, степень загруженности сетевых ресурсов, производительность оборудования и т. п., являются вторичными. "Хорошая сеть" - это такая сеть, пользователи которой не замечают, как она работает.

**1 Диагностика локальных сетей**

## 

## **1.1 Актуальность создания и использования средств и систем**

Несмотря на множество приемов и инструментов обнаружения и устранения неполадок в корпоративных сетях, «почва под ногами» сетевых администраторов все еще остается достаточно зыбкой. Корпоративные сети все чаще включают волоконно-оптические и беспроводные компоненты, наличие которых делает бессмысленным применение традиционных технологий и инструментов, предназначенных для обычных медных кабелей. Вдобавок к нему при скоростях свыше 100 Мбит/с традиционные подходы к диагностике зачастую перестают работать, даже если средой передачи является обычный медный кабель. Однако, возможно, наиболее серьезным изменением в корпоративных сетевых технологиях, с которым пришлось столкнуться администраторам, стал неизбежный переход от сетей Ethernet с разделяемой средой передачи к коммутируемым сетям, в которых в качестве коммутируемых сегментов часто выступают отдельные серверы или рабочие станции.

Правда, по мере осуществления технологических преобразований некоторые старые проблемы решились сами собой. Коаксиальный кабель, в котором выявить электротехнические неисправности всегда было труднее, чем в случае витой пары, становится редкостью в корпоративных средах. Сети Token Ring, главной проблемой которых была их несхожесть с Ethernet (а вовсе не слабость в техническом отношении), постепенно заменяются коммутируемыми сетями Ethernet. Порождающие многочисленные сообщения об ошибках протоколов сетевого уровня протоколы, такие, как SNA, DECnet и AppleTalk, замещаются протоколом IP. Сам же стек протоколов IP стал более стабильным и простым для поддержки, что доказывают миллионы клиентов и миллиарды страниц Web в Internet. Даже закоренелым противникам Microsoft приходится признать, что подключение нового клиента Windows к Internet существенно проще и надежнее установки применявшихся ранее стеков TCP/IP сторонних поставщиков и отдельного программного обеспечения коммутируемого доступа.

Как бы многочисленные современные технологии ни затрудняли выявление неполадок и управление производительностью сетей, ситуация могла бы оказаться еще тяжелее, если бы технология АТМ получила широкое распространение на уровне ПК. Свою положительную роль сыграло и то, что в конце 90-х, не успев получить признание, были отвергнуты и некоторые другие высокоскоростные технологии обмена данными, включая Token Ring с пропускной способностью 100 Мбит/с, 100VG-AnyLAN и усовершенствованные сети ARCnet. Наконец, в США был отклонен очень сложный стек протоколов OSI (который, правда, узаконен рядом правительств европейских стран).

Рассмотри некоторые актуальные проблемы, возникающие у сетевых администраторов предприятий.

Иерархическая топология корпоративных сетей с магистральными каналами Gigabit Ethernet и выделенными портами коммутаторов на 10 или даже 100 Мбит/с для отдельных клиентских систем, позволила увеличить максимальную пропускную способность, потенциально доступную пользователям, как минимум в 10—20 раз. Конечно, в большинстве корпоративных сетей существуют узкие места на уровне серверов или маршрутизаторов доступа, поскольку приходящаяся на отдельного пользователя пропускная способность существенно меньше 10 Мбит/с. В связи с этим замена порта концентратора с пропускной способностью 10 Мбит/с на выделенный порт коммутатора на 100 Мбит/с для конечного узла отнюдь не всегда приводит к значительному увеличению скорости. Однако если учесть, что стоимость коммутаторов в последнее время снизилась, а на большинстве предприятий проложен кабель Категории 5, поддерживающий технологию Ethernet на 100 Мбит/с, и установлены сетевые карты, способные работать на скорости 100 Мбит/с сразу после перезагрузки системы, то становится ясно, почему так нелегко сопротивляться искушению модернизации. В традиционной локальной сети с разделяемой средой передачи анализатор протоколов или монитор может исследовать весь трафик данного сегмента сети.



Рисунок 1.1 - Традиционная локальная сеть с разделяемой средой передачи и анализатором протоколов

Хотя преимущество коммутируемой сети в производительности иногда почти не заметно, распространение коммутируемых архитектур имело катастрофические последствия для традиционных средств диагностики. В сильно сегментированной сети анализаторы протоколов способны видеть только одноадресный трафик на отдельном порту коммутатора, в отличие от сети прежней топологии, где они могли тщательно исследовать любой пакет в домене коллизий. В таких условиях традиционные инструменты мониторинга не могут собрать статистику по всем «диалогам», потому что каждая «переговаривающаяся» пара оконечных точек пользуется, в сущности, своей собственной сетью.



Рисунок 1.2 – Коммутируемая сеть

В коммутируемой сети анализатор протоколов в одной точке может «видеть» только единственный сегмент, если коммутатор не способен зеркально отображать несколько портов одновременно.

Для сохранения контроля над сильно сегментированными сетями производители коммутаторов предлагают разнообразные средства для восстановления полной «видимости» сети, однако на этом пути остается немало трудностей. В поставляемых сейчас коммутаторах обычно поддерживается «зеркальное отображение» портов, когда трафик одного из них дублируется на ранее незадействованный порт, к которому подключается монитор или анализатор.

Однако «зеркальное отображение» обладает рядом недостатков. Во-первых, в каждый момент времени виден только один порт, поэтому выявить неполадки, затрагивающие сразу несколько портов, очень непросто. Во-вторых, зеркальное отражение может привести к снижению производительности коммутатора. В-третьих, на зеркальном порту обычно не воспроизводятся сбои физического уровня, а иногда даже теряются обозначения виртуальных локальных сетей. Наконец, во многих случаях не могут в полной мере зеркально отображаться полнодуплексные каналы Ethernet.

Частичным решением при анализе агрегированных параметров трафика является использование возможностей мониторинга агентов mini-RMON, тем более что они встроены в каждый порт большинства коммутаторов Ethernet Хотя агенты mini-RMON не поддерживают группу объектов Capture из спецификации RMON II, обеспечивающих полнофункциональный анализ протоколов, они тем не менее позволяют оценить уровень использования ресурсов, количество ошибок и объем многоадресной рассылки.

Некоторые недостатки технологии зеркального отображения портов могут быть преодолены установкой «пассивных ответвителей», производимых, например, компанией Shomiti. Эти устройства представляют собой заранее устанавливаемые Y-коннекторы и позволяют отслеживать с помощью анализаторов протокола или другого устройства не регенерированный, а реальный сигнал.

Следующей актуально проблемой, является проблема с особенностями оптики. Администраторы корпоративных сетей обычно используют специализированное оборудование диагностики оптических сетей только для решения проблем с оптическими кабелями. Обычное стандартное программное обеспечение управления устройствами на базе SNMP или интерфейса командной строки способно выявить проблемы на коммутаторах и маршрутизаторах с оптическими интерфейсами. И только немногие сетевые администраторы сталкиваются с необходимостью проводить диагностику устройств SONET.

Что касается волоконно-оптических кабелей, то причин для возникновения возможных неисправностей в них существенно меньше, чем в случае медного кабеля. Оптические сигналы не вызывают перекрестных помех, появляющихся от того, что сигнал одного проводника индуцирует сигнал на другом — этот фактор наиболее усложняет диагностическое оборудование для медного кабеля. Оптические кабели невосприимчивы к электромагнитным шумам и индуцированным сигналам, поэтому их не требуется располагать подальше от электромоторов лифтов и ламп дневного света, т. е. из сценария диагностики все эти переменные можно исключить.

Сила сигнала, или оптическая мощность, в данной точке на самом деле является единственной переменной, которую требуется измерить при поиске неисправностей в оптических сетях. Если же можно определить потери сигнала на всем протяжении оптического канала, то можно будет идентифицировать практически любую проблему. Недорогие дополнительные модули для тестеров медного кабеля позволяют проводить оптические измерения.

Предприятиям, развернувшим крупную оптическую инфраструктуру и самостоятельно ее обслуживающим, может понадобиться приобрести оптический временный рефлектометр (Optical Time Domain Reflecto-meter, OTDR), выполняющего те же функции для оптического волокна, что и рефлектометр для медного кабеля (Time Domain Reflectometer, TDR). Прибор действует подобно радару: он посылает импульсные сигналы по кабелю и анализирует их отражения, на основании которых он выявляет повреждения в проводнике или какую-либо другую аномалию, и затем сообщает експерту, в каком месте кабеля следует искать источник проблемы.

Хотя различные поставщики кабельных соединителей и разъемов упростили процессы терминирования и разветвления оптического волокна, для этого по-прежнему требуется некоторый уровень специальных навыков, и при разумной политике предприятие с развитой оптической инфраструктурой вынуждено будет обучать своих сотрудников. Как бы хорошо ни была проложена кабельная сеть, всегда существует возможность физического повреждения кабеля в результате какого-либо неожиданного происшествия.

При диагностике беспроводных локальных сетей стандарта 802.11b также могут возникнуть проблемы. Сама по себе диагностика, столь же проста, как и в случае сетей Ethernet на базе концентраторов, так как беспроводная среда передачи информации разделяется между всеми обладателями клиентских радиоустройств. Компания Sniffer Technologies первой предложила решение для анализа протоколов таких сетей с пропускной способностью до 11 Мбит/с, и впоследствии большинство лидирующих поставщиков анализаторов представили аналогичные системы.

В отличие от концентратора Ethernet с проводными соединениями, качество беспроводных клиентских соединений далеко от стабильного. Микроволновые радиосигналы, используемые во всех вариантах локальной передачи, слабы и порой непредсказуемы. Даже небольшие изменения положения антенны могут серьезно сказаться на качестве соединений. Точки доступа беспроводной локальной сети снабжаются консолью управления устройствами, и это часто более действенный метод диагностики, чем посещение клиентов беспроводной сети и наблюдение за пропускной способностью и условиями возникновения ошибок с помощью портативного анализатора.

Хотя проблемы синхронизации данных и установки устройств, возникающие у пользователей персональных цифровых секретарей (PDA), более естественно соответствуют задачам группы технической поддержки, а не обязанностям сетевого администратора, нетрудно предвидеть, что в недалеком будущем многие такие устройства превратятся из отдельных вспомогательных средств, дополняющих ПК, в полноправных сетевых клиентов.

Как правило, операторы корпоративных беспроводных сетей будут (или должны) препятствовать развертыванию чрезмерно открытых систем, в которых любой пользователь, находящийся в зоне действия сети и обладающий совместимой интерфейсной картой, получает доступ к каждому информационному кадру системы. Протокол безопасности беспроводных сетей WEP (Wired Equivalent Privacy) обеспечивает аутентификацию пользователей, гарантию целостности и шифрование данных, однако, как это обычно случается, совершенная система безопасности осложняет анализ причин сетевых неполадок. В защищенных сетях с поддержкой WEP специалисты по диагностике должны знать ключи или пароли, защищающие информационные ресурсы и контролирующие доступ в систему. При доступе в режиме приема всех пакетов анализатор протоколов сможет видеть все заголовки кадров, но содержащаяся в них информация без наличия ключей будет бессмысленной.

При диагностировании туннелированных каналов, которые многие производители называют виртуальными частными сетями с удаленным доступом, возникающие проблемы аналогичны имеющим место при анализе беспроводных сетей с шифрованием. Если трафик не проходит через туннелированный канал, то причину неисправности определить нелегко. Это может быть ошибка аутентификации, поломка на одной из оконечных точек или затор в общедоступной зоне Internet. Попытка использования анализатора протоколов для выявления высокоуровневых ошибок в туннелированном трафике будет пустой тратой сил, потому что содержание данных, а также заголовки прикладного, транспортного и сетевого уровней зашифрованы. Вообще, меры, принимаемые в целях повышения уровня безопасности корпоративных сетей, обычно затрудняют выявление неисправностей и проблем производительности. Межсетевые экраны, proxy-серверы и системы выявления вторжений могут дополнительно осложнить локализацию неполадок.

Таким образом, проблема диагностики компьютерных сетей является актуальной и в конечном счете, диагностирование неисправностей является задачей управления. Для большинства критически важных корпоративных систем, проведение продолжительных восстановительных работ не допустимо, поэтому единственным решением будет использование резервных устройств и процессов, способных взять на себя необходимые функции немедленно после возникновения сбоев. На некоторых предприятиях сети всегда имеют дополнительный резервный компонент на случай сбоя основного, т. е. n х 2 компонентов, где n — количество основных компонентов, необходимое для обеспечения приемлемой производительности. Если среднее время восстановления (Mean Time To Repair, MTTR) достаточно велико, то может понадобиться еще большая избыточность. Дело в том, что время устранения неисправности предсказать нелегко, а значительные затраты в течение непредсказуемого периода восстановления являются признаком плохого управления.

Для менее важных систем резервирование может оказаться экономически неоправданным, и в этом случае будет целесообразно вкладывать средства в наиболее эффективные инструменты (и в обучение персонала), чтобы максимально ускорить процесс диагностики и устранения неисправностей на предприятии. Кроме того, поддержку определенных систем можно доверить сторонним специалистам, либо привлекая их на предприятие по контракту, либо пользуясь возможностями внешних центров обработки данных, либо обращаясь к провайдерам услуг по сопровождению приложений (Application Service Providers, ASP) или провайдерам услуг управления. Помимо затрат наиболее значительным фактором, влияющим на решение об обращении к услугам сторонних организаций, можно считать уровень компетентности собственного персонала. Сетевые администраторы должны решить, не является ли некоторая конкретная функция настолько тесно связанной со специфическими задачами предприятия, что от стороннего специалиста нельзя будет ожидать более качественного выполнения работы, чем это будет сделано силами служащих компании.

Почти сразу после того, как были развернуты первые корпоративные сети, надежность которых оставляла желать лучшего, производители и разработчики выдвинули концепцию «самовосстанавливающихся сетей». Современные сети, безусловно, надежнее, чем они были в 90-х гг., но не потому, что неполадки стали самоустраняться. Ликвидация сбоев программного обеспечения и аппаратных средств современных сетей все еще требуют вмешательства человека, и в ближайшей перспективе в таком положении дел не предвидится никаких принципиальных изменений. Методы и инструменты диагностики вполне соответствуют современной практике и технологиям, но они еще не достигли такого уровня, который позволил бы значительно сэкономить время сетевых администраторов в их борьбе с неполадками сетей и дефицитом производительности.

## 

## **1.2 Инструменты диагностики**

Ключевой функцией инструмента диагностики является обеспечение визуального представления реального состояния сети. Традиционно поставляемые производителями инструменты визуализации приблизительно соответствуют уровням модели OSI.

Начнем рассмотрение с физического уровня. Для разрешения проблем на этом уровне, а также в электрических или оптических средах передачи данных предназначены кабельные тестеры и такие специализированные инструменты, такие как временные рефлектометры (Time Domain Reflectometers, TDRs). За более чем 15 лет интенсивного развития корпоративных локальных сетей в ответ на потребности профессиональных сетевых интеграторов в кабельных тестерах реализовано множество функций, например выполнение автоматизированных тестовых последовательностей с возможностью печати сертификационных документов на основании результатов тестирования. Хотя сети Ethernet с пропускной способностью 10 Мбит/с допускают некоторые вольности в отношении качества их прокладки, технологии 100BaseT и Gigabit Ethernet с медным кабелем намного капризнее. Как следствие, современные кабельные тестеры достаточно сложны.

В число лидирующих поставщиков кабельных тестеров входят компании Fluke Networks, Microtest, Agilent, Acterna (прежнее название WWG) и Datacom Textron.

Для диагностики проблем на физическом уровне можно использовать следующие средства:

1) Разъем-заглушку (Hardware loopback) - это разъем, замыкающий выходную линию на входную, что позволяет компьютеру передавать данные самому себе. Разъем-заглушка используется при диагностике оборудования.

2) Расширенный тестер кабеля (Advanced cable tester; Cable tester) - специальное средство позволяющее вести мониторинг трафика сети и отдельного компьютера и выявлять определенные виды ошибок, неисправный кабель или сетевую плату.

3) Рефлектометр (Time-domain reflectometer) - устройство, предназначенное для выявления дефектов в кабельных линиях локационным (рефлектометрическим) методом. Рефлектометр посылает по кабелю короткие импульсы и обнаруживает и классифицирует разрывы, короткие замыкания и другие дефекты, также измеряет длину кабеля и его волновое сопротивление и выдает результаты на экран.

4) Тоновый генератор (Tone generator) - прибор, генерирующий в кабеле переменный или непрерывный тоновый сигнал, по которому тоновый определитель проверяет целостность и качество кабеля. Тоновый определитель - прибор, определяющий целостность и качество кабеля, на основе анализа сигналов, испускаемых тоновым генератором.

5) Цифровой вольтметр (Digital voltmeter) - электронное измерительное устройство общего назначения. Вольтметр позволяет измерять напряжение тока, проходящего через резистор, и определять целостность сетевых кабелей.

Для решения проблем канального, сетевого и транспортного уровней традиционным инструментом, который используется сетевыми администраторами, являются анализаторы протоколов (Protocol analyzer). Эти средства занимаются сбором статистики о работе сети и определением частоты ошибок и позволяют отслеживать и записывать состояния объектов сети. Часто имеют в своем составе встроенный рефлектометр.

Недорогие анализаторы обычно создаются на основе серийно выпускаемых портативных ПК с использованием стандартных сетевых карт с поддержкой режима приема всех пакетов. Основной недостаток анализаторов протоколов, состоит в том, некоторые виды неполадок на канальном уровне для них остаются невидимыми. Кроме того, они не позволяют выявить проблемы физического уровня в электрических или оптических кабелях. Вместе с тем, со временем в анализаторах протоколов появилась возможность исследования неполадок прикладного уровня, включая транзакции баз данных.

В число лидирующих поставщиков анализаторов протоколов локальных сетей входят Network Associates/Sniffer Technologies, Shomiti, Acterna (прежнее название WWG), Agilent, GN Nettest, WildPackets и Network Instruments.

Третьим основным диагностическим инструментом наряду с кабельными тестерами и анализаторами протоколов является зонд или монитор. Монитор сети (Network monitor) - программно-аппаратное устройство, которое отслеживает сетевой трафик и проверяет пакеты на уровне кадров, собирающее информацию о типах пакетов и ошибках.

Эти устройства обычно подключаются к сети на постоянной основе, а не только в случае возникновения проблемы и функционируют в соответствии со спецификациями удаленного мониторинга RMON и RMON II. Протокол RMON описывает метод сбора статистической информации об интенсивности трафика, ошибках, а также об основных источниках и потребителях трафика. Данные RMON относятся в первую очередь к канальному уровню, тогда как в стандарте RMON II добавлена поддержка уровней с третьего по седьмой. В протоколе RMON II предусмотрена возможность сбора пакетов или кадров с сохранением их в буфер — функция, используемая на первом этапе анализа протоколов. С другой стороны, практически любой современный анализатор протоколов собирает больше статистической информации, чем зонд RMON.

Между функциями анализаторов протоколов и зондами RMON нельзя провести четкую границу. Производители анализаторов обычно рекомендуют устанавливать агенты мониторинга и сбора данных по всей большой сети, пользователи же стремятся к тому, чтобы эти распределенные агенты были совместимы с международным стандартом RMON, а не с собственным форматом анализатора. До настоящего времени поставщики зондов RMON по-прежнему продолжают разрабатывать свои собственные протоколы для программного обеспечения декодирования и экспертного анализа, однако инструменты мониторинга и сбора данных, по всей вероятности, будут объединяться. С другой стороны поставщики анализаторов протоколов считают, что их программное обеспечение не предназначено для решения специфических задач RMON, таких, как анализ трафика и составление отчетов о производительности приложений.

Лидирующими поставщиками устройств RMON являются NetScout, Agilent, 3Com и Nortel. Кроме того, производители коммутаторов Ethernet встраивают поддержку основных функций RMON в каждый порт. Можно ожидать, что в современных условиях наиболее эффективным средством мониторинга коммутируемой сети будет использование имеющихся на каждом порте встроенных агентов mini-RMON и дополнение их возможностей системой с полной реализацией функций RMON II или анализатором протоколов с экспертным анализом.

Еще одним инструментом диагностики являются интегрированные диагностические средства. Производители диагностического оборудования объединили функции всех перечисленных традиционных инструментов в портативных устройствах для обнаружения распространенных неисправностей на нескольких уровнях OSI. Например, некоторые из этих устройств осуществляют проверку основных параметров кабеля, отслеживают количество ошибок на уровне Ethernet, обнаруживают дублированные IP-адреса, осуществляют поиск и подключение к серверам Novell NetWare, а также отображают распределение в сегменте протоколов третьего уровня.

В число лидирующих поставщиков интегрированных диагностических инструментов входят Fluke Networks, Datacom Textron, Agilent и Microtest. Компания Fluke несколько лет назад представила продукт OptiView Pro, в котором все компоненты для полномасштабной семиуровневой диагностики объединены в едином портативном устройстве. Фактически Optiview Pro представляет собой ПК под управлением ОС Windows с разъемами под платы расширения, где в дополнение к встроенному анализатору протоколов собственной разработки компании можно установить другой анализатор.

Среди программных средств диагностики компьютерных сетей, можно выделить специальные системы управления сетью (Network Management Systems) - централизованные программные системы, которые собирают данные о состоянии узлов и коммуникационных устройств сети, а также данные о трафике, циркулирующем в сети. Эти системы не только осуществляют мониторинг и анализ сети, но и выполняют в автоматическом или полуавтоматическом режиме действия по управлению сетью - включение и отключение портов устройств, изменение параметров мостов адресных таблиц мостов, коммутаторов и маршрутизаторов и т.п. Примерами систем управления могут служить популярные системы HPOpenView, SunNetManager, IBMNetView.

Средства управления системой (System Management) выполняют функции, аналогичные функциям систем управления, но по отношению к коммуникационному оборудованию. Вместе с тем, некоторые функции этих двух видов систем управления могут дублироваться, например, средства управления системой могут выполнять простейший анализ сетевого трафика.

Экспертные системы. Этот вид систем аккумулирует человеческие знания о выявлении причин аномальной работы сетей и возможных способах приведения сети в работоспособное состояние. Экспертные системы часто реализуются в виде отдельных подсистем различных средств мониторинга и анализа сетей: систем управления сетями, анализаторов протоколов, сетевых анализаторов. Простейшим вариантом экспертной системы является контекстно-зависимая help-система. Более сложные экспертные системы представляют собой так называемые базы знаний, обладающие элементами искусственного интеллекта. Примером такой системы является экспертная система, встроенная в систему управления Spectrum компании Cabletron.

# 2 Техническое и информационное обеспечение технологий и средств диагностики

**2.1 Оборудование для диагностики и сертификации кабельных систем**

К оборудованию данного класса относятся сетевые анализаторы, приборы для сертификации кабелей, кабельные сканеры и тестеры.

## 

## **2.1.1 Сетевые анализаторы**

Сетевые анализаторы представляют собой эталонные измерительные инструменты для диагностики и сертификации кабелей и кабельных систем. В качестве примера можно привести сетевые анализаторы компании Hewlett Packard - HP 4195A и HP 8510C.

Сетевые анализаторы содержат высокоточный частотный генератор и узкополосный приемник. Передавая сигналы различных частот в передающую пару и измеряя сигнал в приемной паре, можно измерить затухание и NEXT. Сетевые анализаторы - это прецизионные крупногабаритные и дорогие (стоимостью более $20000) приборы, предназначенные для использования в лабораторных условиях специально обученным техническим персоналом.

## 

## **2.2.2 Кабельные сканеры**

Данные приборы позволяют определить длину кабеля, NEXT, затухание, импеданс, схему разводки, уровень электрических шумов и провести оценку полученных результатов. Цена на эти приборы варьируется от $1'000 до $3'000. Существует достаточно много устройств данного класса, например, сканеры компаний MicrotestInc., FlukeCorp., Datacom TechnologiesInc., Scope CommunicationInc. В отличие от сетевых анализаторов сканеры могут быть использованы не только специально обученным техническим персоналом, но даже администраторами-новичками.

Для определения местоположения неисправности кабельной системы (обрыва, короткого замыкания, неправильно установленного разъема и т.д.) используется метод "кабельного радара", или Time Domain Reflectometry (TDR). Суть этого метода состоит в том, что сканер излучает в кабель короткий электрический импульс и измеряет время задержки до прихода отраженного сигнала. По полярности отраженного импульса определяется характер повреждения кабеля (короткое замыкание или обрыв). В правильно установленном и подключенном кабеле отраженный импульс совсем отсутствует.

Точность измерения расстояния зависит от того, насколько точно известна скорость распространения электромагнитных волн в кабеле. В различных кабелях она будет разной. Скорость распространения электромагнитных волн в кабеле (NVP – nominal velocity of propagation) обычно задается в процентах к скорости света в вакууме. Современные сканеры содержат в себе электронную таблицу данных о NVP для всех основных типов кабелей и позволяют пользователю устанавливать эти параметры самостоятельно после предварительной калибровки.

Наиболее известными производителями компактных кабельных сканеров являются компании MicrotestInc., WaveTekCorp., Scope Communication Inc.

## 

## **2.2.3 Тестеры кабельных систем**

Тестеры кабельных систем - наиболее простые и дешевые приборы для диагностики кабеля. Они позволяют определить непрерывность кабеля, однако, в отличие от кабельных сканеров, не дают ответа на вопрос о том, в каком месте произошел сбой.

Существуют целые классы средств тестирования кабельных систем, появление которых стало возможным благодаря наличию четких стандартов на характеристики компонентов (TIA/EIA568), а также на процедуры и критерии тестирования кабельных линий СКС (TSB-67).

Для удобства кабельные линии разделены на категории в соответствии с их параметрами. Многие из эксплуатируемых кабельных линий относятся к Категории 3 и предназначены для телефонии и передачи данных в диапазоне частот до 16 МГц (например, 10BaseT Ethernet). Однако наибольшее распространение получили кабельные линии Категории 5, гарантирующие передачу сигнала с частотой до 100 МГц. Комитетами стандартизации закончена работа над составлением перечня более жестких требований к параметрам кабельных линий Категории 5 (улучшенная Категория 5 или 5E), Категории 6 (200-250 МГц), Категории 7 (до 600 МГц) с целью повышения надежности передачи.

Большое количество моделей выпускаемых тестеров СКС предназначено для контроля кабельных линий Категорий 3, 5 и 5E (улучшенная Категория 5). Уже появились первые тестеры для проводки Категории 6 (например, LANcat System 6 компании Datacom или OMNIScanner компании Microtest). Однако основной парк тестеров СКС сегодня все же ориентирован на анализ характеристик линий в диапазоне частот до 100-155 МГц. За исключением анализируемого диапазона частот, другие параметры этих тестеров отличаются друг от друга несущественно, так как тестирование выполняется по одним и тем же методикам. Основные отличия заключаются в характеристиках встроенных рефлектометров для проводных линий (максимальная дальность, точность, разрешение, форма представления результата), в пользовательском интерфейсе и удобстве работы, а также в наборе вспомогательных и сервисных функций.

Среди вспомогательных функций могут быть особенно, полезны следующие:

* двустороннее измерение;
* тестирование волоконно-оптических кабелей;
* карта (схема соединения) жил кабеля;
* обнаружение импульсных помех;
* мониторинг трафика ЛВС;
* составление программ тестирования;
* организация разговорного тракта между основным и удаленным модулем;
* встроенный тональный генератор для трассировки и идентификации и др.

Приведенная ниже информация позволит ознакомиться с измеряемыми параметрами кабельной линии и облегчит выбор прибора для конкретных нужд.

Основными электрическими параметрами, от которых зависит работоспособность кабельной линии, являются:

* целостность цепи (connectivity);
* характеристический импеданс (characteristic impedance) и обратные потери (return loss);
* погонное затухание (attenuation);
* переходное затухание (crosstalk);
* задержка распространения сигнала (propagation delay) и длина линии (cable length);
* сопротивление линии по постоянному току (loop resistance);
* емкость линии (capacitance);
* электрическая симметричность (balance);
* наличие шумов в линии (electrical noise, electromagnetic interference).

Рассмотрим эти характеристики подробнее

1) Целостность цепи

Основная задача этого теста - выявить ошибки монтажа соединителей или кроссировки (замыкания, обрывы, перепутанные жилы). Поскольку ошибки подобного рода на практике преобладают, то существует большое количество недорогих приборов, единственной функцией которых является только контроль целостности цепи. Однако полнофункциональные тестеры СКС, как правило, предоставляют более полную информацию о характере ошибки, вплоть до схемы соединения, по которой монтажник может точно идентифицировать дефект.

## 



## 



Рисунок 2.1 - Тестеры СКС

2) Характеристический импеданс (волновое сопротивление)

Поскольку передача данных ведется на высоких частотах, то немаловажную роль имеет импеданс линии, т. е. ее сопротивление переменному току заданной частоты. Роль играет не только величина сопротивления, но и его постоянство по всей линии (кабелю и соединителям) для всего диапазона рассматриваемых частот. Это объясняется тем, что сигнал, отраженный от точек с аномальным импедансом, будет накладываться на основной сигнал и искажать его.

Для кабеля из витых пар импеданс обычно составляет 100 или 120 Ом. Для линий Категории 5 импеданс нормируется для диапазона частот 1-100 МГц и должен составлять 100 Ом v15%.

Основные причины неоднородности импеданса следующие:

- нарушение шага скрутки в местах разделки кабеля около соединителей (максимальное расстояние, на которое жилы могут быть развиты при разделке, - 13 мм);

- дефекты кабеля (повышенное сопротивление жил, пониженное сопротивление изоляции, нарушение шага скрутки);

- неправильная укладка кабеля (применение скоб и хомутов для крепления, малый радиус изгиба, заломы и "барашки" из-за неправильной отмотки);

- некачественная опрессовка соединителей или использование некачественных соединителей.

Аналогичные проблемы возникают на прошедших тестирование линиях при подключении к ее розеткам некачественных (не соответствующих требованиям заданной категории) коммутационных шнуров, переходников или расщепителей линии (сплиттеров).

Оценка влияния, вносимого неоднородностями импеданса, выражается таким параметром, как обратные потери (отношение амплитуды переданного сигнала к амплитуде отраженного в дБ). Если дефект порождает в линии существенную неоднородность импеданса, то обратные потери будут малы, так как большая часть энергии сигнала будет отражена от неоднородности. Так, в случае обрыва или замыкания кабеля обратные потери будут равны 0.

Все полнофункциональные тестеры СКС имеют встроенный рефлектометр для проводных линий с цифровым или графическим отображением результата, с помощью которого место с аномальным импедансом может быть без труда локализовано. Некоторые рефлектометры позволяют вычислять обратные потери для заданного участка линии, что позволяет определить влияние имеющихся на нем неоднородностей на результирующую характеристику линии.

3) Погонное затухание (Attenuation)

Ослабление сигнала при его распространении по линии оценивается затуханием (выраженное в дБ отношение мощности сигнала, поступившего в нагрузку на конце линии, к мощности сигнала, поданного в линию). Затухание сильно увеличивается с ростом частоты, поэтому оно должно измеряться для всего диапазона используемых частот. Для кабеля категории 5 при частоте 100 Мгц затухание не должно превышать 23.6 Дб на 100 м, а для кабеля категории 3, применяемого по стандарту IEEE 802.3 10BASE-T, допустимая величина затухания на сегменте длиной 100 м не должна превышать 11,5 Дб при частоте переменного тока 10 МГц.

4) Переходное затухание

Данный параметр характеризует степень перекрестных наводок сигнала между парами одного кабеля (отношение амплитуды поданного сигнала к амплитуде наведенного сигнала в дБ). Эта характеристика имеет несколько разновидностей, каждая из которых позволяет оценить разные свойства кабеля.

При определении переходного затухания на ближнем конце линии (Near End Cross Talk, NEXT; Power Sum NEXT, PS-NEXT) подача сигнала и измерение производятся с одной стороны линии для всех частот заданного диапазона. В первом случае для проведения измерения в одной паре сигнал подается поочередно на все остальные пары. Именно это измерение и применяется для тестирования кабельных линий Категории 5. Во втором случае тестирование производится по более жестким правилам: сигнал подается сразу на все остальные пары и измеряется суммарное затухание.

Очевидно, что переходное затухание на ближнем конце линии необходимо измерять с обеих ее сторон, так как влияние дефектов на этот параметр будет тем сильнее, чем ближе они расположены к месту измерения. В новых стандартах предполагается проводить и измерение затухания на разных концах линии одновременно.

Функционирование линии будет надежным только тогда, когда переходное затухание велико, а погонное - мало, поэтому оценку качества линии очень удобно производить на основании комбинированного параметра - защищенности на дальнем конце линии (Attenuation to Crosstalk Ratio, ACR; Power Sum ACR, PS-ACR), выраженного как отношение величин погонного затухания и переходного затухания на ближнем конце линии. Фактически этот параметр показывает, насколько амплитуда принимаемого полезного сигнала выше амплитуды шумов для заданной частоты сигнала.

Однако если передача ведется по нескольким парам одновременно (например, 100Base-T4 и 100VG-AnyLAN), то в таких сетях важное значение имеет и уровень переходного затухания на дальнем конце линии (Far-End CrossTalk, FEXT). Поскольку на приемник поступает суперпозиция полезного сигнала, передаваемого по данной паре, и сигнала, наведенного на нее с другой пары, оценка качества линии производится на основании отношения величин полезного сигнала на дальнем конце линии (т. е. с учетом его затухания) и наведенного сигнала - приведенное переходное затухание на дальнем конце линии (Equal-Level Far-End Cross Talk, ELFEXT; Power Sum ELFEXT, PS-ELFEXT).

Удовлетворительное значение переходного затухания косвенно свидетельствует о симметричности линии и, следовательно, об отсутствии излучения витой парой электромагнитных и приема электромагнитных и радиопомех.

5) Задержка распространения сигнала и длина линии

Для надежной работы на высоких скоростях необходимо, чтобы задержка распространения сигнала не превышала заданную и была одинакова для всех пар кабельной линии. Измерение длины кабеля осуществляется в соответствии с принципом рефлектометрии.

Следует отметить, что некоторые системы передачи (например, 100Base-T4 и 100VG-AnyLAN) весьма чувствительны не только к абсолютному значению задержки распространения сигнала, но и к ее разнице (propagation delay skew) для различных пар одной кабельной линии. Такой перекос задержки и, как следствие, необходимость его измерения возникли после того, как некоторые производители стали выпускать кабели с различной изоляцией пар (известные как "2+2" и "3+1").

6) Уровень шумов в линии

Иногда электромагнитные и радиопомехи делают невозможной устойчивую передачу сигнала в линии. Большинство тестеров СКС позволяют измерить уровень шумов для последующего анализа и устранения их причин.

Самые распространенные шумы - это импульсные помехи от расположенного вдоль трассы мощного электрооборудования (моторов, пускорегулирующей аппаратуры, светильников дневного света и т. п.) или силовой проводки к ним. Очень часто для устранения подобной проблемы кабель достаточно переместить на несколько метров в сторону. Гораздо реже работе мешает расположенное поблизости радиопередающее оборудование. Устранение помех в этом случае потребует экранировки кабеля или его укладки в металлических каналах.

Как видно из вышесказанного, подлежащих определению параметров кабельных линий достаточно много, причем они имеют различное значение для тех или иных приложений. Однако и разнообразие приборов для их измерения не менее велико. Самый простой способ не ошибиться при выборе - исходить из потребностей вашей организации и ее планов на ближайшее будущее.

Не все рассмотренные параметры охватываются стандартами СКС. Например, TSB-67 требует для кабельных систем Категории 5 контроля четырех параметров: правильности подключения линии, длины линии, затухания сигнала, переходного затухания на ближнем конце линии. В то же время спецификации некоторых высокоскоростных систем передачи предъявляют и ряд других, более жестких требований к параметрам кабельных линий. Некоторые из них уже включены в новые стандарты, остальные будут включены в ближайшем будущем.

Если компания занимается монтажом, то лучше приобретать прибор с развитыми сервисными функциями для быстрой локализации ошибок монтажа, с возможностью сохранения результатов для последующей передачи на компьютер и формирования протоколов приемочных испытаний. Кроме того, желательно, чтобы приобретенный прибор обеспечивал возможность модернизации заложенной в нем программы в соответствии с требованиями новых стандартов. Затраты на приобретение прибора такого уровня могут оказаться высоки, но окупятся достаточно быстро.

Если же прибор приобретается для обслуживания существующей СКС, то в целях экономии можно ограничиться недорогим устройством для проверки линий СКС требованиям конкретных приложений (10BaseT, 100BaseTX, ATM 155 и т. п.), которые организация использует в настоящее время или собирается использовать в ближайшем будущем.

## **2.3 Анализаторы протоколов**

В ходе проектирования новой или модернизации старой сети часто возникает необходимость в количественном измерении некоторых характеристик сети таких, например, как интенсивности потоков данных по сетевым линиям связи, задержки, возникающие на различных этапах обработки пакетов, времена реакции на запросы того или иного вида, частота возникновения определенных событий и других характеристик.

Для этих целей могут быть использованы разные средства и прежде всего - средства мониторинга в системах управления сетью, которые уже обсуждались ранее. Некоторые измерения на сети могут быть выполнены и встроенными в операционную систему программными измерителями, примером тому служит компонента ОС Windows Performance Monitor. Даже кабельные тестеры в их современном исполнении способны вести захват пакетов и анализ их содержимого.

Но наиболее совершенным средством исследования сети является анализатор протоколов. Процесс анализа протоколов включает захват циркулирующих в сети пакетов, реализующих тот или иной сетевой протокол, и изучение содержимого этих пакетов. Основываясь на результатах анализа, можно осуществлять обоснованное и взвешенное изменение каких-либо компонент сети, оптимизацию ее производительности, поиск и устранение неполадок. Очевидно, что для того, чтобы можно было сделать какие-либо выводы о влиянии некоторого изменения на сеть, необходимо выполнить анализ протоколов и до, и после внесения изменения.

Анализатор протоколов представляет собой либо самостоятельное специализированное устройство, либо персональный компьютер, обычно переносной, класса Notebook, оснащенный специальной сетевой картой и соответствующим программным обеспечением. Применяемые сетевая карта и программное обеспечение должны соответствовать топологии сети (кольцо, шина, звезда). Анализатор подключается к сети точно также, как и обычный узел. Отличие состоит в том, что анализатор может принимать все пакеты данных, передаваемые по сети, в то время как обычная станция - только адресованные ей. Программное обеспечение анализатора состоит из ядра, поддерживающего работу сетевого адаптера и декодирующего получаемые данные, и дополнительного программного кода, зависящего от типа топологии исследуемой сети. Кроме того, поставляется ряд процедур декодирования, ориентированных на определенный протокол, например, IPX. В состав некоторых анализаторов может входить также экспертная система, которая может выдавать пользователю рекомендации о том, какие эксперименты следует проводить в данной ситуации, что могут означать те или иные результаты измерений, как устранить некоторые виды неисправности сети.

Несмотря на относительное многообразие анализаторов протоколов, представленных на рынке, можно назвать некоторые черты, в той или иной мере присущие всем им:

* *Пользовательский интерфейс.* Большинство анализаторов имеют развитый дружественный интерфейс, базирующийся, как правило, на Windows или Motif. Этот интерфейс позволяет пользователю: выводить результаты анализа интенсивности трафика; получать мгновенную и усредненную статистическую оценку производительности сети; задавать определенные события и критические ситуации для отслеживания их возникновения; производить декодирование протоколов разного уровня и представлять в понятной форме содержимое пакетов.
* *Буфер захвата*. Буферы различных анализаторов отличаются по объему. Буфер может располагаться на устанавливаемой сетевой карте, либо для него может быть отведено место в оперативной памяти одного из компьютеров сети. Если буфер расположен на сетевой карте, то управление им осуществляется аппаратно, и за счет этого скорость ввода повышается. Однако это приводит к удорожанию анализатора. В случае недостаточной производительности процедуры захвата, часть информации будет теряться, и анализ будет невозможен. Размер буфера определяет возможности анализа по более или менее представительным выборкам захватываемых данных. Но каким бы большим ни был буфер захвата, рано или поздно он заполнится. В этом случае либо прекращается захват, либо заполнение начинается с начала буфера.
* *Фильтры.* Фильтры позволяют управлять процессом захвата данных, и, тем самым, позволяют экономить пространство буфера. В зависимости от значения определенных полей пакета, заданных в виде условия фильтрации, пакет либо игнорируется, либо записывается в буфер захвата. Использование фильтров значительно ускоряет и упрощает анализ, так как исключает просмотр ненужных в данный момент пакетов.
* *Переключатели* - это задаваемые оператором некоторые условия начала и прекращения процесса захвата данных из сети. Такими условиями могут быть выполнение ручных команд запуска и остановки процесса захвата, время суток, продолжительность процесса захвата, появление определенных значений в кадрах данных. Переключатели могут использоваться совместно с фильтрами, позволяя более детально и тонко проводить анализ, а также продуктивнее использовать ограниченный объем буфера захвата.
* *Поиск*. Некоторые анализаторы протоколов позволяют автоматизировать просмотр информации, находящейся в буфере, и находить в ней данные по заданным критериям. В то время, как фильтры проверяют входной поток на предмет соответствия условиям фильтрации, функции поиска применяются к уже накопленным в буфере данным.

Методология проведения анализа может быть представлена в виде следующих шести этапов:

1. Захват данных.
2. Просмотр захваченных данных.
3. Анализ данных.
4. Поиск ошибок. (Большинство анализаторов облегчают эту работу, определяя типы ошибок и идентифицируя станцию, от которой пришел пакет с ошибкой.)
5. Исследование производительности. Рассчитывается коэффициент использования пропускной способности сети или среднее время реакции на запрос.
6. Подробное исследование отдельных участков сети. Содержание этого этапа конкретизируется по мере того, как проводится анализ.

Обычно процесс анализа протоколов занимает относительно немного времени - 1-2 рабочих дня.

Большинство современных анализаторов позволяют анализировать сразу несколько протоколов глобальных сетей, таких, как X.25, PPP, SLIP, SDLC/SNA, frame relay, SMDS, ISDN, протоколы мостов/маршрутизаторов (3Com, Cisco, Bay Networks и другие). Такие анализаторы позволяют измерять различные параметры протоколов, анализировать трафик в сети, преобразование между протоколами локальных и глобальных сетей, задержку на маршрутизаторах при этих преобразованиях и т. п. Более совершенные приборы предусматривают возможность моделирования и декодирования протоколов глобальных сетей, 'стрессового' тестирования, измерения максимальной пропускной способности, тестирования качества предоставляемых услуг. В целях универсальности почти все анализаторы протоколов глобальных сетей реализуют функции тестирования ЛВС и всех основных интерфейсов. Некоторые приборы способны осуществлять анализ протоколов телефонии. А самые современные модели могут декодировать и представлять в удобном варианте все семь уровней OSI. Появление ATM привело к тому, что производители стали снабжать свои анализаторы средствами тестирования этих сетей. Такие приборы могут проводить полное тестирование сетей АТМ уровня E-1/E-3 с поддержкой мониторинга и моделирования. Очень важное значение имеет набор сервисных функций анализатора. Некоторые из них, например возможность удаленного управления прибором, просто незаменимы.

Таким образом, современные анализаторы протоколов WAN/LAN/ATM позволяют обнаружить ошибки в конфигурации маршрутизаторов и мостов; установить тип трафика, пересылаемого по глобальной сети; определить используемый диапазон скоростей, оптимизировать соотношение между пропускной способностью и количеством каналов; локализовать источник неправильного трафика; выполнить тестирование последовательных интерфейсов и полное тестирование АТМ; осуществить полный мониторинг и декодирование основных протоколов по любому каналу; анализировать статистику в реальном времени, включая анализ трафика локальных сетей через глобальные сети.

## 

## **2.4 Общая характеристика протоколов мониторинга**

## 

## **2.4.1 Протокол SNMP**

SNMP (англ. Simple Network Management Protocol — простой протокол управления сетью) — это протокол управления сетями связи на основе архитектуры TCP/IP.

На основе концепции TMN в 1980—1990 гг. различными органами стандартизации был выработан ряд протоколов управления сетями передачи данных с различным спектром реализации функций TMN. К одному из типов таких протоколов управления относится SNMP. Протокол SNMP был разработан с целью проверки функционирования сетевых маршрутизаторов и мостов. Впоследствии сфера действия протокола охватила и другие сетевые устройства, такие как хабы, шлюзы, терминальные сервера, LAN Manager сервера , машины под управлением Windows NT и т.д. Кроме того, протокол допускает возможность внесения изменений в функционирование указанных устройств.

Эта технология, призвана обеспечить управление и контроль за устройствами и приложениями в сети связи путём обмена управляющей информацией между агентами, располагающимися на сетевых устройствах, и менеджерами, расположенными на станциях управления. SNMP определяет сеть как совокупность сетевых управляющих станций и элементов сети (главные машины, шлюзы и маршрутизаторы, терминальные серверы), которые совместно обеспечивают административные связи между сетевыми управляющими станциями и сетевыми агентами.

При использовании SNMP присутствуют управляемые и управляющие системы. В состав управляемой системы входит компонент, называемый агентом, который отправляет отчёты управляющей системе. По существу SNMP агенты передают управленческую информацию на управляющие системы как переменные (такие как «свободная память», «имя системы», «количество работающих процессов»).

Агент в протоколе SNMP - это обрабатывающий элемент, который обеспечивает менеджерам, размещенным на управляющих станциях сети, доступ к значениям переменных MIB, и тем самым дает им возможность реализовывать функции по управлению и наблюдению за устройством.

Программный агент - резидентная программа, выполняющая функции управления, а также собирающая статистику для передачу ее в информационную базу сетевого устройства.

Аппаратный агент - встроенная аппаратура (с процессором и памятью), в которой хранятся программные агенты.

Переменные, доступные через SNMP, организованы в иерархии. Эти иерархии и другие метаданные (такие, как тип и описание переменной) описываются Базами Управляющей Информации (http://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9\_%D1%8F%D0%B7%D1%8B%D0%BA Management Information Bases (MIBs)).

На сегодня существует несколько стандартов на базы данных управляющей информации [3, 4]. Основными являются стандарты MIB-I и MIB-II, а также версия базы данных для удаленного управления RMON MIB. Кроме этого, существуют стандарты для специальных MIB устройств конкретного типа (например, MIB для концентраторов или MIB для модемов), а также частные MIB конкретных фирм-производителей оборудования.

Первоначальная спецификация MIB-I определяла только операции чтения значений переменных. Операции изменения или установки значений объекта являются частью спецификаций MIB-II.

Версия MIB-I (RFC 1156) определяет до 114 объектов, которые подразделяются на 8 групп:

* System - общие данные об устройстве (например, идентификатор поставщика, время последней инициализации системы).
* Interfaces - описываются параметры сетевых интерфейсов устройства (например, их количество, типы, скорости обмена, максимальный размер пакета).
* AddressTranslationTable - описывается соответствие между сетевыми и физическими адресами (например, по протоколу ARP).
* InternetProtocol - данные, относящиеся к протоколу IP (адреса IP-шлюзов, хостов, статистика об IP-пакетах).
* ICMP - данные, относящиеся к протоколу обмена управляющими сообщениями ICMP.
* TCP - данные, относящиеся к протоколу TCP (например, о TCP-соединениях).
* UDP - данные, относящиеся к протоколу UDP (число переданных, принятых и ошибочных UPD-дейтаграмм).
* EGP - данные, относящиеся к протоколу обмена маршрутной информацией ExteriorGatewayProtocol, используемому в сети Internet (число принятых с ошибками и без ошибок сообщений).

Из этого перечня групп переменных видно, что стандарт MIB-I разрабатывался с жесткой ориентацией на управление маршрутизаторами, поддерживающими протоколы стека TCP/IP.

В версии MIB-II (RFC 1213), принятой в 1992 году, был существенно (до 185) расширен набор стандартных объектов, а число групп увеличилось до 10.

## **2.3.2 Агенты RMON**

Новейшим добавлением к функциональным возможностям SNMP является спецификация RMON, которая обеспечивает удаленное взаимодействие с базой MIB.

Стандарт на RMON появился в ноябре 1991 года, когда Internet Engineering Task Force выпустил документ RFC 1271 под названием "Remote Network Monitoring Management Information Base" ("Информационная база дистанционного мониторинга сетей"). Данный документ содержал описание RMON для сетей Ethernet.

RMON — протокол мониторинга компьютерных сетей, расширение SNMP, в основе которого, как и в основе SNMP, лежит сбор и анализ информации о характере информации, передаваемой по сети. Как и в SNMP, сбор информации осуществляется аппаратно-программными агентами, данные от которых поступают на компьютер, где установлено приложение управления сетью. Отличие RMON от своего предшественника состоит, в первую очередь, в характере собираемой информации — если в SNMP эта информация характеризует только события, происходящие на том устройстве, где установлен агент, то RMON требует, чтобы получаемые данные характеризовали трафик между сетевыми устройствами.

До появления RMON протокол SNMP не мог использоваться удаленным образом, он допускал только локальное управление устройствами. База RMON MIB обладает улучшенным набором свойств для удаленного управления, так как содержит агрегированную информацию об устройстве, что не требует передачи по сети больших объемов информации. Объекты RMON MIB включают дополнительные счетчики ошибок в пакетах, более гибкие средства анализа графических трендов и статистики, более мощные средства фильтрации для захвата и анализа отдельных пакетов, а также более сложные условия установления сигналов предупреждения. Агенты RMON MIB более интеллектуальны по сравнению с агентами MIB-I или MIB-II и выполняют значительную часть работы по обработке информации об устройстве, которую раньше выполняли менеджеры. Эти агенты могут располагаться внутри различных коммуникационных устройств, а также быть выполнены в виде отдельных программных модулей, работающих на универсальных ПК и ноутбуках (примером может служить LANalyzerNovell).

Интеллект агентов RMON позволяет им выполнять простые действия по диагностике неисправностей и предупреждению о возможных отказах - например, в рамках технологии RMON можно собрать данные о нормальном функционировании сети (т. е. выполнить так называемый baselining), а потом выставлять предупреждающие сигналы, когда режим работы сети отклонится от baseline - это может свидетельсствовать, в частности, о неполной исправности оборудования. Собрав воедино информацию, получаемую от агентов RMON, приложение управления может помочь администратору сети (находящемуся, например, за тысячи километров от анализируемого сегмента сети) локализовать неисправность и выработать оптимальный план действий для ее устранения.

Сбор информации RMON осуществляется аппаратно-программными зондами, подключаемыми непосредственно к сети. Чтобы выполнить задачу сбора и первичного анализа данных, зонд должен обладать достаточными вычислительными ресурсами и объемом оперативной памяти. В настоящее время на рынке имеются зонды трех типов: встроенные, зонды на базе компьютера, и автономные. Продукт считается поддерживающим RMON, если в нем реализована хотя бы одна группа RMON. Разумеется, чем больше групп данных RMON реализовано в данном продукте, тем он, с одной стороны, дороже, а с другой - тем более полную информацию о работе сети он предоставляет.

Встроенные зонды представляют собой модули расширения для сетевых устройств. Такие модули выпускаются многими производителями, в частности, такими крупными компаниями, как 3Com, Cabletron, Bay Networks и Cisco. (Кстати, 3Com и Bay Networks недавно приобрели компании Axon и ARMON, признанных лидеров в области разработки и производства средств управления RMON. Такой интерес к этой технологии со стороны крупнейших производителей сетевого оборудования лишний раз показывает, насколько нужным для пользователей является дистанционный мониторинг.) Наиболее естественным выглядит решение встраивать модули RMON в концентраторы, ведь именно из наблюдения за этими устройствами можно составить себе представление о работе сегмента. Достоинство таких зондов очевидно: они позволяют получать информацию по всем основным группам данных RMON при относительно невысокой цене. Недостатком в первую очередь является не слишком высокая производительность, что проявляется, в частности, в том, что встроенные зонды часто поддерживают далеко не все группы данных RMON. Не так давно 3Com объявила о намерении выпустить поддерживающие RMON драйверы для сетевых адаптеров Etherlink III и Fast Ethernet. В результате окажется возможным собирать и анализировать данные RMON непосредственно на рабочих станциях в сети.

Зонды на базе компьютера - это просто подключенные к сети компьютеры с установленным на них программным агентом RMON. Такие зонды (к числу которых относится, например, продукт Cornerstone Agent 2.5 компании Network General) обладают более высокой производительностью, чем встроенные зонды, и поддерживают, как правило, все группы данных RMON. Они более дороги, чем встроенные зонды, но гораздо дешевле автономных зондов. Помимо этого, зонды на базе компьютера имеют довольно большой размер, что может иногда ограничивать возможности их применения.

Автономные зонды обладают наивысшей производительностью; как легко понять, это одновременно и наиболее дорогие продукты из всех описанных. Как правило, автономный зонд - это процессор (класса i486 или RISC-процессор), оснащенный достаточным объемом оперативной памяти и сетевым адаптером. Лидерами в этом секторе рынка являются компании Frontier и Hewlett-Packard. Зонды этого типа невелики по размеру и весьма мобильны - их очень легко подключать к сети и отключать от нее. При решении задачи управления сетью глобального масштаба это, конечно, не слишком важное свойство, однако если средства RMON применяются для анализа работы корпоративной сети средних размеров, то (учитывая высокую стоимость устройств) мобильность зондов может сыграть весьма положительную роль.

Объекту RMON присвоен номер 16 в наборе объектов MIB, а сам объект RMON объединяет в соответствии с документом RFC 1271, состоит из десяти групп данных.

* Statistics - текущие накопленные статистические данные о характеристиках пакетов, количестве коллизий и т.п.
* History - статистические данные, сохраненные через определенные промежутки времени для последующего анализа тенденций их изменений.
* Alarms - пороговые значения статистических показателей, при превышении которых агент RMON посылает сообщение менеджеру. Позволяет пользователю определить ряд пороговых уровней (эти пороги могут отнситься к самым разным вещам - любому параметру из группы статистики, амплитуде или скорости его изменения и многому другому), по превышении которых генерируется аварийный сигнал. Пользователь может также определить, при каких условиях превышение порогового значения должно сопровождаться аварийным сигналом - это позволит избежать генерации сигнала "по пустякам", что плохо, во-первых, потому, что на постоянно горящую красную лампочку никто не обращает внимания, а во-вторых, потому, что передача ненужных аварийных сигналов по сети приводит к излишней загрузке линий связи. Аварийный сигнал, как правило, передается в группу событий, где и определяется, что с ним делать дальше.
* Host - данных о хостах сети, в том числе и об их MAC-адресах..
* HostTopN - таблица наиболее загруженных хостов сети. Таблица N главных хостов (HostTopN) содержит список N первых хостов, характеризующихся максимальным значением заданного статистического параметра для заданного интервала. Например, можно затребовать список 10 хостов, для которых наблюдалось максимальное количество ошибок в течение последних 24 часов. Список этот будет составлен самим агентом, а приложение управления получит только адреса этих хостов и значения соответствующих статистических параметров. Видно, до какой степени такой подход экономит сетевые ресурсы
* TrafficMatrix - статистика об интенсивности трафика между каждой парой хостов сети, упорядоченная в виде матрицы. Строки этой матрицы пронумерованы в соответствии с MAC-адресами станций - источников сообщений, а столбцы - в соответствии с адресами станций-получателей. Матричные элементы характеризуют интенсивность трафика между соответствующими станциями и количество ошибок. Проанализировав такую матрицу, пользователь легко может выяснить, какие пары станций генерируют наиболее интенсивный трафик. Эта матрица, опять-таки, формируется самим агентом, поэтому отпадает необходимость в передаче больших объемов данных на центральный компьютер, отвечающий за управление сетью.
* Filter - условия фильтрации пакетов. Признаки, по которым фильтруются пакеты, могут быть самыми разнообразными - например, можно потребовать отфильтровывать как ошибочные все пакеты, длина которых оказывается меньше некоторого заданного значения. Можно сказать, что установка фильтра соответствует как бы организации канала для передачи пакета. Куда ведет этот канал - определяет пользователь. Например, все ошибочные пакеты могут перехватываться и направляться в соответсвующий буфер. Кроме того, появление пакета, соответствующего установленному фильтру, может рассматриваться как событие (event), на которое система должна реагировать заранее оговоренным образом.
* PacketCapture - условия захвата пакетов. В состав группы перехвата пакетов (packet capture) входят буфера для захвата, куда направляются пакеты, чьи признаки удовлетворяют условиям, сформулированным в группе фильтров. При этом захватываться может не пакет целиком, а, скажем, только первые несколько десятков байт пакета. Содержимое буферов перехвата можно впоследствии анализировать при помощи различных программных средств, выясняя целый ряд весьма полезных характеристик работы сети. Перестраивая фильтры на те или иные признаки, можно характеризовать разные параметры работы сети.
* Event - условия регистрации и генерации событий. В группе событий (events) определяется, когда следует отправлять аварийный сигнал приложению управления, когда - перхватывать пакеты, и вообще - как реагировать на те или иные события, происходящие в сети, например, на превышение заданных в группе alarms пороговых значений: следует ли ставить в известность приложение управления, или надо просто запротоколировать данное событие и продолжать работать. События могут и не быть связаны с предачей аварийных сигналов - например, направление пакета в буфер перехвата тоже представляет собой событие.

Данные группы пронумерованы в указанном порядке, поэтому, например, группа Hosts имеет числовое имя 1.3.6.1.2.1.16.4.

Десятую группу составляют специальные объекты протокола TokenRing.

Всего стандарт RMON MIB определяет около 200 объектов в 10 группах, зафиксированных в двух документах - RFC 1271 для сетей Ethernet и RFC 1513 для сетей TokenRing.

Отличительной чертой стандарта RMON MIB является его независимость от протокола сетевого уровня (в отличие от стандартов MIB-I и MIB-II, ориентированных на протоколы TCP/IP). Поэтому, его удобно использовать в гетерогенных средах, использующих различные протоколы сетевого уровня.

## **2.5 Обзор популярных системы управления сетями**

Система управления сетью ( Network management system )- аппаратные и/или программные средства для мониторинга и управления узлами сети. Программное обеспечение системы управления сетью состоит из агентов, локализующихся на сетевых устройствах и передающих информацию сетевой управляющей платформе. Метод информационного обмена между управляющими приложениями и агентами на устройствах определяется протоколами.

Системы управления сетями должны обладать целым рядом качеств:

* истинной распределенностью в соответствии с концепцией клиент/сервер,
* масштабируемостью,
* открытостью, позволяющей справиться с разнородным - от настольных компьютеров до мейнфреймов - оборудованием.

Первые два свойства тесно связаны. Хорошая масштабируемость достигается за счет распределенности системы управления. Распределенность означает, что система может включать несколько серверов и клиентов. Серверы (менеджерами) собирают данные о текущем состоянии сети от агентов (SNMP, CMIP или RMON), встроенных в оборудование сети, и накапливают их в своей базе данных. Клиенты представляют собой графические консоли, за которыми работают администраторы сети. Программное обеспечение клиента системы управления принимает запросы на выполнение каких-либо действий от администратора (например, построение подробной карты части сети) и обращается за необходимой информацией к серверу. Если сервер обладает нужной информацией, то он сразу же передает ее клиенту, если нет - то пытается собрать ее от агентов.

Ранние версии систем управления совмещали все функции в одном компьютере, за которым работал администратор. Для небольших сетей или сетей с небольшим количеством управляемого оборудования такая структура оказывается вполне удовлетворительной, но при большом количестве управляемого оборудования единственный компьютер, к которому стекается информация от всех устройств сети, становится узким местом. И сеть не справляется с большим потоком данных, и сам компьютер не успевает их обрабатывать. Кроме того, большой сетью управляет обычно не один администратор, поэтому, кроме нескольких серверов в большой сети должно быть несколько консолей, за которыми работают администраторы сети, причем на каждой консоли должна быть представлена специфическая информация, соответствующая текущим потребностям конкретного администратора.

Поддержка разнородного оборудования - скорее желаемое, чем реально существующее свойство сегодняшних систем управления. К числу наиболее популярных продуктов сетевого управления относятся четыре системы: Spectrum компании CabletronSystems, OpenView фирмы Hewlett-Packard, NetView корпорации IBM и Solstice производства SunSoft - подразделения SunMicrosystems. Три компании из четырех сами выпускают коммуникационное оборудование. Естественно, что система Spectrum лучше всего управляет оборудованием компании Cabletron, OpenView - оборудованием компании Hewlett-Packard, а NetView- оборудованием компании IBM.

При построении карты сети, которая состоит из оборудования других производителей, эти системы начинают ошибаться и принимать одни устройства за другие, а при управлении этими устройствами поддерживают только их основные функции, а многие полезные дополнительные функции, которые отличают данное устройство от остальных, система управления просто не понимает и, поэтому, не может ими воспользоваться.

Для исправления этого недостатка разработчики систем управления включают поддержку не только стандартных баз MIB I, MIB II и RMON MIB, но и многочисленных частных MIB фирм-производителей. Лидер в этой области - система Spectrum, поддерживающая около 1000 баз MIB различных производителей.

Другим способом более качественной поддержки конкретной аппаратуры является использование на основе какой-либо платформы управления приложения той фирмы, которая выпускает это оборудование. Ведущие компании - производители коммуникационного оборудования - разработали и поставляют весьма сложные и многофункциональные системы управления для своего оборудования. К наиболее известным системам этого класса относятся Optivity компании BayNetworks, CiscoWorks компании CiscoSystems, Transcend компании 3Com. Система Optivity, например, позволяет производить мониторинг и управлять сетями, состоящими из маршрутизаторов, коммутаторов и концентраторов компании BayNetwork, полностью используя все их возможности и свойства. Оборудование других производителей поддерживается на уровне базовых функций управления. Система Optivity работает на платформах OpenView компании Hewlett-Packard и SunNetManager (предшественник Solstice) компании SunSoft. Однако, работа на основе какой-либо платформы управления с несколькими системами, такими как Optivity, слишком сложна и требует, чтобы компьютеры, на которых все это будет работать, обладали очень мощными процессорами и большой оперативной памятью.

Тем не менее, если в сети преобладает оборудование от какого-либо одного производителя, то наличие приложений управления этого производителя для какой-либо популярной платформы управления позволяет администраторам сети успешно решать многие задачи. Поэтому разработчики платформ управления поставляют вместе с ними инструментальные средства, упрощающие разработку приложений, а наличие таких приложений и их количество считаются очень важным фактором при выборе платформы управления.

Открытость платформы управления зависит также от формы хранения собранных данных о состоянии сети. Большинство платформ-лидеров позволяют хранить данные в коммерческих базах данных, таких как Oracle, Ingres или Informix. Использование универсальных СУБД снижает скорость работы системы управления по сравнению с хранением данных в файлах операционной системы, но зато позволяет обрабатывать эти данные любыми приложениями, умеющими работать с этими СУБД.

В таблице представлены наиболее важные характеристики наиболее популярных платформ управления

Таблица 2.1 - Характеристики популярных платформ диагностики

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Характеристики | OpenView Network Node Manager 4.1 (Hewlett- Packard) | | Spectrum Enterprise Manager (Cabletron Systems) | | NetView forAIX SNMPManager (IBM) | | Solstice Enterprise Manager (SunSoft) | |
| **Автообнаружение** | | | | | | | | |
| Ограничение по числу промежуточных маршрутизаторов | - | | - | | + | | + | |
| Определение имени хоста по его адресу через сервер DNS | + | | + | | + | | + | |
| Возможность модификации присвоенного имени хоста | + | | - | | + | | + | |
| Распознавание сетевых топологий | Любые сети, работающие по TCP/IP | | Ethernet, TokenRing, FDDI, ATM, распределенные сети, сети с коммутацией | | распознавание по интерфейсам устройств | | Ethernet, Token-Ring, FDDI, распределен- ные сети | |
| Максимальное рекомендуемое число обслуживаемых узлов | 200 - 2000, наибольшее известное - 35000 | | Программных ограничений не существует | | Программных ограничений не существует | | 10000 - 50000 | |
| Поддержка баз данных | Ingres, Oracle | | файлы | | Собств., Oracle, Sybase, ... | | Informix, Oracle, Sybase | |
| **Распределенное управление** | | | | | | | | |
| Один сервер / | много | | клиентов | |  | |  | |
| Число клиентов | до 15 | | Нет программного ограничения | | Протестиро- вано более 30 | | Нет программного ограничения | |
| Клиент использует X-Window | + | | - | | - | | + | |
| Система с GUI запускается на клиенте | + | | + | | + | | + | |
| Собственная карта сети у клиента | + | | + | | + | | - | |
| Задание доступных для просмотра объектов сети | С помощью дополнительного продукта Operations Center (HP) | | + | | + | | - | |
| Много серверов / | | много | | клиентов | |  | |  |
| текущее состояние | | +/- | | +/+ | | +/- | | +/+ |
| планируется | | +/+ | | +/+ | | +/+ | | +/+ |
| Число приложений третьих фирм | | 220 | | 180 | | > 200 | | 400 |
| Число поддерживаемых MIB третьих фирм | | 218 | | > 1000 | | 193 | | Нет данных |
| **Поддержка протокола SNMP**: | | | | | | | | |
| через IP | | + | | + | | + | | + |
| через IPX | | + | | - | | - | | - |
| Поддержка MIB, утвержденных IETF | | Большинство, но нет RMON | | Все | | 20 | | MIB-II |
| Поддержка протокола CMIP | | Дополнительно оплачиваемый продукт - Open View HP Distributed Management Platform | | Дополнительно оплачиваемый продукт | | + | | + |
| Взаимодействие с мейнфреймами | | При помощи приложений третьих фирм | | По SNA через Blue Vision | | Может обращаться к NetView на мейнфрейме | | + |
| Поддержка ОС | | HPUX, SunOS, Solaris | | IBM AIX, Sun OS, HP UX, SGI IRIX, Windows NT | | AIX, OSF/1, Windows NT | | SolarisSPARC |

# 3 Организация диагностики компьютерной сети

Основных причин неудовлетворительной работы сети может быть несколько: повреждения кабельной системы, дефекты активного оборудования, перегруженность сетевых ресурсов (канала связи и сервера), ошибки самого прикладного ПО. Часто одни дефекты сети маскируют другие. И чтобы достоверно определить, в чем причина неудовлетворительной работы, локальную сеть требуется подвергнуть комплексной диагностике. Комплексная диагностика предполагает выполнение следующих работ (этапов).

- Выявление дефектов физического уровня сети: кабельной системы, системы электропитания активного оборудования; наличия шума от внешних источников.

- Измерение текущей загруженности канала связи сети и определение влияния величины загрузки канала связи на время реакции прикладного ПО.

- Измерение числа коллизий в сети и выяснение причин их возникновения.

- Измерение числа ошибок передачи данных на уровне канала связи и выяснение причин их возникновения.

- Выявление дефектов архитектуры сети.

- Измерение текущей загруженности сервера и определение влияния степени его загрузки на время реакции прикладного ПО.

- Выявление дефектов прикладного ПО, следствием которых является неэффективное использование пропускной способности сервера и сети.

Мы остановимся подробнее на первых четырех этапах комплексной диагностики локальной сети, а именно на диагностике канального уровня сети, так как наиболее легко задача диагностики решается для кабельной системы. Как уже было рассмотрено во втором разделе, кабельная система сети полноценно может быть протестирована только специальными приборами - кабельным сканером или тестером. AUTOTEST на кабельном сканере позволит выполнить полный комплекс тестов на соответствие кабельной системы сети выбранному стандарту. При тестировании кабельной системы хотелось бы обратить внимание на два момента, тем более что о них часто забывают.

Режим AUTOTEST не позволяет проверить уровень шума создаваемого внешним источником в кабеле. Это может быть шум от люминесцентной лампы, силовой электропроводки, сотового телефона, мощного копировального аппарата и др. Для определения уровня шума кабельные сканеры имеют, как правило, специальную функцию. Поскольку кабельная система сети полностью проверяется только на этапе ее инсталляции, а шум в кабеле может возникать непредсказуемо, нет полной гарантии того, что шум проявится именно в период полномасштабной проверки сети на этапе ее инсталляции.

При проверке сети кабельным сканером вместо активного оборудования к кабелю подключаются с одного конца - сканер, с другого - инжектор. После проверки кабеля сканер и инжектор отключаются, и подключается активное оборудование: сетевые платы, концентраторы, коммутаторы. При этом нет полной гарантии того, что контакт между активным оборудованием и кабелем будет столь же хорош, как между оборудованием сканера и кабелем. Неоднократно встречаются случаи, когда незначительный дефект вилки RJ-45 не проявляется при тестировании кабельной системы сканером, но обнаруживался при диагностике сети анализатором протоколов.

Диагностика сетевых устройств (или компонента сети) также имеет свои тонкости. При ее проведении применяют различные подходы. Выбор конкретного подхода зависит от того, что выбирается в качестве критерия хорошей работы устройства. Как правило, можно выделить три типа критериев и, следовательно, три основных подхода.

Первый основан на контроле текущих значений параметров, характеризующих работу диагностируемого устройства. Критериями хорошей работы устройства в этом случае являются рекомендации его производителя, или так называемые промышленные стандарты де-факто. Основными достоинствами указанного подхода являются простота и удобство при решении наиболее распространенных, но, как правило, относительно несложных проблем. Однако бывают случаи, когда даже явный дефект большую часть времени не проявляется, а дает о себе знать лишь при некоторых, относительно редких режимах работы и в непредсказуемые моменты времени. Обнаружить такие дефекты, контролируя только текущие значения параметров, весьма затруднительно.

Второй подход основан на исследовании базовых линий параметров (так называемых трендов), характеризующих работу диагностируемого устройства. Основной принцип второго подхода можно сформулировать следующим образом: “устройство работает хорошо, если оно работает так, как всегда”. На этом принципе основана упреждающая (proactive) диагностика сети, цель которой — предотвратить наступление ее критических состояний. Противоположной упреждающей является реактивная (reactive) диагностика, цель которой не предотвратить, а локализовать и ликвидировать дефект. В отличие от первого, данный подход позволяет обнаруживать дефекты, проявляющиеся не постоянно, а время от времени. Недостатком второго подхода является предположение, что изначально сеть работала хорошо. Но “как всегда” и “хорошо” не всегда означают одно и то же.

Третий подход осуществляется посредством контроля интегральных показателей качества функционирования диагностируемого устройства (далее — интегральный подход). Следует подчеркнуть, что с точки зрения методологии диагностики сети между первыми двумя подходами, которые будем называть традиционными, и третьим, интегральным, есть принципиальное различие. При традиционных подходах мы наблюдаем за отдельными характеристиками работы сети и, чтобы увидеть ее “целиком”, должны синтезировать результаты отдельных наблюдений. Однако мы не можем быть уверены, что при этом синтезе не потеряем важную информацию. Интегральный подход, наоборот, дает нам общую картину, которая в ряде случаев бывает недостаточно детальной. Задача интерпретации результатов при интегральном подходе, по существу, обратная: наблюдая целое, выявить, где, в каких частностях заключается проблема.

Из сказанного следует, что наиболее эффективен подход, совмещающий функциональность всех трех описанных выше подходов. Он должен, с одной стороны, основываться на интегральных показателях качества работы сети, но, с другой — дополняться и конкретизироваться данными, которые получаются при традиционных подходах. Именно такая комбинация позволяет поставить точный диагноз проблемы в сети.

## 

## **3.1 Документирование сети**

Ведение документирования сети дает сетевому администратору целый ряд преимуществ. Документирование сети может выступить:

- Инструментом для устранения неисправностей – в том случае, если что-нибудь идет не так как надо, документация может служить руководством при поиске и устранении неисправности. Она сохранит время и деньги.

- Помощью в подготовке нового персонала – новый сотрудник будет скорее готов к работе, если доступна документация по тому участку работы, где ему предстоит работать, что снова сбережет время и деньги.

- Помощью для поставщиков и консультантов - услуги этих людей, как правило, весьма дороги, если им нужно знать какие-либо детали сетевой инфраструктуры, то наличие документации позволит им выполнить свою работу быстрее, что, опять же, приводит к экономии времени.

Каждая сеть имеет свои уникальные особенности, но обладает и многими общими элементами, которые должны быть включены в документацию:

**Топология сети** - обычно эта информация представляется в форме диаграмм, на которых показаны основные сетевые узлы, такие как маршрутизаторы, коммутаторы, файерволы, сервера и как они взаимосвязаны. Принтеры и рабочие станции обычно сюда не включаются.

**Информация о серверах** - то есть, та информация, которая необходима вам для управления и администрирования серверами, такая как имя, функции, IP адреса, конфигурация дисков, ОС и сервис-паки, дата и место покупки, гарантия и т.д...

**Назначение портов** коммутаторов и маршрутизаторов - сюда включается детальная информация о конфигурации WAN, VLAN-ов или даже назначение портов сетевым узлам через патч-панель.

**Конфигурация сетевых служб** — сетевые службы, такие как DNS, WINS, DHCP, и RAS, критичны для операций в сети, следует детально описать, как они структурированы. Данную информацию всегда можно получить с серверов, но документация ее заранее в легкочитаемом формате позволяет сэкономить время.

**Политики и профили доменов** – можно ограничить возможности пользователей с помощью Policy Editor в Windows NT или с помощью Group Policies в Windows 2000. При этом существует возможность создать профили пользователей, хранимые на сервере, а не на локальной машине. Если такие возможности используются, то такая информация должна быть документирована.

**Критически важные приложения** - необходимо включить в документацию как такие приложения поддерживаются, что бывает с ними чаще всего не так и как решать такие проблемы.

**Процедуры** — это само по себе может быть большим проектом. В основном процедуры — средство для реализации политик и могут быть достаточно обширными. В частности, политика может устанавливать, что «Сеть должна быть защищена от неавторизованных пользователей». Однако, для реализации такой политики, потребуется масса усилий. Существуют процедуры для файерволов, сетевых протоколов, паролей, физической безопасности и т.д. Можно также иметь отдельные процедуры для обработки проблем, о которых сообщают пользователи, и процедуры для регулярного обслуживания серверов.

Как показывает практика, большинство средний предприятий, особенно государственных учреждений используют ручной способ ведения документирования сети т.е для них вполне достаточно списков Excel и знаний ответственного за IT специалиста. Однако использование специальных систем документирования сети, позволит значительно снизить риски в случае отказа компонентов или физического повреждения инфраструктуры в результате строительных работ, пожара или наводнения, внезапного увольнения или исчезновения ответственного специалиста и уменьшить время при восстановлении инфраструктуры.

Система документирования инфраструктуры сети (CMS) - это интегрированная система, позволяющая хранить в едином месте и иметь удобный доступ к информации обо всех объектах сети (будь то отдельные компьютеры, соединительные кабели, системы теленаблюдения, пожарной сигнализации и т. п.) и соединениях между ними.

Основной задачей современных систем документирования сети на базе программного обеспечения является достижение гибкости и точности документации, а также управление сетями при низких затратах и минимальных трудностях. Система документирования сети хранит данные о всех пассивных (кабели, разъемы, панели переключений, распределительные шкафы) и активных (маршрутизаторы, коммутаторы, серверы, , ПК, УАТС) компонентах сети, включая информацию о соединениях и их состоянии (Connectivity) в центральной реляционной базе данных (к примеру, Oracle, SQL, DB2), и визуализирует всю систему как в алфавитно-цифровой, так и в графической форме. Кроме того, основываясь на планах зданий и земельных участков, можно отобразить расположение отдельных компонентов и маршруты прокладки кабеля Информация о компонентах и их изображения хранятся в библиотеке компонентов, которая постоянно обновляется. Многие современные системы уже предлагают клиенты Web, позволяющие получать доступ к документации по сети через Internet. Так, обслуживающие техники могут на месте напрямую запрашивать рабочие задания посредством мобильных устройств, а после выполнения квитировать их в производственной системе. Некоторые системы документирования сети даже обладают функцией обнаружения (Discovery) для автоматического выявления посредством SNMP новых активных компонентов и включения их в документацию.

При наличии системы документирования сети пользователь в любое время может получить актуальный и целостный обзор всех сетевых ресурсов инфраструктуры организации. Согласно подсчетам Международной организации управления службами IT (IT Service Management Forum, ITSMF), на протяжении всего жизненного цикла системы IT затраты на ее содержание сокращаются в результате на 80%. Система документирования сети позволяет осуществлять большее (чем при обработке вручную) количество действий, необходимых для функционирования инфраструктуры сети, и при этом значительно экономит время на их выполнение. Вдобавок предотвращаются ошибки при вводе данных или их дублирование. В систему можно вводить автоматизированные процессы для изменения инфраструктуры (Change Requests) и, наконец, автоматически создавать рабочие задания, к примеру, при ремонтных работах или переездах. Деятельность обслуживающего персонала на местах становится намного эффективнее, за счет чего существенно упрощаются процессы обслуживания и изменения компьютерной сети. Расчеты показали, что сокращение усилий, а соответственно, и финансовых затрат на планирование и документирование необходимых изменений в сети может достигать 90%.

Согласно статистике по Network Operating Centers (NOC), около 80% всех неполадок в сети вызваны неисправностью проводки. При использовании системы документирования сети предприятия могут быстро локализовать проблемную зону и, таким образом, оперативно устранить неполадки. Более того, посредством системы документирования сети можно планировать и организовывать избыточные маршруты передачи сигнала, с тем чтобы в случае неполадок просто подключить их.

В настоящее время системы документирования сети используют преимущественно крупные компании, а также поставщики энергии и муниципальные предприятия, обладающие протяженной и сложной инфраструктурой ИТК. Ведение документации вручную превратилось бы для них в непосильную ношу. Системы документирования применяют и телекоммуникационные предприятия, которые обязаны обеспечивать доступность инфраструктуры для своих клиентов и подтверждать это фактически. Все чаще делают ставку на системы документирования сети больницы и другие учреждения, в которых доступность и надежность структуры сети являются жизненной необходимостью. Для повседневной деятельности эксплуатационных организаций и владельцев зданий, предоставляющих сеть для нескольких предприятий на одной территории, системы документирования сети тоже имеют огромное значение.

В качестве примера рассмотри некоторые из подобных систем.

**Friendly Pinger** - это мощное и удобное приложение для администрирования, мониторинга и инвентаризации компьютерных сетей. Представляет следующие возможности:

* Визуализация компьютерной сети в красивой анимационной форме с отображением, какие компьютеры включены, а какие нет;
* Оповещение об остановке/запуске серверов;
* Просмотр, кто, к каким файлам обращается на компьютере по сети;
* Автоматический сбор информации о программном и аппаратном обеспечении компьютеров в сети.

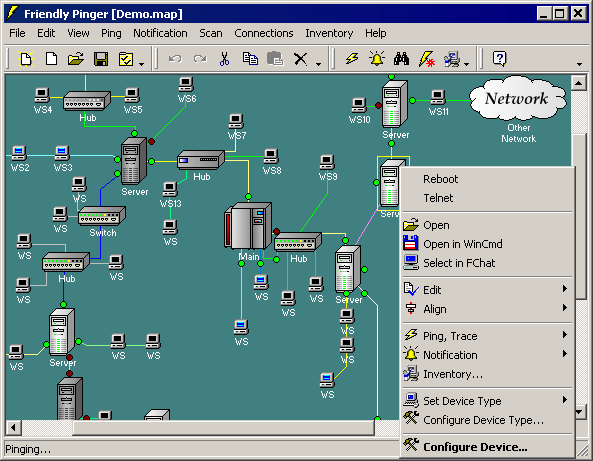


Рисунок 3.1- Карта сети

**10-Strike LANState** - программа для администраторов и простых пользователей сетей Microsoft Windows. С помощью LANState можно наблюдать текущее состояние сети в графическом виде, управлять серверами и рабочими станциями, вести мониторинг удаленных устройств с помощью периодического опроса компьютеров, отслеживать подключения к сетевым ресурсам, получать своевременные оповещения о различных событиях.

LANState содержит множество полезных функций для администраторов и пользователей сети, например, отправка сообщений, перезагрузка и завершение работы удаленных компьютеров, пинг, определение имени по ip адресу, трассировка маршрута, сканирование портов и хостов. Также имеется возможность получения различной информации об удаленных компьютерах (без инсталляции серверной части на них). Например, просмотр реестра по сети, просмотр удаленного event log'а, просмотр списка установленных программ. Поддерживаются Windows 95/98/Me/NT/2000/XP.

Для пользователей сети: программа позволяет наглядно видеть какие компьютеры в сети включены, а какие - нет. В любой момент программу можно вызвать из трея Windows и быстро обратиться к ресурсам нужного компьютера (замена окна сетевого окружения). Можно настроить сигнализацию на включение/выключение определенных компьютеров и серверов в сети, на доступность файлов и папок, на запуск web- и FTP-серверов, и на другие события. LANState осуществляет контроль подключений к общим ресурсам и отслеживает обращения к файлам из сети. Есть возможность выяснить, кто и к каким файлам на компьютере обращается по сети, в том числе и через административные ресурсы.

Для администраторов: управление компьютерами в сети, получение разнообразной информации об удаленных компьютерах (списки пользователей, запущенные службы и приложения, установленные программы, доступ к реестру и журналу событий), удаленное администрирование, перезагрузка, включение/выключение, и т.п. Сигнализация позволяет своевременно узнать о включении/выключении компьютеров и серверов в сети, разрыве VPN-подключений, изменении размеров или доступности файлов и папок.

Рассмотрим процесс создания схемы локальной сети с помощью этой программы. LANState поддерживает сканирование SNMP-устройств и может рисовать схему сети автоматически с созданием линий, соединяющих хосты. При этом номера портов коммутаторов проставляются в подписях к линиям. Для автоматического построения схемы сети:

1. SNMP должен быть включен на коммутаторах. Программа должна быть разрешена в брандмауэре для успешной работы по протоколу SNMP.

2. Запустить Мастер Создания Карты Сети.

3. Выбрать сканирование сети по диапазону IP-адресов. Указать диапазоны. Устройства с SNMP должны находиться внутри указанных диапазонов.

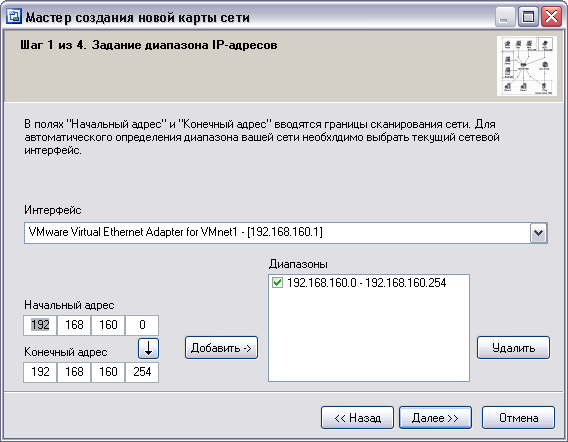


Рисунок 3.2 - Задание диапазона адресов

4. Выбрать методы сканирования и настроить их параметры. Поставить галочку рядом с опцией "Поиск устройств с SNMP..." и указать правильные community strings для подключения к коммутаторам.

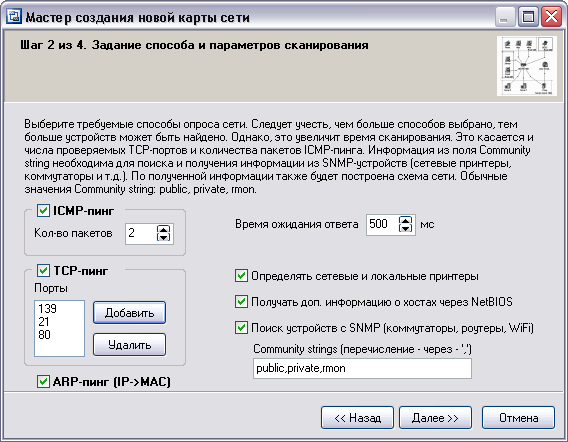


Рисунок 3.3 - Параметры и способы сканирования

5. После сканирования программа должна нарисовать схему сети. Если сканирование SNMP прошло успешно, соединения между сетевыми устройствами будут нарисованы автоматически.

Схема сети может быть выгружена в картинку, либо в схему Microsoft Visio

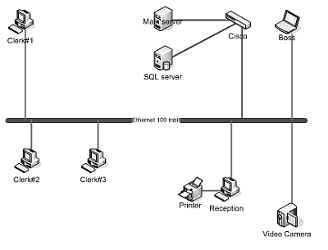


Рисунок 3.4 - Укрупненная схема сети

## **3.2 Методика упреждающей диагностики**

Методика упреждающей диагностики заключается в следующем. Администратор сети должен непрерывно или в течение длительного времени наблюдать за работой сети. Такие наблюдения желательно проводить с момента ее установки. На основании этих наблюдений администратор должен определить, во-первых, как значения наблюдаемых параметров влияют на работу пользователей сети и, во-вторых, как они изменяются в течение длительного промежутка времени: рабочего дня, недели, месяца, квартала, года и т. д.

Наблюдаемыми параметрами обычно являются:

- параметры работы канала связи сети - утилизация канала связи, число принятых и переданных каждой станцией сети кадров, число ошибок в сети, число широковещательных и многоадресных кадров и т. п.;

- параметры работы сервера - утилизация процессора сервера, число отложенных (ждущих) запросов к диску, общее число кэш-буферов, число "грязных" кэш-буферов и т. п.

Зная зависимость между временем реакции прикладного ПО и значениями наблюдаемых параметров, администратор сети должен определить максимальные значения параметров, допустимые для данной сети. Эти значения вводятся в виде порогов (thresholds) в диагностическое средство. Если в процессе эксплуатации сети значения наблюдаемых параметров превысят пороговые, то диагностическое средство проинформирует об этом событии администратора сети. Такая ситуация свидетельствует о наличии в сети проблемы.

Наблюдая достаточно долго за работой канала связи и сервера, можно установить тенденцию изменения значений различных параметров работы сети (утилизации ресурсов, числа ошибок и т. п.). На основании таких наблюдений администратор может сделать выводы о необходимости замены активного оборудования или изменения архитектуры сети.

В случае появления в сети проблемы, администратор в момент ее проявления должен записать в специальный буфер или файл дамп канальной трассы и на основании анализа ее содержимого сделать выводы о возможных причинах проблемы.

## 

## **3.2 Организация процесса диагностики**

Не подвергая сомнению, важность упреждающей диагностики, приходиться констатировать, что на практике она используется редко. Чаще всего (хоть это и неправильно) сеть анализируется только в периоды ее неудовлетворительной работы. И обычно в таких случаях локализовать и исправить имеющиеся дефекты сети требуется быстро. Предлагаемую нами методику можно даже рассмотреть, как частный случай методики упреждающей диагностики сети.

Любая методика тестирования сети существенно зависит от имеющихся в распоряжении системного администратора средств. По мнению некоторых администраторов, в большинстве случаев необходимым и достаточным cредством для обнаружения дефектов сети (кроме кабельного сканера) является анализатор сетевых протоколов. Он должен подключаться к тому домену сети (collision domain), где наблюдаются сбои, в максимальной близости к наиболее подозрительным станциям или серверу

Если сеть имеет архитектуру с компактной магистралью (collapsed backbone) и в качестве магистрали используется коммутатор, то анализатор необходимо подключать к тем портам коммутатора, через которые проходит анализируемый трафик. Некоторые программы имеют специальные агенты или зонды (probes), устанавливаемые на компьютерах, подключенных к удаленным портам коммутатора. Обычно агенты (не путать с агентами SNMP) представляют собой сервис или задачу, работающую в фоновом режиме на компьютере пользователя. Как правило, агенты потребляют мало вычислительных ресурсов и не мешают работе пользователей, на компьютерах которых они установлены. Анализаторы и агенты могут быть подключены к коммутатору двумя способами.

При первом способе (см. рисунок 3.5) анализатор подключается к специальному порту (порту мониторинга или зеркальному порту) коммутатора, если таковой имеется, и на него по очереди направляется трафик со всех интересующих портов коммутатора.

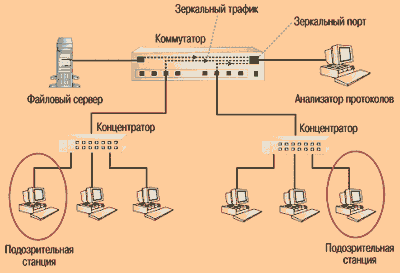


Рисунок 3.5 – Первый способ подключения анализатора

Если в коммутаторе специальный порт отсутствует, то анализатор (или агент) следует подключать к портам интересующих доменов сети в максимальной близости к наиболее подозрительным станциям или серверу (см. рисунок 3.6 ). Иногда это может потребовать использования дополнительного концентратора. Данный способ предпочтительнее первого. Исключение составляет случай, когда один из портов коммутатора работает в полнодуплексном режиме. Если это так, то порт предварительно необходимо перевести в полудуплексный режим.

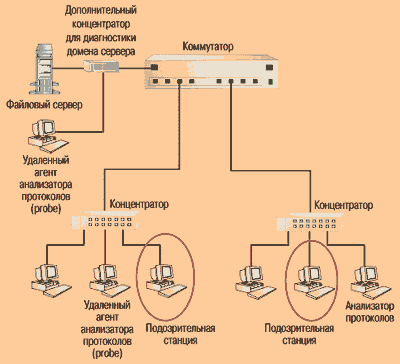


Рисунок 3.6 - Второй способ подключения анализатора

На рынке имеется множество разнообразных анализаторов протоколов - от чисто программных до программно-аппаратных. Несмотря на функциональную идентичность большинства анализаторов протоколов, каждый из них обладает теми или иными достоинствами и недостатками. В этой связи надо обратить внимание на две важные функции, без которых эффективную диагностику сети провести будет затруднительно.

Во-первых, анализатор протоколов должен иметь встроенную функцию генерации трафика Во-вторых, анализатор протоколов должен уметь "прореживать" принимаемые кадры, т. е. принимать не все кадры подряд, а, например, каждый пятый или каждый десятый с обязательной последующей аппроксимацией полученных результатов. Если эта функция отсутствует, то при сильной загруженности сети, какой бы производительностью ни обладал компьютер, на котором установлен анализатор, последний будет "зависать" и/или терять кадры. Это особенно важно при диагностике быстрых сетей типа Fast Ethernet и FDDI.

Предлагаемую методику мы будем иллюстрировать на примере использования чисто программного анализатора протоколов Observer компании Network Instruments - этомощный анализатор сетевых протоколов и средство для мониторинга и диагностики сетей Ethernet, беспроводных сетей стандарта 802.11 a/b/g, сетей Token Ring и FDDI. Observer позволяет в режиме реального времени измерять характеристики работы сети, осуществлять декодирование сетевых протоколов (поддерживается более 500 протоколов), создавать и анализировать тренды характеристик работы сети.

Рассмотрим поэтапно действия системного администратора для проведения диагностики сети в случае, когда прикладное программное обеспечение в сети Ethernet стало работать медленно, и необходимо оперативно локализовать и ликвидировать дефект.

**Первый этап****: Измерение утилизации сети и установление корреляции между замедлением работы сети и перегрузкой канала связи.**

Утилизация канала связи сети - это процент времени, в течение которого канал связи передает сигналы, или иначе - доля пропускной способности канала связи, занимаемой кадрами, коллизиями и помехами.

Параметр "Утилизация канала связи" характеризует величину загруженности сети. Канал связи сети является общим сетевым ресурсом, поэтому его загруженность влияет на время реакции прикладного программного обеспечения. Первоочередная задача состоит в определении наличия взаимозависимости между плохой работой прикладного программного обеспечения и утилизацией канала связи сети. Предположим, что анализатор протоколов установлен в том домене сети (collision domain), где прикладное ПО работает медленно. Средняя утилизация канала связи составляет 19%, пиковая доходит до 82%. Но сделать на основании этих данных достоверный вывод о том, что причиной медленной работы программ в сети является перегруженность канала связи нельзя.

Часто можно слышать о стандарте де-факто, в соответствии с которым для удовлетворительной работы сети Ethernet утилизация канала связи "в тренде" (усредненное значение за 15 минут) не должна превышать 20%, а "в пике" (усредненное значение за 1 минуту) - 35-40%. Приведенные значения объясняются тем, что в сети Ethernet при утилизации канала связи, превышающей 40%, существенно возрастает число коллизий и, соответственно, время реакции прикладного ПО. Несмотря на то, что такие рассуждения в общем случае верны, безусловное следование подобным рекомендациям может привести к неправильному выводу о причинах медленной работы программ в сети. Они не учитывают особенности конкретной сети, а именно: тип прикладного ПО, протяженность домена сети, число одновременно работающих станций.

Чтобы определить, какова же максимально допустимая утилизация канала связи в каждом конкретном случае, рекомендуется следовать приведенным ниже правилам.

***Правило 1.1*** Если в сети Ethernet в любой момент времени обмен данными происходит не более чем между двумя компьютерами, то любая сколь угодно высокая утилизация сети является допустимой.

Сеть Ethernet устроена таким образом, что если два компьютера одновременно конкурируют друг с другом за захват канала связи, то через некоторое время они синхронизируются друг с другом и начинают выходить в канал связи строго по очереди. В таком случае коллизий между ними практически не возникает.

Если рабочая станция и сервер обладают высокой производительностью, и между ними идет обмен большими порциями данных, то утилизация в канале связи может достигать 80-90% (особенно в пакетном режиме - burst mode). Это абсолютно не замедляет работу сети, а, наоборот, свидетельствует об эффективном использовании ее ресурсов прикладным ПО.

Таким образом, если в сети утилизация канала связи высока, надо постараться определить, сколько компьютеров одновременно ведут обмен данными. Это можно сделать, например, собрав и декодировав пакеты в интересующем канале в период его высокой утилизации.

***Правило 1.2*** Высокая утилизация канала связи сети только в том случае замедляет работу конкретного прикладного ПО, когда именно канал связи является "узким местом" для работы данного конкретного ПО.

Кроме канала связи узкие места в системе могут возникнуть из-за недостаточной производительности или неправильных параметров настройки сервера, низкой производительности рабочих станций, неэффективных алгоритмов работы самого прикладного ПО.

В какой мере канал связи ответственен за недостаточную производительность системы, можно выяснить следующим образом. Выбрав наиболее массовую операцию данного прикладного ПО (например, для банковского ПО такой операцией может быть ввод платежного поручения), следует определить, как утилизация канала связи влияет на время выполнения такой операции. Проще всего это сделать, воспользовавшись функцией генерации трафика, имеющейся в ряде анализаторов протоколов (например, в Observer). С помощью этой функции интенсивность генерируемой нагрузки следует наращивать постепенно, и на ее фоне производить измерения времени выполнения операции. Фоновую нагрузку целесообразно увеличивать от 0 до 50-60% с шагом не более 10%.

Если время выполнения операции в широком интервале фоновых нагрузок не будет существенно изменяться, то узким местом системы является не канал связи. Если же время выполнения операции будет существенно меняться в зависимости от величины фоновой нагрузки (например, при 10% и 20% утилизации канала связи время выполнения операции будет значительно различаться), то именно канал связи, скорее всего, ответственен за низкую производительность системы, и величина его загруженности критична для времени реакции прикладного ПО. Зная желаемое время реакции ПО, легко можно определить, какой утилизации канала связи соответствует желаемое время реакции прикладного ПО.

В данном эксперименте фоновую нагрузку не следует задавать более 60-70%. Даже если канал связи не является узким местом, при таких нагрузках время выполнения операций может возрасти вследствие уменьшения эффективной пропускной способности сети.

***Правило 1.3*** Максимально допустимая утилизация канала связи зависит от протяженности сети.

При увеличении протяженности домена сети допустимая утилизация уменьшается. Чем больше протяженность домена сети, тем позже будут обнаруживаться коллизии. Если протяженность домена сети мала, то коллизии будут выявлены станциями еще в начале кадра, в момент передачи преамбулы. Если протяженность сети велика, то коллизии будут обнаружены позже - в момент передачи самого кадра. В результате накладные расходы на передачу пакета (IP или IPX) возрастают. Чем позже выявлена коллизия, тем больше величина накладных расходов и большее время тратится на передачу пакета. В результате время реакции прикладного ПО, хотя и незначительно, но увеличивается.

*Выводы.* Если в результате проведения диагностики сети вы определили, что причина медленной работы прикладного ПО - в перегруженности канала связи, то архитектуру сети необходимо изменить. Число станций в перегруженных доменах сети следует уменьшить, а станции, создающие наибольшую нагрузку на сеть, подключить к выделенным портам коммутатора.

**Второй этап:** **Измерение числа коллизий в сети.**

Если две станции домена сети одновременно ведут передачу данных, то в домене возникает коллизия. Коллизии бывают трех типов: местные, удаленные, поздние. Местная коллизия (local collision) - это коллизия, фиксируемая в домене, где подключено измерительное устройство, в пределах передачи преамбулы или первых 64 байт кадра, когда источник передачи находится в домене. Алгоритмы обнаружения местной коллизии для сети на основе витой пары (10BaseT) и коаксиального кабеля (10Base2) отличны друг от друга.

В сети 10Base2 передающая кадр станция определяет, что произошла локальная коллизия по изменению уровня напряжения в канале связи (по его удвоению). Обнаружив коллизию, передающая станция посылает в канал связи серию сигналов о заторе (jam), чтобы все остальные станции домена узнали, что произошла коллизия. Результатом этой серии сигналов оказывается появление в сети коротких, неправильно оформленных кадров длиной менее 64 байт с неверной контрольной последовательностью CRC. Такие кадры называются фрагментами (collision fragment или runt). В сети 10BaseT станция определяет, что произошла локальная коллизия, если во время передачи кадра она обнаруживает активность на приемной паре (Rx).

Удаленная коллизия (remote collision) - это коллизия, которая возникает в другом физическом сегменте сети (т. е. за повторителем). 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 10Base2). Для сетей 10BaseT/100BaseT показателем является отсутствие одновременной активности на приемной и передающей парах (Tx и Rx).

Поздняя коллизия (late collision) - это местная коллизия, которая фиксируется уже после того, как станция передала в канал связи первые 64 байт кадра. В сетях 10BaseT поздние коллизии часто фиксируются измерительными устройствами как ошибки CRC. Если выявление локальных и удаленных коллизий, как правило, еще не свидетельствует о наличии в сети дефектов, то обнаружение поздних коллизий - это явное подтверждение наличия дефекта в домене. Чаще всего это связано с чрезмерной длиной линий связи или некачественным сетевым оборудованием.

Помимо высокого уровня утилизации канала связи коллизии в сети Ethernet могут быть вызваны дефектами кабельной системы и активного оборудования, а также наличием шумов. Даже если канал связи не является узким местом системы, коллизии несущественно, но замедляют работу прикладного ПО. Причем основное замедление вызывается не столько самим фактом необходимости повторной передачи кадра, сколько тем, что каждый компьютер сети после возникновения коллизии должен выполнять алгоритм отката (backoff algorithm): до следующей попытки выхода в канал связи ему придется ждать случайный промежуток времени, пропорциональный числу предыдущих неудачных попыток. В этой связи важно выяснить, какова причина коллизий - высокая утилизация сети или "скрытые" дефекты сети. Чтобы это определить, мы рекомендуем придерживаться следующих правил:.

***Правило 2.1*** Не все измерительные приборы правильно определяют общее число коллизий в сети. Практически все чисто программные анализаторы протоколов фиксируют наличие коллизии только в том случае, если они обнаруживают в сети фрагмент, т. е. результат коллизии. При этом наиболее распространенный тип коллизий - происходящие в момент передачи преамбулы кадра (т. е. до начального ограничителя кадра (SFD)) - программные измерительные средства не обнаруживают, так уж устроен набор микросхем сетевых плат Ethernet. Наиболее точно коллизии обнаруживают аппаратные измерительные приборы, например LANMeter компании Fluke.

***Правило 2.2*** Высокая утилизация канала связи не всегда сопровождается высоким уровнем коллизий.

Уровень коллизий будет низким, если в сети одновременно работает не более двух станций (см. этап 1) или если небольшое число станций одновременно ведут обмен длинными кадрами (что особенно характерно для пакетного режима). В этом случае до начала передачи кадра станции "видят" несущую в канале связи, и коллизии редки.

***Правило 2.3*** Признаком наличия дефекта в сети служит такая ситуация, когда невысокая утилизация канала (менее 30%) сопровождается высоким уровнем коллизий (более 5%).

Если кабельная система предварительно была протестирована сканером, то наиболее вероятной причиной повышенного уровня коллизий является шум в линии связи, вызванный внешним источником, или дефектная сетевая плата, неправильно реализующая алгоритм доступа к среде передачи (CSMA/CD).

Компания Network Instruments в анализаторе протоколов Observer оригинально решила задачу выявления коллизий, вызванных дефектами сети. Встроенный в программу тест провоцирует возникновение коллизий: он посылает в канал связи серию пакетов с интенсивностью 100 пакетов в секунду и анализирует число возникших коллизий. При этом совмещенный график отображает зависимость числа коллизий в сети от утилизации канала связи.

Долю коллизий в общем числе кадров имеет смысл анализировать в момент активности подозрительных (медленно работающих) станций и только в случае, когда утилизация канала связи превышает 30%. Если из трех кадров один столкнулся с коллизией, то это еще не означает, что в сети есть дефект.

В анализаторе протоколов Observer график, меняет цвет в зависимости от числа коллизий и наблюдаемой при этом утилизации канала связи.

***Правило 2.4*** При диагностике сети 10BaseT все коллизии должны фиксироваться как удаленные, если анализатор протоколов не создает трафика.

Если администратор пассивно (без генерации трафика) наблюдает за сетью 10BaseT и физический сегмент в месте подключения анализатора (измерительного прибора) исправен, то все коллизии должны фиксироваться как удаленные.

Если тем не менее видны именно локальные коллизии, то это может означать одно из трех: физический сегмент сети, куда подключен измерительный прибор, неисправен; порт концентратора или коммутатора, куда подключен измерительный прибор, имеет дефект, или измерительный прибор не умеет различать локальные и удаленные коллизии.

***Правило 2.5*** Коллизии в сети могут быть следствием перегруженности входных буферов коммутатора.

Следует помнить, что коммутаторы при перегруженности входных буферов эмулируют коллизии, дабы "притормозить" рабочие станции сети. Этот механизм называется "управление потоком" (flow control).

***Правило 2.6*** Причиной большого числа коллизий (и ошибок) в сети может быть неправильная организация заземления компьютеров, включенных в локальную сеть.

Если компьютеры, включенные в сеть не имеют общей точки заземления (зануления), то между корпусами компьютеров может возникать разность потенциалов. В персональных компьютерах "защитная" земля объединена с "информационной" землей. Поскольку компьютеры объединены каналом связи локальной сети, разность потенциалов между ними приводит к возникновению тока по каналу связи. Этот ток вызывает искажение информации и является причиной коллизий и ошибок в сети. Такой эффект получил название ground loop или inter ground noise.

Аналогичный эффект возникает в случае, когда сегмент коаксиального кабеля заземлен более чем в одной точке. Это часто случается, если Т-соединитель сетевой платы соприкасается с корпусом компьютера.

Обращаем ваше внимание на то, что установка источника бесперебойного питания не снимает описанных трудностей. Наиболее подробно данные проблемы и способы их решения рассматриваются в материалах компании APC (American Power Conversion) в "Руководстве по защите электропитания" (Power Protection Handbook).

При обнаружении большого числа коллизий и ошибок в сетях 10Base2 первое, что надо сделать, - проверить разность потенциалов между оплеткой коаксиального кабеля и корпусами компьютеров. Если ее величина для любого компьютера в сети составляет более одного вольта по переменному току, то в сети не все в порядке с топологией линий заземления компьютеров.

**Третий этап**: **Измерение числа ошибок на канальном уровне сети.**

В сетях Ethernet наиболее распространенными являются следующие типы ошибок.

Короткий кадр - кадр длиной менее 64 байт (после 8-байтной преамбулы) с правильной контрольной последовательностью. Наиболее вероятная причина появления коротких кадров - неисправная сетевая плата или неправильно сконфигурированный или испорченный сетевой драйвер.

Длинный кадр (long frame) - кадр длиннее 1518 байт. Длинный кадр может иметь правильную или неправильную контрольную последовательность. В последнем случае такие кадры обычно называют jabber. Фиксация длинных кадров с правильной контрольной последовательностью указывает чаще всего на некорректность работы сетевого драйвера; фиксация ошибок типа jabber - на неисправность активного оборудования или наличие внешних помех.

Ошибки контрольной последовательности (CRC error) - правильно оформленный кадр допустимой длины (от 64 до 1518 байт), но с неверной контрольной последовательностью (ошибка в поле CRC).

Ошибка выравнивания (alignment error) - кадр, содержащий число бит, не кратное числу байт.

Блики (ghosts) - последовательность сигналов, отличных по формату от кадров Ethernet, не содержащая разделителя (SFD) и длиной более 72 байт. Впервые данный термин был введен компанией Fluke с целью дифференциации различий между удаленными коллизиями и шумами в канале связи.

Блики являются наиболее коварной ошибкой, так как они не распознаются программными анализаторами протоколов по той же причине, что и коллизии на этапе передачи преамбулы. Выявить блики можно специальными приборами или с помощью метода стрессового тестирования сети (мы планируем рассказать об этом методе в последующих публикациях).

Некоторые сетевые администраторы считают, что степень влияния ошибок канального уровня сети на время реакции прикладного ПО сильно преувеличена.

В соответствии с общепринятым стандартом де-факто число ошибок канального уровня не должно превышать 1% от общего числа переданных по сети кадров. Как показывает опыт, эта величина перекрывается только при наличии явных дефектов кабельной системы сети. При этом многие серьезные дефекты активного оборудования, вызывающие многочисленные сбои в работе сети, не проявляются на канальном уровне сети. При выявлении ошибок на этом этапе рекомендуем придерживаться следующих правил:

***Правило 3.1*** Прежде чем анализировать ошибки в сети, выясните, какие типы ошибок могут быть определены сетевой платой и драйвером платы на компьютере, где работает ваш программный анализатор протоколов.

Работа любого анализатора протоколов основана на том, что сетевая плата и драйвер переводятся в режим приема всех кадров сети (promiscuous mode). В этом режиме сетевая плата принимает все проходящие по сети кадры, а не только широковещательные и адресованные непосредственно к ней, как в обычном режиме. Анализатор протоколов всю информацию о событиях в сети получает именно от драйвера сетевой платы, работающей в режиме приема всех кадров.

Не все сетевые платы и сетевые драйверы предоставляют анализатору протоколов идентичную и полную информацию об ошибках в сети. Сетевые платы 3Com вообще никакой информации об ошибках не выдают. Если вы установите анализатор протоколов на такую плату, то значения на всех счетчиках ошибок будут нулевыми.

EtherExpress Pro компании Intel сообщают только об ошибках CRC и выравнивания. Сетевые платы компании SMC предоставляют информацию только о коротких кадрах. NE2000 выдают почти полную информацию, выявляя ошибки CRC, короткие кадры, ошибки выравнивания, коллизии.

Сетевые карты D-Link (например, DFE-500TX) и Kingstone (например, KNE 100TX) сообщают полную, а при наличии специального драйвера - даже расширенную, информацию об ошибках и коллизиях в сети.

Ряд разработчиков анализаторов протоколов предлагают свои драйверы для наиболее популярных сетевых плат.

***Правило 3.2*** Необходимо обратить внимание на "привязку" ошибок к конкретным MAC-адресам станций.

При анализе локальной сети, можно обратить внимание, что ошибки обычно "привязаны" к определенным МАС-адресам станций . Однако коллизии, произошедшие в адресной части кадра, блики, нераспознанные ситуации типа короткого кадра с нулевой длиной данных не могут быть "привязаны" к конкретным МАС-адресам.

Если в сети наблюдается много ошибок, которые не связаны с конкретными МАС-адресами, то их источником скорее всего является не активное оборудование. Вероятнее всего, такие ошибки - результат коллизий, дефектов кабельной системы сети или сильных внешних шумов. Они могут быть также вызваны низким качеством или перебоями питающего активное оборудование напряжения.

Если большинство ошибок привязаны к конкретным MAC-адресам станций, то надо постараться выявить закономерность между местонахождением станций, передающих ошибочные кадры, расположением измерительного прибора и топологией сети.

***Правило 3.3*** В пределах одного домена сети (collision domain) тип и число ошибок, фиксируемых анализатором протоколов, зависят от места подключения измерительного прибора.

Другими словами, в пределах сегмента коаксиального кабеля, концентратора или стека концентраторов картина статистики по каналу может зависеть от места подключения измерительного прибора. Многим администраторам сетей данное утверждение может показаться абсурдным, так как оно противоречит принципам семиуровневой модели OSI. Впервые столкнувшись с этим явлением, на практике, можно не поверить результату и решить, что измерительный прибор неисправен. Однако проверка данного феномена с разными измерительными приборами, от чисто программных до программно-аппаратных дает тот же результат.

Одна и та же помеха может вызвать фиксацию ошибки CRC, блика, удаленной коллизии или вообще не обнаруживаться в зависимости от взаимного расположения источника помех и измерительного прибора. Одна и та же коллизия может фиксироваться как удаленная или поздняя в зависимости от взаимного расположения конфликтующих станций и измерительного прибора. Кадр, содержащий ошибку CRC на одном концентраторе стека, может быть не зафиксирован на другом концентраторе того же самого стека.

Следствием приведенного эвристического правила является тот факт, что программы сетевого мониторинга на основе протокола SNMP не всегда адекватно отражают статистику ошибок в сети. Причина этого в том, что встроенный в активное оборудование агент SNMP всегда следит за состоянием сети только из одной точки. Так, если сеть представляет собой несколько стеков "неинтеллектуальных" концентраторов, подключенных к "интеллектуальному" коммутатору, то SNMP-агент коммутатора может иногда не видеть части ошибок в стеке концентраторов.

Подтверждение приведенного правила можно найти на серверах Web компаний Fluke (www.fluke.com) и Net3 Group (www.net3group.com).

***Правило 3.4*** Для выявления ошибок на канальном уровне сети измерения необходимо проводить на фоне генерации анализатором протоколов собственного трафика.

Генерация трафика позволяет обострить имеющиеся проблемы и создает условия для их проявления. Трафик должен иметь невысокую интенсивность (не более 100 кадров/с) и способствовать образованию коллизий в сети, т. е. содержать короткие (<100 байт) кадры.

При выборе анализатора протоколов или другого диагностического средства внимание следует обратить прежде всего на то, чтобы выбранный инструмент имел встроенную функцию генерации трафика задаваемой интенсивности. Эта функция имеется, в частности, в анализаторах Observer компании Network Instruments и NetXray компании Cinco (ныне Network Associates).

***Правило 3.5*** Если наблюдаемая статистика зависит от места подключения измерительного прибора, то источник ошибок, скорее всего, находится на физическом уровне данного домена сети (причина - дефекты кабельной системы или шум внешнего источника). В противном случае источник ошибок расположен на канальном уровне (или выше) или в другом, смежном, домене сети.

***Правило 3.6*** Если доля ошибок CRC в общем числе ошибок велика, то следует определить длину кадров, содержащих данный тип ошибок.

Как уже отмечали ранее, ошибки CRC могут возникать в результате коллизий, дефектов кабельной системы, внешнего источника шума, неисправных трансиверов. Еще одной возможной причиной появления ошибок CRC могут быть дефектные порты концентратора или коммутатора, которые добавляют в конец кадра несколько "пустых" байтов.

При большой доле ошибок CRC в общем числе ошибок целесообразно выяснить причину их появления. Для этого ошибочные кадры из серии надо сравнить с аналогичными хорошими кадрами из той же серии. Если ошибочные кадры будут существенно короче хороших, то это, скорее всего, результаты коллизий. Если ошибочные кадры будут практически такой же длины, то причиной искажения, вероятнее всего, является внешняя помеха. Если же испорченные кадры длиннее хороших, то причина кроется, вероятнее всего, в дефектном порту концентратора или коммутатора, которые добавляют в конец кадра "пустые" байты.

Сравнить длину ошибочных и правильных кадров проще всего посредством сбора в буфер анализатора серии кадров с ошибкой CRC.

Таблица 3.1 - Типы ошибок и коллизий, фиксируемые измерительным средством для этапов 2 и 3

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Причина ошибок | Локальные коллизии | Удаленные коллизии | Поздние коллизии | Короткий кадр | Длинный кадр | Jabber | Oшибка CRC |
| Дефектная сетевая плата | >5% при U<30% | >5% при U<30% | Есть | Есть | Есть | Есть | Есть |
| Дефектный драйвер платы |  |  |  | Есть | Есть | Есть | Есть |
| Дефектный концентратор, повторитель, трансивер | >5% при U<30% | >5% при U<30% | Есть |  |  | Есть | Есть |
| Неправильное подключение активного оборудования | >5% при U<30% | >5% при U<30% | Есть |  |  | Есть |  |
| Слишком длинный кабель |  |  | Есть |  |  |  | Есть |
| Более 4 повторителей или объединенных в каскад концентраторов |  |  | Есть |  |  |  |  |
| Неправильное заземление компьютеров или коаксиального кабеля | >5% при U<30% | >5% при U<30% | Есть |  |  | Есть | Есть |
| Дефекты кабельной системы и пассивного оборудования | >5% при U<30% | >5% при U<30% | Есть |  |  | Есть | Есть |
| Источник шума рядом с кабельной системой | >5% при U<30% | >5% при U<30% | Есть |  |  | Есть | Есть |
| Примечание. U - утилизация канала связи | | | | | | | |

Если администратор впервые диагностирует свою сеть и в ней наблюдаются проблемы, то не следует ожидать, что в сети дефектен только один компонент.

Наиболее надежным способом локализации дефектов является поочередное отключение подозрительных станций, концентраторов и кабельных трасс, тщательная проверка топологии линий заземления компьютеров (особенно для сетей 10Base2).

Если сбои в сети происходят в непредсказуемые моменты времени, не связанные с активностью пользователей, проверьте уровень шума в кабеле с помощью кабельного сканера. При отсутствии сканера визуально убедиться, что кабель не проходит вблизи сильных источников электромагнитного излучения: высоковольтных или сильноточных кабелей, люминесцентных ламп, электродвигателей, копировальной техники и т. п.

Таким образом, отсутствие ошибок на канальном уровне еще не гарантирует того, что информация в сети не искажается.

В начале данного раздела уже упоминалось, что влияние ошибок канального уровня на работу сети сильно преувеличено. Следствием ошибок нижнего уровня является повторная передача кадров. Благодаря высокой скорости сети Ethernet (особенно Fast Ethernet) и высокой производительности современных компьютеров, ошибки нижнего уровня не оказывает существенного влияния на время реакции прикладного ПО.

Как показывает опыт компаний представляющих услуги по диагностике сетей, очень редко встречаются случаи, когда ликвидация только ошибок нижних (канального и физического) уровней сети позволяет существенно улучшить время реакции прикладного ПО. В основном проблемы были связаны с серьезными дефектами кабельной системы сети.

Значительно большее влияние на работу прикладного ПО в сети оказывают такие ошибки, как бесследное исчезновение или искажение информации в сетевых платах, маршрутизаторах или коммутаторах при полном отсутствии информации об ошибках нижних уровней. Слово "информация", употребляется потому, так как в момент искажения данные еще не оформлены в виде кадра.

Причина таких дефектов в следующем. Информация искажается (или исчезает) "в недрах" активного оборудования - сетевой платы, маршрутизатора или коммутатора. При этом приемо-передающий блок этого оборудования вычисляет правильную контрольную последовательность (CRC) уже искаженной ранее информации, и корректно оформленный кадр передается по сети. Никаких ошибок в этом случае, естественно, не фиксируется. SNMP-агенты, встроенные в активное оборудование, здесь ничем помочь не могут.

Иногда кроме искажения наблюдается исчезновение информации. Чаще всего оно происходит на дешевых сетевых платах или на коммутаторах Ethernet-FDDI. Механизм исчезновения информации в последнем случае понятен. В ряде коммутаторов Ethernet-FDDI обратная связь быстрого порта с медленным (или наоборот) отсутствует, в результате другой порт не получает информации о перегруженности входных/выходных буферов быстрого (медленного) порта. В этом случае при интенсивном трафике информация на одном из портов может пропасть.

Опытный администратор сети может возразить, что кроме защиты информации на канальном уровне в протоколах IPX и TCP/IP возможна защита информации с помощью контрольной суммы.

В полной мере на защиту с помощью контрольной суммы можно полагаться, только если прикладное ПО в качестве транспортного протокола задействует TCP или UDP. Только при их использовании контрольной суммой защищается весь пакет. Если в качестве "транспорта" применяется IPX/SPX или непосредственно IP, то контрольной суммой защищается лишь заголовок пакета.

Даже при наличии защиты с помощью контрольной суммы описанное искажение или исчезновение информации вызывает существенное увеличение времени реакции прикладного ПО.

Если же защита не установлена, то поведение прикладного ПО может быть непредсказуемым.

Помимо замены (отключения) подозрительного оборудования выявить такие дефекты можно двумя способами.

Первый способ заключается в захвате, декодировании и анализе кадров от подозрительной станции, маршрутизатора или коммутатора. Признаком описанного дефекта служит повторная передача пакета IP или IPX, которой не предшествует ошибка нижнего уровня сети. Некоторые анализаторы протоколов и экспертные системы упрощают задачу, выполняя анализ трассы или самостоятельно вычисляя контрольную сумму пакетов.

Вторым способом является метод стрессового тестирования сети.

***Выводы.*** Основная задача диагностики канального уровня сети - выявить наличие повышенного числа коллизий и ошибок в сети и найти взаимосвязь между числом ошибок, степенью загруженности канала связи, топологией сети и местом подключения измерительного прибора. Все измерения следует проводить на фоне генерации анализатором протоколов собственного трафика.

Если установлено, что повышенное число ошибок и коллизий не является следствием перегруженности канала связи, то сетевое оборудование, при работе которого наблюдается повышенное число ошибок, следует заменить.

Если не удается выявить взаимосвязи между работой конкретного оборудования и появлением ошибок, то проведите комплексное тестирование кабельной системы, проверьте уровень шума в кабеле, топологию линий заземления компьютеров, качество питающего напряжения.

# 4 Экономическая часть

Главным для обеспечения максимальной экономической эффективности является выполнение мониторинга и управления с минимальными затратами труда и денежных средств. Она определяется на основе сравнения с базовым вариантом. В данном случае за базовый вариант принимаем ручной мониторинг, сбор статистики и управление виртуальной сетью.

Источником экономии при этом является:

-сокращение времени выполнения рутинных операций, которое может быть использовано для творческой, аналитической работы;

## **4.1 Расчет капитальных затрат на создание технико-программного обеспечения**

Капиталовложения в создание технико-программного обеспечения (ТПО) носят единовременный характер и включают в себя:

- затраты на лицензированные программные продукты;

- затраты на создание программного изделия;

- затраты на оборудование. Капиталовложения находят по формуле 4.1:

, (4.1)



где: К1 - затраты на оборудование, грн.;

К2 - затраты на лицензионные программные продукты, грн. (0 грн., т.к. всё необходимое программное обеспечение уже было установлено);

К3 - затраты на создание ТПО, грн

## **4.1.1 Расчёт затрат на оборудование**

Затраты на оборудование рассчитываются по формуле 4.2:

, грн (4.2)



где Ni - количество единиц i - того оборудования, необходимого для реализации ТПО (ЭВМ и др.), шт.;

Сi - цена единиц i - того оборудования в грн.;

n - общее количество различных видов оборудования;

*k*1 - коэффициент транспортно - заготовительных расходов (1.01);

*k*2 - коэффициент увеличения затрат на производственно - хозяйственный инвентарь (1,015).

Для разработки программного изделия необходима такая техника:

- компьютер (3200 грн.);

- производственно - хозяйственный инвентарь (100 грн.). Данные по затратам на оборудование сведены в таблицу 4.1.

Таблица 4.1- Затраты на оборудование

|  |  |
| --- | --- |
| Наименование | Стоимость  Грн |
| - компьютер  - производственно – хозяйственный инвентарь (дискеты, CD, картриджы и т.д.) | 3200  80 |

Тогда по формуле 4.2:

грн.



## 

## **4.1.2 Расчёт затрат на создание ТПО**

Затраты на создание ТПО находят по формуле:

, (4.3)



где: *З*1 - затраты труда программистов-разработчиков, грн.;

*З*2 - затраты компьютерного времени, грн.;

*З*3 - косвенные (накладные) расходы, грн.

Затраты труда программистов находят по формуле 4.4:

, грн (4.4)



где: *Nk -* количество разработчиков k-й профессии, чел. Принимаем *Nk =* 1 человек.

*rk -* часовая зарплата разработчика k-й профессии, грн.;

*Кзар -* коэффициент начислений на фонд заработной платы, доли. Принимаем *К* = 1.475.

*Тk -* трудоёмкость разработки.

Часовая зарплата разработчика определяется по формуле 4.5:

(4.5)



где: *M*k *-* месячная зарплата к-го разработчика, грн.;

*-* месячный фонд времени его работы, час.



Принимаем *M*k = 600грн;  *=* 160 часов*.*



Тогда по формуле 4.5 рассчитаем *rk:*

грн/час.



Трудоёмкость разработки включает время выполнения работ, представленных в таблице 4.2. Общая трудоемкость *Тk* = 720 часов.

Тогда по формуле 4.4 найдем *31:*

грн.



Затраты компьютерного времени вычисляются по формуле 4.6:

, (4.6)



где: *Сk -* стоимость компьютерного часа, грн.;

*F0 -* затраты компьютерного времени на разработку программы, час (74 дня 8 часов = 592 часа).

Стоимость компьютерного часа исчисляется по формуле 4.7:

, (4.7)



где: *СА* - амортизационные отчисления, грн.;

*СЭ -* энергозатраты, грн.;

*СТО -* затраты на техобслуживание, грн.

Амортизационные отчисления определяются по формуле 4.8:

, (4.8)



где: *Сi -* балансовая стоимость i-го оборудования, которое использовалось для создания ТПО, грн.

*NАi -* годовая норма амортизации i-го оборудования. Принимаем *NАi* = 0,15.

*FГодi* - фонд времени работы i -го оборудования, час. Принимаем *FГодi =*1920 часов для ЭВМ и *FГодi =* 400 часов для принтера и сканера.

Таблица 4.2 - Этапы выполнения разработок

|  |  |  |
| --- | --- | --- |
| Этапы работ | | Содержание работ |
| 1 Техническое задание | | Краткая характеристика программы; основание и назначение разработки; требования к программе и программной документации; стадии и этапы разработки программы; порядок контроля и приёмки выполнения. |
| 2 Эскизный проект | | Предварительная разработка структуры входных и выходных данных; уточнение метода решения задачи;  разработка и описание общего алгоритма решения;  разработка технико-экономического обоснования. |
| 3 Технический проект | | Уточнение структуры входных и выходных данных, определение формы их представления; разработка подробного алгоритма; определение семантики и синтаксиса языка; разработка структуры программы;  окончательное определение конфигурации технических средств; разработка мероприятий по внедрению программы. |
| 4 Рабочий проект | Описание программы на выбранном языке; отладка;  разработка методики испытаний; проведение предварительных испытаний (тестирование);  корректировка программы; разработка программной документации. | |
| 5 Внедрение | Подготовка и передача программы для сопровождения;  обучение персонала использованию программы;  внесение корректировок в программу и документацию. | |

Из формулы 4.8 получим:

грн.



Энергозатраты определяются по формуле 4.9:

, (4.9)



где: *РЭ -* расход электроэнергии, потребляемой компьютером. *РЭ =* 0,4 кВт/ч;

*СкВт* - стоимость 1 кВт/ч электроэнергии, грн. *СкВт =* 0,16 грн.

Тогда по формуле 4.9 получим размер энергозатрат:

грн.



Затраты на техобслуживание определяются по формуле 4.10:

, (4.10)



где: *rТО -* часовая зарплата работника обслуживающего оборудование, грн. Принимаем *rТО* =300/160 =1,875 грн/час (по формуле 4.5).

*λ -* периодичность обслуживания, определяется по формуле 4.11:

, (4.11)



где: *NТО* - количество обслуживаний оборудования в месяц. Принимаем

*NТО* = 2.

*Fмес* - месячный фонд времени работы оборудования, час. Принимаем *Fмес* =1920/12 = 160 часов.

Тогда по формуле 4.11:

.



Применяя формулу 4.10, получим затраты на техобслуживание:

грн.



Отсюда по формуле 4.7 найдем себестоимость компьютерного часа:

грн.



Таким образом, по формуле 4.6 определим затраты компьютерного времени:

грн.



Размер косвенных расходов *З3* можно найти по формуле 4.12:

, (4.12)



где: *С1* - расходы на содержание помещений, грн. (2-2,5% от стоимости здания);

*С2* - расходы на освещение, отопление, охрану и уборку помещения, грн. (0,2-0,5% от стоимости здания);

*С3* **-** прочие расходы (стоимость различных материалов, используемых при разработке проекта, услуги сторонних организаций и т.п.), грн. (100 - 120% от стоимости вычислительной техники).

Площадь помещения равна 50 м2, следовательно, его стоимость составляет 5000 грн. (1м2 помещения стоит 100 грн.).

*С1* = 5000·0,02 = 100 грн.

*С2* = 5000·0,002 = 10 грн.

*С3* = 3362,49·1=3362,49 грн.

Тогда, используя формулу 4.12, получим размер косвенных затрат:

*З3* =100+ 10+3362,49 =3472,49 грн.

Из формулы 4.3 затраты на создание ТПО:

грн.



Капиталовложения определим по формуле 4.1:

грн.



## **4.2 Расчет годовой экономии от автоматизации управленческой** **деятельности**

## 

## **4.2.1 Расчет годовой экономии**

Годовая экономия от автоматизации управленческой деятельности вычисляется по формуле 4.13:

, грн., (4.13)



где: - трудоемкость выполнения i-ой управленческой операции соответственно в ручном и автоматизированном режиме, час.;



- повторяемость выполнения i-ой управленческой операции соответственно в ручном и автоматизированном режиме в течение года, шт.



*Са, Ср* - часовая себестоимость выполнения операций в ручном и автоматизированном вариантах, грн.

Трудоемкости операций выполняемых при автоматическом режиме приведены в таблице 4.3.

Таблица 4.3 - Трудоемкости операций, выполняемых при автоматическом режиме

|  |  |  |
| --- | --- | --- |
| Операция | Трудоёмкость  *Тai,час* | Периодичность выполнения в год |
| 1 Проверка работоспособности сети | 0,03 | 720 |
| 2 Контроль пользователей | 0,017 | 720 |
| 3 Контроль процессов | 0,03 | 720 |

Трудоемкости операций выполняемых при ручном счете приведены в таблице 4.4

Таблица 4.4 - Трудоемкости операций, выполняемых при ручном режиме

|  |  |  |
| --- | --- | --- |
| Операция | Трудоёмкость  *Тpi,час* | Периодичность выполнения в год |
| 1 Проверка работоспособности сети | 0,08 | 720 |
| 2 Контроль пользователей | 0,05 | 720 |
| 3 Контроль процессов | 0,08 | 720 |

## **4.2.2 Расчет себестоимости выполнения управленческих операций в ручном варианте**

Расчет себестоимости выполнения управленческих операций в ручном варианте рассчитывается по формуле 4.14:

(4.14)



где: *-* затраты на оплату труда персонала, грн.;



*-* косвенные расходы, грн.



Затраты на оплату труда персонала рассчитываются по формуле 4.15:

, (4.15)



где: *Nk* - количество работников k-й профессии, выполнявших работу до автоматизации, чел;

*rk -* часовая зарплата одного работника k-й профессии, грн.;

*Кзар* - коэффициент начислений на фонд заработной платы, доли (1.475);

k - число различных профессий, используемых в ручном варианте.

Часовая зарплата работника k-й профессии рассчитывается следующим образом по формуле 4.16:

, (4.16)



где: *Mk* - месячный оклад работника, грн.;

*-* месячный фонд времени работ работника, час.



грн.



грн.



Косвенные затраты - *,* рассчитываются по формуле 4.17:



, (4.17)



где: *-* расходы на содержание помещений, грн. (2-2,5 % от стоимости помещения);



- расходы на освещение, отопление, охрану и уборку помещений, грн. (0,2-0,5 % от стоимости помещения);



- прочие расходы, грн. (100-120 % фонда оплаты).



Площадь помещения равна 24,5 м2, соответственно его стоимость 2450 грн.

грн.



грн.



грн.



Косвенные затраты по формуле 4.17 составляют:

грн.



Себестоимость выполнения управленческих операций в ручном варианте рассчитаем по формуле 4.14:

грн.



## **4.2.3 Расчет себестоимости выполнения управленческих операций в автоматизированном варианте**

Расчет себестоимости выполнения управленческих операций в автоматизированном варианте рассчитывается по формуле 4.18:

, грн. (4.18)



где: - затраты на оплату труда персонала, грн.;



- стоимость компьютерного времени, грн.;



- косвенные расходы, грн.



Затраты на оплату труда персонала:

, грн.



где: *Np -* количество работников р-й профессии, выполнивших работу после автоматизации, чел.;

*rp -* часовая зарплата одного работника р-й профессии, грн.;

*Kзар -* коэффициент начислений на фонд заработной платы, доли (1.475);

Р - число различных профессий, используемых в автоматизированном варианте.

Часовая зарплата рабочего определяется по формуле:

, грн.,



где: *Mk -* месячная зарплата k-го рабочего, грн.;

*-* месячный фонд времени его работы, час.



час,



где: 8 - количество рабочих часов в день;

20 - количество рабочих дней в месяце.

грн.



грн.



Стоимость компьютерного времени определяется по формуле 4.19:

, грн., (4.19)



где: *Са-* амортизационные отчисления, грн.;

*Сэ*- энергозатраты, грн.;

*СТО* - затраты на техобслуживание, грн.

Амортизационные отчисления определяются по формуле 4.20:

, грн., (4.20)



где: *Са* - балансовая стоимость i-го оборудования, которое используется для работы с программным продуктом, грн.;

*NА -* годовая норма амортизации i-го оборудования, доли (0,15);

*Fгод*- годовой фонд времени работы i-го оборудования.

Принимаем *Fгод* =1920 часов для ЭВМ и *Fгод =* 400 часов для принтера и сканера.

грн.



Энергозатраты, которые рассчитываются по формуле 4.9 равны:

*СЭ*=0,064 грн.

Периодичность обслуживания рассчитывается по формуле 4.21:

, грн.,



где: Nто - количество обслуживаний оборудования в месяц (2 раза);

*Fмec -* месячный фонд времени работы оборудования, (160 час).

грн.



Затраты на техобслуживание рассчитываются по формуле 4.10:

*СТО =* 1,875·0,013 = 0,023 грн.

Тогда себестоимость компьютерного часа равна по формуле 4.19:

грн.



Косвенные расходы **-** прочие расходы (стоимость различных материалов, используемых при разработке проекта, услуги сторонних организаций и т.п.), грн. (100 - 120% от стоимости вычислительной техники).



Площадь помещения равна 24,5 м2, соответственно его стоимость 2450 грн.

грн.



грн.



*С3* = 3362,49·1/1920 = 1,75 грн.

Тогда, используя формулу 4.12, получим размер косвенных затрат:

*З3* =0,026+ 0,003+1,75 =1,78 грн.

Таким образом, себестоимость выполнения управленческих операций в автоматизированном варианте по формуле 4.18 равна:

грн.



Себестоимости управляющих операций в ручном и автоматизированном вариантах представлены в таблице 4.5.

Таблица 4.5 - Себестоимость одной управляющей операции в ручном и автоматизированном вариантах

|  |  |  |
| --- | --- | --- |
| Показатель | Обозначение | Затраты, грн. |
| Стоимость операции в ручном варианте | Ср | 12,197 |
| Стоимость операции в автоматизированном режиме | Са | 7,63 |

Годовая экономия от внедрения автоматизации управленческой деятельности по формуле 4.13 с учетом данных из таблиц 4.3-4.5 равна:



Повышение производительности труда посчитаем по формуле 4.22

, (4.22)



где: *Тручн, Тавт* - трудоемкости операций в ручном и автоматизированном вариантах;

*Фд -* годовой действительный фонд времени.



Производительность увеличиться на 16%.

## 

## **4.3 Расчет годового экономического эффекта применительно к**

## **источнику получения экономии**

В случае создания одного ТПО экономический эффект определяется по формуле 4.23:

*Эф = Эг - Ен·К* (4.23)

где: *Эф* - годовая экономия текущих затрат, грн.;

*К -* капитальные затраты на создание программного изделия, грн.

*Ен -* нормативный коэффициент экономической эффективности капиталовложений, доли. *Ен* зависит от особенностей применения средств автоматизации в различных отраслях; он равен 0,42.

*Эф =* 4547,9– 0,42·10660,943 = 70,3 грн.

## **4.4 Расчет коэффициента экономической эффективности и срока окупаемости капиталовложений**

Коэффициент экономической эффективности капиталовложений показывает величину годового прироста прибыли или снижения себестоимости в результате использования ТПО на одну гривну единовременных затрат (капиталовложений) рассчитывается по формуле 4.24:

*Ер = Эг/К* (4.24)

*Ер =* 4547,9/10660,943 = 0,44.

Разработанная программа является экономически эффективной, так как выполняется неравенство:

*Ер≥ Ен,*

*0,43**≥0,42.*

Срок окупаемости капиталовложений - период времени, в течение которого окупаются затраты на ТПО:

**.**



года или 2 года и 3,6 месяца.



При эффективном использовании капиталовложений расчётный срок окупаемости *Тр* должен быть меньше нормативного:

*Тр*< *Тн* = 2,4 года.

2,3< 2,4.

# 

# 5 Охрана труда

## 

## **5.1 Обеспечение электробезопасности**

Для обеспечения электробезопасности внутри здания создается сеть заземления, которая может использоваться и для улучшения электромагнитной защиты кабельной проводки, т.е. улучшения характеристик передачи данных, в низкочастотном диапазоне (менее 0,1 МГц). Надежно защитить кабельное соединение позволяют непрерывное экранирование по всей длине кабеля и полная заделка экрана — по крайней мере, с одного конца.

Заземление «питающей» сети не влияет на качество передачи сигнала по экранированному кабельному соединению. Электрический ток всегда «выбирает» путь с самым низким сопротивлением. Поскольку сопротивление переменному току зависит от частоты электромагнитных волн, то и «траектория» его движения определяется частотой. Защитная сеть заземления внутри здания состоит из одиночных проводников, определённым образом соединённых друг с другом. На низких частотах их сопротивление достаточно невелико и они хорошо проводят ток. При повышении частоты волновое сопротивление увеличивается и одиночный проводник начинает себя вести подобно катушке индуктивности. Соответственно, переменные токи с частотой ниже 0,1 МГц будут свободно «стекать» по сети заземления, а при повышении частоты — по возможности выбирать альтернативный путь. Это не противоречит правилам обеспечения электробезопасности, так как сеть заземления должна гасить опасные утечки тока, исходящие от высоковольтных сетей электропитания (50—60 Гц). А для транспортировки данных представляют интерес частоты намного выше 0,1 МГц, поэтому защитное заземление слабо влияет на качество передачи сигнала.

Независимо от типа «питающей» кабельной системы для обеспечения электробезопасности необходимо всегда использовать заземление. В реальной жизни проблемы с высоким напряжением, вызванные пробоем или коротким замыканием в сетях электропитания, встречаются только при работе на низких частотах. Все физически доступные токопроводящие предметы (металлические покрытия, корпуса и т.п.) должны быть соединены с защитной сетью заземления. Это относится и к экранированным, и к неэкранированным соединениям.

Одностороннее и двустороннее заземление. На высоких частотах «скин-эффект» предотвращает проникновение электромагнитных полей внутрь экрана. Случайная электромагнитная волна отражается от внешней поверхности экрана, как луч света от зеркала. Это физическое явление не зависит от наличия заземления. Последнее становится необходимым на низких частотах, когда сопротивление экрана уменьшается и токи начинают свободно распространяться по экрану и защитной сети.

Заземление экрана на одном конце обеспечивает дополнительную защиту сигнала от низкочастотных электрических полей, а защита от магнитных полей создается за счет сплетения проводников в «витую пару». При заземлении с двух сторон образуется токовая петля, в которой случайное магнитное поле генерирует ток. Его направление таково, что создаваемое им магнитное поле нейтрализует случайное поле. Таким образом, двустороннее заземление защищает от воздействия случайных магнитных полей. Двустороннее заземление требуется при передаче низкочастотных сигналов через электрически загрязненную среду с сильными магнитными полями (так как лишь тогда индуцированные токи могут распространяться через защитную сеть).

При использовании двустороннего заземления для случайных токов создается альтернативный путь по сети заземления. Если токи становятся слишком большими, кабельный экран может не справиться с ними. В этом случае чтобы отвести случайные токи от экрана, необходимо обеспечить другой путь, например параллельную шину для «земли». Принятие решения о ее создании зависит от качества сети заземления, применяемой системы разводки питания, величины паразитных токов в сети заземления, электромагнитных характеристик среды и т.п.

Распределительный шкаф обеспечивает эффективную электромагнитную совместимость. Если сбой электропитания происходит внутри здания, ток отводится по защитной сети заземления к «земле» — столь огромной проводящей поверхности, что ее потенциал не зависит от величины тока. А поскольку ток сбоя распределяется по весьма значительной области, его влияние на работу сети оказывается незначительным. На высоких частотах полное сопротивление защитной сети становится слишком большим, т.е. практически исчезает электрический контакт с «землей». Чтобы предотвратить работу экрана в качестве антенны, его надо соединить с точкой, потенциал которой не изменяется, — так называемой «локальной землей». Задача решается с помощью распределительного шкафа: внутри него соединяются все металлические части, и этот большой проводящий объект приобретает свойства «земли».

Антенные эффекты: для них нет проблем для экранированных кабельных систем. Когда размеры проводника, например в кабеле типа «витая пара», становятся сопоставимыми с длиной волны сигнала, проводник превращается в антенну. При увеличении частоты сигнала длина волны уменьшается и проводящий объект излучает более эффективно. Излучение удается снизить за счет скручивания проводников, однако этот способ эффективен только до частоты порядка 30 МГц. Поскольку максимальная длина соединения в кабельной системе ограничена 90 м, то частоты, на которых может происходить излучение, находятся намного выше 0,1 МГц. Это означает, что сеть заземления никак не влияет на возможное излучение экрана.

Однако экран в гораздо меньшей степени является потенциальной антенной, чем кабель, по которому передаётся сигнал. Чтобы излучать электромагнитные волны, случайные токи должны распространяться по проводящей структуре. Экран кабеля соединён с «локальной землей», потенциал которой не изменяется, а следовательно, никакие токи в него не попадают. Если на «локальной земле» все-таки появляются случайные токи, они никогда не проходят по экрану, поскольку волновое сопротивление по длине экрана намного выше, чем сопротивление элементов распределительного шкафа.

## 

## **5.2 Анализ опасных и вредных производственных факторов**

В соответствии с ГОСТ 12.0.003-74 ССБТ «Опасные и вредные производственные факторы. Классификация» на человека во время его производственной деятельности воздействуют опасные и вредные производственные факторы.

Опасные производственные факторы – это факторы, воздействие которых на работающего может привести к травме или резкому, внезапному ухудшению здоровья.

Вредные производственные факторы – это факторы, воздействие которых на работающего может привести к профессиональному заболеваниюили снижениюработоспособности человека.

В разрабатываемой системе есть только один потенциальный источник вредных производственных факторов – персональный компьютер.

Данная система будет использоваться в помещении системного администратора размерами 3.5х7х3 м на одном рабочем месте.

При работе с компьютером, как и при работе с любыми электроприборами, на человека воздействуют следующие опасные производственные факторы:

- поражение электрическим током;

- возникновение пожара;

- вредные производственные факторы;

- шум, связанный с работой вентиляторов системы охлаждения, приводов чтения CD и floppy-дисков, окружающими работниками;

- нерациональное освещение;

- излучение при использовании мониторов на электронно-лучевых трубках;

- ионизация воздуха;

- напряжение на зрительные органы;

- значительная нагрузка на пальцы и кисти рук;

- параметры микроклимата не соответствующие нормам;

- неправильная организация рабочего места;

- режим работы, не соответствующий нормам.

Воздействие этих факторов приводит к основным нарушениям здоровья у пользователей ЭВМ:

- зрительный дискомфорт, вызванный параметрами освещения, характеристиками монитора, спецификой работы;

- расстройство центральной нервной системы;

- заболевание кожи;

- нарушение репродуктивной функции;

- головная боль;

- повышение кровяного давления;

- изменение ритма сердечных сокращений;

- нарушение слуха;

- профессиональные заболевания кистей рук.

В данном случае деятельность относится к категории В (творческая работа).

Необходимо разработать мероприятия, позволяющие полностью исключить опасные производственные факторы и снизить влияние вредных производственных факторов [11].

## **5.3 Требования к организации рабочего места и режима труда**

Рабочее место соответствует требованиям ДНАОП 0.00-1.31-99.

Требования к производственным помещениям:

- наиболее пригодное помещение с односторонним расположением окон;

- площадь застекления 25-50%;

- окна ориентированы на север или северо-восток;

- окна должны быть оборудованы регулирующими устройствами;

- все поверхности должны иметь матовую или полуматовую структуру;

- недопустимо расположение в цокольных и подвальных этажах;

- поверхность пола должна быть ровной, нескользкой, удобной для отчистки и иметь антистатические свойства;

- при помещении должны быть комнаты отдыха;

- помещения должны быть оборудованы системами отопления, кондиционирования, приточно-вытяжной вентиляции;

- помещения не должны граничить с взрывоопасными, пожароопасными и шумоопасными помещениями;

- должно соблюдаться рациональное световое оформление помещений.

Требования к организации рабочих мест:

- рабочие места с ПЭВМ располагаются рядами так, чтобы свет падал слева;

- объём рабочего пространства помещения не менее 20 м3/чел, площадь одного рабочего места не более 6 м2.

Требования к рабочему столу:

- высота 680-800 мм;

- ширина 600-1400 мм;

- глубина 800-1000 мм;

- обязательно наличие пространства для ног с подставкой для ног (ширина 330 мм, высота 400мм).

Рабочий стул:

- подъёмно-поворотный и регулируемый;

- конструкция рабочего стула (кресла) обеспечивает поддержание рациональной рабочей позы при работе на ПЭВМ, позволяет изменять позу с целью снижения статического напряжения мышц шейно-плечевой области спины для предупреждения развития утомления. Тип рабочего стула (кресла) выбирается в зависимости от характера и продолжительности работы с ПЭВМ;

- поверхность сиденья, спинки и других элементов стула (кресла) должна быть полумягкой, с не электризуемым и воздухопроницаемым покрытием, обеспечивающим лёгкую очистку от загрязнений.

Размещение оборудования на рабочем столе:

- расстояние до монитора зависит от диагонали монитора (для 15-17"-600-700 мм);

- экран должен находится ниже уровня глаз на 5-10 градусов. Его расположение регулируется с помощью подставки или кронштейна под дисплеем;

- целесообразным является расположение экрана перпендикулярно к линии взора, что достигается наклоном экрана на 5-10 градусов к вертикальной плоскости;

- расстояние от края до клавиатуры 10мм минимум.

Эргономические параметры мониторов:

- яркость знака – 35-200 кд/м2;

- внешняя освещенность экрана – 100-250 лк;

- неравномерность яркости элементов знаков – не более ±25%;

- неравномерность яркости рабочего поля экрана – не более ±20%;

- формат матрицы знака - не менее 7х9 элементов изображения;

- отношение ширины знака к его высоте для прописных букв от 0,7 до 0,9;

- отражающая способность, зеркальное и смешанное отражение – не более 1%;

- частота кадров при работе с позитивным контрастом – не менее 60 Гц;

- частота кадров при режиме обработки текстов - не менее 72 Гц;

- антибликовое покрытие – обязательно;

- допустимый уровень шума – не более 50 дБ.

Требования к клавиатуре:

- возможность свободного перемещения;

- угол наклона поверхности – 5-15°;

- высота среднего ряда клавиш – не более 30 мм;

- размер клавиш: минимальный – 13мм, оптимальный – 15мм;

- расстояние между клавишами – не менее 3 мм;

- сопротивление нажатию: минимальное – не менее 0,25 Н, оптимальное – не более 1,5 Н.

# ЗАКЛЮЧЕНИЕ

По мере увеличения компьютерной сети организации или предприятия усложняется ее обслуживание и диагностика, с чем сталкивается администратор при первом же ее отказе. Наиболее сложно диагностировать многосегментные сети, где ЭВМ разбросаны по большому числу помещений, далеко отстоящих друг от друга. По этой причине сетевой администратор (чаще всего он же и эксперт по диагностике) должен заранее начинать изучать особенности своей сети уже на фазе ее формирования и готовить себя и сеть к будущему ремонту. Методы и инструменты диагностики вполне соответствуют современной практике и технологиям, но они еще не достигли такого уровня, который позволил бы значительно сэкономить время сетевых администраторов в их борьбе с неполадками сетей и дефицитом производительности.

Чтобы оценить качество работы сети, необходимо не только провести анализ функционирования всех ее компонентов, но и правильно обобщить и интерпретировать статистику наблюдений и полученные результаты диагностики. Главная задача при проведении диагностики - локализовать проблему (умозрительно или с помощью воспроизведения в ходе эксперимента), что уже - 99% ее решения.

В настоящее время существует большое количество стандартов и протоколов, программных средств и программно-аппаратных комплексов различных фирм-производителей, которые позволяют провести комплексную диагностику и тестирование компьютерной сети.

В специальной части дипломного проекта рассмотрены основные подходы к организации диагностики компьютерной сети, показаны преимущества ведения документирования сети, с помощью специальных систем документирования, определены и подробно рассмотрены этапы проведения комплексной диагностики сетей.

Не следует забывать, что корпоративные сети постоянно обретают новые возможности благодаря таким продуктам, как устройства балансировки нагрузки, шлюзы VPN, proxy-серверы, кэширующие серверы, серверы потоковых данных и устройства управления пропускной способностью, поэтому непрерывно появляются новые задачи диагностики и тема данного дипломного проекта еще долго не потеряет своей актуальности.

**Список ссылок**

1. www.colan.ru Стив Штайнке. Диагностика сетей третьего тысячелетия

2 Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. - СПб.: Питер, 2003. – 864 с.

3. Столлингс В. Современные компьютерные сети. – СПб.: Питер, 2003. – 784 с.

4. Таненбаум Э. Компьютерные сети. - СПб.: Питер, 2004. – 992 с.

5. У.Ричард Стивенс Протоколы TCP/IP. Практическое руководство, BHV, Санкт-Петербург, 2003.

6. А. В. Фролов и Г. В. Фролов, Локальные сети персональных компьютеров. Использование протоколов IPX, SPX, NETBIOS, Москва, “Диалог-МИФИ”, 1993.

7. ISDN. Цифровая сеть с интеграцией служб. Понятия, методы, системы. П. Боккер, Москва, Радио и связь, 1991.

8. Справочник “Протоколы информационно-вычислительных сетей”. Под ред. И. А. Мизина и А. П. Кулешова, Радио и связь, Москва 1990.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  | | --- | | Таблица 2.1 - Сравнительные характеристики тестеров СКС | | |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | | **Характеристики** | **Microtest Penta- Scanner+** | **Microtest Penta- Scanner 350** | **Fluke DSP-100** | **Fluke DSP-2000** | **Wavetek LT8155** | **Datacom Technologies LANcat System 5** | **Datacom Technologies LANcat System 6** | **Scope Wirescope 155** | | Точность уровня II (Level II Accuracy) | Есть | Есть | Есть | Есть | Есть | Есть | Есть | Есть | | **Переходное затухание на ближнем конце линии (Near-End Crosstalk)** | | | | | | | | | | Диапазон (Range), МГц | 0,7-100 | 0,7-350 | 0,1-155 | 0,1-155 | 1-155 | 1-100 | 1-250 | 1-155 | | Чувствительность (Sensitivity) на 100 МГц, дБ | 60 | 75 | 60 | 60 | 75 | 60 | 60 | 62 | | Измерение PS-NEXT | - | - | - | Есть |  | Есть | Есть | Есть | | **Затухание сигнала (Signal Attenuation)** | | | | | | | | | | Диапазон (Range) на 100 МГц, МГцT | 1-100 | 1-350 | 0,1-155 | 0,1-155 | 0,1-155 | 1-100 | 1-250 | 1-155 | | Чувствительность (Sensitivity), дБ | 50 | 50 | 60 | 60 | 70 | 60 | 60 | 25 | | **Рефлектометр (Time Domain Reflectometer, TDR)** | | | | | | | | | | Точность (Accuracy) | 4% | 4% | 4% | 4% | 3% | 1% | 1% | 4% | | Разрешение по дальности (Resolution), м | 0,3 | 0,3 | 0,3 | 0,3 | 0,3 | 0,3 | 0,3 | 0,6 | | Дальность для кабеля из витых пар (UTP Range), м | 0-900 | 0-900 | 0-1200 | 0-1200 | 0-300 | 1,5-600 | 1,5-600 | 3-900 | | Дальность для коаксиального кабеля (Coax Range), м | 0-1200 | 0-1200 | 3-1200 | 3-1200 | 0-300 | 1,5-1200 | 1,5-1200 | 3-900 | | **Диагностика** | | | | | | | | | | Защищенность на дальнем конце (ACR) | Есть | Есть | Есть | Есть | Есть | Есть | Есть | Есть | | Защищенность на дальнем конце (ACR) | - | - | - | - | - | Есть | Есть | Есть | | Импульсные шумы (Impulse Noise) | Есть | Есть | Есть | Есть | Есть | Есть | Есть | Есть | | Сопротивление линии по постоянному току (DC Loop Resistance) | Есть | Есть | Есть | Есть | Есть | Есть | Есть | Есть | | Характеристический импеданс (Characteristic Impedance) | Есть | Есть | Есть | Есть | Есть | Есть | Есть | Есть | | Опции для тестирования волоконно-оптических кабелей | - | - | - | - | Есть | Есть | Есть | Есть | | Схема разводки кабеля | Есть | Есть | Есть | Есть | Есть | Есть | Есть | Есть | | |  |

