Министерство образования и науки Украины
Харьковский национальный университет радиоэлектроники

Бабич Анна Витальевна

1 Введение в диагностику компьютерных сетей

Харьков
2010

Содержание

Введение

Представлена компьютерная сеть как объект диагностирования, рассмотрены основные понятия и определения, используемые в данном курсе, рассмотрены подходы к представлению компьютерной сети как объекта диагностирования. Выполнена классификация неисправностей компьютерной сети, согласно которой сетевые неисправности делятся на следующие группы: явные адресуемые дефекты, явные сетевые дефекты, скрытые сетевые дефекты, явные узкие места, скрытые узкие места. Рассмотрены особенности проявления каждой из групп сетевых неисправностей, а также рекомендуемый набор методов и инструментов для их выявления. Приведена классификация методов диагностирования компьютерных сетей в зависимости от используемых аппаратно-программных средств, а также от решаемой диагностической задачи. В рамках классификации средств диагностирования компьютерных сетей рассмотрены особенности, преимущества и недостатки систем управления сетью, средств управления системой, встроенных систем диагностики и управления, анализаторов протоколов, оборудования для диагностики и сертификации кабельной системы, экспертных систем.

Теория

1.1 КС как объект диагностирования. Основные понятия и определения

В терминах стандарта технической диагностики цифровых устройств диагностирование [1,2] - определение технического состояния объекта диагностирования. Однако, применительно к КС данное определение необходимо расширить, поскольку при исправном техническом состоянии каждого из компонентов КС в отдельности может иметь место ситуация, когда общее качество работы КС оказывается неудовлетворительным с точки зрения пользователя или сетевых задач, решаемых в КС. Таким образом, необходимо ввести в рассмотрение ряд понятий и определений для компьютерной сети как объекта диагностирования (ОД), на которые мы будем опираться в течение данного учебного курса.

Так, под **диагностированием КС** будет пониматься комплекс средств, методов и алгоритмов, направленных на обнаружение места и причины несоответствия состояния КС как ОД исправному, а также на предотвращение возникновения такого несоответствия.

Исправное состояние [1,2] - состояние объекта, при котором он соответствует всем требованиям нормативно-технической и конструкторской документации. Применительно к КС как ОД к таким требованиям относятся: техническое задание заказчика, требования к качеству обслуживания пользователей Интернет и корпоративных сетей Quality of Service (QoS), установленные комитетом IETF, соглашения об уровне обслуживания Service Level Agreement (SLA), стандарты де-факто, сведения о пиковых значениях характеристик компонентов сети, полученные в результате выполнения упреждающей диагностики.

Другими словами, состояние КС как ОД определяется: качеством работы сети. Качество работы сети с точки зрения пользователя определяется временем реакции прикладного ПО сервера на запрос клиента. В ситуации, когда имеет место физическая недоступность узла-сервера - время реакции стремится к бесконечности. Необходимо учитывать, что под термином «время реакции сети» в области диагностирования и оптимизации КС понимаются различные величины, характеризующиеся разными значениями:

1) Интервал времени между возникновением запроса пользователя к какому-либо сетевому сервису на сервере и получением ответа на этот запрос. В этом случае проводится исследование всех компонентов тракта передачи данных, включая системные ресурсы конечных узлов. Как показали исследования, проведенные группой американских психологов, данный вид времени реакции не должен превышать 2 секунды. Если время реакции оказывается большим, то пользователи чувствуют себя некомфортно, быстро устают, часто делают ошибки, производительность труда становится низкой. Также по имеющемуся соглашению в промышленности, передача, выполняемая любым узлом в ответ на любой запрос должна занимать не более 100 мс. В случае глобальной сети - 200-250 мс для любого ответа на любой тип запроса узла.

2) Интервал времени между отправлением кадра с сетевого адаптера узла-источника к сетевом адаптеру узла-приемника. В этом случае проводится исследование качества канала передачи данных. Здесь оптимальное значение времени реакции определяется временем, затрачиваемым на передачу кадра минимальной длины с учетом межкадрового интервала. Так, для протокола Ethernet 10 Мб/с это время будет составлять 67.2 мкс.

Все прочие критерии, такие как число ошибок передачи данных, степень загруженности сетевых ресурсов, производительность оборудования, являются вторичными. Таким образом, под неудовлетворительной работой понимается постоянное или перемежающееся отсутствие доступа к разделяемым ресурсам сети, большое время реакции прикладного серверного ПО на запрос клиента.

КС как объект диагностирования (ОД) определяется соотношением (1.1), связывающим критерий качества работы КС y с факторами, оказывающими на него влияние:

$$y = \varphi(S_p\{x_1, x_2 \ldots x_k\}, S_a\{x_1, x_2 \ldots x_l\}, S_{sys}\{x_1, x_2 \ldots x_m\}, S_{nos}\{x_1, x_2 \ldots x_n\}),$$

(1.1)

где y - время реакции прикладного ПО сервера на запрос клиента; факторы, характеризующие компоненты КС как ОД и влияющие на значение критерия качества работы КС, представлены следующими множествами: $S_p\{x_1, x_2 \ldots x_k\}$ - совокупность характеристик кабельной системы и другого пассивного оборудования, $S_a\{x_1, x_2 \ldots x_l\}$ - совокупность характеристик активного сетевого оборудования (сетевые платы, концентраторы, коммутаторы, маршрутизаторы), $S_{sys}\{x_1, x_2 \ldots x_m\}$ - совокупность характеристик системных ресурсов сервера и рабочих станций, $S_{nos}\{x_1, x_2 \ldots x_n\}$ - совокупность конфигурационных и сетевых настроек сетевой операционной системы.

Особенностью КС как ОД является то, что при исправном техническом состоянии каждого из сетевых компонентов в отдельности - может иметь место ситуация, когда работа сети в целом не отвечает требуемому уровню качества и, следовательно, КС с точки зрения пользователей и выполняемых в ней сетевых задач исправной не является. Это объясняется наличием ошибок на этапе проектирования и развертывания сети, несбалансированности нагрузки и сетевых компонентов, использования ПО с неэффективными алгоритмами реализации.

Структурная схема КС как ОД может быть представлена в соответствии с компонентным подходом, где каждый из компонентов сети является совокупностью компонентов уровня L-1, каждый из которых, в свою очередь, представлен совокупностями компонентов уровня L-2 и т.д. Каждый из компонентов конечного (низшего) уровня является потенциальным носителем неисправности, то есть может оказаться причиной неудовлетворительного качества работы сети. Иерархическое упорядочение, характеризующее рассмотренный подход, позволяет получить наиболее полную модель неисправностей КС и, следовательно, повысить эффективность процедуры постановки диагноза.

В качестве примера, демонстрирующего описанный выше подход, представлен фрагмент модели некоторой сети (рис. 1.1), состоящий из пяти взаимосвязанных компонентов: рабочей станции, коллизионного домена A, коммутатора, коллизионного домена B, сервера. Каждый коллизионный домен может представлять собой концентратор вместе с кабельной системой (как в домене A) или только полу/полнодуплексное соединение между рабочей станцией/сервером и коммутатором (как в домене B). На рисунке 1.2 приведено иерархическое упорядочение компонентов для представленного фрагмента сети.

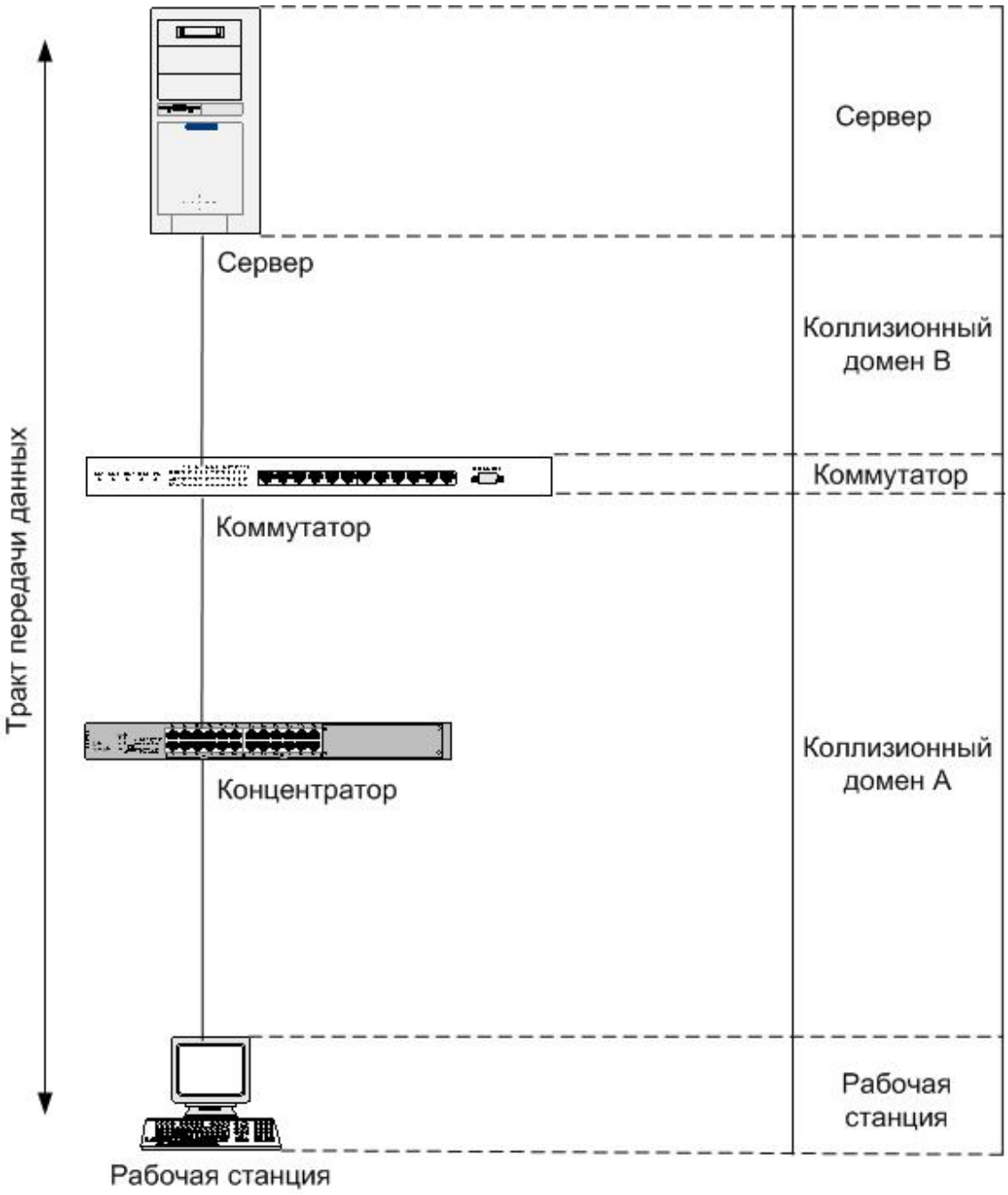

Рисунок 1.1 - Иерархический компонентный подход к представлению КС как ОД

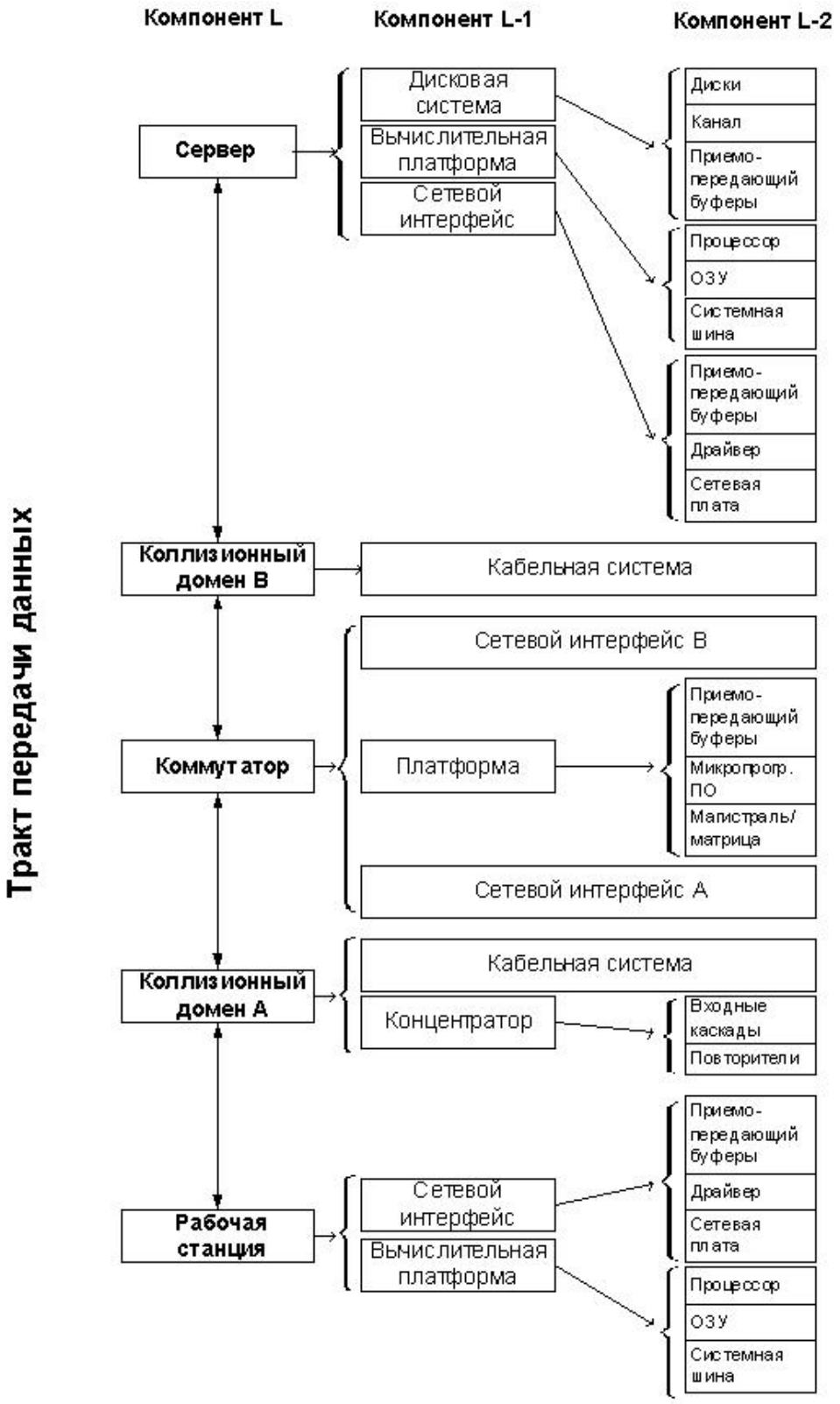

Рисунок 1.2 - Иерархическое упорядочение компонентов КС

Д. Нессер [3] предлагает рассматривать КС как ОД на основе поуровневой верификации функционирования стеков сетевых протоколов, базирующейся на анализе характеристик и процессов, по которым следует судить о корректности работы данного стека или какого-либо из его уровней. Указанные характеристики и процессы могут быть как общие для всех существующих стеков протоколов (доля широковещательных передач, дубликатные адреса, перекрытие запросов с ответами, повторные передачи, последовательность открытия сеанса связи, механизмы сохранения соединения, механизмы рассылки сообщений, сообщения об ошибках в сети), так и присущие только конкретно заданному стеку (стек протоколов TCP/IP: все типы пакетов протокола ICMP, время жизни TCP-пакета, размер окна). Данный подход отличается высокой сложностью и значительными временными затратами и применяется, в основном, при тонкой оптимизации сети, когда качество работы сети является в целом удовлетворительным, дефекты, узкие места и другие факторы, снижающие скорость работы сети, отсутствуют, и ставится цель выявления оптимального сочетания параметров настройки сети.

Тест [1,2] - вход-выходная последовательность, предназначенная для установления соответствия технического состояния объекта заданным техническим состояниям. В сети тест осуществляется сервисным оборудованием аппаратной либо программной реализации. К первому относится проверка кабеля кабельным сканером, тестером, мультиметром, терминатором на целостность либо идентификацию места и причины неисправности. Ко второму: команда ping - проверка целостности кабеля, исправности сетевого адаптера либо идентификация неисправности. Следует заметить, что тест может носить как активный, связанный с выполнением действий, влияющих на функционирование сети, например, проверка кабельной системы или стрессовое диагностирование, так и пассивный характер, осуществляемый путем наблюдения за сетью и сбора статистической информации без вмешательства в работу сети.

Элементарная проверка (ЭП) - процедура, состоящая в подаче теста и наблюдении реакции на него сетевого компонента либо фактора, его характеризующего, выполняемая в целях выявления неисправности, влияющей на техническое состояние сети.

Реакция - информация о техническом состоянии тестируемого компонента, получаемая при подаче на него теста и позволяющая сделать выводы о соответствии либо несоответствии объекта заданным техническим состояниям.

Результат элементарной проверки - сравнение реакции с эталоном при подаче теста. Проверка является **положительной**, если реакция свидетельствует о соответствии технического состояния тестируемого компонента эталонному. Результат элементарной проверки **отрицателен**, если реакция свидетельствует о несоответствии технического состояния тестируемого компонента эталонному.

1.2 Классификация неисправностей КС

Все сетевые неисправности, негативно влияющие на критерий качества работы сети, разделяют на следующие группы: **явные адресуемые дефекты, явные сетевые дефекты, скрытые сетевые дефекты, явные узкие места, скрытые узкие места.**

К категории адресуемых относятся дефекты, причиной возникновения которых является недостижимость конечных либо промежуточных узлов компьютерной сети, выявляемая в процессе попытки получения доступа к ресурсам недостижимого узла. Недостижимость узлов сети может быть следствием физического дефекта сетевых компонентов (некорректный монтаж кабельной системы, отказы повторителей, концентраторов, внешние наводки, отказы сетевых адаптеров) либо некорректной конфигурации сетевого подключения (установка сетевой карты с неподдерживаемым протоколом, неверно заданная маска подсети, дублированный IP-адрес).

К категории **явных** относятся **дефекты**, следствием которых является искажение кадров в процессе их передачи по сети. Основной причиной искажения кадров в сети являются дефекты пассивного сетевого оборудования, влияние внешних помех и некоторые неисправности приемо-передающих модулей активного сетевого оборудования. В качестве примера явных дефектов можно привести неисправности в кабельной системе, которые проявляются либо в виде ошибок соединения, сообщения о которых выдаются операционной системой клиента, либо в виде ошибок канального уровня, перехватывающихся анализатором протоколов и многофункциональным сканером. По разным оценкам, доля дефектов только пассивного сетевого оборудования составляет от 65 до 85%. В отличие от скрытых, явные дефекты сети достаточно просто обнаружить с помощью средств пассивной диагностики. Для этого все проходящие по сети кадры необходимо проанализировать на предмет наличия в них искажений. Тенденция развития сетевых технологий такова, что относительная доля явных дефектов постоянно снижается. С одной стороны, это вызвано переходом с коаксиального кабеля на витую пару и оптику, что повышает помехоустойчивость каналов передачи информации. С другой стороны, активное сетевое оборудование становится все более сложным, и это повышает вероятность появления в нем скрытых дефектов.

Скрытые дефекты замедляют работу сети, но не вызывают появления искаженных кадров. К таким относятся: некорректная настройка датчика межкадровой паузы на сетевой плате, приводящая либо к захвату сети дефектной сетевой платой, либо к ее постоянному простою; искажение информации после проверки контрольной суммы в активном сетевом оборудовании; дефекты в микропрограммном обеспечении коммутаторов, приводящие к необоснованному удалению кадров из портов либо к взаимной блокировке портов.

Кроме адресуемых, явных и скрытых сетевых дефектов на приведенный выше критерий качества работы сети влияет пропускная способность сети как объекта диагностирования, которая соответствует уровню ее самого низкопроизводительного компонента, так называемого узкого места. Им могут быть активное оборудование (коммутатор, концентратор, маршрутизатор, сервер), программное обеспечение, один или несколько параметров настройки оборудования или программного обеспечения, настройки сетевой операционной системы.

Ниже приведены примеры скрытых дефектов.

«Сетевая плата плохо слышит паузу». Одним из широко распространенных недостатков сетевых плат является дефект, когда датчик паузы в сетевой плате настроен на время,

несколько большее, чем 9,6 мкс (для Ethernet). В этом случае, при наличии нескольких активных станций, станция с такой сетевой платой будет ждать более длинной паузы и, следовательно, уступать канал всем остальным станциям, когда те одновременно с ней хотят передавать данные. Свои кадры «глухая» станция будет передавать только в те моменты, когда ни одна другая станция коллизионного домена не имеет кадров для передачи. В результате «глухая станция» будет работать медленней всех остальных станций, однако никаких искаженных кадров в сети не появится.

«Искажение информации после проверки контрольной последовательности CRC». Этот недостаток может встречаться в любом активном сетевом оборудовании и заключается в том, что искажение информации происходит уже после ее приема из сети и проверки CRC. Предположим, что сетевая плата или коммутатор принимает кадр из сети, проверяет поле CRC и, не обнаружив ошибки, передает данные драйверу. Если из-за какой-либо ошибки, например дефекта приемного буфера сетевой платы, данные окажутся искажены, то такое искажение информации может остаться незамеченным сетевой ОС (при отсутствии проверки контрольной суммы на транспортном уровне). Как и в предыдущем случае, никаких искаженных кадров в сети не появится.

«Скрытые дефекты» в микропрограммном обеспечении коммутаторов». Недостатки в микропрограммном обеспечении коммутаторов приводят к удалению кадров из обращения при высокой пиковой нагрузке или к взаимной блокировке портов (высокая пиковая загрузка одного порта вызывает блокировку другого порта). Разработчики пассивных средств диагностики отреагировали на тенденцию увеличения доли «скрытых дефектов» выпуском экспертных систем для обнаружения симптомов «скрытых дефектов». Первой это сделала компания Network General (сейчас Network Associates) в анализаторе протоколов Sniffer, обеспечив себе в течение двух лет доминирующую позицию на рынке анализаторов протоколов. Затем в гонку вступила компания Hewlett-Packard с продуктом LAN Internetwork Advisor, а вслед за ней компания Wandel & Goltermann (сейчас Wavetek Wandel Goltermann) с продуктом Mentor. Сегодня все серьезные игроки на рынке диагностических средств предлагают экспертные системы в качестве интегральной составляющей анализатора сетевых протоколов или дополнительной опции. Таким образом, экспертная система становится обязательным атрибутом для эффективной диагностики сети, что иногда очень существенно удорожает стоимость диагностического средства.

К **явным узким местам** относятся общие сетевые ресурсы с недостаточной пропускной способностью: неадекватная прикладным задачам, выполняемым в наблюдаемой сети, производительность процессора или дисковой подсистемы сервера, недостаточная пропускная способность коммутатора или канала связи. Узкие места явного типа можно обнаружить с помощью измерения основных системных характеристик компонентов сети, их сравнения между собой и выявления наиболее загруженного компонента, который и будет узким местом.

Скрытыми узкими местами являются такие алгоритмы, процессы или параметры настройки оборудования либо программного обеспечения, из-за которых пропускная способность сети оказывается неадекватно низкой. К категории скрытых узких мест относятся параметры настройки оборудования, вызывающие широковещательные штормы, или параметры настройки прикладного ПО, приводящие к увеличению доли коротких кадров. К категории скрытых узких

мест следует отнести и алгоритмы работы прикладного ПО, следствием которых является неэффективное использование пропускной способности сети, например, некорректно реализованная методология поиска файлов, зацикливание запроса, перекрытие запросов с ответами. Для выявления скрытых узких мест пассивные измерения характеристик компонентов сети являются недостаточными, здесь требуется проведение дополнительных экспериментов с воздействием на уровень нагрузки сетевого трафика.

Повышение эффективности работы прикладного ПО не входит в задачи диагностирования сетей. Тем не менее, именно неэффективные алгоритмы работы либо настройки прикладного ПО могут являться причиной неудовлетворительного времени реакции сервера на запрос клиента. Таким образом, в задачи диагностирования компьютерных сетей должна быть включена задача определения среды-носителя неисправности: сеть либо прикладное ПО.

Дж. Хогдалл [4] предлагает классификацию сетевых неисправностей в соответствии с уровнями модели OSI (таблица 1.1). Здесь явно указываются причины сетевых дефектов, что является преимуществом по сравнению с компонентным представлением КС, где оперируемым является только местонахождение дефекта. Тем не менее, здесь модель неисправностей сети не включает в себя структуру сети по ее компонентам, а базируется на уровнях модели OSI, в соответствии с которыми выполняются разработка и функционирование аппаратного и программного обеспечения сети. Таким образом, компонент-носитель дефекта не указан явно, а подразумевается, исходя из наборов функций, задействованных на каждом уровне модели OSI и являющихся стандартными.

Таблица 1.1 - Классификация сетевых неисправностей по Хогдаллу

Физический уровень	неисправности и ошибки в кабельной проводке (соединители, расщепленные пары, обрывы, короткие замыкания некорректная длина линии), отказы повторителей, концентраторов или портов, внешние наводки, насыщение полосы пропускания
Канальный уровень	ошибки CRC, коллизии и фрагментация кадров (в Ethernet), ошибки линии, ошибки пакета, очистка кольца и аварийная сигнализация (в Token Ring), проблемы в мостах и коммутаторах (задержки, отбрасывание пакетов, искажения данных), широковещательные штормы
Сетевой уровень	ошибки CRC датаграммы или поля полезной нагрузки, проблемы адресации подсетей, проблемы маршрутизации (задержки, отбрасывания пакетов, искажения данных), широковещательные штормы
Транспортный уровень	повторные транспортные пересылки, избыточная фрагментация или отбрасывание пакетов (поверх IP), размер пересылаемого сегмента, размер приемного окна и его превышение (в TCP)
Сеансовый уровень	согласование MTU блока или буфера, поиск ресурсов по логическим именам, регистрация ресурсов по именам, повторная установка соединений.
Представительский	несовместимость версий протоколов, замена кодовых таблиц

уровень	ASCII на EBCDIC, некорректные сведения в базе данных MIB протокола SNMP
Прикладной уровень	зацикливание запросов, перекрытие запросов на чтение или запись файлов, длительный поиск ресурсов, замедленная обработка данных клиентом или сервером, недостаточное заполнение пакетов данными, низкая пропускная способность между оконечными узлами сети.

1.3 Классификация методов диагностирования КС

В зависимости от используемых средств:

- **пассивное диагностирование**, выполняется в целях поиска дефектов и узких мест с использованием пассивных средств диагностирования (анализаторы сетевых протоколов и программы на основе SNMP с поддержкой RMON1/RMON2) и основано 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, отклонение от которых является симптомом дефекта. К таким относятся: уровень утилизации сети в пике и в тренде, доля трафика с ошибками от общего сетевого трафика, доля трафика с коллизиями от общего сетевого трафика и пр. Пассивный метод диагностирования также называют методом диагностирования «от противного», так как о качестве работы сети судят по отсутствию симптомов дефектов. Основными достоинствами указанного подхода являются простота и удобство при решении наиболее распространенных, но, как правило, относительно несложных проблем, локализуются явные дефекты и узкие места. Например, утилизация сети Ethernet в течение длительного времени составляет 60% и более, число ошибок составляет значительную долю от общего числа переданных кадров и т.п. 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. Поэтому пассивные средства диагностики сетей являются необходимым инструментом для администратора сети, но не достаточным.

-**активное диагностирование**, подразумевает подачу тестовых воздействий на компоненты исследуемой сети при отсутствии рабочего трафика в сети. Данный подход позволяет выявить в сети скрытые узкие места и скрытые дефекты, а также отделить дефекты сети от дефектов прикладного ПО, так как выводы о наличии в сети указанных факторов делаются не только в результате пассивного наблюдения за основными характеристиками сети, но и на основании измерений скорости работы сети. Также к активному диагностированию относится поиск дефектов в кабельной системе с помощью оборудования для диагностики кабельных систем, так как данное оборудование подразумевает отключение исследуемого кабельного сегмента от сети. Активное диагностирование позволяет решить широкий круг задач, начиная от локализации скрытых сетевых дефектов и скрытых узких мест в архитектуре сети, определения пороговых значений трафика, допустимых в данной сети, определения пиковых нагрузок работы конкретных сетевых устройств, и заканчивая тестированием ПО для определения его требований к

пропускной способности сетевых ресурсов.

В зависимости от решаемой задачи:

- **упреждающее диагностирование**, должно проводиться непрерывно или в течение длительного времени и заключается в наблюдении за работой сети с момента установки сети помощью пассивных средств диагностирования. Наблюдения должны проводиться с момента установки сети. На основании этих наблюдений администратор должен определить:

- как значения наблюдаемых параметров влияют на работу пользователей сети,

- как значения наблюдаемых параметров изменяются в течение длительного промежутка времени: рабочего дня, недели, месяца, квартала, года и пр.

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;

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

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.

- **реактивное диагностирование**, выполняется при возникновении сбоя в сети, приводящего к резкому ограничению в доступе к сетевым ресурсам и необходимо быстро локализовать фактор, вызвавший появление рассматриваемого сбоя. При реактивном диагностировании применяются активные диагностические средства, в ряде случаев, в сочетании с пассивными в качестве средств наблюдения. К реактивному диагностированию относится, в частности, поиск дефекта в кабельной системе.

-**стрессовое диагностирование,** позволяет получить интегральную оценку качества работы сети и локализовать скрытые дефекты. Стрессовое диагностирование проводится для получения интегральной оценки качества работы сети и определения запаса производительности сети после ее создания или модернизации; для выявления скрытых дефектов сетевых адаптеров и сетевых драйверов; для измерения производительности и выявления скрытых дефектов активного сетевого оборудования (концентраторов, коммутаторов, маршрутизаторов); для сравнения эффективности различных сетевых архитектур. При выполнении стрессового диагностирования в сети или ее фрагменте создается диапазон нагрузок в максимально возможном диапазоне. Одновременно с этим измеряются скоростные характеристики сети. Если выясняется, что скорость рабочих станций и пропускная способность сети соответствуют тем

значениям, которые ожидаются от сети с данной архитектурой, значит, дефектов нет. Если же какие-то станции работают с низкой скоростью или отключаются от сервера, значит, дефекты есть. В качестве основного критерия качества работы сети при проведении стрессового диагностирования используется скорость выполнения файловых операций каждой рабочей станцией сети. Этот критерий выбран, прежде всего, потому, что если в каком-либо компоненте рабочей станции есть дефект, то с вероятностью близкой к 100%, он проявится в низкой скорости выполнения файловых операций. Другая причина выбора критерия заключается в том, что скорость файловых операций не очень сложно измерить. Если скорость мала, то, изменяя режим работы станций, легко определить причину этого. Ограничением для данного вида диагностирования является необходимость отсутствия рабочего трафика в сети при его проведении.

1.4 Классификация средств диагностирования КС

Средства, применяемые для диагностирования и мониторинга КС, можно разделить на несколько крупных классов:

- **Системы управления сетью (Network Management Systems)** - централизованные программные системы, построенные в соответствии с моделью TMN, 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 HP OpenView, Sun NetManager, IBM NetView, Tivoli. В соответствии с рекомендациями ISO можно выделить следующие функции систем управления сетью:

Управление конфигурацией сети и именованием - состоит в конфигурировании компонентов сети, включая их местоположение, сетевые адреса и идентификаторы, управление параметрами сетевых операционных систем, поддержание схемы сети. Также эти функции используются для именования объектов.

Обработка ошибок - выявление, определение и устранение последствий сбоев и отказов в работе сети.

Анализ производительности - помогает на основе накопленной статистической информации оценивать время ответа системы и величину трафика, а также планировать развитие сети.

Управление безопасностью - включает в себя контроль доступа и сохранение целостности данных. В функции входит процедура аутентификации, проверки привилегий, поддержка ключей шифрования, управления полномочиями. К этой же группе можно отнести важные механизмы управления паролями, внешним доступом, соединения с другими сетями.

Учет работы сети - включает регистрацию и управление используемыми ресурсами и устройствами. Эта функция оперирует такими понятиями как время использования и плата за ресурсы.

- **Средства управления системой (System Management**) - часто выполняют функции, аналогичные функциям систем управления, но по отношению к другим объектам. В первом случае объектом управления является программное и аппаратное обеспечение компьютеров сети, а во втором - коммуникационное оборудование. Ниже перечислены основные функции средств управления:

Учет используемых аппаратных и программных средств. Система автоматически собирает информацию об обследованных компьютерах и создает записи в базе данных об аппаратных и программных ресурсах. После этого администратор может быстро выяснить, чем он располагает и где это находится. Например, узнать о том, на каких компьютерах нужно обновить драйверы принтеров, какие ПК обладают достаточным количеством памяти и дискового пространства и т. п.

Распределение и установка программного обеспечения. После завершения обследования администратор может создать пакеты рассылки программного обеспечения - очень эффективный способ для уменьшения стоимости такой процедуры. Система может также позволять централизованно устанавливать и администрировать приложения, которые запускаются с файловых серверов, а также дать возможность конечным пользователям запускать такие приложения с любой рабочей станции сети.

Удаленный анализ производительности и возникающих проблем. Администратор может удаленно управлять мышью, клавиатурой и видеть экран любого ПК, работающего в сети под управлением той или иной сетевой операционной системы. База данных системы управления обычно хранит детальную информацию о конфигурации всех компьютеров в сети для того, чтобы можно было выполнять удаленный анализ возникающих проблем.

Примерами средств управления системой являются такие продукты, как System Management Server компании Microsoft или LANDeskManager фирмы Intel, а типичными представителями средств управления сетями являются системы HPOpenView, SunNetManager и IBMNetView.

- **Встроенные системы диагностики и управления (Embedded systems) -** Эти системы выполняются в виде программно-аппаратных модулей, устанавливаемых в коммуникационное оборудование, а также в виде программных модулей, встроенных в операционные системы. Они выполняют функции диагностики и управления только одним устройством, и в этом их основное отличие от централизованных систем управления. Примером средств этого класса может служить модуль управления концентратором Distributed 5000, реализующий функции автосегментации портов при обнаружении неисправностей, приписывания портов внутренним сегментам концентратора и некоторые другие. Как правило, встроенные модули управления "по совместительству" выполняют роль SNMP-агентов, поставляющих данные о состоянии устройства для систем управления [5].

- **Анализаторы протоколов (Protocol analyzers)** - Представляют собой программные или аппаратно-программные системы, которые ограничиваются в отличие от систем управления

функциями мониторинга и анализа трафика в сетях, в том числе и беспроводных [6]. Выделяют ряд критериев оценки анализаторы протоколов [7]:

– Возможность декодирования сетевых протоколов и поддержки физических интерфейсов.

– Качество интерфейса программного обеспечения (буфер захвата, фильтры, переключатели, постфильтрационный поиск, диапазон статистических данных).

– Наличие многоканальности.

– Генерация трафика.

– Возможность интеграции с ПК.

– Размер и вес.

– Соотношение цены и предоставляемых услуг.

- **Оборудование для диагностики и сертификации кабельных систем** - Условно это оборудование можно поделить на четыре основные группы: сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры (мультиметры).

Сетевые мониторы (называемые также сетевыми анализаторами) [8-10] представляют собой эталонные измерительные инструменты для диагностики и сертификации кабелей и кабельных систем. В качестве примера можно привести сетевые анализаторы компании HewlettPackard - 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 $20'000) приборы, предназначенные для использования в лабораторных условиях специально обученным техническим персоналом.

Назначение устройств для сертификации кабельных систем [8-10] непосредственно следует из их названия. Сертификация выполняется в соответствии с требованиями одного из международных стандартов на кабельные системы.

Кабельные сканеры [8-10] используются для диагностики медных кабельных систем. 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., DatacomTechnologiesInc., ScopeCommunicationInc. В отличие от сетевых анализаторов сканеры могут быть использованы не только специально обученным техническим персоналом, но даже администраторами-новичками.

Тестеры [8-10] предназначены для проверки кабелей на отсутствие физического разрыва. Это наиболее простые и дешевые приборы для диагностики кабеля. Они позволяют определить непрерывность кабеля, но не дают ответа на вопрос о том, в каком месте произошел сбой.

Многофункциональные устройства анализа и диагностики. В последние годы, в связи с повсеместным распространением локальных сетей возникла необходимость разработки недорогих портативных приборов, совмещающих функции нескольких устройств: анализаторов протоколов, кабельных сканеров и, даже, некоторых возможностей ПО сетевого управления. В качестве примера такого рода устройств можно привести Compas компании MicrotestInc. или 675 LANMeter компании FlukeCorp.

В связи с повсеместным распространением оптоволоконных сетей связи все большую значимость приобретают инструменты тестирования ВОЛС.

Визуальный дефектоскоп - VFL (Visual Fault Locator) может использоваться, чтобы проверить полярность, а также чтобы обнаружить недопустимые изгибы или обрыв кабеля. VFL - это мощный инфракрасный лазер, посылающий излучаемый им поток в один конец кабеля. При этом VFL определяет непрерывность, идентифицирует правильность подключения коннекторов.

Анализатор оптических потерь - OLTS (Optical Loss Test Set) включает в себя два компонента: источник света и измеритель мощности оптического сигнала. Использование средств диагностики этого типа позволяет проверить целостность волокна и проверить соответствие кабеля установленным стандартам. Многие устройства производят такое сравнение автоматически.

Третий тип устройств для тестирования оптического кабеля- это устройства сертификации оптических систем - CTS (Certifying Test Set) - усложненное OLTS. Данное оборудование может измерить и вычислить потерю сигнала, проверить полярность, определить длину кабеля, сравнить их со встроенной библиотекой стандартов, представить карту соединения. Также есть возможность сохранять всю полученную информацию для последующего переноса на компьютер, что поможет сделать глубокий анализ и составить отчет. CTS состоит из основного и нескольких удаленных устройств (в каждом конце кабеля, участвующего в тестировании), включающих в себя измеритель мощности оптического сигнала и дуальный источник длин волн.

Оптические рефлектометры OTDR (Optical Domain Reflectometer) - диагностические инструменты, которые используются, чтобы характеризовать потерю мощности оптического сигнала, посылая короткий импульс света с одного конца волокна и анализируя свет, отраженный от другого конца волокна. Регистрируя показания, OTDR определяет оптическую мощность, время прохода сигнала и отображает эти данные в виде графика. Данные устройства позволяют производить измерение элементов, входящих в сеть, включая длину частей волокна, однородность ослабления сигнала, местоположение коннекторов. Таким образом, можно визуально определить местонахождение рефлексивных событий (связи, обрывы волокна) и нерефлексивные события (соединения, недопустимые или напряженные изгибы), анализируя график, или при помощи таблицы событий, которая может быть сгенерирована устройствами OTDR.

Рис.1.3 - Оптический рефлектометр

Рефлектометр MTS 8000 **-** это новая мультимодульная тестовая платформа для оптоволоконных систем. В этом приборе одновременно инсталлирован рефлектометр, оптический тестер, измеритель оптической мощности, локатор визуальных дефектов, оптический микроскоп, оптическая гарнитура, OTDR. Конструктивное решение, разработанное специалистами Acterna, позволяет одновременно устанавливать в MTS 8000 большое количество сменных оптических модулей, благодаря чему пользователь получает возможность измерения всех необходимых характеристик в зависимости от типа работ. Процессор, установленный в MTS 8000 позволяет тестировать сеть по заранее предустановленным наборам тестов. Внутренняя память устройства составляет 8МБ. Новой интересной особенностью является возможность установки жесткого диска емкостью до 6 ГБ. Для удобства и возможности оперативной работы в MTS 8000 установлены накопители FDD, CD-RW, а также USB-порты.

- **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 является экспертная система анализа сети Expert Analysis из семейства продуктов Distributed Sniffer System [11].

В основе системы лежит уникальная база знаний, накопленная специалистами компании Network General с 1986 года и основанная на опыте работы с пользователями различных сетей и разработках групп Станфордского и Массачусетского университетов, а также компании Nippon Telephone and Telegraph (NTT).

Основное назначение системы - сокращение времени простоя и ликвидация узких мест сети с

помощью автоматической идентификации аномальных явлений и автоматической генерации методов их разрешения. Система экспертного анализа предоставляет диагностическую информацию трех категорий:

Симптом - событие в сети, которому администратор сети должен уделить дополнительное внимание (например, физическая ошибка при обращении к узлу сети или единичная повторная передача файла). Необязательно означает возникновение частичной потери работоспособности, однако при высоком уровне периодичности требует внимания администратора.

Диагноз - неоднократное повторение симптома, требующее обязательного анализа со стороны администратора сети. Обычно диагноз описывает ситуации, характеризующие серьезные неисправности в сети (например, дублируемый сетевой адрес). На этапе диагноза происходит перевод события, приводящего к частичной потере работоспособности сети, на язык, понятный оператору и администратору.

Объяснение - контекстно-зависимое экспертное заключение системы анализа для каждого симптома или диагноза. Объяснение содержит описание нескольких возможных причин сложившейся ситуации, обоснование подобного заключения и рекомендации по их устранению.

Система автоматического анализа Expert Analysis основана на уникальной многозадачной технологии анализа пакетов, которая состоит из следующих шагов.

- Циркулирующие в сети пакеты непрерывно захватываются и помещаются в кольцевой буфер захвата (первая задача).

- Одновременно с этим несколько задач-анализаторов протоколов (по одной на каждое из семейств протоколов) сканируют буфер захвата и генерируют информацию в едином внутреннем формате.

- Стандартизованная информация поступает на группу задач-экспертов. Каждая из этих программ является экспертом лишь в своей узкой области, например, в знании протокола взаимодействия клиента с сервером NetWare. Если эксперт находит событие, связанное с его областью интересов, он генерирует некоторый соответствующий объект (например, "пользователь Guest сервера IBSO") в объектно-ориентированной базе данных о сети, называемой BlackboardKnowledgeBase, и связывает его с соответствующими объектами более низкого уровня. В результате возникает некоторая сложная структура, отображающая все объекты сети, относящиеся к некоторому протоколу, и все возможные связи между ними на всех семи уровнях модели ISO/OSI.

- Существует вторая группа задач-экспертов, постоянно анализирующая состояние базы данных и выдающих сообщения о ненормальном функционировании сети (симптомы или диагнозы). В общей сложности система ExpertAnalysis оперирует с более чем 200 различными событиями, приводящими к частичной потере работоспособности сети.

Подобная многозадачная система анализа является уникальной на рынке анализаторов, соответствует требованиям, предъявляемым к экспертным системам диагностики, ремонта и мониторинга, гарантирует достоверность поставленного диагноза. Однако рассмотренная ЭС

относится к разряду дорогих систем высшего класса и, следовательно, недоступна широкому кругу пользователей.

Еще одним примером ЭС с элементами искусственного интеллекта является программа *OptiView Protocol Expert* [12], разработанная компанией Fluke Networks и являющаяся представителем семейства распределенных систем анализа и мониторинга вычислительных сетей 10/100/1000 Ethernet. Назначение системы, как и Expert Analysis, направлено на сокращение времени простоя и ликвидацию узких мест сети.

Все обнаруженные события рассматриваемая система классифицирует по уровням сетевой модели OSI:

- уровень приложений: Excessive ARP, Excessive BOOTP, NFS retransmission, all ICMP errors, HTTP Get Response, Slow Server Connect, Slow Server Response;

- транспортный уровень: TCP/IP checksum error, TCP/IP retransmission, TCP/IP fast retransmission, TCP/IP zero window, TCP/IP frozen window, TCP/IP long ack, TCP/IP SYN attack;

- сетевой уровень: duplicate IP or IPX address, IP TTL expiring, IP illegal source address, ISL Illegal VLAN ID, unstable MST, HSRP coup/resign;

- канальный уровень: illegal MAC source address, broadcast/multicast storms, physical errors.

Рассматриваемая система распознает широкий ряд проблем, которые могут указать на наличие скрытого дефекта или узкого места в компоненте сети, выдает сообщения об их появлении, однако не предоставляет рекомендации по ее исправлению. Таким образом, для гарантии корректности поставленного диагноза необходимым условием является высокий уровень знаний в сетевой области у пользователя данной системы. Также, высокая стоимость системы не способствует ее повсеместному внедрению в большинство вычислительных сетей.

Текущий контроль знаний

Самоконтроль: Введение в диагностику локальных вычислительных сетей

1. Отметьте фактор, приводящий к ухудшению качества работы сети и относящийся к физическому уровню модели ЭМ ВОС в соответствии с классификацией Хогдалла:

- ❑ Расщепленные пары
- ❑ Широковещательные штормы
- ❑ Проблемы в мостах и коммутаторах (задержки, отбрасывание пакетов, искажения данных) .

_____ узкое место - общие сетевые ресурсы с недостаточной пропускной способностью

- ❑ явное
- ❑ скрытое
- ❑ определение не соответствует ни одному из приведенных терминов

_____ узкое место - такие алгоритмы, процессы или параметры настройки оборудования либо программного обеспечения, из-за которых пропускная способность сети оказывается неадекватно низкой.

- ❑ явное
- ❑ скрытое

- ❑ определение не соответствует ни одному из приведенных терминов

Дефекты, следствием которых является искажение кадров в процессе их передачи по сети, относятся к категории:

- ❑ явных
- ❑ скрытых
- ❑ не характеризуют ни одну из указанных категорий

Упреждающая диагностика - это:

- ❑ Процедура, выполняющаяся один раз при вводе сети в эксплуатацию
- ❑ Процедура, выполняющаяся только при отсутствии в сети работающих пользователей
- ❑ Процедура, для которой задействуются пассивные средства диагностирования
- ❑ Процедура, для которой задействуются активные средства диагностирования