

СОДЕРЖАНИЕ

[1 ОБСЛУЖИВАНИЕ ТЕХНИЧЕСКИХ И ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ КОМПЬЮТЕРНЫХ СЕТЕЙ 5](#_Toc123279936)

[1.1 Методы обеспечения качества обслуживания (QoS) и задачи управления 5](#_Toc123279937)

[Вопросы и упражнения 45](#_Toc123279938)

[1.2 Эксплуатация технических средств сетевой инфраструктуры 47](#_Toc123279939)

[Пассивное сетевое оборудование 48](#_Toc123279940)

[Активное сетевое оборудование 53](#_Toc123279941)

[Логические (информационные) аспекты работы ЛВС 60](#_Toc123279942)

[Службы каталогов 77](#_Toc123279943)

[Контрольные вопросы 87](#_Toc123279944)

[1.3 Архитектура и функции систем управления сетями 88](#_Toc123279945)

[1.4 Средства мониторинга и анализа локальных сетей 124](#_Toc123279946)

[Принципы локализации неисправностей 127](#_Toc123279947)

[Нагрузочное тестирование сети 132](#_Toc123279948)

[Программные средства диагностики 144](#_Toc123279949)

[Номенклатура и особенности работы тест-программ 149](#_Toc123279950)

[Диагностика неисправностей средств сетевых коммуникаций 154](#_Toc123279951)

[Введение в диагностику кабельных систем 154](#_Toc123279952)

[Оборудование для проверки кабельных систем 162](#_Toc123279953)

[1.5 Организация профилактических работ на объектах сетевой инфраструктуры 168](#_Toc123279954)

[Способы резервного копирования данных. Принцип работы хранилищ данных. Средства резервного копирования и восстановления данных. Проведение регулярного резервирования 189](#_Toc123279955)

[Аудит сетевой инфраструктуры 213](#_Toc123279956)

[Порядок проведения аудита локальной вычислительной сети 213](#_Toc123279957)

[Сбор данных. Инвентаризация сети 215](#_Toc123279958)

[Автоматизация инвентаризации сети 216](#_Toc123279959)

[Анализ данных и подготовка отчета 218](#_Toc123279960)

[Эксплуатационная документация по локальной сети 219](#_Toc123279961)

[Анализ состава и лицензионной чистоты программного обеспечения 221](#_Toc123279962)

[1.6 Диагностика неисправностей технических средств и сетевой инфраструктуры сети 232](#_Toc123279963)

[Модернизация ПК 232](#_Toc123279964)

[Обоснование модернизации сети 239](#_Toc123279965)

[Технические причины 239](#_Toc123279966)

[1.7 Восстановление сети после аварии 243](#_Toc123279967)

[Вопросы и упражнения 260](#_Toc123279968)

[Cписок литературы 268](#_Toc123279969)

# 1 ОБСЛУЖИВАНИЕ ТЕХНИЧЕСКИХ И ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ КОМПЬЮТЕРНЫХ СЕТЕЙ

# 1.1 Методы обеспечения качества обслуживания (QoS) и задачи управления

**Сетевые характеристики**

Компьютерная сеть представляет собой сложную и дорогую систему, решающую ответственные задачи и обслуживающую большое количество пользователей. Поэтому очень важно, чтобы сеть не просто работала, но работала качественно.

Понятие «качество обслуживания» можно трактовать очень широко, включая в него все возможные и желательные для пользователя свойства сети и поставщика услуг, поддерживающего работу этой сети. Для того чтобы пользователь и поставщик услуг могли более конкретно обсуждать проблемы обслуживания и строить свои отношения на формальной основе, существует ряд общепринятых характеристик качества предоставляемых сетью услуг. Мы будем рассматривать в этой главе только характеристики качества транспортных услуг сети, которые намного проще поддаются формализации, чем характеристики качества информационных услуг. Характеристики качества транспортных услуг отражают такие важнейшие свойства сети, как производительность, надежность и безопасность.

Часть этих характеристик может быть оценена количественно и измерена при обслуживании пользователя. Пользователь и поставщик услуг могут заключить соглашение об уровне обслуживания, в котором оговорить требования к количественным значениям некоторых характеристик, например к доступности предоставляемых услуг.

Термин «качество обслуживания» часто употребляется в узком смысле, как одно из современных направлений в сетевых технологиях, цель которого состоит в разработке методов качественной передачи трафика через сеть. Характеристики качества обслуживания объединяет то, что все они отражают отрицательное влияние механизма очередей на передачу трафика, такие как временное снижение скорости передачи трафика, доставку пакетов с переменными задержками и потери пакетов из-за перегрузки буферов коммутаторов.

**Типы характеристик**

Список ключевых слов: надежность, производительность и безопасность транспортных услуг, планирование использования ресурсов и контроль над их использованием, масштабируемость сети, долговременные характеристики сети, среднесрочные характеристики сети, краткосрочные характеристики сети, методы контроля и предотвращения перегрузок, соглашение об уровне обслуживания.

Субъективные оценки качества

Если опросить пользователей, чтобы выяснить, что они вкладывают в понятие качественных сетевых услуг, то можно получить очень широкий спектр ответов. Среди них, скорее всего, встретятся следующие мнения:

* сеть работает быстро, без задержек;
* трафик передается надежно;
* услуги предоставляются бесперебойно по схеме 24x7 (то есть 24 часа в сутки семь дней в неделю);
* служба поддержки работает хорошо, давая полезные советы и помогая разрешить проблемы;
* услуги предоставляются по гибкой схеме, мне нравится, что можно в любой момент и в широких пределах повысить скорость доступа к сети и увеличить число точек доступа;
* поставщик не только передает мой трафик, но и защищает мою сеть от вирусов и атак злоумышленников;
* я всегда могу проконтролировать, насколько быстро и без потерь сеть передает мой трафик;
* поставщик предоставляет широкий спектр услуг, в частности помимо стандартного доступа в Интернет он предлагает хостинг для моего персонального веб-сайта и услуги IР-телефонии.

Эти субъективные оценки отражают пожелания пользователей к качеству сетевых сервисов. Пользователи, клиенты — это важнейшая сторона любого бизнеса, в том числе бизнеса сетей передачи данных, но существует и еще одна сторона — поставщик услуг (коммерческий, если это публичная сеть, и некоммерческий, если это корпоративная сеть). Для того чтобы пользователи и поставщики услуг могли обоснованно судить о качестве сервисов, существуют формализованные характеристики качества сетевых услуг, которые позволяют количественно оценить тот или иной аспект качества.

**Характеристики и требования к сети**

Работая в сети, пользователь формулирует определенные требования к ее характеристикам. Например, пользователь может потребовать, чтобы средняя скорость передачи его информации через сеть была не ниже 2 Мбит/с. Очевидно, что он при этом использует характеристику «средняя скорость передачи информации через сеть» и определяет тот диапазон значений этой характеристики, который для него означает хорошее качество сервиса.

Все множество характеристик качества транспортных услуг сети можно отнести к одной из следующих групп:

* производительность;
* надежность;
* безопасность;
* характеристики, интересные только поставщику услуг.

Первые три группы соответствуют трем наиболее важным для пользователя характеристикам транспортных услуг — возможности без потерь и перерывов в обслуживании (надежность) передавать с заданной скоростью (производительность) защищенную от несанкционированного доступа и подмены информацию (безопасность). Понятно, что поставщик сетевых услуг, стремясь удовлетворить требования пользователей, также уделяет внимание этим характеристикам. В то же время существует ряд важных для поставщика характеристик сети, которые не интересуют пользователей.

Дело в том, что сеть обслуживает большое количество пользователей, и поставщику услуг нужно организовать работу своей сети таким образом, чтобы одновременно удовлетворить требования всех пользователей. Как правило, это сложная проблема, так как основные ресурсы сети — линии связи и коммутаторы (маршрутизаторы) — разделяются между информационными потоками пользователей. Поставщику необходимо найти такой баланс в распределении ресурсов между конкурирующими потоками, чтобы требования всех пользователей были соблюдены. Решение этой задачи включает планирование использования ресурсов и контроль над их использованием в процессе передачи пользовательского трафика. Поставщика интересуют те характеристики ресурсов, с помощью которых он обслуживает пользователей. Например, его интересует производительность коммутатора, так как поставщик должен оценить, какое количество потоков пользователей он может обслужить с помощью данного коммутатора. Для пользователя производительность коммутатора не представляет интерес, ему важен конечный результат — будет его поток обслужен качественно или нет.

Итак, в четвертой группе собраны характеристики качества, которые интересуют только поставщика услуг. Примером такой характеристики может служить масштабируемость, то есть способность сети работать качественно при значительном увеличении числа пользователей без изменения применяемой в этой сети технологии.

Временная шкала

Рассмотрим еще один способ классификации характеристик — в соответствии с временной шкалой, на которой эти характеристики определяются.

**Долговременные характеристики** определяются на промежутках времени от нескольких месяцев до нескольких лет. Их можно назвать характеристиками проектных решений. Примерами таких характеристик являются набор моделей и количество коммутаторов в сети, топология и пропускная способность линий связи. Эти параметры сети прямо влияют на характеристики качества услуг сети. Одно проектное решение может оказаться удачным и сбалансированным, так что потоки трафика не будут испытывать перегрузок; другое может создавать узкие места для потоков, так что задержки и потери пакетов превысят допустимые пределы. Понятно, что полная замена или глубокая модернизация сети связана с большими затратами финансовых средств и времени, поэтому они происходят не слишком часто и продолжают оказывать влияние на качество сети в течение продолжительного времени.

**Среднесрочные характеристики** определяются на интервалах времени от нескольких секунд до нескольких дней. Примерами характеристик этого диапазона являются средние скорости потоков трафика или средние значения задержек пакетов, определяемые на достаточно продолжительном промежутке времени, который включает обслуживание большого количества пакетов. Примером методов, влияющих на среднесрочные характеристики, являются методы определения маршрутов трафика. Маршруты трафика могут быть неизменными в течение часов или дней, если топология сети и параметры трафика остаются постоянными, а каналы и коммутаторы сети не отказывают.

**Краткосрочные характеристики** относятся к темпу обработки отдельных пакетов и измеряются в микросекундном и миллисекундном диапазонах. Например, время буферизации или время пребывания пакета в очереди коммутатора или маршрутизатора являются характеристиками этой группы. Для анализа и обеспечения требуемого уровня краткосрочных характеристик разработано большое количество методов, получивших название методов контроля и предотвращения перегрузок (congestions control and congestion avoidance).

**Соглашение об уровне обслуживания**

Естественной основой нормального сотрудничества поставщика услуг и пользователей является договор. Договор всегда заключается между клиентами и поставщиками услуг публичных сетей передачи данных, однако не всегда в нем указываются количественные требования к эффективности предоставляемых услуг. Очень часто в договоре услуга специфицируется очень общо, например, «предоставление доступа в Интернет».

Однако существует и другой тип договора, называемый соглашением об уровне обслуживания (Service Level Agreement, SLA). В таком соглашении поставщик услуг и клиент описывают качество предоставляемой услуги в количественных терминах, пользуясь характеристиками эффективности сети. Например, в SLA может быть записано, что поставщик обязан передавать трафик клиента без потерь и с той средней скоростью, с которой пользователь направляет его в сеть. При этом оговорено, что это соглашение действует только в том случае, если средняя скорость трафика пользователя не превышает, например, 3 Мбит/с, в противном случае поставщик получает право просто не передавать избыточный трафик. Для того чтобы каждая сторона могла контролировать соблюдение этого соглашения, необходимо еще указать период времени, на котором будет измеряться средняя скорость, например день, час или секунда. Еще более определенным соглашение SLA становится в том случае, когда в нем указываются средства и методы измерения характеристик сети, чтобы у поставщика и пользователя не было расхождений при контроле соглашения.

Соглашения SLA могут заключаться не только между поставщиками коммерческих услуг и их клиентами, но и между подразделениями одного и того же предприятия. В этом случае поставщиком сетевых услуг может являться, например, отдел информационных технологий, а потребителем — производственный отдел.

**Производительность**

Список ключевых слов: предложенная нагрузка, гистограмма распределения, задержка доставки пакета, плотность распределения задержки доставки пакета, статистические, или вероятностные, характеристики, среднее значение задержки, джиттер, коэффициент вариации, максимальная задержка, максимальная вариация задержки, время реакции сети, время оборота, скорость передачи данных, средняя скорость передачи данных, пиковая скорость передачи данных, период пульсации, величина пульсации, коэффициент пульсации трафика, узкое место составного пути.

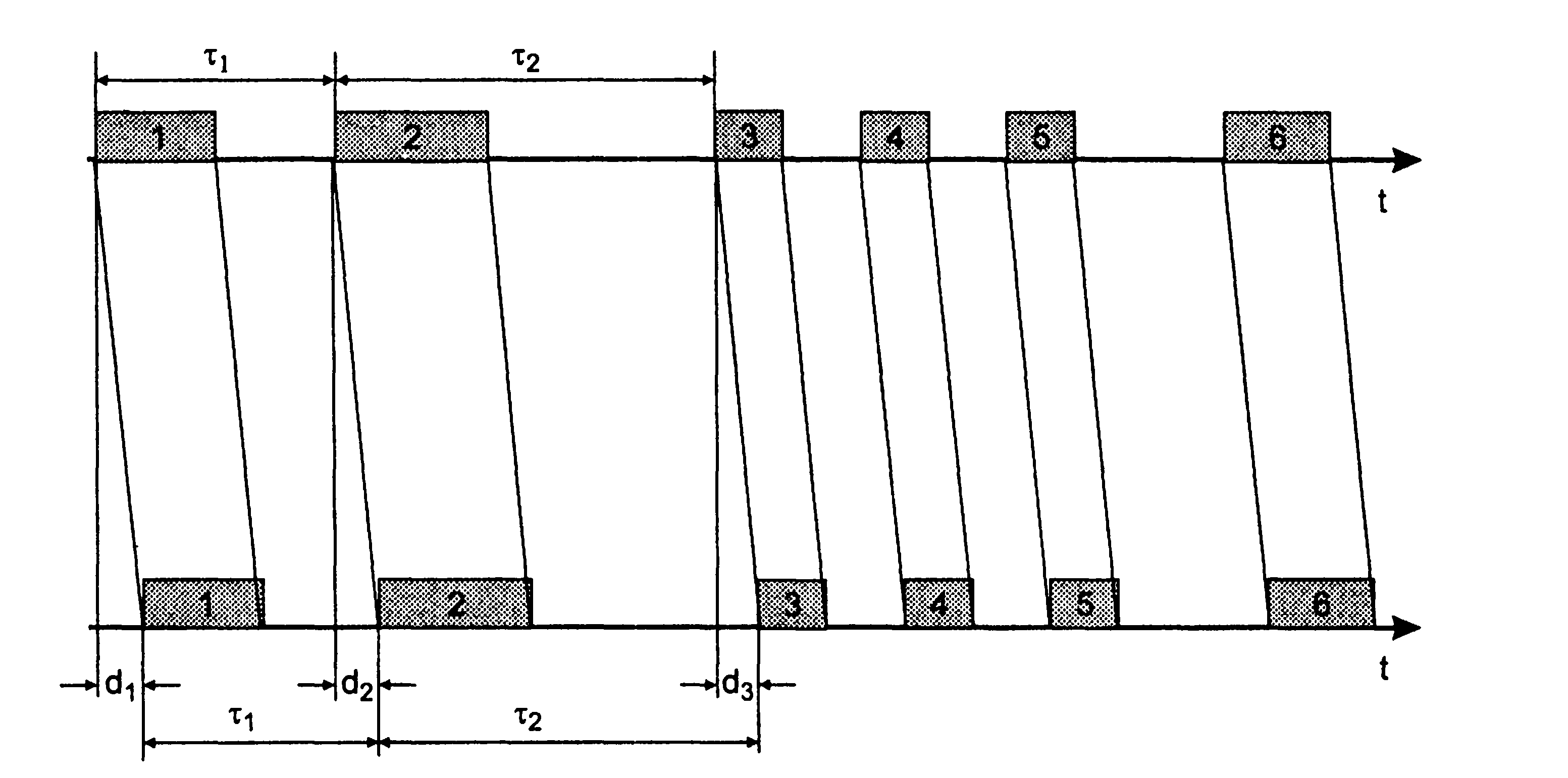
Мы уже знакомы с такими важными долговременными характеристиками производительности сетевых устройств, как пропускная способность каналов или производительность коммутаторов и маршрутизаторов. Наибольший интерес данные характеристики представляют для поставщиков услуг — на их основе поставщик услуг может планировать свой бизнес, рассчитывая максимальное количество клиентов, которое он может обслужить, определяя рациональные маршруты прохождения трафика и т. п.

Однако клиента интересуют другие характеристики производительности, которые позволят ему количественно оценить, насколько быстро и качественно сеть передает его трафик. Для того чтобы определить эти характеристики, воспользуемся моделью идеальной сети.

**Идеальная сеть**

Будем считать, что сеть работает идеально, если она передает каждый бит информации с постоянной задержкой, равной скорости распространения света в физической среде. Пусть каналы идеальной сети обладают некоторой конечной (а не бесконечной, как хотелось бы) пропускной способностью, поэтому источник информации передает пакет в сеть не мгновенно, а за некоторое конечное время (которое равно, как мы уже знаем, частному от деления объема пакета в битах на пропускную способность канала доступа в сеть).

Результат передачи пакетов такой идеальной сетью иллюстрирует рис.1.1.1. На верхней оси показаны значения времени поступления пакетов в сеть от узла отправителя, а на нижнем — значения времени поступления пакетов в узел назначения. Другими словами, можно сказать, верхняя ось показывает предложенную нагрузку сети, а нижняя — результат передачи этой нагрузки через сеть. Мы отсчитываем значения времени отправления и поступления от момента попадания первого бита пакета в сеть или в узел назначения соответственно.

Рис.1.1.1. Передача пакетов идеальной сетью

Как видно из рисунка, идеальная сеть доставляет все пакеты узлу назначения:

* не потеряв ни один из них (и не исказив информацию ни в одном из них);
* в том порядке, в котором они были отправлены;
* с одной и той же и минимально возможной задержкой (d1= d2 и т. д.).

Важно, что все интервалы между соседними пакетами сеть сохраняет в неизменном виде. Например, если интервал между первым и вторым пакетами составляет при отправлении xt секунд, а между вторым и третьим — т2, то такими же интервалы останутся в узле назначения.

Надежная доставка всех пакетов с минимально возможной задержкой и сохранением временных интервалов между ними удовлетворит любого пользователя сети независимо от того, трафик какого приложения он передает по сети — веб-сервиса или 1Р-телефонии.

Теперь посмотрим, какие отклонения от идеала могут встречаться в реальной сети и какими характеристиками можно эти отклонения описывать (рис.1.1.2).

Пакеты доставляются сетью узлу назначения с различными задержками. Как мы уже знаем, это неотъемлемое свойство сетей с коммутацией пакетов. Случайный характер процесса образования очереди приводит к случайным задержкам, при этом задержки отдельных пакетов могут быть значительными, в десятки раз превосходя среднюю величину задержек (dj ≠ d2 ≠ d3 и т. д.). Неравномерность задержек приводит к неравномерным интервалам между соседними пакетами. То есть изменяется характер временных соотношений между соседними пакетами, а это может катастрофически сказаться на качестве работы некоторых приложений. Например, при цифровой передаче речи (или более обобщенно — звука), неравномерность интервалов между пакетами, несущими замеры голоса, приводит к существенным искажениям речи.

Рис.1.1.2. Передача пакетов реальной сетью

Пакеты могут доставляться узлу назначения не в том порядке, в котором они были отправлены, например, на рис.1.1.2 пакет 4 поступил в узел назначения раньше, чем пакет 3. Такие ситуации встречаются в дейтаграммных сетях, когда различные пакеты одного потока передаются через сеть различными маршрутами, а следовательно, ожидают обслуживания в разных очередях с разным уровнем задержек. Очевидно, что пакет 3 проходил через перегруженный узел или узлы, так что его суммарная задержка оказалась настолько большой, что пакет 4 прибыл раньше него.

Пакеты могут теряться в сети или же приходить в узел назначения с искаженными данными, что равносильно потере пакета, так как большинство протоколов не может восстановить искаженные данные, а только определяет этот факт по значению контрольной последовательности кадра (Frame Check Sequence, FCS).

Средняя скорость информационного потока на входе узла назначения может отличаться от средней скорости потока, направленного в сеть узлом отправителем. Виной этому являются не задержки пакетов, а их потери. Так, в примере, показанном на рис.1.1.2, средняя скорость исходящего потока уменьшается из-за потери пакета 5. Чем больше потерь и искажений пакетов происходит в сети, тем ниже скорость информационного потока.

Очевидно, что множество отдельных значений времени передачи каждого отдельного пакета в узел назначения дают исчерпывающую характеристику качества передачи трафика сетью. Однако это слишком громоздкая и, более того, избыточная характеристика производительности сети. Для того чтобы представить характеристики качества передачи последовательности пакетов через сеть в компактной форме, применяются статистические методы. Статистические характеристики выявляют закономерности в поведении сети, которые устойчиво проявляются только на длительных периодах времени. Когда мы говорим о длительном периоде времени, то мы понимаем под этим период времени, в миллионы раз больший, чем время передачи одного пакета, которое в современной сети измеряется микросекундами. Так, время Fast Ethernet 100 мкс, Gigabit Ethernet — около 10 мкс, ячейки ATM — от долей микросекунды до 3 мкс (в зависимости от скорости передачи). Поэтому для получения ус тойчивых результатов нужно наблюдать поведение сети по крайней мере в тече ние минут, а лучше — нескольких часов.

Существует две группы статистических характеристик, которые относятся к производительности сети:

характеристики задержек пакетов;

характеристики скорости передачи данных.

**Характеристики задержек пакетов**

Основным инструментом статистики является так называемая гистограмма распределения оцениваемой величины. В данном случае оцениваемой величиной является задержка доставки пакета.

Будем считать, что нам удалось измерить задержку доставки каждого пакета и сохранить полученные результаты. Для того чтобы получить гистограмму распределения, мы должны разбить весь диапазон возможных задержек на несколько интервалов и подсчитать, сколько пакетов из нашей последовательности измерений попало в каждый интервал. В результате мы получим гистограмму, показанную на рис.1.1.3. Здесь диапазон 25-75 мс, в который попали все значения задержек, разбит на шесть интервалов (сеть вносит фиксированную задержку в 25 мс, связанную с распространением сигнала и буферизацией пакета). Значит, мы можем использовать в качестве характеристики производительности нашей сети шесть чисел: nl, n2, nЗ, n4, n5 и n6. Это уже более компактная форма представления последовательности задержек. Но нужно соблюдать баланс между желанием сократить до минимума количество интервалов и информативностью полученных характеристик.

Гистограмма задержек дает хорошее представление о производительности сети. По ней можно судить, какие уровни задержек более вероятны, а какие менее. Чем больше период времени, в течение которого собираются данные для построения гистограммы, тем с более высокой степенью вероятности можно предсказать поведение сети в будущем. Например, пользуясь гистограммой на рис.1.1.3, можно сказать, что с вероятностью 0,6 задержка пакета не превысит 50 мс. Для нахождения такой оценки мы сложили общее количество пакетов, задержки которых попали во все интервалы, меньшие 50 мс, и разделили эту величину на общее количество пакетов. Другими словами, мы нашли долю пакетов, задержки которых не превышают 50 мс.

При увеличении количества интервалов и времени наблюдения мы в пределе получаем непрерывную функцию, которая называется плотностью распределения задержки доставки пакета (показана пунктиром). В соответствии с теорией, от нижней до верхней границ данного диапазона. Таким образом может быть вычислена вероятностное значение задержки пакета.

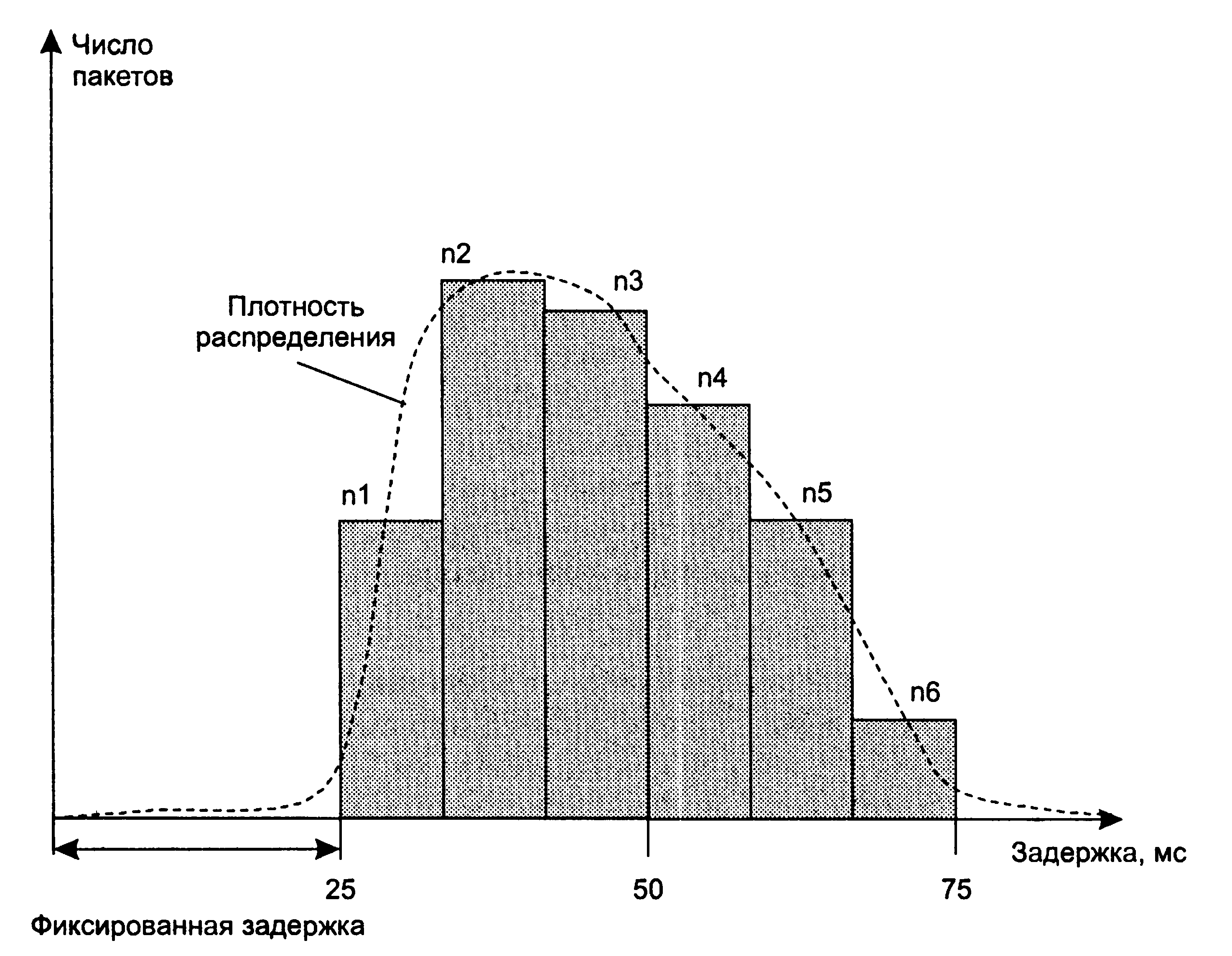
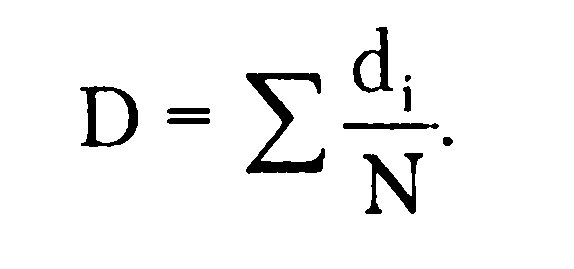


Рис.1.1.3. Гистограмма распределения задержек

Только что мы впервые столкнулись с тем, что большое количество сетевых характеристик являются статистическими (вероятностными). Мы не можем со стопроцентной уверенностью сказать, что характеристика имеет некоторое конкретное значение. Мы можем говорить об этом только с какой-то вероятностью, потому что процессы перемещения данных в сети с коммутацией пакетов являются случайными процессами по своей сути.

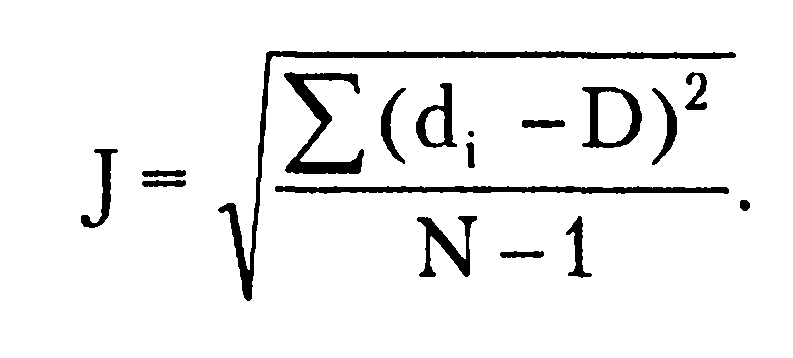
Определим еще несколько часто используемых статистических характеристик задержки пакета.

**Среднее значение задержки (D)** вычисляется как сумма всех задержек di? деленная на количество всех измерений N:



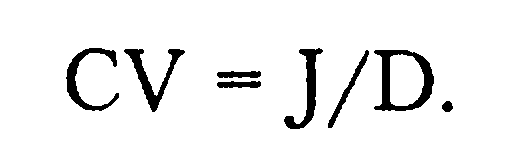
Джиттер1 (J) представляет собой среднее отклонение каждой отдельной задержки от среднего значения задержки:

1 Термин «джиттер» является примером сетевого «жаргона», математики называют эту величину стандартным отклонением.



Как среднее значение задержки, так и джиттер измеряются в секундах. Очевидно, что если все задержки d, равны между собой, то вариация отсутствует, что подтверждают приведенные формулы — в этом случае D = di и J = 0.

Коэффициент вариации — это безразмерная величина, которая равна отношению джиттера к среднему значению задержки:



Коэффициент вариации характеризует трафик без привязки к абсолютным значениям временной оси. Идеальный равномерный поток данных всегда будет обладать нулевым значением коэффициента вариации. Коэффициент вариации, равный 1, означает достаточно пульсирующий трафик, так как средние отклонения интервалов от некоторого среднего периода следования пакетов равны этому периоду.

**Максимальная задержка** — это величина, которую задержки пакетов не должны превосходить с заданной вероятностью. Мы недавно вычисляли такую величину по гистограмме задержек. Чтобы получить оценку, достаточно определенно говорящую о качестве работы сети, обычно задают высокую вероятность, например 0,95 или 0,99. Действительно, если пользователю скажут, что сеть будет обеспечивать уровень задержек в 100 мс с вероятностью 0,5, то это его не очень обрадует, так как он ничего не будет знать об уровне задержек половины своих пакетов.

**Максимальная вариация задержки** — максимальное значение, на которое отклонение задержки от среднего значения задержки не превосходит с некоторой вероятностью.

**Время реакции** сети является интегральной характеристикой производительности сети с точки зрения пользователя. Именно эту характеристику имеет в виду пользователь, когда говорит: «Сегодня сеть работает медленно». Время реакции определяется как интервал времени между возникновением запроса пользователя к какой-либо сетевой службе и получением ответа на этот запрос. Время реакции сети можно представить в виде нескольких слагаемых, например (рис.1.1.4): время подготовки запросов на клиентском компьютере (t клиент1), время передачи запросов между клиентом и сервером через сеть (tсеть), время обработки запросов на сервере (tcepвep), время передачи ответов от сервера клиенту через сеть (снова tсеть) и время обработки получаемых от сервера ответов на клиентском

компьютере (t клиент2).

Время реакции сети характеризует сеть в целом, в том числе качество работы аппаратного и программного обеспечения серверов. Для того чтобы отдельно оценить транспортные возможности сети, чаще используется другая характеристика — время оборота данных по сети.

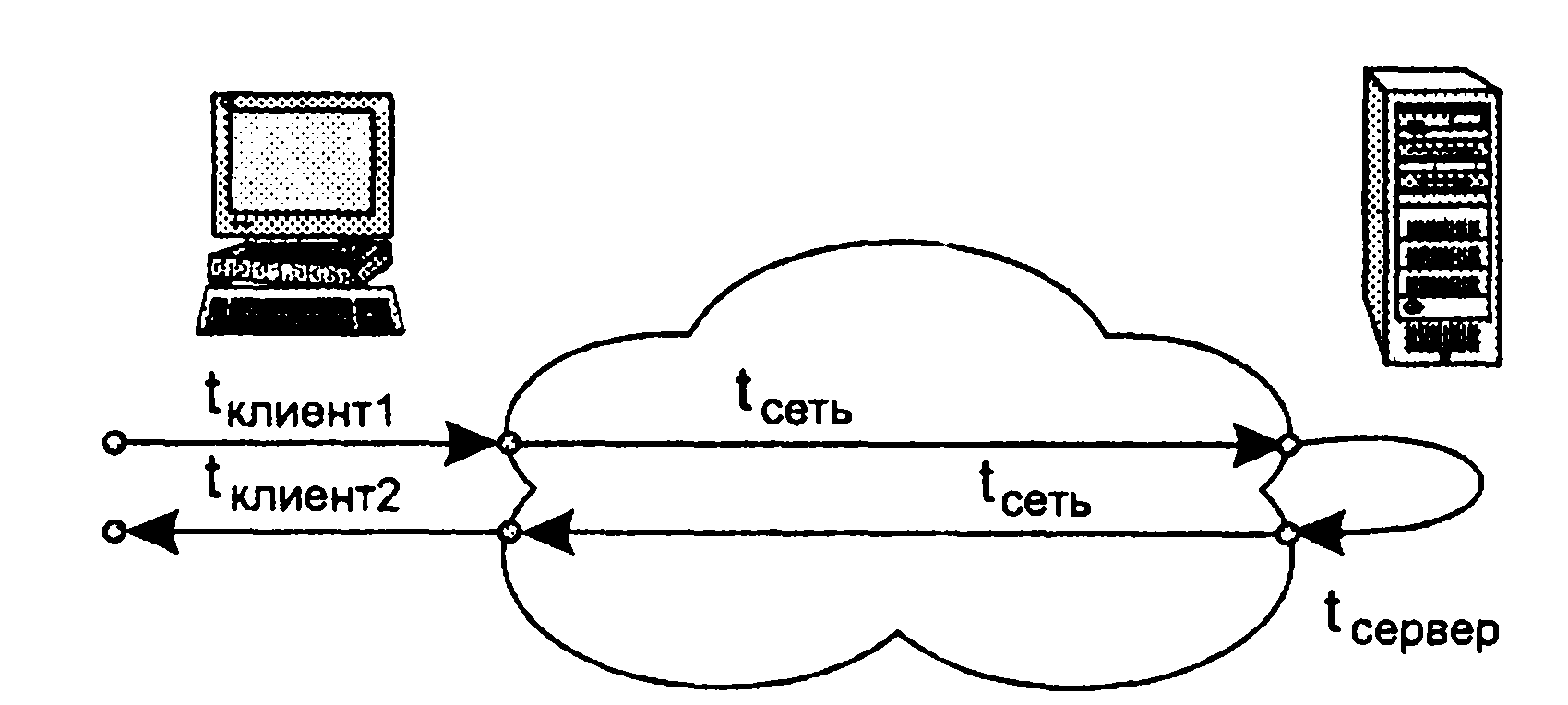
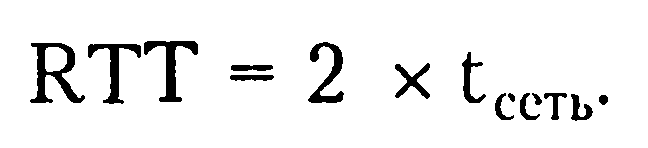


Рис.1.1.4. Время реакции и время оборота

Время оборота (Round Trip Time, RTT) — это «чистое» время транспортировки данных от узла отправителя до узла назначения и обратно без учета времени, затраченного узлом назначения на подготовку ответа:



RTT является полезной характеристикой в том случае, когда значения времени передачи данных по сети в прямом и обратном направлениях отличаются друг от друга. Как и для односторонних задержек, значение RTT можно оценивать по его среднему и максимальному (с заданной вероятностью) значениям.

В зависимости от типа приложения клиент может использовать тот или иной набор характеристик задержек. Рассмотрим, например, работу приложения, воспроизводящего музыку через Интернет. Поскольку эта услуга не является интерактивной, она допускает значительные задержки передачи отдельных пакетов, например несколько минут. Однако пакеты должны приходить равномерно, то есть вариация задержки должна не превышать 100-150 мс, иначе качество воспроизведения музыки резко упадет. Поэтому в данном случае требования к сети должны включать ограничения на среднюю вариацию задержки или максимальное значение вариации задержки.

**Характеристики скорости передачи**

Скорость передачи данных (information rate) измеряется на каком-либо промежутке времени как частное от деления объема переданных данных за этот период на продолжительность периода. Таким образом, данная характеристика всегда является средней скоростью передачи данных.

Однако в зависимости от величины интервала, на котором измеряется скорость, для этой характеристики традиционно используется одно из двух наименований: средняя или пиковая скорость.

Средняя скорость передачи данных (Sustained Information Rate, SIR)1 определяется на достаточно большом периоде времени. Это среднесрочная характеристика, период времени должен быть достаточным, чтобы можно было говорить об устойчивом поведении такой случайной величины, которой является скорость.

1 Традиционно, для одной и той же характеристики может существовать несколько названий. Мы приводим только те из них, которые, по нашему мнению, наилучшим образом отражают их смысл.

Должен быть оговорен период контроля этой величины, например 10 секунд. Это означает, что каждые 10 секунд вычисляется скорость информационного потока и сравнивается с требованием к этой величине. Если такие контрольные измерения не проводить, это лишило бы пользователя возможности предъявлять претензии поставщику в некоторых конфликтных ситуациях. Например, если поставщик в один из дней месяца вообще не будет передавать пользовательский трафик, а в остальные дни разрешит пользователю превышать оговоренный предел, то средняя скорость за месяц окажется в норме. В этой ситуации только регулярный контроль скорости поможет пользователю отстоять свои права.

Этот период обычно называют периодом пульсации. Очевидно, что при передаче трафика можно говорить об этой величине только с некоторой степенью вероятности. Например, требование к этой характеристике может быть сформулировано так: «Скорость информации не должна превышать 2 Мбит/с на периоде времени 10 мс с вероятностью 0,95». Часто значение вероятности опускают, подразумевая близость ее к единице. Пиковая скорость является краткосрочной характеристикой. PIR позволяет оценить способность сети справляться с пиковыми нагрузками, характерными для пульсирующего трафика и приводящими к перегрузке. Если в SLA оговорены обе скорости (SIR и PIR), очевидно, что периоды пульсации должны сопровождаться периодами относительного «затишья», когда скорость падает ниже средней. В противном случае показатель средней скорости соблюдаться не будет.

**Величина пульсации** (обычно обозначаемая В) используется для оценки емкости буфера коммутатора, необходимого для хранения данных во время перегрузки. Величина пульсации равна общему объему данных, поступающих на коммутатор в течение разрешенного интервала Т (периода пульсации) передачи данных с пиковой скоростью (PIR):



В главе 3, обсуждая коммутацию каналов, мы упоминали еще об одном показателе — коэффициенте пульсации трафика. Мы определили его как отношение максимальной скорости на каком-либо небольшом периоде времени к средней скорости трафика, измеренной на длительном периоде времени. Неопределенность временных периодов делает коэффициент пульсации качественной характеристикой трафика.

Скорость передачи данных можно измерять между любыми двумя узлами, или точками, сети, например между клиентским компьютером и сервером, между входным и выходным портами маршрутизатора. Для анализа и настройки сети очень полезно знать данные о пропускной способности отдельных элементов сети. Важно отметить, что из-за последовательного характера передачи различными элементами сети общая пропускная способность сети любого составного пути в сети будет равна минимальной из пропускных способностей составляющих элементов маршрута. Поэтому максимальная скорость передачу данных всегда ограничена пропускной способностью таких элементов. Для повышения пропускной способности составного пути необходимо в первую очередь обратить внимание на самые медленные элементы, называемые узкими местами (bottleneck).

**Надежность**

Список ключевых слов: доля потерянных пакетов, среднее время наработки на отказ, вероятность отказа, интенсивность отказов, доступность, отказоустойчивость, альтернативный маршрут следования трафика, методы повторной передачи пакетов, положительная квитанция, отрицательная квитанция, метод простоя источника, метод скользящего окна, размер окна.

**Характеристики потерь пакетов**

В качестве характеристики потери пакетов используется доля потерянных пакетов (обозначим ее L), равная отношению количества потерянных пакетов (NL) к общему количеству переданных пакетов (N):



Может также использоваться аналогичная характеристика, оперирующая не количествами потерянных и переданных пакетов, а объемами данных, содержавшихся в этих пакетах.

**Доступность и отказоустойчивость**

Для описания надежности отдельных устройств используются такие показатели надежности, как среднее время наработки на отказ, вероятность отказа, интенсивность отказов. Однако эти показатели пригодны только для оценки надежности простых элементов и устройств, которые при отказе любого своего компонента переходят в неработоспособное состояние. Сложные системы, состоящие из многих компонентов, могут при отказе одного из компонентов сохранять свою работоспособность. В связи с этим для оценки надежности сложных систем применяется другой набор характеристик.

**Доступность** (availability) означает долю времени, в течение которого система или служба находится в работоспособном состоянии.

Доступность является долговременной статистической характеристикой, поэтому измеряется на большом промежутке времени, которым может быть день, месяц или год. Примером высокого уровня доступности является коммуникационное оборудование телефонных сетей, лучшие представители которого обладают так называемой доступностью «пять девяток». Это означает, что доступность равна 0,99999, что соответствует чуть более 5 минутам простоя в год. Оборудование и услуги передачи данных только стремятся к такому рубежу, но рубеж трех девяток уже достигнут. Доступность услуги является универсальной характеристикой, которая используется как пользователями, так и поставщиками услуг.

Еще одной характеристикой надежности сложных систем является отказоустойчивость (fault tolerance). Под отказоустойчивостью понимается способность системы скрывать от пользователя отказ отдельных ее элементов.

Например, если коммутатор оснащен двумя коммутационными центрами, работающими параллельно, то отказ одного их них не приведет к полному останову коммутатора. Однако производительность коммутатора снизится, он будет обрабатывать пакеты вдвое медленней. В отказоустойчивой системе отказ одного из элементов приводит к некоторому снижению качества ее работы (деградации), а не к полному останову. В качестве еще одного примера можно назвать использование двух физических каналов для соединения коммутаторов. В нормальном режиме работы трафик передается по двум каналам со скоростью С Мбит/с, а при отказе одного из них трафик будут продолжать передаваться, но уже со скоростью С/2 Мбит/с. Однако из-за того, что во многих случаях количественно определить степени деградации системы или услуги достаточно сложно, отказоустойчивость чаще всего используется как качественная характеристика.

Далее мы рассмотрим наиболее часто применяемые методы обеспечения высокой надежности транспортных услуг.

**Альтернативные маршруты**

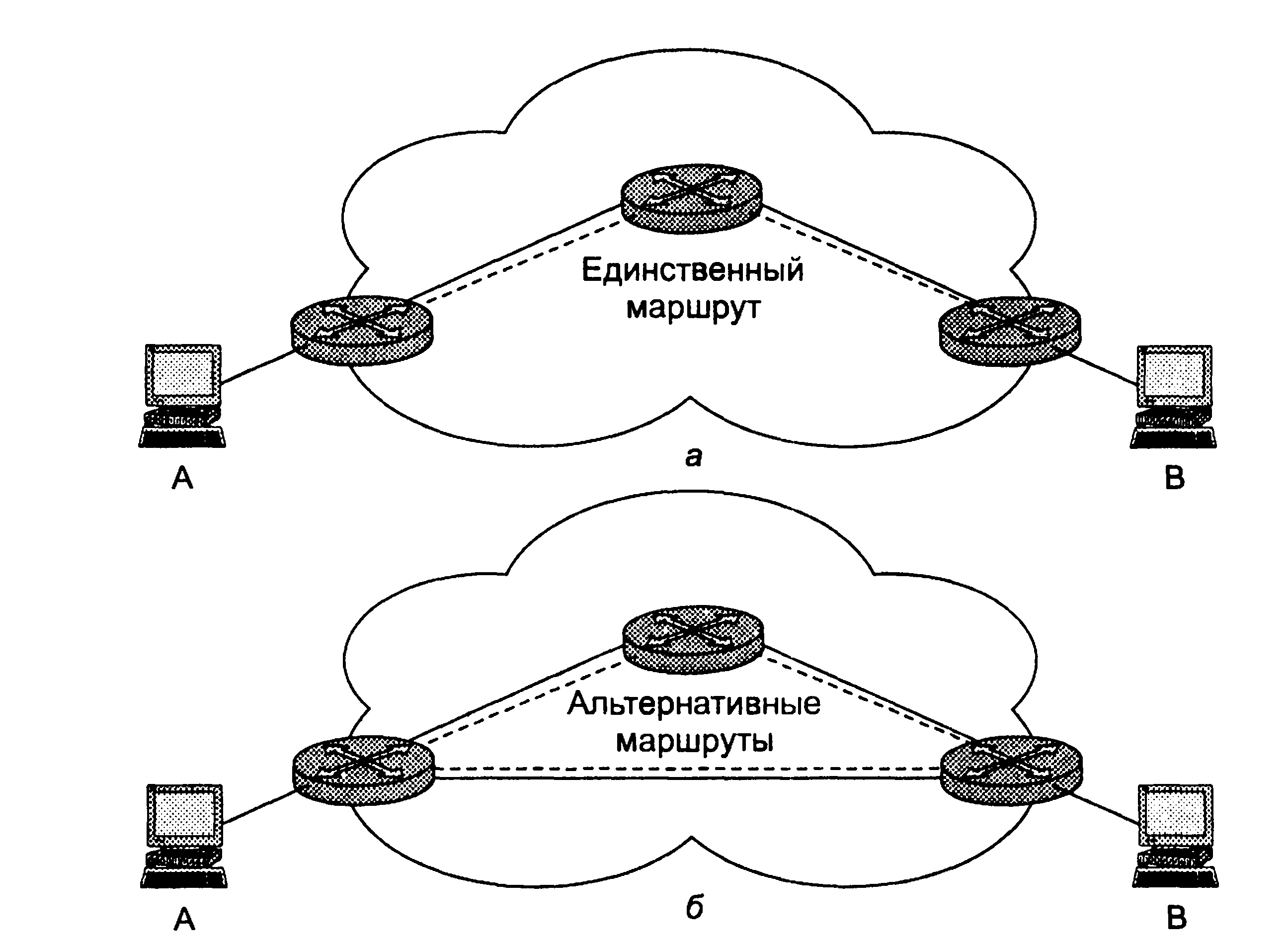
Доступность услуги можно улучшить двумя способами.

Первый состоит в использовании в сети надежных элементов, которые редко отказывают, но этот путь всегда ограничен возможностями технологии производства электронных компонентов (интегральных схем, печатных плат и т. п.).

Другой путь основан на введении избыточности в структуру системы: ключевые элементы системы должны существовать в нескольких экземплярах, чтобы при отказе одного из них функционирование системы обеспечивали другие. Поэтому коммутаторы и маршрутизаторы, работающие на магистрали сети, всегда строятся с использованием избыточных блоков — источников питания, процессоров и интерфейсов.

Для того чтобы обеспечить требуемый уровень доступности транспортного сервиса, поставщик должен иметь отказоустойчивую сеть. Другого пути здесь нет, так как в крупной системе, каковой является сеть, часто будут возникать отказы многочисленных составляющих ее элементов — каких-либо каналов или коммутаторов. Несмотря на то что эти элементы сами по себе являются отказоустойчивыми, предел их устойчивости может быть достигнут, и тогда сеть должна компенсировать их отказ другими средствами.

В хорошо спроектированной сети такими средствами являются альтернативные маршруты следования трафика. В примере сети на рис.1.1.5, а альтернативные пути для передачи трафика между точками А и В отсутствуют. Поэтому такой дизайн сети не обладает свойством отказоустойчивости, поставщику сети приходится полагаться только на отказоустойчивость каналов связи и коммутаторов на пути между А и В.

Рис.1.1.5. Альтернативные маршруты

В примере на рис.1.1.5, б сеть может передавать трафик между точками А и В по двум альтернативным маршрутам. Очевидно, что при отказе оборудования вдоль одного из маршрутов второй остается работоспособным, и сеть продолжает предоставлять услугу пользователю. При этом сеть может затратить некоторое время на переход от одного маршрута к другому. В течение переходного периода возможны потери пользовательского трафика, поэтому сокращение этого периода — одна из главных целей техники обеспечения отказоустойчивости сетей.

Существует несколько способов использования альтернативных маршрутов в сети.

Сеть определяет альтернативный маршрут только после отказа основного. Это означает, что в таблицах продвижения коммутаторов сети для каждого информационного потока определен только один маршрут. После отказа линии связи или коммутатора на пути следования этого потока коммутаторы сети с помощью некоторого протокола маршрутизации начинают поиск альтернативного пути. Обычно нахождение такого пути занимает десятки секунд или несколько минут — в зависимости от масштаба сети и сложности ее топологии. Это самый медленный способ использования альтернативных маршрутов, и очевидно, он связан с потерями пользовательских данных в переходный период.

Сеть заранее находит и использует два маршрута для определенного потока, образуя избыточный поток, незаметный для пользователя. Хотя данные передаются по обоим маршрутам, к пользователю попадают данные только одного. То есть один из маршрутов считается основным, другой — резервным. При отказе основного маршрута пользователь получает данные по резервному маршруту. Этот способ самый быстрый, поэтому он обеспечивает высшее качество обслуживания пользовательского потока. Однако он связан с большими потерями производительности сети, так как вместо одного потока сеть организует два. Обычно такой способ применяют для поддержания небольшого количества критически важных для пользователя потоков, которым требуется высокий уровень качества обслуживания и доступности сервиса.

Сеть заранее находит два маршрута, однако использует только один. При отказе основного маршрута переход на альтернативный маршрут происходит быстрее, чем при использовании первого способа, так как не тратится время на его поиск. Этот способ также гораздо более экономичен, чем второй. Но потери данных здесь выше, чем у второго способа, так как теряются те данные, которые уже были отправлены вдоль отказавшего маршрута.

В компьютерных сетях применяют в основном первый и третий способы использования альтернативных маршрутов. Технологии второго способа (два активных маршрута) задействуются в компьютерных сетях только тогда, когда к сетям предъявляются требования повышенной надежности. Широкое применение нашел второй способ в первичных высокоскоростных сетях, которые, как мы уже упоминали, были созданы для передачи телефонного трафика. Эти сети вносят свой существенный вклад в обеспечение высокого уровня доступности телефонных сетей, отсюда и особые требования к надежности.

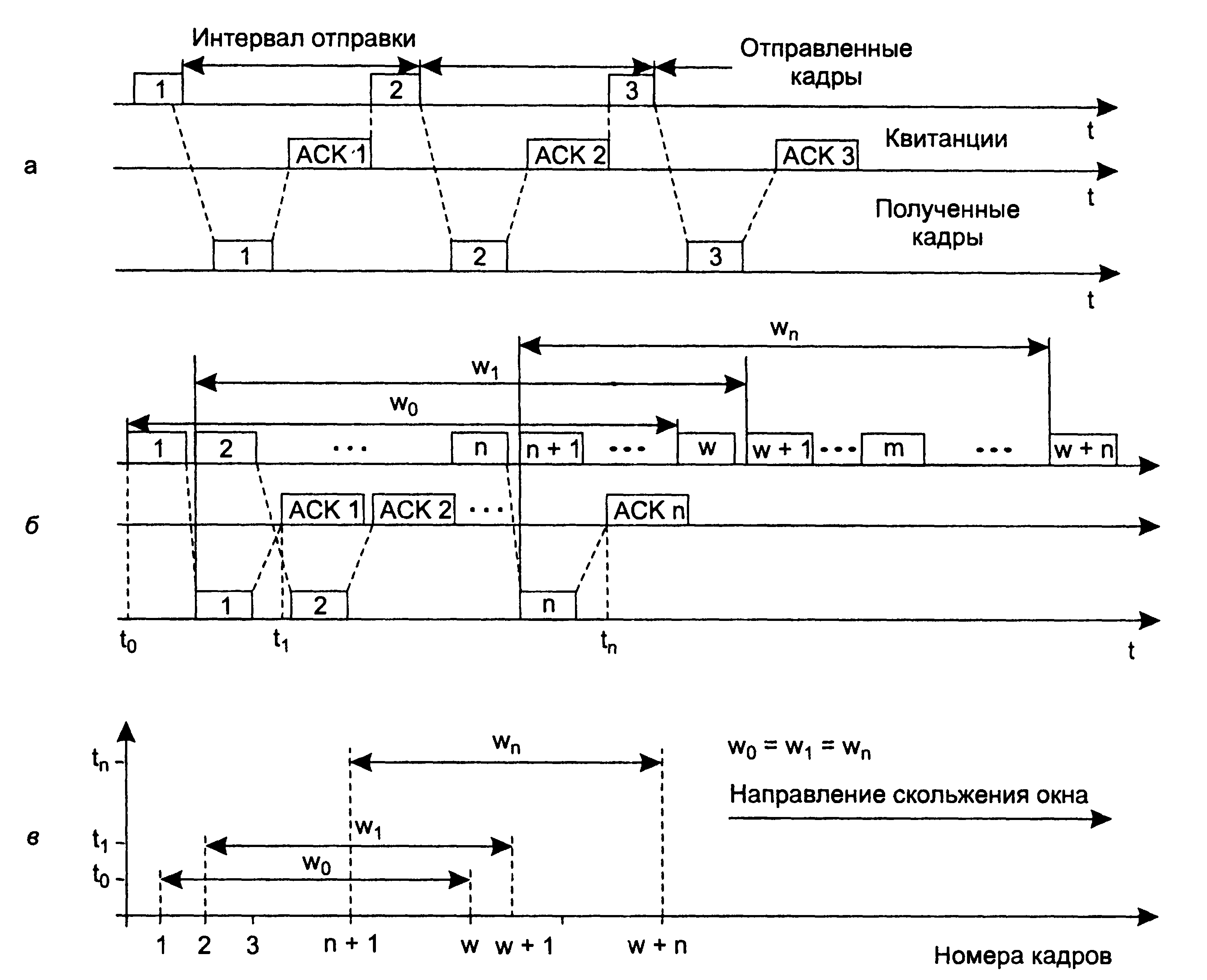
**Повторная передача и скользящее окно**

В тех случаях, когда другие методы обеспечения надежности не срабатывают и пакеты теряются, применяют методы повторной передачи пакетов. Эти методы требуют использования протоколов, ориентированных на соединение.

Чтобы убедиться в необходимости повторной передачи данных, отправитель нумерует отправляемые кадры и для каждого кадра ожидает от приемника так называемой положительной квитанции (Positive Acknowledgment, ACK) — служебного кадра, извещающего о том, что исходный кадр получен и данные в нем корректны. Для того чтобы организовать такую нумерацию, и нужна процедура логического соединения — она дает точку отсчета, с которой начинается нумерация. Время ожидания квитанции ограничено — при отправке каждого кадра передатчик запускает таймер, и, если по истечении заданного времени положительная квитанция на получена, кадр считается утерянным. Приемник в случае получения кадра с искаженными данными может отправить отрицательную квитанцию (Negative Acknowledgment, NACK) — явное указание на то, что данный кадр нужно передать повторно.

Существует два метода организации процесса обмена квитанциями: метод простоя источника и метод скользящего окна.

Метод простоя источника требует, чтобы источник, пославший кадр, ожидал получения квитанции (положительной или отрицательной) от приемника и только после этого посылал следующий кадр (или повторял искаженный). Если же квитанция не приходит в течение тайм-аута, то кадр (или квитанция) считается утерянным и его передача повторяется. На рис.1.1.6, а видно, что в этом случае производительность обмена данными ниже потенциально возможной, — хотя передатчик и мог бы послать следующий кадр сразу же после отправки предыдущего, он обязан ждать прихода положительной квитанции. (Далее, где это не искажает существо рассматриваемого вопроса, положительные квитанции для краткости будут называться просто «квитанциями».)

Рис.1.1.6. Методы восстановления искаженных и потерянных кадров

Недостатки этого метода коррекции особенно заметны на низкоскоростных каналах связи, то есть в территориальных сетях.

Второй метод называется методом скользящего окна (sliding window). В этом методе для повышения скорости передачи данных источнику разрешается передать некоторое количество кадров в непрерывном режиме, то есть в максимально возможном для источника темпе без получения на эти пакеты квитанций. Количество пакетов, которые разрешается передавать таким образом, называется размером окна. Рисунок 6.6, б иллюстрирует применение данного метода для окна размером W пакетов.

В начальный момент, когда еще не послано ни одного пакета, окно определяет диапазон пакетов с номерами от 1 до W включительно. Источник начинает передавать пакеты и получать в ответ квитанции. Для простоты предположим, что квитанции поступают в той же последовательности, что и пакеты, которым они соответствуют. В момент t1 при получении первой квитанции К1 окно сдвигается на одну позицию, определяя новый диапазон от 2 до (W + 1).

Процессы отправки пакетов и получения квитанций идут достаточно независимо друг от друга. Рассмотрим произвольный момент времени tn, когда источник получает квитанцию на пакет с номером п. Окно сдвигается вправо и определяет диапазон разрешенных к передаче пакетов от (n + 1) до (W + n). Все множество пакетов, выходящих из источника, можно разделить на перечисленные ниже группы (см. рис.1.1.6, б).

Пакеты с номерами от 1 до п уже были отправлены и квитанции на них получены, то есть они находятся за пределами окна слева.

Пакеты, начиная с номера (n + 1) и заканчивая номером (W + n), находятся в пределах окна и потому могут быть отправлены, не дожидаясь прихода какой-либо квитанции. Этот диапазон может быть разделен еще на два поддиапазона:

О пакеты с номерами от (n + 1) до m уже отправлены, но квитанции на них еще не получены;

О пакеты с номерами от m до (W + n) пока не отправлены, хотя запрета на это нет.

Все пакеты с номерами, большими или равными (W + n + 1), находятся за

пределами окна справа и поэтому пока не могут быть отправлены.

Перемещение окна вдоль последовательности номеров пакетов иллюстрирует рис.1.1.6, в. Здесь t0 — исходный момент, t1 и tn — моменты прихода квитанций на первый и n-й пакет соответственно. Каждый раз, когда приходит квитанция, окно сдвигается влево, но его размер при этом не меняется и остается равным W.

При отправке пакета в источнике устанавливается тайм-аут. Если за это время квитанция на отправленный пакет не придет, пакет (или квитанция на него) считается утерянным, и пакет передается снова.

Если же поток квитанций поступает регулярно в пределах допуска в W пакетов, то скорость обмена достигает максимально возможной величины для данного канала и принятого протокола.

В некоторых реализациях скользящего окна от приемника не требуется посылать квитанции на каждый принятый корректный пакет. Если среди пришедших пакетов нет «прогалин», то приемнику достаточно послать квитанцию только на последний принятый пакет, и эта квитанция будет свидетельствовать отправителю о том, что все предыдущие пакеты также дошли благополучно.

В других методах используются отрицательные квитанции. Отрицательные квитанции бывают двух типов — групповые и избирательные. Групповая квитанция содержит номер пакета, начиная с которого нужно повторить передачу всех пакетов, отправленных передатчиком в сеть. Избирательная отрицательная квитанция требует повторной передачи только одного пакета.

Метод скользящего окна имеет два параметра, которые могут существенно влиять на эффективность передачи данных между передатчиком и приемником, — это размер окна и величина тайм-аута ожидания квитанции. Выбор тайм-аута зависит не от надежности сети, а от задержек передачи пакетов сетью.

В надежных сетях, в которых пакеты искажаются и теряются редко, для повышения скорости обмена данными размер окна нужно увеличивать, так как при этом передатчик будет посылать пакеты с меньшими паузами. В ненадежных сетях размер окна следует уменьшать, так как при частых потерях и искажениях пакетов резко возрастает объем вторично передаваемых через сеть пакетов, а значит, пропускная способность сети во многом расходуется вхолостую, и полезная пропускная способность сети падает.

Размер окна может быть постоянным параметром алгоритма скользящего окна. В этом случае он выбирается при установлении соединения и не меняется в течение сеанса. Существуют также адаптивные версии алгоритма, когда размер окна меняется в течение сеанса в соответствии с текущим состоянием сети и узла назначения.

Надежность сети в подобных алгоритмах определяется по таким признакам потерь пакетов, как истечение тайм-аута для положительной квитанции или приходе дубликата квитанции на определенный пакет. Дубликат говорит о том, что в узле назначения истек тайм-аут ожидания очередного пакета, и узел запрашивает отправку этого пакета вторично. При наступлении таких событий узел отправитель уменьшает размер окна, стараясь найти оптимальный режим передачи данных.

Размер окна может быть также изменен узлом назначения. Причиной уменьшения размера окна является перегрузка узла назначения, который не успевает обработать поступающие пакеты. Мы вернемся к этой проблеме позже, в разделе «Обратная связь» главы 7, когда будем изучать методы борьбы с перегрузками.

Существуют также реализации метода скользящего окна, в которых в качестве размера окна используется не количество пакетов, а количество байтов. Наиболее известным примером такого подхода является протокол TCP.

В общем случае метод скользящего окна более сложен в реализации, чем метод простоя источника, так как передатчик должен хранить в буфере все пакеты, на которые пока не получены положительные квитанции. Кроме того, при использовании данного метода требуется отслеживать несколько параметров алгоритма: размер окна W, номер пакета, на который получена квитанция, номер пакета, который еще можно передать до получения новой квитанции.

**Безопасность**

Список ключевых слов: уровень защищенности, компьютерная безопасность, сетевая безопасность, брандмауэр, конфиденциальность, доступность,

целостность, шифрование, криптосистема, аутентификация, электронная подпись, идентификация, авторизация, аудит, защищенный канал.

Компьютерные сети — замечательное средство доступа к самой разнообразной информации, а также средство общения. Однако, как и у каждой красивой медали, у компьютерных сетей есть и обратная сторона. Она проявляется в разнообразных потенциальных угрозах целостности и конфиденциальности информации, которую вы доверяете сети. Например, предприятия, имеющие постоянное соединение с Интернетом, регулярно страдают от атак злоумышленников на их информационные ресурсы. Подвергаются атакам и пользователи, соединяющиеся с Интернетом по модему на небольшое время. Информация, находящаяся на их компьютерах, также может пострадать от вирусов, «живущих» в почтовых сообщениях или проникающих через «дырки» в системах мгновенной доставки сообщений, таких как ICQ.

*Немного статистики*

*В отчете о проблемах и тенденциях в сферах компьютерной преступности и безопасности за 2002 год (Issues and Trends: 2002 CSI/FBI Computer Crime and Security Survey), опубликованном в апреле 2002 года, отмечается резкий рост числа обращений в правоохранительные органы по поводу компьютерных преступлений. 90 % респондентов (преимущественно из крупных компаний и правительственных структур) сообщили, что за последние 12 месяцев в их организациях имели место нарушения информационной безопасности; 80 % констатировали финансовые потери от этих нарушений; 44 % (223 респондента) смогли и/или захотели оценить потери количественно — общая сумма составила более 455 млн долларов.*

Злоумышленники, которые пытаются получить несанкционированный доступ к информации или разрушить ее, могут использовать для атак не только Интернет, но и корпоративную сеть. Действительно, никогда нельзя ручаться за то, что кто-нибудь из служащих предприятия не захочет превысить свои служебные полномочия и попытаться прочитать документ, который он не имеет права читать. Возможны также попытки разрушить информацию предприятия изнутри (стереть файлы, вывести из строя компьютер и т. п.).

Очевидно, что пользователи сети хотели бы, чтобы их информация была надежно защищена от такого рода инцидентов. Уровень защищенности информации пользователя сетевых услуг является еще одной важной характеристикой сети. Защищенность не является количественной характеристикой, ее можно оценить только качественно — высокий (средний, низкий) уровень защищенности. Обычно уровень защищенности информации в определенной сети оценивается экспертом.

Компьютерная и сетевая безопасность

При всем своем многообразии средства защиты информации делятся на два больших класса:

средства компьютерной безопасности предназначены для защиты внутренних информационных ресурсов, находящихся в локальной сети или на отдельном компьютере пользователя;

средства сетевой безопасности предназначены для защиты информации в процессе ее передачи через сеть.

Это деление достаточно естественное, так как функции по обеспечению безопасности в этих двух случаях существенно различаются. В первом случае нужно защитить от несанкционированного доступа все ресурсы, находящиеся внутри собственной локальной сети. Это — аппаратные ресурсы (серверы, дисковые массивы, маршрутизаторы), программные ресурсы (операционные системы, СУБД, почтовые службы и т. п.) и сами данные, хранящиеся в файлах и обрабатываемые в оперативной памяти. Очевидно, что для этого необходимо контролировать трафик, входящий в сеть из публичной сети (сегодня это преимущественно Интернет), и стараться перекрыть доступ извне для любой информации, с помощью которой злоумышленник может попытаться использовать внутренние ресурсы сети во вред их владельцу.Наиболее часто используемым средством защиты этого типа является брандмауэр, устанавливаемый в местах всех соединений внутренней сети с Интернетом. Брандмауэр (firewall) представляет собой межсетевой экран, который контролирует обмен сообщениями, ведущийся по протоколам всех уровней, и не пропускает подозрительный трафик в сеть.

Брандмауэр может использоваться и внутри сети, защищая одну подсеть от другой, что может быть необходимо в крупных компаниях с достаточно независимыми подразделениями. Помимо брандмауэра аналогичные проблемы призваны решать встроенные средства безопасности операционных систем и приложений, таких как базы данных, а также встроенные аппаратные средства компьютера.

В плане обеспечения сетевой безопасности приходится защищать информацию, которая находится вне пределов нашей досягаемости, а в виде IP-пакетов «путешествует» через сети поставщиков услуг Интернета. Интернет сегодня используется предприятиями не только как сверхмощный источник информации, хранящейся на многочисленных веб-сайтах, но и как дешевая транспортная среда, позволяющая объединить сеть центрального отделения с сетями филиалов, а также подключить к ресурсам предприятия телекомьютеров — сотрудников, находящихся дома или в командировке работающих с корпоративной сетью удаленно. При этом во многих случаях предприятию жизненно важно, чтобы передаваемая через Интернет информация не была искажена, уничтожена или просмотрена посторонними людьми. Для решения этой задачи сегодня широко используется механизм виртуальных частных сетей (VPN).

Автономно работающий компьютер можно эффективно защитить от внешних покушений разнообразными способами, например просто заперев на замок клавиатуру или сняв жесткий накопитель и поместив его в сейф. Компьютер, работающий в сети, по определению не может полностью отгородиться от мира, он должен общаться с другими компьютерами, возможно, даже удаленными от него на большое расстояние, поэтому обеспечение безопасности в сети является задачей значительно более сложной. Логический вход чужого пользователя в ваш компьютер является штатной ситуацией, если вы работаете в сети. Обеспечение безопасности в такой ситуации сводится к тому, чтобы сделать подобное проникновение контролируемым — каждому пользователю сети должны быть четко определены его права на доступ к информации, внешним устройствам, на выполнение системных действии на каждом из компьютеров сети.

Помимо проблем, порождаемых возможностью удаленного входа в сетевые компьютеры, сети по своей природе подвержены еще одному виду опасности — перехвату и анализу передаваемых по сети сообщений, а также созданию «ложного» трафика. Большая часть средств обеспечения сетевой безопасности направлена на предотвращение именно этого типа нарушений.

Вопросы сетевой безопасности приобретают особое значение сейчас, когда проектировщики корпоративных сетей все чаще отказываются от выделенных линий в пользу транспортных возможностей публичных сетей (Интернет, frame relay).

Конфиденциальность, целостность и доступность данных

Безопасная информационная система — это система, которая, во-первых, защищает данные от несанкционированного доступа, во-вторых, всегда готова предоставить их своим пользователям, в-третьих, надежно хранит информацию и гарантирует неизменность данных. Таким образом, безопасная система по определению обладает свойствами конфиденциальности, доступности и целостности.

Конфиденциальность (confidentiality) — гарантия того, что секретные данные будут доступны только тем пользователям, которым этот доступ разрешен (такие пользователи называются авторизованными).

Доступность (availability) — гарантия того, что авторизованные пользователи всегда получат доступ к данным.

Целостность (integrity) — гарантия сохранности данными правильных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом изменять, модифицировать, разрушать или создавать данные.

Целью злоумышленников может быть нарушение каждой их составляющих информационной безопасности — доступности, целостности или конфиденциальности. Требования безопасности могут меняться в зависимости от назначения системы, характера используемых данных и типа возможных угроз. Трудно представить систему, для которой были бы не важны свойства целостности и доступности, но свойство конфиденциальности не всегда является обязательным. Например, если вы публикуете информацию в Интернете на веб-сервере и вашей целью является сделать ее доступной для самого широкого круга людей, то конфиденциальность в данном случае не требуется. Однако требования целостности и доступности остаются актуальными.

Действительно, если вы не предпримете специальных мер по обеспечению целостности данных, злоумышленник может, например, внести такие изменения в помещенный на веб-сайте прайс-лист, которые снизят конкурентоспособность вашего предприятия, или испортить коды свободно распространяемого вашей фирмой программного продукта, что, безусловно, скажется на ее деловом имидже.

Не менее важной в данном примере является и доступность данных. Затратив немалые средства на создание и поддержание сервера в Интернете, предприятие вправе рассчитывать на отдачу: увеличение числа клиентов, количества продаж и т. д. Однако существует вероятность того, что злоумышленник предпримет атаку, в результате которой помещенные на сервер данные станут недоступными для тех, кому они предназначались. Примером таких злонамеренных действий может служить «бомбардировка» сервера IP-пакетами с неправильным обратным адресом, которые в соответствии с логикой работы протокола IP могут вызывать тайм-ауты и, в конечном счете, сделать сервер недоступным для всех остальных запросов.

ПРИМЕЧАНИЕ

Понятия конфиденциальности, доступности и целостности могут быть определены не только по отношению к информации, но и к другим ресурсам вычислительной сети, например внешним устройствам или приложениям. Возможность «незаконного» использования такого рода ресурсов способна привести к нарушению безопасности системы. Свойство конфиденциальности, примененное к устройству печати, означает, что доступ к нему имеют те и только те пользователи, которым этот доступ разрешен, причем они могут выполнять только те операции с устройством, которые для них определены. Свойство доступности устройства интерпретируется как его готовность к использованию всякий раз, когда в этом возникает необходимость. Благодаря свойству целостности злоумышленник не может изменить параметры настройки устройства, что могло бы привести к изменению очередности работ и даже к выводу устройства из строя. Легальность использования сетевых устройств важна не только постольку, поскольку она влияет на безопасность данных. Устройства могут предоставлять различные услуги (распечатка текстов, отправка факсов, доступ в Интернет, электронная почта и т. п.), незаконное потребление которых наносит материальный ущерб, что также является нарушением безопасности предприятия.

Сервисы сетевой безопасности

В разных программных и аппаратных продуктах, предназначенных для защиты данных; часто используются одинаковые подходы, приемы и технические решения. Такие средства, называемые также сервисами сетевой безопасности, решают самые разнообразные задачи по защите системы, обеспечивая, например, контроль доступа, включающий процедуры аутентификации и авторизации, аудит, шифрование информации, антивирусную защиту, контроль сетевого трафика и пр. Технические средства безопасности могут быть либо встроены в программное (операционные системы и приложения) и аппаратное (компьютеры и коммуникационное оборудование) обеспечение сети, либо реализованы в виде отдельных продуктов, созданных специально для решения проблем безопасности. Определим основные из них.

Шифрование — это краеугольный камень всех систем информационной безопасности, будь то система аутентификации или авторизации, защищенный канал или система безопасного хранения данных. Любая процедура шифрования, превращающая информацию из обычного «понятного» вида в «нечитабельный» зашифрованный вид, естественно должна быть дополнена процедурой дешифрирования, которая после применения к зашифрованному тексту снова делает его «понятным». Пара процедур — шифрование и дешифрирование — называется криптосистемой.

Аутентификация предотвращает доступ к сети нежелательных лиц и разрешает вход для легальных пользователей. Термин «аутентификация» в переводе с латинского означает «установление подлинности». В качестве объектов, требующих аутентификации, могут выступать не только пользователи, но и различные устройства, приложения, текстовая и другая информация. Так, пользователь, обращающийся с запросом к корпоративному серверу, должен доказать ему свою легальность, но он также должен убедиться сам, что ведет диалог действительно с сервером своего предприятия. Другими словами, сервер и клиент должны пройти процедуру взаимной аутентификации. Здесь мы имеем дело с аутентификацией на уровне приложений. При установлении сеанса связи между двумя устройствами также часто предусматриваются процедуры взаимной аутентификации на более низком, канальном уровне. Аутентификация данных означает доказательство целостности этих данных, а также факт их поступления именно от того человека, который объявил об этом. Для этого используется механизм электронной подписи. Аутентификацию следует отличать от идентификации.

Идентификация заключается в сообщении пользователем системе своего идентификатора, в то время как аутентификация — это процедура доказательства пользователем того, что он является тем, за кого себя выдает, в частности доказательство того, что именно ему принадлежит введенный им идентификатор. Идентификаторы пользователей применяются в системе с теми же целями, что и идентификаторы любых других объектов (файлов, процессов, структур данных), и они не всегда связаны непосредственно с обеспечением безопасности.

Авторизация — процедура контроля доступа легальных пользователей к ресурсам системы с предоставлением каждому из них именно тех прав, которые определены ему администратором. Помимо предоставления пользователям прав доступа к каталогам, файлам и принтерам, система авторизации может контролировать возможность выполнения пользователями различных системных функций, таких как локальный доступ к серверу, установка системного времени, создание резервных копий данных, выключение сервера и т. п.

Аудит — фиксация в системном журнале событий, связанных с доступом к защищаемым системным ресурсам. Подсистема аудита современных ОС позволяет дифференцированно задавать перечень интересующих администратора событий с помощью удобного графического интерфейса. Средства учета и наблюдения обеспечивают возможность обнаружить и зафиксировать важные события, связанные с безопасностью; любые попытки (в том числе и неудачные) создать, получить доступ или удалить системные ресурсы.

Технология защищенного канала обеспечивает безопасность передачи данных по открытой транспортной сети, например по Интернету, за счет:

* взаимной аутентификации абонентов при установлении соединения;
* защиты передаваемых по каналу сообщений от несанкционированного доступа;
* обеспечения целостности поступающих по каналу сообщений.

Характеристики сети поставщика услуг

Список ключевых слов: расширяемость сети, масштабируемость сети, управляемость сети, совместимость, или интегрируемость, сети.

Рассмотрим основные характеристики, которыми оперирует поставщик услуг, оценивая эффективность своей сети. Эти характеристики часто являются качественными, то есть не могут быть выражены числами и соотношениями.

Расширяемость и масштабируемость

Термины «расширяемость» и «масштабируемость» иногда неверно используют как синонимы.

Расширяемость означает возможность сравнительно легкого добавления отдельных компонентов сети (пользователей, компьютеров, приложений, служб), наращивания длины сегментов кабелей и замены существующей аппаратуры более мощной.

При этом принципиально важно, что легкость расширения системы иногда может обеспечиваться в определенных пределах. Например, локальная сеть Ethernet, построенная на основе одного разделяемого сегмента толстого коаксиального кабеля, обладает хорошей расширяемостью в том смысле, что позволяет легко подключать новые станции. Однако такая сеть имеет ограничение на число станций — оно не должно превышать 30-40. Хотя сеть допускает физическое подключение к сегменту и большего числа станций (до 100), при этом резко снижается производительность сети. Наличие такого ограничения и является признаком плохой масштабируемости системы при ее хорошей расширяемости.

Масштабируемость означает, что сеть позволяет наращивать количество узлов и протяженность связей в очень широких пределах, при этом производительность сети не ухудшается.

Для обеспечения масштабируемости сети приходится применять дополнительное коммуникационное оборудование и специальным образом структурировать сеть. Обычно масштабируемое решение обладает многоуровневой иерархической структурой, которая позволяет добавлять элементы на каждом уровне иерархии без изменения главной идеи проекта.

Примером хорошо масштабируемой сети является Интернет, технология которого (TCP/IP) оказалась способной поддерживать сеть в масштабах земного шара. Организационная структура Интернета, которую мы рассмотрели в главе 5, образует несколько иерархических уровней: сети пользователей, сетей локальных поставщиков услуг и так далее вверх по иерархии вплоть до сетей межнациональных поставщиков услуг. Технология TCP/IP, на которой построен Интернет, также позволяет строить иерархические сети. Основной протокол Интернета (IP) основан на двухуровневой модели: нижний уровень составляют отдельные сети (чаще всего сети корпоративных пользователей), а верхний уровень — это составная сеть, объединяющая эти сети. Стек TCP/IP поддерживает также концепцию автономной системы. В автономную систему входят все составные сети одного поставщика услуг, так что автономная система представляет собой более высокий уровень иерархии. Наличие автономных систем в Интернете позволяет упростить решение задачи нахождение оптимального маршрута — сначала ищется оптимальный маршрут между автономными системами, а затем каждая автономная система находит оптимальный маршрут внутри себя.

Не только сама сеть должна быть масштабируемой, но и устройства, работающие на магистрали сети, также должны обладать этим свойством, так как рост сети не должен приводить к необходимости постоянной смены оборудования. Поэтому магистральные коммутаторы и маршрутизаторы строятся обычно по модульному принципу, позволяя наращивать количество интерфейсов и производительность обработки пакетов в широких пределах.

Управляемость

Управляемость сети подразумевает возможность централизованно контролировать состояние основных элементов сети, выявлять и разрешать проблемы, возникающие при работе сети, выполнять анализ производительности и планировать развитие сети. Управляемость подразумевает наличие в сети некоторых автоматизированных средств администрирования, которые взаимодействуют с программным и аппаратным обеспечением сети с помощью коммуникационных протоколов.

В идеале средства администрирования сети представляют собой систему, осуществляющую наблюдение и контроль за каждым элементом сети — от простейших до самых сложных устройств, при этом сеть рассматривается как единое целое, а не как разрозненный набор отдельных устройств.

Хорошая система администрирования наблюдает за сетью и, обнаружив проблему, активизирует определенное действие, исправляет ситуацию и уведомляет администратора о том, что произошло и какие шаги предприняты. Одновременно с этим система администрирования должна накапливать данные, на основании которых можно планировать развитие сети. Наконец, система администрирования должна быть независима от производителя и обладать удобным интерфейсом, позволяющим выполнять все действия с одной консоли.

Решая тактические задачи, администраторы и технический персонал сталкиваются с ежедневными проблемами обеспечения работоспособности сети. Эти задачи требуют быстрого решения, обслуживающий сеть персонал должен оперативно реагировать на сообщения о неисправностях, поступающих от пользователей или автоматических средств администрирования сети. Постепенно становятся заметными более общие проблемы производительности, конфигурирования сети, обработки сбоев и безопасности данных, требующие стратегического подхода, то есть планирования сети. Планирование, кроме того, подразумевает умение прогнозировать изменения в требованиях пользователей к сети, решение вопросов применения новых приложений, новых сетевых технологий и т. п.

Совместимость, или интегрируемость, сети означает, что сеть способна включать в себя самое разнообразное программное и аппаратное обеспечение, то есть в ней могут сосуществовать различные операционные системы, поддерживающие разные стеки коммуникационных протоколов, а также аппаратные средства и приложения от разных производителей. Сеть, состоящая из разнотипных элементов, называется неоднородной, или гетерогенной, а если гетерогенная сеть работает без проблем, то она является интегрированной. Основной путь построения интегрированных сетей — использование модулей, выполненных в соответствии с открытыми стандартами и спецификациями.

Выводы

Главным требованием, предъявляемым к компьютерной сети, является обеспечение высокого качества предоставляемых сетью услуг. При широком понимании в понятие «качество обслуживания» включают все возможные характеристики услуг и сети, желательные для пользователя.

Формализованные характеристики позволяют обоснованно судить о качестве сетевых услуг. Требования к качеству услуг выражаются с помощью значений формализованных характеристик.

Качество транспортных услуг оценивается характеристиками четырех групп:

* производительность;
* надежность;
* безопасность;

характеристики сети поставщика услуг (сюда входят расширяемость, масштабируемость, управляемость, совместимость).

Производительность сети оценивается с помощью статистических характеристик двух типов: характеристик скорости передачи информации и характеристик задержек передачи пакетов. В первую группу входит средняя скорость и максимальная скорость на периоде пульсации, а также длительность этого периода. Во вторую группу входят: средняя величина задержки,

* конфиденциальность — гарантия того, что секретные данные будут доступны только тем пользователям, которым этот доступ разрешен (такие пользователи называются авторизованными);
* доступность — гарантия того, что авторизованные пользователи всегда получат доступ к данным;
* целостность — гарантия сохранности данными правильных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом изменять, модифицировать, разрушать или создавать данные.

Для защиты информации в сетях используются механизмы шифрования, аутентификации, авторизации и аудита. Передача данных через сеть осуществляется с помощью комбинированной техники защищенного канала.

# Вопросы и упражнения

1. Чем характеристика отличается от требования?

2. Какие характеристики входят в понятие «качество обслуживания» при его широкой трактовке?

3. Что объединяет характеристики QoS в узком значении этого термина?

4. Назовите характеристики качества обслуживания, которые интересуют только пользователя? Только поставщика услуг? И пользователя, и поставщика?

5. Какие характеристики производительности интересуют только поставщика услуг?

6. Между какими сторонами заключается соглашение об уровне обслуживания?

7. Предложите набор характеристик, которые вы хотели бы видеть в SLA, если вы хотите передавать через сеть трафик IР-телефонии.

8. Какой вид представления информации используется для результатов измерений задержек пакетов?

9. В чем преимущество использования такой характеристики, как коэффициент вариации по сравнению с джиттером?

10. Какая составляющая не учитывается при определении времени оборота?

11. Может ли трафик передаваться с большими задержками, но без джиттера?

12. Назовите параметры пульсации. Все ли эти параметры являются независимыми?

13. Зависит ли средняя скорость потока от величины задержек пакетов?

14. Какая характеристика надежности транспортной услуги используется в краткосрочном периоде, а какая в среднесрочном?

15. Опишите два основных подхода к обеспечению надежности сети.

16. Сколько существует основных способов использования альтернативных маршрутов для повышения надежности передачи трафика? Каковы их достоинства и недостатки?

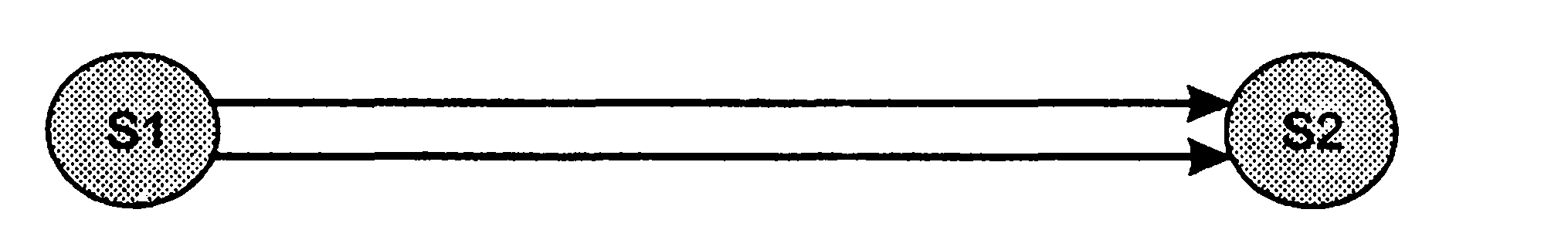
17. Назовите две составляющие информационной безопасности.

18. Объясните разницу между масштабируемостью и расширяемостью.

19. Два коммутатора для повышения надежности связаны двумя физическими

каналами (рис.1.1.7). Оцените объем потерянных данных при отказе канала для двух вариантов использования этих каналов в качестве альтернативных маршрутов:

* по схеме, в которой сеть заранее находит и использует оба маршрута;
* по схеме, в которой сеть заранее находит оба маршрута, однако использует только один.

Рис.1.1.7. Альтернативные маршруты

Протяженность каждого канала составляет 5000 км, скорость передачи данных — 155 Мбит/с, скорость распространения сигнала в канале равна 200 000 км/с. В обоих случаях коммутатор S2 обнаруживает факт отказа канала и переключается на резервный канал за 10 мс.

20. Оцените коэффициент использования канала, если данные по нему передаются с помощью протокола, использующего алгоритм простоя источника. Скорость передачи данных равна 100 Мбит/с, время оборота составляет 10 мс, пакеты не теряются и не искажаются. Размер пакета фиксирован и равен 1500 байт. Размером квитанции можно пренебречь.

21. Определите минимальный размер окна, который позволяет передавать пакеты по каналу без простоя источника. Скорость передачи данных равна 100 Мбит/с, время оборота составляет 10 мс, пакеты не теряются и не искажаются. Размер пакета фиксирован и равен 1500 байт. Размером квитанции можно пренебречь.

## 1.2 Эксплуатация технических средств сетевой инфраструктуры

**1.2 Эксплуатация технических средств сетевой инфраструктуры**

Физические аспекты эксплуатации

Построение любой сети требует укладки кабеля, соединения различных узлов и единиц техники, создание грамотной и эффективной топологии сети. Важную роль в этом процессе играет сетевое оборудование. Огромное количество разнообразных устройств, техники и прочих элементов входит в это понятие. Все это разделяется на пассивное и активное оборудование.

Условно можно разделить на активное и пассивное оборудования.

Активное оборудование— «интеллектуальное» и часто управляемое сетевое оборудование. Его отличительная черта — необходимость потребления электроэнергии. Соответственно, обязательной частью этой группы элементов СКС являются источники бесперебойного питания (ИБП).

Пассивное оборудование**.** В эту группу входят компоненты, не требующие потребления электроэнергии. Сюда входит оборудование, служащее для передачи сигнала (кабельные компоненты), и приспособления для его структурирования, защиты и обслуживания.

**Пассивное сетевое оборудование**

Одного определения, что такое «пассивное сетевое оборудование» не существует. К этой группе относят компоненты для построения СКС, не потребляющие электроэнергию. Пассивное Сетевое Оборудование – это оборудование, основная функция которого состоит в обеспечении передачи сигнала – а именно проводники и приспособления для их организации и защиты: кабель, Патч-корды, розетки, конвекторы, патч-панели, кабель-каналы и т.п (рис.2.1.1).

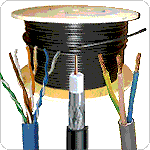


Рис.2.1.1 – Кабель

Структурированная кабельная система начинается с кабеля. Это основная и наиболее протяженная ее часть. В СКС применяется два основных типа информационных кабелей: медные и оптоволоконные. К первому типу относятся используемый в телекоммуникации коаксиальный кабель, телефонный кабель и самый распространенный сетевой кабель – витая пара (UTP). Второй – это оптоволокно, наиболее совершенная на сегодняшний день среда передачи информации. Оптоволокно дороже, сложнее в монтаже, требует бережного обращения, но его впечатляющая пропускная способность и низкие потери с лихвой компенсируют эти недостатки. Область применения оптического кабеля – это магистральные трассы, по которым передается большое количество данных. Витая пара проще, неприхотливее, и используется там, где нет смысла прокладывать оптоволокно. Для того, чтобы защитить информационный кабель, его укладывают в кабельные лотки, кабель-каналы (короба).

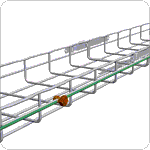


Рис.2.1.2 – Кабельные лотки

Пластиковые (ПВХ) и металлические лотки и короба защищают информационный кабель от повреждений, изломов, агрессивного воздействия внешней среды и доступа посторонних. На магистральных трассах и в технических помещениях в основном используются металлические лотки (оцинкованные, неоцинкованные или из нержавеющей стали.), ввиду их большой вместимости. Закрытые металлические лотки применяются также для защиты от внешних электромагнитных помех, так как они являются экраном. Лотки могут быть сетчатыми, перфорированными или цельными, закрытыми или открытыми – в зависимости от места, где они употребляются: улица, надпотолочное пространство, кабельная шахта и др.

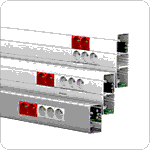


Рис.2.1.3 – Кабель-каналы

Внутри помещений, там, где кабель необходимо подвести к конечному пользователю, применяются меньшие по размерам пластиковые кабель каналы (короба). Они более привлекательны и хорошо вписываются в интерьер. Дизайн и цвет подбирается по вкусу, от стандартного глянцевого белого до любых современных расцветок и фактур. Такие свойства кабель канала, как низкая цена, простота монтажа, быстрый доступ к кабелям и пожаробезопасность сделали его распространение повсеместным.

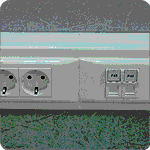


Рис.2.1.4 – Розетка

Конечная точка, к которой подводится кабель-канал или скрытый за стеной кабель – это сетевая розетка. Розетка встраивается в стену и надежно фиксирует подключаемые к ней кабели. Стандартный разъем компьютерной розетки – под коннектор RJ 45 (8Р8С), телефонной – RJ 11 или RJ 12. Основная функция розетки – упорядочивать информационные кабели в помещении и обеспечивать надежное подключение патч-корда.

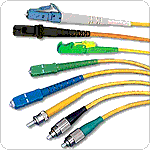


Рис.2.1.5 – Патч-корд

Патч-корд – это коммутационный кабель, соединяющий конечного пользователя с сетью, или использующийся для подключения активного сетевого оборудования. Тип Патч-корд соответствует типу используемого кабеля: витой пары, телефонного или оптического. Требования к качеству его изготовления очень высоки. Для того чтобы самостоятельно обжать даже относительно простой Патч-корд из витой пары, необходим профессиональный инструмент для зачистки кабеля и обжима конвекторов. Оптические же Патч-корды гораздо сложнее. Поэтому правильнее использовать готовые заводские Патч-корд. Они намного прочнее, переносят больше циклов переключений, для чего оснащены специальными «хвостовиками». «Хвостовики» позволяют выдергивать Патч-корд из разъема без риска выдернуть сам кабель из коннектора, или нарушить какой-либо контакт (как это может случиться с самодельными аналогами).



Рис.2.1.6 – Коннектор

Разъемы, находящиеся на концах

Патч-корд, называются коннекторами. Коннектор RJ 45, стандарт витой пары (UTP), обжимается согласно цветовой схеме «распиловкой». Для его подключения в основном используется прямая, реже – обратная схема обжима. К стандартным оптическим коннекторам относят следующие типы: ST, SC, LC, FC и FDDI. Они монтируются на концы оптического кабеля методом химической сварки, либо механической фиксации. Для подключения тонкого коаксиального кабеля используются в основном ВNС-коннекторы. Они либо припаиваются, либо обжимаются на конце кабеля.

Основные разновидности коаксиальных коннекторов: Т-образный, соединяющий сетевой кабель с сетевой платой; баррел-коннектор применяющийся для сращивания двух отрезков кабеля; и терминатор (заглушка), устанавливающаяся на концах кабеля. Кабели, идущие от конечных пользователей, обычно группируются на патч-панели.

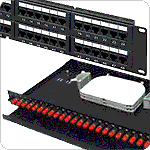


Рис.2.1.7 – Патч-панель

Коммутационная Патч-панель – это неотъемлемый элемент СКС, упорядочивающий ее и облегчающий обслуживание. Патч-панели объединяют все кабели, идущие от рабочих мест, которые затем подключаются к портам активного сетевого оборудования. Коммутация осуществляется патч-кордами. Патч-панель позволяет легко поменять определенные кабели, не задевая проходящих рядом линий. Достаточно просто переключить один или несколько патч-кордов на панели. Стандартная коммутационная панель имеет 12, или кратное 12ти количество разъемов (портов) и монтируется в 19-дюймовую стойку, но бывают и настенные панели. Монтаж кабеля и расшивка патч-панели производится с помощью обжимного инструмента.

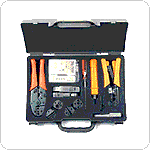


Рис.2.1.8 – Обжимной инструмент

Невозможно заниматься профессиональным монтажом, не имея профессионального инструмента. Сюда входят: нож для зачистки витой пары (UTP)от оболочки, клещи для обжима коннекторов, а также тестер – оборудование для проверки, с помощью которого обжатая витая пара проверяется на работоспособность, или устанавливается причина неисправности. Надежно обжатая витая пара, в итоге, дает соединение без потерь, что положительно сказываются на работоспособности всей системы.

**Активное сетевое оборудование**

Значение средств связи и сетевых коммуникаций в жизнедеятельности современной успешной компании сложно переоценить. На сегодня проблема выбора сетевого оборудования приобретает все большую актуальность при построении надежной и легко масштабируемой инфраструктуры организаций. Как правило, для крупных и малых организаций существует ряд типовых задач по созданию вычислительных и телефонных сетей, таких как:

* Создание локальной сети в рамках офиса или здания;
* Объединение в единую сеть группу разрозненных филиалов компании;
* Создание единого центра коммутации вычислительных и телефонных сетей;
* Повышение безопасности и контроля существующей сети;
* Интеграция различных каналов передачи данных в единую сеть (fiberchanel, Ethernet, wi-fi,3g, wimax);

На сегодняшний день представлена масса разнообразного оборудования, от usb-ethernet адаптеров до, многозадачных модульных маршрутизаторов корпоративного уровня.

Виды активного сетевого оборудования и их применение для различных задач:

* + Сетевые Коммутаторы 2 уровня или (switch) – устройства, служащие для объединения компьютеров в пределах одной сети. Подходят для создания локальной сети в офисе или объединения нескольких офисов в пределах одного здания.



Рис.2.1.9 – Сетевой коммутатор 2 уровня - Cisco 2960-48TT



Рис.2.1.10 – Сетевой коммутатор 2 уровня - HP A3100 EI Switch Series



Рис.2.1.11 – Сетевой коммутатор 2 уровня - D-link - DGS-3024

* Сетевые коммутаторы 3 уровня – особый тип сетевого оборудования, способный объединять несколько различных сетей, требует специализированной настройки, но в ряде случаев способен заменить такое устройство как маршрутизатор, более дороге по стоимости и обслуживанию. Подходит для объединения в единую сеть нескольких филиалов имеющих различные подсети в условиях стабильной топологии сети.



Рис.2.1.12 – Сетевой коммутатор 3 уровня - HP E2910 al Switch Series

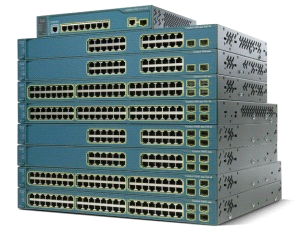


Рис.2.1.13 – Сетевой коммутатор 3 уровня - cisco Catalyst 3650



Рис.2.1.14 – Сетевой коммутатор 3 уровня - D-link - DES-3828

Маршрутизаторы – это преимущественно устройства корпоративного класса, способные динамически объединять различные сети, фильтровать, транслировать и шифровать данные, передаваемые по сети. Маршрутизаторы являются устройствами самого высокого уровня, которые используются интернет-провайдерами, и крупными организациями с целью объединения и контроля над группой сетей. Лидером на рынке является компания Cisco. В арсенале компании Cisco имеется довольно широкий целевой диапазон оборудования от офисных решений до обеспечения работы сложных ИТ-систем, требующих непрерывности функционирования, гибкой поддержки подключений к глобальной сети, широких возможностей для совместной работы и защиты инвестиций. На сегодня маршрутизаторы Cisco с интеграцией сервисов второго поколения (ISR G2) являются вершиной эволюции сетевых устройств и создают новое рабочее пространство без границ за счет виртуализации сервисов, функций поддержки видео и превосходных эксплуатационных характеристик.

Помимо дорогостоящих маршрутизаторов, для решения задач объединения различных сред передачи сигналов существуют отдельные недорогие специализированные устройства – Медиаконвертеры. С их помощью, возможно, конвертировать оптический канал данных в цифровой и обратно. Из преимуществ подобных устройств можно отметить невысокую стоимость, простоту установки и использования.



Рис.2.1.15 – Медиаконвертор D-Link-DMC-1910T



Рис.2.1.16 – Медиаконвертор Allied Telesys-AT-MC103XL

Точки доступа для беспроводных сетей (wi-fi, 3G) - это отдельные недорогие устройства, которые можно добавить к существующей проводной сети. Такое решение будет удобным при реализации беспроводной сети в пределах офиса, позволит сэкономить на монтаже при переезде.



Рис.2.1.17 – Точка доступа Cisco-Aironet-1140



Рис.2.1.18 – Точка доступа D-Link-DWL-3200AP

Вопросы обеспечения сетевой безопасности актуальны для сетей любого уровня, в которых используется подключение к интернету, и породили целый класс сетевого оборудования, называемого Межсетевые экраны или Firewall. Основной функцией аппаратного Firewall является защита от различных сетевых угроз, внешних вторжений, фильтрация трафика на наличие вредоносных программ. Сегодня рынок межсетевых экранов представлен такими компаниями как: Cisco, Zyxel, D-link.



Рис.2.1.19 – Межсетевой экран Cisco ASA5505



Рис.2.1.20 – Межсетевой экран ZyWALL 1050



Рис.2.1.21 – Межсетевой экран D-link DFL-1600

Стоит отметить что, типовые задачи создания сетевой инфраструктуры могут быть решены с использованием оборудования различных классов. Так, например, создание локальной сети в пределах здания можно реализовать, используя оборудование как для домашнего сегмента - SOHO, так и применив устройства корпоративного уровня. Разумеется, применяя оборудование разных классов, приходится говорить о совершенно различных бюджетах, отличающихся в десятки раз. При этом в обоих случаях сеть будет функционировать, но разница в применении корпоративных и домашних устройств заключается, в первую очередь, в надежности оборудования и количестве дополнительных функций. Поэтому при выборе сетевого оборудования необходимо четко и ясно представлять задачу, для решения которой оно будет использоваться.

Активное и пассивное сетевое оборудование позволяет логически разделить сеть на сегменты и наладить взаимосвязь между ними. Так, для объединения нескольких элементов сети в сегмент используют концентраторы или коммутаторы. Концентратор, или хаб, пересылает получаемый сигнал на все активные элементы сети, создавая между ними и передающим сигнал оборудованием необоснованный трафик. Концентраторы являются пассивным сетевым оборудованием, так как сигнал никаким образом они не преобразуют.

Технология Ethernet, метод доступа CSMA/CD

Ethernet– пакетная технология компьютерных сетей, преимущественно локальных.

Стандарты Ethernet определяют проводные соединения и электрические сигналы на физическом уровне, формат кадров и протоколы управления доступом к среде – на канальном уровне модели OSI. Ethernet в основном описывается стандартами IEEE группы 802.3. Ethernet стал самой распространённой технологией ЛВС в середине 90-х годов прошлого века, вытеснив такие устаревшие технологии, как Arcnet, FDDI и Token Ring.

В сетях Ethernet используется метод доступа к среде передачи данных, называемый методом коллективного доступа с опознаванием несущей и обнаружением коллизий (carrier-sense-multiply-access with collision detection,

CSMA/CD).

Физическое вмешательство в инфраструктуру сети

Как и проектирование структурированных систем, их монтаж производится в несколько этапов, каждый из которых имеет большое значение для обеспечения наиболее оптимального уровня работоспособности будущей системы.

* Установка кабельных каналов. Как правило, суть данного процесса заключается в подготовке будущих мест установки информационных узлов, а также средств передачи информации. Зачастую монтаж таких каналов производится во всевозможных коробах, трубах и гофротрубках.
* Подготовка отверстия в перекрытиях и стенах для монтажа комплектующих и прокладывания кабелей между помещениями и зданиями.
* Прокладка кабелей в подготовленных ранее кабельных каналах. Данный процесс должен проводиться с учетом возможности будущей замены всех кабелей на более современные и обладающие более высокой скоростью передачи данных.
* Установка информационных розеток на каждом из рабочих мест и подведение к ним кабелей.
* Сборка и монтаж конструктивных элементов СКС – всевозможных телекоммуникационных стоек, настенных рам и шкафов.
* Проведение комплектного тестирования работоспособности системы и выявление дефектов. Данный этап можно назвать заключительных в процессе монтажа СКС, но от этого не менее важным. Именно от качественно тестирования и заблаговременного выявления дефектов, во многом зависит работоспособность всей системы в будущем.
* Сдачи компьютерной инфраструктуры в использование.
* Следует отметить, что качественный монтаж СКС является только составляющей хорошей работы всей системы.

# Логические (информационные) аспекты работы ЛВС

Сеть Интернет представляет собой глобальное объединение компьютерных сетей и информационных ресурсов, принадлежащих множеству различных людей и организаций. Это объединение является децентрализованным, и единого общеобязательного свода правил (законов) пользования сетью Интернет не установлено. Существуют, однако, общепринятые нормы работы в сети Интернет, направленные на то, чтобы деятельность каждого пользователя сети не мешала работе других пользователей. Фундаментальное положение этих норм таково: правила использования любых ресурсов сети Интернет (от почтового ящика до канала связи) определяют владельцы этих ресурсов и только они.

Логические (информационные) аспекты работы компьютерных сетей регламентируется следующими правилами:

- недопустимо использование несанкционированного ПО (в том числе сетевого);

- пользователи не должны использовать ЛВС для передачи другим компьютерам или оборудованию сети бессмысленной или бесполезной информации, создающей паразитную нагрузку на эти компьютеры или оборудование, в объемах, превышающих минимально необходимые для проверки работоспособности сети и доступности отдельных ее элементов.

1. Ограничения на информационный шум (спам)

Развитие Сети привело к тому, что одной из основных проблем пользователей стал избыток информации. Поэтому сетевое сообщество выработало специальные правила, направленные на ограждение пользователя от ненужной/незапрошенной информации (спама). В частности, являются недопустимыми:

1.1. Массовая рассылка не согласованных предварительно электронных писем (mass mailing). Под массовой рассылкой подразумевается как рассылка множеству получателей, так и множественная рассылка одному получателю.

1.2. Несогласованная отправка электронных писем объемом более одной страницы или содержащих вложенные файлы.

1.3. Несогласованная рассылка электронных писем рекламного, коммерческого или агитационного характера, а также писем, содержащих грубые и оскорбительные выражения и предложения.

1.4. Размещение в любой конференции Usenet или другой конференции, форуме или электронном списке рассылки статей, которые не соответствуют тематике данной конференции или списка рассылки (off-topic).

1.5. Размещение в любой конференции сообщений рекламного, коммерческого или агитационного характера, кроме случаев, когда такие сообщения явно разрешены правилами такой конференции либо их размещение было согласовано с владельцами или администраторами такой конференции предварительно.

1.6. Размещение в любой конференции статьи, содержащей приложенные файлы, кроме случаев, когда вложения явно разрешены правилами такой конференции либо такое размещение было согласовано с владельцами или администраторами такой конференции предварительно.

1.7. Рассылка информации получателям, высказавшим ранее явное нежелание получать эту информацию.

1.8. Использование собственных или предоставленных информационных ресурсов (почтовых ящиков, адресов электронной почты, страниц WWW и т.д.) в качестве контактных координат при совершении любого из вышеописанных действий, вне зависимости от того, из какой точки Сети были совершены эти действия.

2. Запрет несанкционированного доступа и сетевых атак

Не допускается осуществление попыток несанкционированного доступа к ресурсам Сети, проведение или участие в сетевых атаках и сетевом взломе, за исключением случаев, когда атака на сетевой ресурс проводится с явного разрешения владельца или администратора этого ресурса. В том числе запрещены:

2.1. Действия, направленные на нарушение нормального функционирования элементов Сети (компьютеров, другого оборудования или программного обеспечения), не принадлежащих пользователю.

2.2. Действия, направленные на получение несанкционированного доступа, в том числе привилегированного, к ресурсу Сети (компьютеру, другому оборудованию или информационному ресурсу), последующее использование такого доступа, а также уничтожение или модификация программного обеспечения или данных, не принадлежащих пользователю, без согласования с владельцами этого программного обеспечения или данных либо администраторами данного информационного ресурса.

2.3. Передача компьютерам или оборудованию Сети бессмысленной или бесполезной информации, создающей паразитную нагрузку на эти компьютеры или оборудование, а также промежуточные участки сети, в объемах, превышающих минимально необходимые для проверки связности сетей и доступности отдельных ее элементов.

3. Соблюдение правил, установленных владельцами ресурсов

Помимо вышеперечисленного, владелец любого информационного или технического ресурса Сети может установить для этого ресурса собственные правила его использования.

Правила использования ресурсов либо ссылка на них публикуются владельцами или администраторами этих ресурсов в точке подключения к таким ресурсам и являются обязательными к исполнению всеми пользователями этих ресурсов.

Пользователь обязан соблюдать правила использования ресурса либо немедленно отказаться от его использования.

4. Недопустимость фальсификации

Значительная часть ресурсов Сети не требует идентификации пользователя и допускает анонимное использование. Однако в ряде случаев от пользователя требуется предоставить информацию, идентифицирующую его и используемые им средства доступа к Сети. При этом пользователю запрещается:

4.1. Использование идентификационных данных (имен, адресов, телефонов и т.п.) третьих лиц, кроме случаев, когда эти лица уполномочили пользователя на такое использование. В то же время пользователь должен принять меры по предотвращению использования ресурсов Сети третьими лицами от его имени (обеспечить сохранность паролей и прочих кодов авторизованного доступа).

4.2. Фальсификация своего IP-адреса, а также адресов, используемых в других сетевых протоколах, при передаче данных в Сеть.

4.3. Использование несуществующих обратных адресов при отправке электронных писем.

5. Настройка собственных ресурсов

При работе в сети Интернет пользователь становится ее полноправным участником, что создает потенциальную возможность для использования сетевых ресурсов, принадлежащих пользователю, третьими лицами. В связи с этим пользователь должен принять надлежащие меры по такой настройке своих ресурсов, которая препятствовала бы недобросовестному использованию этих ресурсов третьими лицами, а также оперативно реагировать при обнаружении случаев такого использования.

Примерами потенциально проблемной настройки сетевых ресурсов являются:

• открытый ретранслятор электронной почты (SMTP-relay);

• общедоступные для неавторизованной публикации серверы новостей (конференций, групп);

• средства, позволяющие третьим лицам неавторизованно скрыть источник соединения (открытые прокси-серверы и т.п.);

• общедоступные широковещательные адреса локальных сетей;

• электронные списки рассылки с недостаточной авторизацией подписки или без возможности ее отмены.

6. Паразитный трафик.

Под паразитным трафиком понимается трафик, генерируемый сканерами сетей, трассировщиками, анализаторами. Даже если Вы не имеете никакой сетевой активности, некоторое количество трафика (1-2 килобайта в секунду) всё равно будет поступать.

Паразитный трафик - это входящий трафик, получение которого не было явно инициировано самим пользователем или установленным на компьютере программным обеспечением. Стоит помнить, что сеть Интернет "живет" своей интенсивной сетевой жизнью, в ней постоянно что-то происходит. Передается разнообразный служебный трафик, широковещательные пакеты, ICMP-пакеты, keepalive-пакеты и др. Наличие реального IP-адреса не только позволяет Вам получить доступ к любому сервису Интернета, но также делает доступным Ваш компьютер из Интернета. Следовательно, любой желающий (человек или сетевой вирус) может просканировать Ваш компьютер на наличие уязвимостей, попытаться провести сетевую атаку или просто командой ping проверить доступность Вашего компьютера из сети.

Сканирование сетевых портов - процесс организации множества входящих соединений от удаленных систем на различные сетевые порты локальной системы. Сканирование сетевых портов обычно производится с целью выяснения информации о работающих на сканируемой системе сервисах. На самом деле ничего страшного в этом нет - это вполне нормальное явление (в том случае, если Ваш компьютер не подвержен никаким уязвимостям и надежно защищен брандмауэром). Следствием подобной сетевой активности и является паразитный трафик. Следует отметить, что паразитный трафик может приходить на Ваш IP-адрес даже в том случае, если компьютер у Вас выключен. Как бы это невероятно не звучало, но это возможно. Протокол UDP, являющийся структурной частью протокола IP, позволяет отправлять пакеты на любой IP-адрес, не требуя для этого установления соединения с удаленным компьютером. А это значит, что если кто-то очень сильно захотел Вам "насолить", то теоретически он вполне может это сделать. К счастью, подобные серьезные сетевые атаки довольно редки, так как требуют определенных знаний сетевых технологий, а большинство "сетевых хулиганов" ими не располагают, а просто пользуются чужими программами. Как показывает практика, обычный пользователь особого интереса для настоящего хакера не представляет и должны быть очень веские причины чтобы Вас "взламывать".

Отделить этот паразитный трафик от всего остального, равно как избавится от него совсем, невозможно. Это мировая практика - паразитный трафик есть во всем мире и эффективные методы по его полному устранению пока еще не изобрел никто. Как правило, такой трафик незначителен, но если компьютер постоянно в сети, то за месяц теоретически может набежать несколько десятков Мб.

7. Как минимизировать паразитный трафик?

1. Установка критических обновлений для ОС Windows.

Windows Update - это расширение Windows, позволяющее обновлять программные компоненты компьютера.

2. Отключение служб Windows.

Можно отключить: Windows Error Reporting Service/Служба отчетов об ошибках: Позволяет регистрировать ошибки для служб и приложений, выполняющихся в нестандартной среде. При возникновении ошибки отправляет информацию об ошибке в корпорацию Microsoft; Windows Time/Служба времени Windows: Управляет синхронизацией даты и времени на всех клиентах и серверах в сети.

3. Межсетевые экраны (брандмауэры).

 Для защиты информации на локальных компьютерах или в локальных сетях широко применяются программы, называемые брандмауэрами (синонимы - файрвол, межсетевой экран). Эти программы играют роль фильтра, ограждающего локальный компьютер или локальную сеть компьютеров от несанкционированного доступа из сети. Персональный брандмауэр устанавливается на локальном компьютере и предназначен для защиты персональной информации. Для защиты информации на локальных компьютерах или в локальных сетях широко применяются программы, называемые брандмауэрами (синонимы - файрвол, межсетевой экран).

8. Антивирусные программы.

Сегодня и работа, и отдых немыслимы без Интернета, и этим активно пользуются авторы вирусов, хакеры и спамеры - часто в одном лице. Хакеры создают новые вирусы и другие вредоносные программы, чтобы незаконно проникать на наши компьютеры, подчинять их себе и затем рассылать с них спам. Угрозы информационной безопасности становятся всё более комплексными. Количество вредоносных программ, по некоторым данным, уже приближается к ста тысячам, появились десятки новых их типов и разновидностей - всё чаще смешанных, объединяющих все последние достижения "черной" компьютерной индустрии. Сама эта индустрия набирает обороты, уже начались "гангстерские войны" между кланами компьютерных преступников. У большинства антивирусов есть два режима использования - сканер и монитор. Сканер занимается тем, что тщательно проверяет файлы, расположенные на диске, при этом Вы можете указать для проверки отдельные файлы, директории или весь винчестер. Монитор же является резидентной программой (т.е. он запущен все время, пока включен компьютер) и "на лету" проверяет запускаемые Вами программы и файлы, к которым эти программы обращаются. Как правило, монитор производит менее тщательную проверку, чем сканер, но все же он позволяет выловить наиболее распространенные вредоносные программы. К сожалению, у антивирусов есть один минус - они довольно ощутимо тормозят работу, ведь им надо проанализировать каждый файл, перед тем как разрешить его использование. Именно из-за этих "тормозов" пользователи очень часто отключают антивирусы.

**Расширяемость и масштабируемость сети**

*Расширяемость* (extensibility) означает возможность простого добавления отдельных элементов сети (пользователей, компьюте­ров, приложений, служб), наращивания длины сегментов сети и замены существующей аппаратуры более мощной.

*Масштабируемость* означает, что сеть позволяет наращивать количество узлов и протяженность связей в очень широких пределах, при этом производительность сети не ухудшается. Для обеспечения масштабируемости сети приходится применять дополнительное коммуникационное оборудование и специальным образом структурировать сеть [27].

Чтобы понять, как можно построить сеть с хорошей расширяемостью и масштабируемостью, рассмотрим фундаментальное по­нятие ЛВС —«методы доступа компьютеров к сети и методы ком­мутации трафика в сети».

*Метод доступа к сети* — метод, с помощью которого, как правило, организуется доступ рабочих станций к передающей среде. Различают две группы методов доступа к разделяемой среде в ЛВС: методы случайного и детерминированного доступа, показанные на рис. 2.1.22.

***Методы случайного доступа*** подразумевают, что каждая станция произвольным образом, независимо от других, может обращаться к моноканалу. Их также называют методами множественного доступа. Они бывают двух видов.

*Множественный доступ с контролем несущей и обнаружением коллизий* (МДКН/ОК) применяется в сетях, где все абоненты имеют равные приоритеты на доступ к сети. Суть метода заключается в следующем:

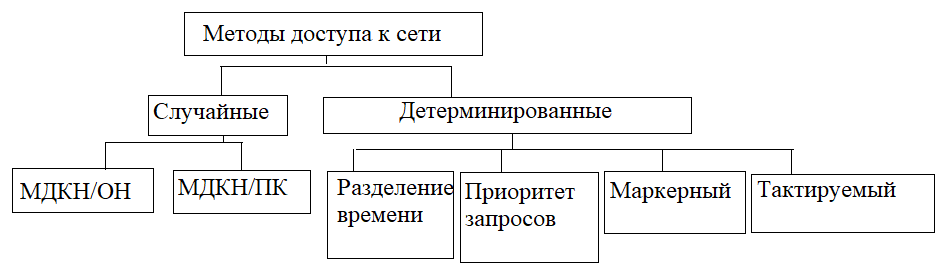


Рис. 2.1.22. Методы доступа к разделяемой среде в ЛВС

1) абонент ждет освобождения сети, после чего начинает персдачу, одновременно контролируя состояние сети на предмет обнаружения коллизий;

2) если коллизия обнаружена, то абонент усиливает ее для гарантии обнаружения всеми передающими абонентами. а затем прекращает передачу, как и другие передававшие абоненты;

3) затем абонент выдерживает случайную паузу и повторяет свою попытку передать данные, снова контролируя столкновения.

Коллизия возникает в результате соперничества за канал: станция В может передать свой кадр, не зная, что станция А уже захватила канал, поскольку от станции А к станции В сигнал распространяется за конечное время. Такая коллизия называется ранней и является нормальным явлением в методе МДКН/ОК. В результате станция В. начав передачу, входит в конфликт со станцией А. Каждая станция способна одновременно и передавать данные, и «слушать» канал.

В методе МДКН/ОК конфликт обнаруживается абонентом только во время передачи пакета. Если конфликт происходит после передачи пакета (поздняя коллизия), то он относится к необнаруженному конфликту и воспринимается получателем как ошибочный пакет. Интервал времени возникновения поздней коллизии является исходным при расчете диаметра (максимального расстояния между хостами) Ethernet -сети.

В качестве примера рассчитаем диаметр Ethernet -сети, в которой скорость передачи данных vD = 10 Мбит/с = 107 бод; скорость сигнала vS= 3•108 м/с; длина минимального пакета Lmin= 64 байт = 512 бит.

Расчет проводим этапами:

1. определяем время передачи пакета: T= Lmin / vD = 512/107 = 512•10-7 (с);
2. определим расстояние S, которое пройдет сигнал по кабелю за это время:

*S=vsT=* 3-108-512-10-7 = 15 360 (м);

1. удвоенная длина кабеля должна быть меньше этого значе­ния, т.е. кабель должен быть короче: 15 360 : 2 = 7 680 (м). По стан­дарту Ethernet максимальный диаметр сети не должен превышать 2 500 м (стандарт указывает значение более чем с трехкратным за­пасом).

Метод МДКН/ОК является надежным и обеспечивает полное равноправие всех абонентов в сети, так как ни один из них не мо­жет надолго «захватить» сеть. Легкость подключения и отключе­ния станций, кроме того, гарантирует хорошую расширяемость Ethernet-ceти. Однако такая сеть ограничивает число станций несколькими десятками — при превышении этого числа время ожидания абонентом доступа к среде передачи резко возрастает, что свидетельствует о плохой масштабируемости данной системы.

Метод *множественного доступа с контролем несущей и пре­дотвращением коллизий* (МДКН/ПК) отличается от предыдущего метода тем, что в сети сталкиваются (если сталкиваются) не сооб­щения, а специальные сигналы, предшествующие сообщениям. Указанные сигналы существенно снижают вероятность того, что произойдет столкновение следующих за ними сообщений. Метод МДКН/ПК обеспечивает, кроме того, меньшее время простоя канала, однако достигается это за счет усложнения оборудования.

***Методы детерминированного доступа*** позволяют эффективно использовать разделяемую среду передачи данных в сильно загруженных сетях и повысить уровень безопасности сети по сравнению с методами случайного доступа. Это достигается введе­нием в сеть дополнительного оборудования.

Метод доступа *разделение времени.* Все время работы сети делится на интервалы и во время каждого интервала через канал передаются данные только одной из станций. Устройство управления последовательно опрашивает станции на наличие у них сообщений для передачи. Станция, получившая разрешение, осущест­вляет передачу и по окончании уведомляет об этом устройство управления, которое, получив уведомление, по списку приорите­тов посылает разрешение на передачу следующей станции, и т.д. После того как все станции получат разрешение на передачу, нач­нется новый цикл.

Метод доступа *приоритет запросов* реализуется в сети, состо­ящей из интеллектуальных концентраторов. Каждый концентра­тор циклически выполняет опрос своих портов. Станция, желаю­щая передать пакет, посылает сигнал концентратору, запрашивая передачу кадра и указывая свой приоритет. Если сеть свободна, то концентратор разрешает передачу, а если занята, — ставит запрос в очередь, которая обрабатывается в соответствии с порядком по­ступления запросов и с учетом приоритетов. Одновременно в сети присутствует только один кадр, т.е. сохраняется эффект разделя­емой среды.

*Маркерный* метод доступа используется в сетях «шина», «звез­да» и «кольцо». Право на передачу станции получают здесь в по­рядке, задаваемом с помощью уникального кадра — маркера. Все узлы сети играют активную роль, участвуя в ретрансляции, усиле­нии, анализе и модификации проходящих сигналов. Маркер име­ет поле занятости с кодом либо «свободный», либо «занятый». Свободный маркер циркулирует по кольцу и в каждом узле задер­живается на время его анализа на занятость и ретрансляции.

Получив свободный маркер, станция, готовая к передаче кадра с данными, меняет состояние маркера на «занятый», передает его дальше по кольцу и добавляет к нему кадр. Этот тандем совершает оборот по кольцу и возвращается к станции-отправителю. По пути станция-получатель копирует кадр, но изменить состояние марке­ра на свободный может только узел, который изменил его на «за­нятое». По возвращении занятого маркера с кадром данных к станции-отправителю кадр удаляется из кольца, а состояние мар­кера меняется на свободное и т.д. Как видим, данный метод по­зволяет ликвидировать простои в сети и организовать одновре­менную передачу несколькими станциями сети. «Платить» за это приходится низкой масштабируемостью.

*Тактируемый* метод доступа позволяет нескольким абонентам одновременно и в любой момент вести передачу. В сети использу­ются от двух до восьми пакетов — слотов, выполняющих функцию временных меток и содержащих небольшую порцию данных (от 8 до 32 байт). Свободные (без данных) или занятые (с данными) слоты переносят данные по «кольцу» и тактируют работу сети. В каждом слоте существуют бит занятости, поле сетевого адреса приемника и передатчика, а также бит признака конца передачи.

Алгоритм доступа к сети следующий:

1. отправитель разбивает информацию на слоты установленно­го размера и ждет прихода свободного слота, после чего загружает в этот слот первую часть информации. Вторую часть данных он помещает в следующий свободный слот, и так — до полной пере­дачи всего объема информации;
2. абонент-приемник выбирает из слотов адресованную ему информацию и устанавливает в принятом слоте бит подтвержде­ния. Так продолжается до последнего адресованного слота;
3. передающий абонент получает свои слоты обратно по «кольцу», анализирует бит подтверждения и помечает их как свободные.

Ни один из методов доступа к сети, использующий разделяемую среду передачи, не позволяет обеспечить хорошую масштабируемость сети, а детерминированные методы не позволяют обе­спечить и достаточно хорошую расширяемость. Допустимые размеры одного сегмента ЛВС во всех случаях ограничены несколькими десятками хостов. Протоколы и методы доступа, применяемые в ЛВС, предназначены для функционирования на ограниченных расстояниях, поэтому сегмент ЛВС не удается рас­ширить за пределы определенной физической области (диаметр сети). Как видим, ЛВС с разделяемой средой передачи нельзя считать действительно расширяемыми. Для обеспечения высокого уровня как масштабируемости, так и расширяемости сети следует использовать методы коммутации потоков данных, характерные для глобальных сетей. Рассмотрим их более подробно.

**Методы коммутации в ТКС.** Система коммутации решает зада­чу внутрисетевого распределения информационных потоков. Существуют два основных принципа коммутации:

* + 1. непосредственное соединение — без запоминания передаваемой информации;
    2. соединение с накоплением информации.

При *непосредственном соединении (коммутации каналов)* осуществляется физическое соединение входящих линий с исходящими линиями по соответствующему адресу, поэтому здесь возможна организация диалога между абонентами (время задержки в передаче сообщения невелико) и абоненты имеют возможность вести передачу сообщений после установления соединения неза­висимо от нагрузки, поступающей от других абонентов. Однако в случае отсутствия свободных каналов пользователь получает отказ в установлении связи, поэтому систему с коммутацией каналов называют системами с потерями вызовов.

*Соединение (коммутация*) с *накоплением информации* бывает двух видов: коммутация сообщений и коммутация пакетов. В *си­стемах с коммутацией сообщений* пользователь не получает отка­за в случае отсутствия свободных каналов. Его сообщение времен­но записывается в память коммутационной станции и выдается после освобождения канала, поэтому системы с накоплением называются системами с ожиданием. Данный метод нашел применение на телеграфной сети общего пользования.

В *системах с коммутацией пакетов* исходящее сообщение де­лится на «пакеты», каждый из которых содержит часть полезной информации и заголовок. Заголовок пакета, в свою очередь, со­держит: идентификатор, определяющий принадлежность пакета к сообщению, адреса абонентов, порядковый номер пакета и др.

Реализация всех методов коммутации (пакетов, каналов и (или) сообщений) в телекоммуникационных сетях «лежит на плечах» устройств, называемых маршрутизаторами

**Технологии масштабируемости.** Существуют три основные технологии масштабирования:

* + - 1. нивелирование времени ожидания связи;
      2. распределение;
      3. репликация.

***Нивелирование времени ожидания связи*** применяется в случае географического масштабирования в целях сведения к минимуму времени ожидания ответа на запрос от удаленного сервера. Например, если была запрошена сл)жба удаленной машины, аль­тернативой ожиданию ответа от сервера будет осуществление на запрашивающей стороне других возможных действий. Это озна­чает разработку запрашивающего приложения в расчете на ис­пользование исключительно асинхронной связи. Когда будет по­лучен ответ, приложение прервет свою работу и вызовет специальный обработчик для завершения запроса, отправленного ранее.

Асинхронная связь часто используется в системах пакетной об­работки и параллельных приложениях, в которых во время ожида­ния одной задачей завершения связи предполагается выполнение других более или менее независимых задач. Для осуществления запроса может быть запущен новый управляющий поток выполнения. Хотя он будет блокирован на время ожидания ответа, дру­гие потоки процесса продолжат свое выполнение.

Однако многие приложения не в состоянии эффективно ис­пользовать асинхронную связь. Например, когда в интерактивном приложении пользователь посылает запрос, он обычно просто ждет ответа от сервера. В этих случаях наилучшим решением бу­дет сократить необходимый объем взаимодействия, например переместив часть вычислений, обычно выполняемых на сервере, на клиента, процесс которого запрашивает службу. Стандартный слу­чай применения этого подхода — доступ к базам данных с использованием форм. Обычно заполнение формы сопровождается посылкой отдельного сообщения на каждое поле и ожиданием под­тверждения приема от сервера, как показано на рис. 2.1.23, *а.*

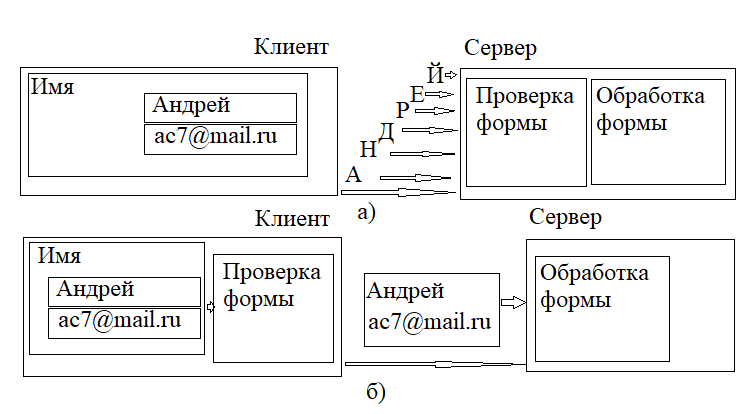


Рис. 2.1.23. Различие в обработке формы на сервере (а) и на клиенте (б)

Сервер, например, может перед приемом введенного значения проверить его на синтаксические ошибки. Более успешное реше­ние, показанное на рис. 2.1.23, б, заключается в том, чтобы перенести код для заполнения формы и, возможно, проверки введенных дан­ных на клиента, чтобы он мог послать серверу целиком заполнен­ную форму. Такой подход в настоящее время широко поддержива­ется Web-сайтами посредством Лауа-апплетов — программных компонентов, выполняющий узкую функцию (например, интерак­тивную) в среде другой программы, например в интернет-брау­зере.

***Распределение*** — технология масштабирования, предполага­ющая разбиение компонентов на мелкие части и последующее разнесение этих частей по системе. Примером распределения яв­ляется система доменных имен Интернета (DNS), организованная иерархически, в виде дерева доменов, которые разбиты на непе­рекрывающиеся зоны, как показано на рис. 1.10. Имена каждой зоны обрабатываются одним сервером имен. Известно [25], что каждое доменное имя является именем хоста в Интернете, кото­рое ассоциируется с сетевым адресом этого хоста. В основном ин­терпретация имени означает получение сетевого адреса соответ­ствующего хоста. Рассмотрим, например, имя nt.vu.cs. flits. Для интерпретации этого имени оно сначала передается на сервер зоны, отмемечен- ной на рис. 2.2.24 как Z,. Этот сервер возвращает адрес сервера зоны Z2, который, вероятно, сможет обработать остаток имени: vu.cs. flits. Сервер зоны Z2 вернет адрес сервера зоны Z3, который способен обработать последнюю часть имени и вернуть адрес со­ответствующего хоста. Данный пример демонстрирует, как служ­ба именования, предоставляемая DNS, распределена по несколь­ким машинам, чтобы избежать обработки всех запросов на интер­претацию имен одним сервером.

***Репликация*** компонентов распределенной системы применяет­ся при рассмотрении проблем масштабирования, часто проявля­ющихся в виде падения производительности. Репликация не толь­ко повышает доступность, но и помогает выровнять загрузку ком­понентов, что ведет к повышению производительности. Кроме того, в географически рассредоточенных системах наличие близ­ко лежащей копии позволяет уменьшить остроту проблемы ожи­дания завершения связи.

Кэширование представляет собой особую форму репликации, причем различия между ними нередко малозаметны или вообще искусственны. Как и в случае репликации, результатом кэширова­ния является создание копии ресурса, обычно в непосредственной близости от клиента, использующего этот ресурс. В противопо­ложность репликации, *кэширование* — это действие, предприни­маемое потребителем ресурса, а не его владельцем.

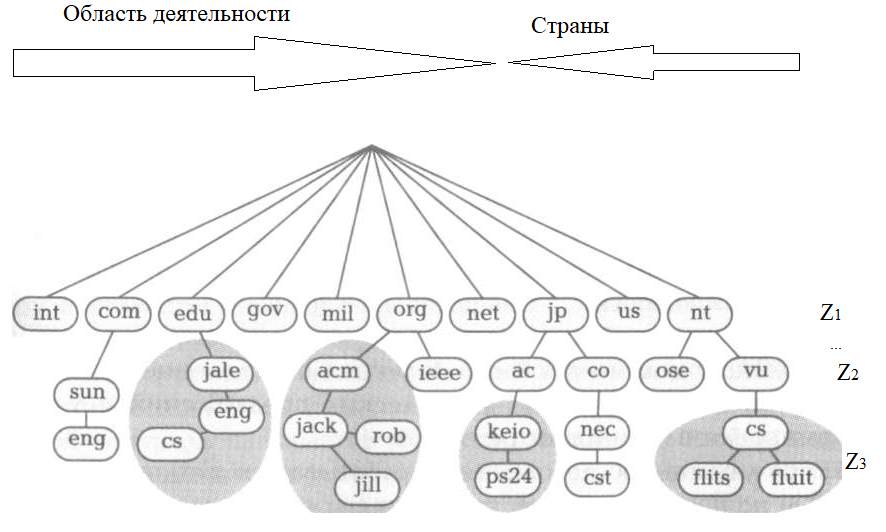


Рис. 2.2.24. Система доменных имен зоны Интернета

На масштабируемость может плохо повлиять один существенный недостаток кэширования и репликации. Поскольку мы получаем множество копий ресурса, модификация одной копии делает ее от­личной от остальных. Соответственно кэширование и репликация вызывают проблемы непротиворечивости, причем допустимая сте­пень противоречивости зависит от степени загрузки ресурсов. Так, множество пользователей Интернета считают допустимой работу с кэшированным документом через несколько минут после его поме­щения в кэш без дополнительной проверки. Однако существует мно­жество случаев, когда необходимо гарантировать строгую непроти­воречивость, например при операциях на электронной бирже.

Проблема строгой непротиворечивости заключается в том, что изменение в одной из копий должно немедленно распространять­ся на все остальные. Кроме того, если два изменения происходят одновременно, часто бывает необходимо, чтобы эти изменения вносились в одном и том же порядке во все копии. Для обработки ситуаций такого типа обычно требуется механизм глобальной син­хронизации. К сожалению, реализовать масштабирование подоб­ных механизмов очень трудно или вообще невозможно. Это озна­чает, что масштабирование путем репликации может включать в себя отдельные немасштабируемые решения.

## Службы каталогов

Служба каталогов -- это сетевой сервис, представляющий централизованные средства управления ресурсами автоматизированной системы. Под ресурсами подразумеваются все компоненты сетевой инфраструктуры, которые используются для выполнения функций АСУ: пользователи, файлы и каталоги, устройства, сетевые сервисы и т.д. (Рис. 2.2.25.).

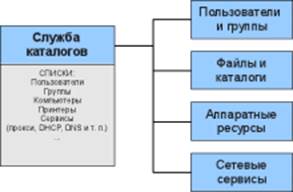


Рис. 2.2.25. Служба каталогов

Как правило, служба каталогов состоит из базы данных, в которой размещены сведения о сетевых ресурсах и серверного ПО, представляющего механизмы доступа к этой базе. Как база данных сервиса каталогов, так и ее управляющая программа могут быть распределены на несколько серверов (рис. 2.2.26.).

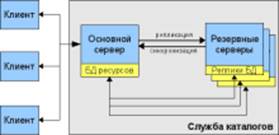


Рис. 2.2.26. Распределенная служба каталогов

Основными функциями службы каталогов являются следующие:

Управление пользователями и группами (создание/удаление, настройка прав доступа).

Управление ресурсами (представление в общий доступ, установка ограничений, удаленное администрирование и т.п.).

Разграничение прав доступа (как правило, на уровне пользователей, групп и отдельных ресурсов).

Среди дополнительных функций сервиса каталогов можно указать, например, такие:

- поиск ресурсов;

- распространение сетевых политик;

- интеграция с другими сервисами.

Сетевая политика -- совокупность правил, определяющих методы и средства взаимодействия с общими ресурсами в корпоративной сети.

Сетевые ресурсы в службе каталогов обычно представлены в виде иерархической структуры. Такой способ наиболее близок к реальной организационной модели подавляющего большинства предприятий и организаций. Корень иерархии описывает предприятие в целом, нижележащие уровни -- подразделения и отдельные элементы. Для единообразного обращения к любому элементу иерархии протокол взаимодействия представляет унифицированную схему адресации -- либо собственную, либо совместимую со стандартными схемами.

Рассмотрим основные особенности некоторых сервисов каталогов, различных по представляемым возможностям.

Network Information Service (NIS/YP)NIS (Сетевая Информационная Служба) -- служба каталогов, разработанная и реализованная Sun Microsystems для систем на основе UNIX. NIS первоначально назывались Yellow Pages (YP), но из-за проблем с торговым знаком Sun изменила это название. Старое название (yp) используется в названиях утилит NIS.

NIS - это иерархическая система, в которой существует три типа хостов: основные (master) серверы, вторичные (slave) серверыи клиентские машины (рис. 2.2.27.). В качестве источников данных для клиентов используются системные файлы (в терминах NIS --карты ресурсов) основного сервера NIS: passwd, hosts, group, services и прочие. В сети может быть один основной сервер NIS и ни одного или более вторичных серверов. Вторичные серверы хранят копии общих файлов основного сервера для обеспечения избыточности. Клиенты могут быть настроены как на работу с основным сервером NIS, так и со вторичными. Чтобы получить доступ к запрашиваемой информации клиент должен являться членом домена NIS.

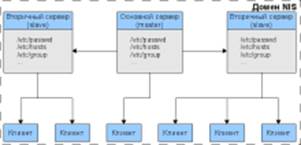


Рис. 2.2.27. Структура Network Information Service (NIS)

Домен NIS -- это совокупность доверенных ресурсов с уникальным в пределах сети именем. Имя домена NIS и способ именования ресурсов напоминает адресацию в системе доменных имен (DNS), но никакого отношения к DNS не имеет. Информация о домене хранится на основном сервере NIS и реплицируется на вторичные сервера наравне с прочими ресурсами. Один основной сервер может вести базы нескольких доменов NIS.

Общий доступ реализуется по следующей схеме: когда клиентскому приложению требуется доступ к некоему ресурсу, то локальные обращения (например, к файлу hosts) транслируются в вызовы удаленных процедур сервера NIS, с которым связан клиент. Поскольку NIS использует RPC, то NIS-серверы работают на тех портах, которые им представляет сервис RPC (т.е. у службы NIS нет выделенного номера порта, в отличие от, например, ftp-сервера или веб-сервера).

Установление связи с сервером NIS выполняется путем широковещательной рассылки запросов. Если в сети имеется несколько серверов (основной и несколько вторичных), то клиент NIS (обычно это программа ypbind) будет использовать адрес первого ответившего и направлять все свои запросы на этот сервер. Время от времени ypbind будет проверять доступность сервера. Если тот не ответит за разумное время, то клиент снова начнет процедуру опроса сети в поисках «живого» сервера.

Сервис NIS поддерживается большинством UNIX-систем общего назначения и представляет простые и удобные средства для организации централизованного управления сетью. NIS хорошо интегрируется с такими сетевыми сервисами, как например DHCP или NFS.

Среди сновных проблемы NIS выделим две:

использовании RPC, что может привести к неработоспособности клиентов при недоступности NIS-сервера;

передача карт в открытом виде, что может привести к нарушению информационной безопасности.

Из-за второго недостатка NIS не рекомендуется применять в публичных сетях. Для устранения недостатков NIS были разработаны усовершенствованные спецификации протокола (NYS и NIS+), но они не столь популярны.

Модель OSI определяет самые разные аспекты взаимодействия открытых систем. Имеется в ней и спецификация X.500, описывающая службу каталогов. X.500 -- это серия рекомендаций разработанных ITU-T в 1993 г. и получивших статус международного стандарта (ISO/IEC 9594-1). Спецификация X.511 описывает протокол DAP для доступа к каталогам X.500. DAP, принятый в качестве международного стандарта, оказался избыточным и сложным в реализации и на его основе были разработаны адаптированные версии, среди которых NDS и LDAP.

Протокол LDAP (Lightweight Directory Access, упрощенный протокол доступа к каталогу) -- бинарный клиент-серверный протокол прикладного уровня, предназначенный для доступа к распределенной службе каталогов через Интернет. Этот протокол может использоваться как в качестве шлюза к любым X.500-совместимым каталогам (Рис. 2.2.28.), так и в качестве основного сервиса каталогов (Рис. 2.2.29.). Спецификация текущей версии (LDAP v3) приведена в RFC 4510.

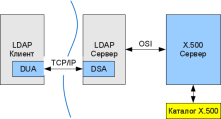


Рис. 2.2.28. LDAP в роли шлюза к каталогу X.500

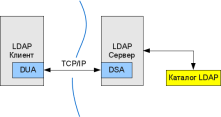


Рис. 2.2.29. LDAP в качестве самостоятельного сервиса

В терминах X.500 каталог представляет собой «совокупность открытых систем, совместно предоставляющих службы каталогов». Проще говоря, это распределенная клиент-серверная база данных, доступ к которой возможен через унифицированные интерфейсы. Пользователь каталога, который может быть человеком или другим каким-то объектом, получает доступ к каталогу (Directory) с помощью клиентского приложения (DUA). Клиент взаимодействует с одним или более серверами через агентов системы каталогов (DSA) (рисунок 4).

LDAP устанавливает порядок взаимодействия между клиентом и сервером на основе обмена сообщениями. Сообщения определяют запрашиваемые клиентом операции, ответы сервера и формат передаваемых данных. LDAP -- это сессионный протокол, требующий установления, поддержания и разрыва соединения между клиентом и сервером, поэтому основным транспортом для него является TCP. Для сервиса LDAP имеется стандартный порт 389 (TCP/UDP, см. описание «хорошо известных» (well-known) портов в локальном файле /etc/services).

Основной единицей информации, хранимой в каталоге, является отдельная запись (entry). Каждая запись представляет какой-либо реальный объект: человека, компьютер, организацию и т.д. Запись описывает объект через набор присущих ему атрибутов. Атрибуты представляют собой пары вида «имя -- значение». Фактическое значение атрибута зависит от его типа (Рис. 2.2.30.).

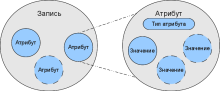


Рис. 2.2.30. Записи и атрибуты LDAP

Записи хранятся в иерархической структуре, называемой «Информационное дерево каталога» (Directory Information Tree, DIT). Обращение к записям осуществляется по их уникальным именам (DN, distinguished name). DN включает полный путь к записи от корня DIT и этим напоминает путь к файлу в файловой системе. Помимо DN используется и относительное уникальное имя (RDN, relative distinguished name).

Если сравнивать DN и RDN с именами файлов, то DN можно представить так:

- /home/user/documents/somefile.txt.

а, RDN так:

- somefile.txt.

По сути же, DN есть цепочка из RDN'ов элементов структуры разного уровня.

В LDAP используется унифицированная схема именования и набор обязательных и опциональных атрибутов предопределенных типов, которые имеют короткие алиасы. Некоторые типы атрибутов записей приведены в таблица 1. Простой пример DIT с несколькими записями приведен на (Рис. 2.2.31.).

Таблица 1.2.1. Атрибуты

|  |  |  |
| --- | --- | --- |
| Тип атрибута | Краткая запись (алиас) | Пояснение |
| CommonName | cn | Общее имя |
| StateOrProvinceName | st | Географическое название региона |
| OrganizationName | o | Название организации |
| OrganizationalUnitName | ou | Название структурного подразделения |
| CountryName | c | Страна |
| StreetAddress | street | Улица (как часть адреса) |
| domainComponent | dc | Элемент домена |
| userid | uid | Уникальный идентификатор пользователя |



Рис. 2.2.31. Пример информационного дерева каталога (DIT) в LDAP

LDAP изначально ориентирован на использование в сильно распределенной среде, поэтому каталог или его части могут быть размещены на различных серверах. Клиент может обращаться к любому из серверов LDAP. Доступ к ним может осуществляться по реферальному или цепочечному принципам.

В случае реферальной обработки запросов LDAP-сервер возвращает клиенту, вместо ответа, информацию о том, на каком из серверов можно получить нужные данные. При цепочечной обработке LDAP-сервер сам опрашивает другие сервера в поисках ответа на клиентсткий запрос.

Репликация каталога LDAP может выполняться по следующим сценариям:

multi-master-- все LDAP-серверы равноправны, в сети отсутствует четко определенный сервер, управляющий данными;

master-slave-- главный (master) сервер управляет всеми изменениями каталога и рассылает их на подчиненные (slave) серверы. Этот сценарий может быть расширен до делегирования функций синхронизации одному из подчиненных серверов, который и будет реплицировать данные на остальные slave-серверы.

Наиболее известной (но не единственной) открытой реализацией протокола LDAP является проект Open LDAP.

Начиная с версии Windows 2000 Server Microsoft стала использовать собственную, LDAP-совместимую службу каталогов Active Directory.

I **ТЕХНИЧЕСКАЯ И ПРОЕКТНАЯ ДОКУМЕНТАЦИЯ**

Проектирование ЛВС должно проводиться в соответствии с Постановлением Правительства РФ от 16.02.2008 № 87 «О составе разделов проектной документации и требованиях к их содержа­нию», региональными строительными нормами и требованиями технического задания. Кроме того, при проектировании ЛВС должны учитываться требования существующего законодатель­ства и нормативных документов по экологии, охране труда и по­жарной безопасности.

В начале всех работ исполнителем проводится *предпроектное обследование,* целями которого являются определение комплекса мероприятий и разработка технических предложений с учетом сформированных типовых решений.

По результатам обследования разрабатывается *техническое зада­ние (ТЗ) на проектирование,* являющееся основой для создания лю­бого проекта. В идеальном случае развернутое техническое задание на проектирование компьютерной сети должен предоставить заказ­чик. В случае отсутствия у заказчика соответствующих специалистов, которые могли бы составить полноценное ТЗ на проектирование ЛВС, включающее в себя все параметры системы, он может обра­титься за помощью к специалистам исполнителя. Интернет-ресурс [68] содержит конкретный пример ТЗ на проектирование ЛВС.

**Проектная документация ЛВС (стадия «П»).** Состав проектной документации ЛВС регламентируется указанным ранее Постанов­лением Правительства РФ № 87. Разработанная концепция ЛВС и техническое задание на ее проектирование дает основания для создания *эскизного плана ЛВС* — единого комплекса решений, предназначенного для обеспечения заданного режима эксплуата­ции ЛВС. Эскизный проект определяет оптимальную структуру ЛВС и трассу прокладки кабельных проводок, расположение и со­став ОСИС организации, представление о бюджете проекта, а так­же ряд других параметров, которые позволят облегчить выбор конкретных решений.

Проектная документация ЛВС представляет собой текстовые и графические материалы, определяющие объемно-планировочные, конструктивные и технические решения для строительства или реконструкции (модернизации) ЛВС. Основой для разработки проекта ЛВС служат *архитектурно-строительная, технологиче­ская* и *инженерная части* технического задания.

**Рабочая документация ЛВС (стадия «Р»).** На следующем этапе разрабатывается рабочая документация ЛВС, которая использует­ся на этапе строительства ЛВС. Составив и согласовав с заказчи­ком ТЗ на проектирование сети и состав проектной документации, специалисты исполнителя приступают к разработке рабочей доку­ментации, включающей в себя документы, чертежи, схемы, жур­налы и описания, необходимые для производства работ на объек­те заказчика. Рабочая документация (по сути — рабочий проект) описывает, что, где, каким образом и согласно каким стандартам, нормам и правилам должно быть установлено на объекте.

Перед тем как приступить к работам, сотрудники исполнителя в обязательном порядке согласовывают с заказчиком разработан­ную *рабочую документацию.* Затем начинается монтаж ОСИС. За соответствием выполняемых работ рабочему проекту ЛВС в орга­низации исполнителя следят инженеры — авторы проектов ЛВС. Такой контроль называется авторским надзором. Любые измене­ния и отступления от рабочего проекта ЛВС оперативно согласо­вываются с заказчиком и вносятся в проект.

По завершении работ выпускается *исполнительная документа­ция,* которая некоторым образом повторяет рабочий проект ЛВС, но учитывает все изменения, внесенные в рабочий проект ЛВС в течение производства монтажных и наладочных работ, а также результаты тестирования телекоммуникационного оборудования и кабельных линий. Исполнительная документация передается за­казчику, а также эксплуатационной службе здания, где смонтиро­ваны ОСИС. Исполнительная документация необходима для си­стемных администраторов, службы эксплуатации здания, для об­служивания и возможности дальнейшей модернизации сети.

Заключительным этапом проектирования ЛВС является разра­ботка сметной документации, в которой определяется полная сто­имость оборудования, строительно-монтажных и пусконаладоч- ных работ.

После завершения проектирования ЛВС и создания рабочей документации, согласно которой будут осуществляться работы по построению всей сетевой инфраструктуры на объекте, проводит­ся контроль соответствия выполнения работ проектной докумен­тации. Этой цели служит авторский надзор — следующее звено технологической цепочки при создании инженерных систем. Ав­торский надзор подразумевает постоянное участие и контроль над технологией монтажа со стороны отдела технического контроля компании исполнителя. Наличие данного этапа очень важно, по­скольку позволяет избежать ошибок во время выполнения работ и исключает возможность несоответствия построенной системы и согласованного проекта ЛВС.

В процессе выполнения работ иногда возникает необходимость корректировки рабочего проекта сети. При наличии авторского надзора эти моменты выполняются обычно быстро и безболезнен­но, с последующей фиксацией в исполнительной документации.

Завершается цикл работ по инсталляции ЛВС подписанием акта приемки-сдачи. Порядок безопасной технической эксплуата­ции ОСИС обычно регламентирует документ «Правила эксплуата­ции и хранения техники. Эксплуатация ЛВС». В Приложении 1 приведен примерный вид этого документа.

# КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Перечислите состав документации по проектированию ЛВС.
2. Опишите три технологии масштабируемости.

В чем заключается смысл расширяемости и масштабируемо­сти сети?

## 1.3 Архитектура и функции систем управления сетями

**1.3 Архитектура и функции систем управления сетями**

Архитектура и области управления сетями

Системы управления сетями представляют собой сложные программно-аппаратные комплексы, поэтому существует граница целесообразности их применения, которая зависит от сложности сети. В небольшой сети можно применять отдельные программы управления наиболее сложными устройствами. Однако при увеличении сети появляется проблема объединения разных программ управления устройствами в единую систему управления, решая которую придется возможно, откататься от них программ и заменить их интегрированной системой управления.

Первые системы управления корпоративными сетями были ориентированы на управление коммуникационным оборудованием и контроль трафика сети. Именно эти функции имеют чаще всего в виду, когда говорят о системе управления сетью. Кроме систем управления сетями существуют н системы управления другими элементами корпоративной сети: системы управления ОС, системами управления базами данных (СУБД), корпоративными приложениями и пр.

Типовая архитектура систем управления сетями. Независимо от объекта управления желательно, чтобы система управления выполняла ряд функций, которые определены международными стандартами, обобщающими опыт применения систем управления в различных областях. Стандарты X.700.ISO 7498-4 делят задачи системы управления на пять трупп (36):

1) управление конфигурацией сети;

2) обработка ошибок;

3) анализ производительности и надежности;

4) управление безопасностью;

5) учет работы сети.

Рассмотрим задачи этих функциональных областей управления применительно к системам управлении сетями.

**Управление конфигурацией сети** заключается в конфигурировании параметров как элементов сети, так и сети в целом. Для элементов сети, таких как маршрутизаторы, мультиплексоры, с помощью этой труппы задач определяются сетевые адреса, идентификаторы, географическое положение и пр. Для сети в целом управление конфигурацией обычно начинается с построения карты сети, т.е. отображения реальных связей между элементами сети и изменения связей между элементами сети — образования новых физических или логических каналов, изменения таблиц коммутации и маршрутизации.

Управление конфигурацией, как и другие задачи системы управления, могут выполняться в автоматическом, ручном или полуавтоматическом режимах. Например, карта сети может составляться автоматически, на основании зондирования реальной сети пакетами-исследователями (программными Агентами, или просто Агентами), либо может быть введена оператором системы управления вручную. Чаще всего применяются полуавтоматические методы, когда автоматически полученную карту оператор подправляет вручную.

Одной из наиболее сложных задач управления конфигурацией сети является настройка коммутаторов и маршрутизаторов на поддержку маршрутов и виртуальных путей между пользователями сети. Согласованную ручную настройку таблиц маршрутизации при полном или частичном отказе от использования протокола маршрутизации (а в некоторых глобальных сетях, например Х.25. такого протокола просто не существует) многие системы управления сетью общего назначения просто не выполняют. Однако существуют специализированные системы конкретных производителей, например система NetSys компании CiscoSystems, которые решают ее для маршрутизаторов этой же компании.

**Обработка ошибок** — выявление, определение и устранение последствий сбоев и отказов в работе сети. На этом уровне выполняются регистрация сообщений об ошибках и их фильтрация. Маршрутизация и попытка устранения последствий их возникновения. Фильтрация позволяет выделить из интенсивного потока сообщений об ошибках, который обычно наблюдается в большой сети, только важные сообщения. Маршрутизация обеспечивает их доставку нужному элементу системы управления, а корреляционный анализ позволяет найти причину, породившую поток взаимосвязанных сообщений (например, обрыв кабеля может быть причиной большого количества сообщений о недоступности сетей и серверов).

Устранение ошибок может быть как автоматическим, так н полуавтоматическим. В автоматическом режиме система непосредственно управляет оборудованием или программными комплексами и обходит откатавший элемент за счет резервных каналов. В полуавтоматическом режиме основные решенияи действия по устранению неисправности выполняют люди, а система управления только помотает в организации этого процесса: оформляет квитанции на выполнение работ и отслеживает их поэтапное выполнение (подобно системам групповой работы).

Если при этом процесс управления сбоями поддерживается процессом управления конфигурациями, удаленным администрированием, то становится возможным архивировать различные сетевые настройки на сервере и проводить регулярное обслуживание сетевого оборудования. Кроме того, необходимо ежедневно проверять сетевые настройки и сравнивать их с ожидаемыми, что позволяет быстро распознавать возможные атаки на сетевые устройства. Вот почему гак важно включать в число областей управления сетью инструмент управления конфигурациями, который может быть как простой системой, способной лишь распознавать устройства, гак и более сложной системой, способной проверять log-файлы устройств, обнаруживать ошибки конфигураций и составлять статистику использования устройств.

В качестве примера в табл. 1.3.1 приведен перечень типовых наблюдаемых параметров управления сетью.

Таблица 1.3.1

|  |  |  |
| --- | --- | --- |
| № п/п | Параметр | Содержание параметра |
| 1 | Скорость распространения | Величина, обратная времени передачи пакета  между абонентами с момента поступления данных в сеть; это время зависит от используемой среды передачи, пропускной способности сети и расстояния между абонентами |
| 2 | Задержка очереди | Среднее времяожидания пакета в очередиустройства до посылки или по прибытию, до его передачи приложению |
| 3 | Задержка | Время, в течение которого пакет перелается от источника к пункту назначения, включающее в себя все промежуточные задержки распространения в очередь задержки |
| 4 | Ширина:  а) полосы  6) полосы узкого  места | Характеризует пропускную способность сетевого соединения (объем данных, передаваемыхза единицу времени).  Покатывает скорость передачи пакета через самые медленные узлы сети |
| 5 | Пропускная  способность | Покатывает объем данных, которые можнопередать через сетевое соединение в единицу времени |
| 6 | Латентность | Время движения пакета от источника до пункта назначения |
| 7 | Потеря пакетов | Процент пакетов, теряющихся при передаче |
| 8 | Неустойчивость | Варьирование временной задержки пакетов |

**Задачи анализа производительности и надежности связаны** с оценкой времени реакции системы, пропускной способности реального или виртуального канала связи между двумя конечными абонентами сети, интенсивности трафика в отдельных сегментах и каналах сети, вероятности искажения данных при их передаче через сеть, а также коэффициента готовности сети или ее определенной транспортной службы.

Анализ проводится после сбора необходимой статистической информации. Функции анализа производительности и надежности сети нужны как для оперативного управления сетью, так и для планирования развития сети. Результаты анализа производительности и надежности позволяют контролировать соглашение об уровне обслуживания, заключаемое между пользователем сети и ее администраторами или компанией, продающей услуги. Подобное соглашения в количественной форме оговаривают все перечисленные ранее функции управления безопасностью (например, максимальное время устранения отката, реальный коэффициент готовности службы в течение года, месяца и пр.).

**Управление безопасностью** включает в себя:

* контроль доступа:
* сохранение целостности данных.

В функции управления безопасностью входят процедуры аутентификации, проверки привилегий, поддержка ключей шифрования, управления полномочиями, а также механизмы управления паролями, внешним доступом и соединения с другими сетями.

**Учет работы сети** включает в себя регистрацию и управление используемыми ресурсами и устройствами. Эта функция оперирует понятиями «время использования» и «плата за ресурсы».

Из приведенного списка групп задач системы управления видно, что последние выполняют не только функции мониторинга н анализа работы сети, необходимые для получения исходных данных для настройки сети, но и функции активного воздействия на есть — управления конфигурацией и безопасностью, которые нужны для отработки выработанного плана настройки и оптимизации сети. Сам этап создания плана настройки сети обычно остается за пределами функций системы управления, хотя некоторые системы управления имеют в своем составе экспертные подсистемы, помогающие администратору или интегратору определить необходимые меры по настройке сет.

На практике уже несколько лет прослеживается отчетливая тенденция интеграции систем управления сетями и систем управления системами в единые интегрированные продукты управления корпоративными сетями. Наблюдается также интеграция систем управления телекоммуникационными сетями с системами управления корпоративными сетями. Эта близость функций систем управления сетями н систем управления системами породила разработчикам стандартов OSI не делать различия между ними н разрабатывать общие стандарты управления. В связи с этим целесообразно рассмотреть, как преломляются общие функциональные задачи системы управления, определенные в стандартах X.700IS0 7498-4, в задачи такого конкретного класса систем управления, как системы управления компьютерами и их системным и прикладным ПО, которые называются системами управления системой (SystemManagementSystem).

Обычно система управления системой выполняет следующие функции:

* учет используемых аппаратных и ПС. Система автоматически собирает информацию об установленных в сети компьютерах и создаст записи в специальной базе данных об аппаратных и программных ресурсах. После этого администратор может быстро выяснить, какими ресурсами он располагает и где тот или иной ресурс находится (например, узнать о том.на каких компьютерах нужно обновить драйверы принтеров, какие компьютеры обладают достаточным количеством памяти, дискового пространства н т. п.);
* распределение и установка программного обеспечения. После завершения обследования администратор может создать пакеты рассылки нового ПО, которое нужно инсталлировать на всех компьютерах сети или на какой-либо группе компьютеров. В большой сети, где проявляются преимущества системы управления, такой способ инсталляции может существенно уменьшить трудоемкость этой 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. Эта группа функций позволяет удаленно измерять наиболее важные параметры компьютера, ОС, СУБД и т.д. (например, коэффициент использования процессора, интенсивность страничных прерываний, коэффициент использования физической памяти, интенсивность выполнения транзакций). Для разрешения проблем эта группа функций может давать администратору возможность брать на себя удаленное управление компьютером в режиме эмуляции графического интерфейса популярных ОС. База данных системы управления обычно хранит детальную информацию о конфигурации всех компьютеров в сети для того, чтобы можно было выполнять удаленный анализ возникающих проблем.

Как видно из описания функций системы управления системами, они повторяют функции системы управления сетью, но только для других объектов. Действительно, функция учета используемых аппаратных и ПС соответствует функции построения карты сети, функция распределения и установки ПО соответствует функции управления конфигурацией коммутаторов и маршрутизаторов, а функция анализа производительности и возникающих проблем соответствует функции производительности.

Архитектура систем управления сетями IBM. В отличие от рассмотренной архитектуры системы управления сетью, которая отвечает стандартам X.700/ISO 7498-4, система управления сетями IBM имеет собственную архитектуру сетевого управления, в основе которой также лежат пять функциональных групп, ориентированных на пользователя:

1) управление конфигурацией — идентифицирует ресурсы физических и логических систем и обеспечивает управление их взаимоотношениями; 2) управление производительностью и учетом использования ресурсов — обеспечивает квалификацию, измерение, сообщение и управление реакцией, доступностью, утилизацией и использованием компонентов сети;

3) управление проблемами — обеспечивает обнаружение, диагностику, решение, а также средства отслеживания и управления проблемой;

4) управление операциями — обеспечивает средства для запроса и управления распределенными сетевыми ресурсами из центрального пункта;

5) управление изменениями — обеспечивает планирование и применение модификаций в аппаратном и программном обеспечении системы.

Сравнение функций сетевого управления OSI и IBM представлено в табл. 1.3.2.

**Управление конфигурацией** в архитектуре IBM затрагивает как физические, так и логические ресурсы информационных систем и их взаимоотношение друг с другом. Эта информация обычно состоит из названий ресурсов, адресов, местоположений, контактов и телефонных номеров. Функция управления конфигурацией IBM почти соответствует концепции OSI об управлении конфигурацией. Так же как и в стандартной архитектуре, пользователи с помощью средств управления конфигурацией могут поддерживать ведомость сетевых ресурсов, а управление конфигурацией помогает гарантировать быстроту и точность отражения изменений сетевой конфигурации в базе данных конфигурационного управления и т. д.

Таблица 1.3.2

|  |  |
| --- | --- |
| Области управления OSI | Области управления IBM |
| Управление конфигурацией сети | Управление конфигурацией |
| Анализ производительности и надежности | Управление производительностью и учетом сетевых ресурсов |
| Учет работы сети |
| Обработка ошибок | Управление проблемами |
| Управление безопасностью | - |
| - | Управление операциями |
| - | Управление изменениями |

**Управление производительностью и учетом использования ресурсов** позволяет пользователям определять, будут ли удовлетворены задачи производительности сети. Функция включает в себя учет ресурсов, контролирование времени реакции, доступности, утилизации и компонентной задержки, а также регулировку, отслеживание и управление производительностью. Информация от работы каждой из этих функций может привести к инициированию процедуры определения проблемы, если уровни производительности не отвечают требуемым условиям.

**Управление проблемами.** Система определяет проблему как сбойную ситуацию, которая приводит к потере пользователем всех функциональных свойств и ресурсов системы. К задачам системы управления проблемами относятся:

1) определение проблемы. Система выявляет проблему и выполняет шаги, необходимые для начала диагностики проблемы. Назначение этой области — изолировать проблему в конкретной подсистеме (например, в каком-нибудь аппаратном устройстве, программном изделии, компоненте микрокода или сегменте носителя);

2) диагноз проблемы. Система определяет точную причину проблемы и воздействие, необходимое для решения этой проблемы. Если диагноз проблемы выполняется вручную, то он следует за определением проблемы. Если он выполняется автоматически, то это обычно делается одновременно с определением проблемы, чтобы можно было выдать результаты вместе;

3) обход проблемы и восстановление. Выполняются попытки обойти проблему либо частично, либо полностью. Обычно эта операция является временной, причем подразумевается, что далее последует полное ее решение;

4) решение проблемы. Включает в себя усилия, необходимые для устранения проблемы. Решение проблемы обычно начинается после установления ее диагноза и часто включает в себя корректирующее воздействие, которое должно быть занесено в график (например, замена отказавшего дисковода);

5) отслеживание и управление проблемой до ее полного решения. В частности, если для решения проблемы необходимо внешнее воздействие, то критическая для системы информация, описывающая эту проблему, включается в запись управления проблемой и вводится в БД этой проблемы.

**Управление операциями** включает в себя управление распределенными сетевыми ресурсами из центрального пункта. Оно предусматривает два набора функций: услуги общих операций и услуги управления операциями. Услуги общих операций обеспечивают управление ресурсами с помощью прикладных программ. Услуги управления операциями обеспечивают возможность управления дистанционными ресурсами путем активации и дезактивации ресурсов, отмены команды и установки часов сетевых ресурсов.

**Управление изменениями** помогает пользователям управлять сетевыми или системными изменениями путем обеспечения отправки, извлечения, установки и удаления файлов изменений в отдаленных узлах. Кроме того, управление изменениями обеспечивает активацию узла. Изменения имеют место либо из-за изменений в требованиях пользователя, либо из-за необходимости обойти проблему.

**Многоуровневая архитектура управления TMN**

Кроме разделения задач управления на пять функциональных групп следует разделять задачи управления на уровни в соответствии с иерархической организацией корпоративной сети. Корпоративная сеть строится иерархически, отражая иерархию самого предприятия и его задач.

Нижний уровень сети составляют элементы сети: отдельные компьютеры, коммуникационные устройства, каналы передачи данных. На следующем уровне иерархии эти элементы образуют сети разного масштаба: сети рабочей группы, отдела, отделения и, наконец, сеть предприятия в целом.

Для построения интегрированной системы управления разнородными элементами сети обычно применяется иерархический подход. Применительно к системам управления сетями наиболее проработанным и эффективным для создания многоуровневой иерархической системы является стандарт TelecommunicationManagementNetwork (TMN) [54].

На каждом уровне иерархии модели TMN решаются задачи одних и тех же пяти функциональных групп, рассмотренных ранее (управления конфигурацией, производительностью, ошибками, безопасностью и учетом), однако на каждом уровне эти задачи имеют свою специфику. Чем выше уровень управления, тем более общий характер приобретает собираемая о сети информация, а сугубо технический характер собираемых данных по мере повышения уровня меняется на производственный, финансовый и коммерческий. Модель TMN упрощенно можно представить в виде двухмерной диаграммы, представленной на рисунок 1.3.1.

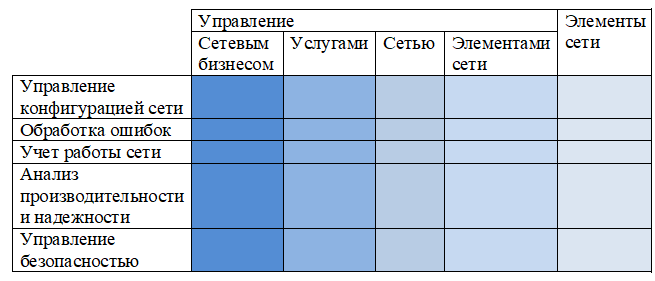


Рис.1.3.1 – Многоуровневое представление задач управления сетью

Нижний уровень — уровень элементов сети — состоит из отдельных устройств сети: каналов, усилителей, оконечной аппаратуры, мультиплексоров, коммутаторов и т.п. Элементы могут содержать встроенные средства для поддержки управления (датчики, интерфейсы управления), а могут требовать для связи с системой управления разработки специального оборудования — устройств связи с объектом. Современные технологии обычно имеют встроенные функции управления, которые позволяют выполнять хотя бы минимальные операции контроля состояния устройства и за передаваемым устройством трафиком.

Следующий уровень — уровень управления элементами сети — представляет собой элементарные системы управления, которые автономно управляют отдельными элементами сети, например коммутатором или мультиплексором. Уровень управления элементами изолирует верхние слои системы управления от деталей и особенностей управления конкретным оборудованием. Этот уровень ответственен за моделирование поведения оборудования и функциональных ресурсов нижележащей сети.

Выше лежит уровень управления сетью, который координирует работу элементарных систем управления, позволяя контролировать конфигурацию составных каналов, согласовывать работу транспортных подсетей разных технологий и т. п. С помощью этого уровня сеть начинает работать как единое целое, передавая данные между своими абонентами.

Следующий уровень — уровень управления услугами — занимается контролем и управлением за транспортными и информационными услугами, которые предоставляются конечным пользователям сети. В задачу этого уровня входят подготовка сети к предоставлению определенной услуги, ее активизация, обработка вызовов клиентов. Формирование услуги заключается в фиксации в БД значений параметров услуги, например требуемой средней пропускной способности, максимальных величин задержек пакетов и т. п.

В функции этого уровня входит выдача уровню управления сетью задания на конфигурирование виртуального или физического канала связи для поддержания услуги. После формирования услуги данный уровень занимается контролем качества ее реализации, т. е. соблюдением сетью всех принятых на себя обязательств в отношении производительности и надежности транспортных услуг. Результаты контроля качества обслуживания нужны, в частности, для подсчета оплаты за пользование услугами клиентами сети.

Уровень бизнес-управления занимается вопросами долговременного планирования сети с учетом финансовых аспектов деятельности организации, владеющей сетью. На этом уровне помесячно и поквартально подсчитываются доходы от эксплуатации сети и ее отдельных составляющих, учитываются расходы на эксплуатацию и модернизацию сети, принимаются решения о развитии сети с учетом финансовых возможностей.

**Схема «Менеджер—Агент»** — основа управления сетью. Выделение в системах управления типовых групп функций и разбиение этих функций на уровни еще не дает ответа на вопрос, каким же образом устроены системы управления, из каких элементов они состоят и какие архитектуры связей этих элементов используются на практике. Оказывается, в основе построения любой системы управления сетью лежит концепция, называемая «Менеджер—Агент». Примером Агента может служить программа слежения за действиями пользователей терминальных клиентов LanAgent, которая осуществляет контроль и мониторинг всех действий пользователей:

* перехватывает все нажатия клавиш;
* делает снимки экрана;
* отслеживает установку, удаление, запуск и закрытие программ;
* следит за изменением и содержимым буфера обмена данными;
* следит за состоянием файлов, папок и списком посещенныхсайтов;
* ведет учет документов, распечатываемых на принтере, и логов запускаемых программ.

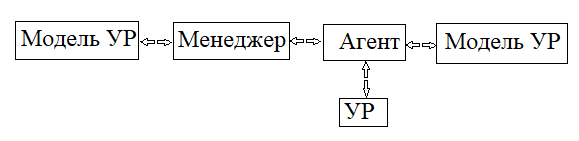


Рис.1.3.2 – Взаимодействие Агента, Менеджера и управляемого ресурса

Подобные Агенты позволяют выявлять деятельность пользователей, не имеющую отношения к тематике отдела предприятия или офиса.

На основе схемы «Агент—Менеджер» могут быть построены системы управления сетями практически любой сложности с большим количеством Агентов и Менеджеров разного типа. Схема «Менеджер—Агент» представлена на Рис.1.3.2. Агент здесь является посредником между основной управляющей программой менеджером и управляемым ресурсом (УР), в качестве которого могут выступать: канал передачи данных, ОС и (или) маршрутизатор. Для того чтобы один и тот же Менеджер мог управлять различными реальными ресурсами, создается модель управляемого ресурса, которая отражает только те его характеристики, которые нужны для контроля и управления ресурсом. Например, модель маршрутизатора обычно включает в себя такие характеристики, как количество портов, их тип, таблица маршрутизации, количество кадров и пакетов протоколов канального, сетевого и транспортного уровней, прошедших через эти порты.

Менеджер получает от Агента только те данные, которые описываются моделью ресурса. Агент же является некоторым экраном, освобождающим Менеджера от ненужной информации о деталях реализации ресурса. Агент поставляет Менеджеру обработанную и представленную в нормализованном виде информацию. На основе этой информации Менеджер принимает решения по управлению, а также выполняет дальнейшее обобщение данных о состоянии управляемого ресурса, например строит зависимость загрузки порта от времени.

Для получения требуемых данных от объекта, а также для выдачи на него управляющих воздействий Агент взаимодействует с реальным ресурсом нестандартным способом (вне протокола). Когда Агенты встраиваются в коммуникационное оборудование, разработчик оборудования предусматривает точки и способы взаимодействия внутренних узлов устройства с Агентом. При разработке Агента для ОС разработчик Агента пользуется теми интерфейсами, которые существуют в этой ОС, например интерфейсами ядра, драйверов и приложений. Агент может снабжаться специальными датчиками для получения информации, например датчиками релейных контактов или датчиками температуры.

Менеджер и Агент работают с одной и той же моделью управляемого ресурса, однако в использовании этой модели Агентом и Менеджером имеется существенное различие. Агент наполняет модель управляемого ресурса текущими значениями характеристик данного ресурса, в связи с чем модель Агента называют базой данных управляющей информации — ManagementInformationBase (MIB). Менеджер использует модель, чтобы знать о том, чем характеризуется ресурс, какие характеристики он может запросить у Агента и какими параметрами можно управлять.

Менеджер взаимодействует с Агентами по стандартному протоколу. Этот протокол должен позволять Менеджеру запрашивать значения параметров, хранящихся в базе MIB, а также передавать Агенту управляющую информацию, на основе которой тот должен управлять устройством. Различают управление inband, т.е. по тому же каналу, по которому передаются пользовательские данные, и управление out-of-band, т.е. вне канала, по которому передаются пользовательские данные. Например, если Менеджер взаимодействует с Агентом, встроенным в маршрутизатор, по протоколу SNMP, передаваемому по той же ЛВС, что и пользовательские данные, то это будет управление inband. Если же Менеджер контролирует коммутатор первичной сети, работающий по технологии частотного уплотнения FDM, с помощью отдельной сети Х.25, к которой подключен Агент, то это будет управление out-of-band.

Управление inband более экономично, так как не требует создания отдельной инфраструктуры передачи управляющих данных.

Однако управление out-of-band более надежно, так как предоставляется возможность управлять оборудованием сети и тогда, когда какие-то элементы сети вышли из строя и по основным каналам оборудование недоступно. Стандарт многоуровневой системы управления TMN для управления ТКС создает отдельную управляющую сеть, которая обеспечивает режим out-of-band.

Обычно Менеджер работает с несколькими Агентами, обрабатывая получаемые от них данные и выдавая на них управляющие воздействия. Агенты могут встраиваться в управляемое оборудование, а могут работать на отдельном компьютере, связанном с управляемым оборудованием по какому-либо интерфейсу. Менеджер обычно работает на отдельном компьютере, который выполняет также роль консоли управления для оператора или администратора системы. Модель «Менеджер — Агент» лежит в основе таких популярных стандартов управления, как SNMP (стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур UDP/TCP) и стандарты управления ISO/OSI на основе протокола CMIP (выполняет специальные функции, не предусмотренные протоколом SNMP).

Агенты могут отличаться различным уровнем интеллекта —

они могут обладать как самым минимальным интеллектом, необходимым для подсчета проходящих через оборудование кадров и пакетов, так и высоким, достаточным для выполнения самостоятельных действий по выполнению последовательности управляющих действий в аварийных ситуациях, построению временных зависимостей, фильтрации аварийных сообщений.

**Платформенный подход**. При построении систем управления крупными локальными и корпоративными сетями обычно используется платформенный подход, когда индивидуальные программы управления разрабатываются не «с нуля», а используют службы и примитивы, предоставляемые специально разработанным для этих целей программным продуктом — платформой. Примерами платформ для систем управления являются SunNetManager, CdbletronSpectrum, IMB/TivoliTMN 10. Эти платформы создают общую операционную среду для приложений системы управления точно так же, как универсальные ОС, такие как Unix или Windows NT, создают операционную среду для приложений любого типа.

Платформа обычно включает в себя поддержку протоколов взаимодействия Менеджера с Агентами — SNMP, набор базовых средств для построения Менеджеров и Агентов, а также средства графического интерфейса для создания консоли управления. В набор базовых средств обычно входят функции, необходимые для построения карты сети, средства фильтрации сообщений от Агентов, средства ведения базы данных. Набор интерфейсных функций платформы образует интерфейс прикладного программирования (API) системы управления. Пользуясь этим API, разработчики в ОС той или иной платформы прямо создают законченные системы управления специфическим оборудованием.

Обычно платформа управления поставляется с каким-либо универсальным Менеджером, который может выполнять некоторые базовые функции управления без программирования. Чаще всего к этим функциям относятся функции построения карты сети, Функции отображения состояния управляемых устройств и функции фильтрации сообщений об ошибках. Например, одна из наиболее популярных платформ HP OpenView поставляется с Менеджером NetworkNodeManager, который выполняет перечисленные функции.

Компании, производящие коммуникационное оборудование, разрабатывают добавочные Менеджеры для популярных платформ, которые выполняют функции управления оборудованием данного производителя более полно.

Хорошая платформа системы управления сетью позволяет отслеживать изменение параметров сети в реальном времени и представлять их графически на мониторе администратора сети.

Эти платформы опираются на единые для всех протоколов архитектуры и содержат Агенты, базу данных управления MIB и рабочую станцию управления и слежения.

**Технология RMON**. Эффективным добавлением к функциональным возможностям SNMP является спецификация RMON, которая обеспечивает удаленное взаимодействие с базой MIB. До появления RMON протокол SNMP не мог использоваться удаленным образом, он допускал только локальное управление устройствами. База RMONMIB обладает улучшенным набором свойств для удаленного управления, так как содержит агрегированную информацию об устройстве, что не требует передачи по сети больших объемов информации.

Объекты RMONMIB включают в себя 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 RMONMIB 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 могут быть выполнены в виде отдельных программных модулей, работающих на универсальных ПК и ноутбуках (примером может служить LANalyzerNovell).

Объект RMON в базе MIB объединяет следующие объекты:

* Statistics — статистические данные о количестве пакетов, коллизий и т. п.;
* History — статистические данные, сохраненные через определенные промежутки времени для анализа тенденций их изменений;
* Alarms — пороговые значения статистических показателей, при превышении которых Агент RMON посылает сообщение Менеджеру;
* Host — данные о хостах сети, включая их МАС-адреса;
* HostTopN — таблица наиболее загруженных хостов сети;
* TrafficMatrix — статистика об интенсивности трафика между каждой парой хостов сети, упорядоченная в виде матрицы;
* Filter — условия фильтрации пакетов;
* PacketCapture — условия захвата пакетов;
* Event — условия регистрации и генерации событий.

Отличительной чертой стандарта RMONMIB 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 сетях с различными протоколами сетевого уровня.

**Протоколы управления: SNMP, CMIP, TMN**

Большая часть работы по управлению компьютерными сетями состоит из слежения за работой устройств, контроля производительности компьютерной сети, диагностики проблем и устранения причин возникновения этих проблем. К настоящему моменту разработаны два аналогичных протокола для управления ЛВС:

* простой протокол для управления вычислительной сетью — SimpleNetworkManagementProtocol (SNMP) — для решения коммуникационных проблем TCP/IP;
* протокол общего управления информацией — CommonManagementInformationProtocol (CMIP) — продукт международного комитета по стандартизации.

Каждый из этих протоколов имеет свои преимущества, и производители сетевых систем разрабатывают средства управления ЛВС с учетом требований обоих протоколов. Протоколы SNMP и CMIP имеют общую цель, состоящую в облегчении задач управления и диагностики при работе в ЛВС. Оба протокола используют рассмотренную в предыдущем подразделе базу MIB, состоящую из набора переменных, тестовых точек и контрольных параметров, которые поддерживаются всеми устройствами ЛВС и могут контролироваться администратором ЛВС. Оба протокола поддерживают также расширения MIB, вводимые различными производителями в целях сбора большого количества служебной информации при запросах в ЛВС.

При разработке систем управления компьютерными сетями Производители сочетают возможности протоколов SNMP и CMIP. Совместимость обоих протоколов позволяет производителям создавать системы управления ЛВС, которые смогут принимать информацию как от SNMP, так и от CMIP, а хранить ее в общем формате.

**Различия SNMP и CMIP**. Протоколы SNMP и CMIP различаются способами, при помощи которых они извлекают и выдают данные о вычислительной сети. Эти протоколы предлагают различные функции, требуют разных затрат вычислительной мощности и используют разное количество памяти. Каждый из этих протоколов использует собственный набор протоколов низкого уровня для передачи и приема информации, необходимой для управления ЛВС, и каждый протокол поддерживается различными комитетами по стандартизации.

**Доступ к данным**. Протоколы SNMP и CMIP имеют функции извлечения данных, но делают это разными способами. Протокол SNMP предназначен для получения сведений о конкретных устройствах, а протокол CMIP ориентирован на извлечение наборов данных. При использовании SNMP необходима точная формулировка запроса об интересующем вас предмете. В случае CMIP вы имеете возможность сделать общий запрос и затем уточнять его, определяя, какая информация вас не интересует.

**Опрос/отчет**. Протокол SNMP работает через опросы, т.е. центральное устройство управления (возможно, ваша рабочая станция) периодически опрашивает каждое устройство в ЛВС для определения его статуса. В протоколе CMIP используются отчеты, в которых устройства информируют центральную управляющую станцию об изменениях в своем статусе.

При большом числе устройств протокол SNMP может вызвать большой трафик ЛВС и замедлить ее работу, но он может работать с любыми устройствами, включая самые примитивные, которые не могут сами определить свою неисправность.

**Размеры и производительность**. Система управления ЛВС на базе протокола SNMP может быть меньших размеров, более быстродействующей и менее дорогостоящей по сравнению с CMIP. Система CMIP требует более быстродействующего компьютера и большего объема памяти.

**Протоколы транспортного уровня**. Для передачи запросов и ответов при управлении ЛВС в SNMP используются простые датаграммы, при которых связывающиеся стороны должны предусматривать возможность неполучения данных адресатом. Это значит, что отправитель должен повторить передачу несколько раз, прежде чем констатировать факт неработоспособности адресата. В SNMP для маршрутизации сообщений могут быть использованы простые коммуникационные протоколы (например, IPX или IP и UDP).

Использование в протоколе CMIP сеансового обмена информацией делает его более удобным при необходимости получения большого количества данных. Однако это может затруднить управление сетью при возникновении неполадок. Если ЛВС выйдет из строя или практически перестанет функционировать, то SNMP будет продолжать посылать управляющие запросы до тех пор, пока один из них не пройдет. Сеансовый обмен информацией, на котором базируется CMIP, становится невозможным, как только пропадает связь в результате сбоя в работе ЛВС.

**Стандарты протоколов**. Протокол CMIP является протоколом OSI, поэтому контролируется Международной организацией по стандартизации ISO. Производители систем, реализующих протокол CMIP, могут проверять свои изделия в Корпорации открытых систем — CorporationofOpenSystems (COS), где производится тестирование на совместимость с протоколами OSI.

В противоположность этому SNMP не является международным стандартом. Однако, подобно TCP/IP, SNMP, контролируется Советом по архитектуре Интернета (InternetActivitiesBoar), осуществляющим надзор за архитектурой Интернета, включая его протоколы и связанные с ними процедуры, а также надзор за созданием новых стандартов Интернета.

На практике главным преимуществом SNMP перед CMIP является то, что изделий на базе SNMP гораздо больше. Несмотря на определенные преимущества CMIP был использован в небольшом количестве сетевых устройств. Продукты же на базе SNMP — маршрутизаторы, Ethernet-разветвители, волоконно-оптические и прочие устройства — широко распространены. Причиной этого отчасти является разница в возрасте этих протоколов — SNMP гораздо старше. Но в настоящее время многие компании разрабатывают системы управления вычислительными сетями, использующие CMIP или комбинацию SNMP и CMIP.

Протокол SNMP больше ориентирован на управление конкретными устройствами, в то время как CMIP лучше подходит для коммуникаций между двумя или несколькими системами управления ЛBC. С этих позиций SNMP и CMIP могут играть взаимно дополняющую роль. В зависимости от размеров и сложности ЛВС может оказаться, что лучшей является система управления, исполь3Ующая как CMIP, так и SNMP.

Рассмотрим, как происходит управление сетью на базе протокола SNMP. Протокол SNMP создавался специально для контроля удаленных сегментов сети без применения постоянного мониторинга и необходимости непосредственного присутствия администратора. Он позволяет выполнять статистическую оценку работы сети за длительные периоды и осуществлять подробный анализ ее функционирования в течение коротких промежутков времени.

Чтобы сеть, не дожидаясь поступления запроса, могла проинформировать управляющую станцию о проблеме, SNMP предусматривает возможность отправки незапрашиваемого отклика — так называемого прерывания (trap). С помощью функции отправки прерываний управляемое устройство — Агент SNMP — способно уведомить управляющую станцию, например, о достижении либо превышении заранее указанных значений и, таким образом, привлечь к себе внимание. При получении определенных или любых прерываний станция управления сетью уведомит пользователя, например путем отправки сообщения по электронной почте или подачи сигнала на пейджер.

Для коммутаторов, поддерживающих протокол SNMP, существует много различных баз управляющей информации (MIB). По сути, эти базы представляют собой словари-справочники, в которых перечислены разрешенные запросы с возможными откликами на них и соответствующим описанием. Каждая поддерживаемая производителем база MIB позволяет консоли управления получить более или менее подробное описание текущего состояния сети поблизости от устройства, за которым ведется наблюдение, включая и его самого.

В отличие от частных MIB, обычно предназначенных для поддержки определенного типа коммутатора и программного кода, стандартные базы MIB, опирающиеся на документы RFC, позволяют эффективно следить за всей коммутируемой сетью. Для обеспечения диагностики наиболее полезны следующие базы MIB, перечисленные в порядке возрастающей детализации данных:

a) RFC 1213 — MIB II; б) RFC 2021 — RMON 2; в) RFC 1643 -Ethernet-Like Interface MIB; г) RFC 2819 — RMON Ethernet.

При использовании SNMP для мониторинга сети необходимо обратить особое внимание на вопросы безопасности. Если Агенты SNMP не защищены от несанкционированного доступа, то злоумышленник, находящийся где угодно, в состоянии отследить работу вашей сети или даже поменять настройки коммутаторов. Часто протокол SNMP включен по умолчанию и защищен несложным паролем, одинаковым как для коммутаторов, так и для других Агентов SNMP.

Пароли SNMP называют также общей строкой, поскольку в нее включаются и имя, и пароль, которые вводятся с учетом регистра и знаков препинания. Пароль передается в виде открытого текста, что само по себе создает дополнительную опасность. Чтобы закрыть эту лазейку, в третьей версии SNMP предусмотрены процедуры аутентификации и шифрование передачи. Необходимо, как минимум, сразу же изменить пароль, заданный по умолчанию, Агенты SNMP можно настроить таким образом, чтобы разным пользователям предоставлялись разные уровни доступа, они откликались бы на запросы от конкретной подсети и игнорировали запросы от других подсетей, отвечали бы на запросы только конкретных IP-адресов. Помимо перечисленных настроек возможны и другие.

Маршрутизаторы, через которые пролегает путь к Агентам SNMP, способны накладывать на использование SNMP дополнительные ограничения. Брандмауэры (firewall) могут полностью блокировать работу SNMP. Но получения доступа к Агенту с помощью SNMP недостаточно — Агент должен поддерживать базу MIB, к которой обращен ваш запрос. Большинство производителей реализуют поддержку стандартных баз MIB в нужном объеме, однако некоторые этого не делают. В отдельных случаях необходимо обновить ОС коммутатора, чтобы он мог поддерживать желаемую общую или частную базу MIB.

Если коммутатор не отвечает на запрос SNMP, то это может быть следствием отсутствия в коммутаторе необходимой базы MIB. С помощью протокола SNMP можно получить любую информацию о вашей сети, если Агент поддерживает соответствующую базу MIB.

**Стек протоколов TNM**. В основе любой системы управления сетью, как уже отмечалось ранее, лежит схема взаимодействия Агента с Менеджером, показанная на рис. 1.3.3. Агенты и Менеджеры представляют собой программно-аппаратные модули, устанавливаемые в телекоммуникационное оборудование, либо программные модули, встроенные в ОС и выполняющие функции диагностики и управления телекоммуникационным устройством.



Рис.1.3.3 – Общая схема взаимодействия Агент—МенеджерПодключение сетевого элемента (СЭ) к архитектуре TMN также выполняется по принципу «Агент—Менеджер», причем Агент реализуется в сетевом элементе, а Менеджер — в центре управления (ЦУ).

Агент и Менеджер являются активными взаимодействующими компонентами TMN, которые распределены по сети и общаются путем обмена сообщениями. Сообщения со стороны Менеджера переносят запросы на выполнение операций (ЗО), которые предусмотрены в информационных структурах обслуживаемых Агентом объектов. Агент может передавать уведомления (УВ), генерируемые либо в ответ на запрос Менеджера, либо автономно. В теле уведомления могут передаваться атрибуты, характеризующие состояние объекта. Процесс Агент является ключевым звеном любого сетевого элемента, совместимого с TMN: телефонной станции, маршрутизатора, центра эксплуатационного управления и т.д.

Кроме того, подключение сетевого элемента к архитектуре TMN предполагает наличие иерархического стека протоколов, каждый из которых на каждом уровне стека отвечает за обмен блоками данных этого уровня. Стек протоколов обеспечивает последовательное преобразование информации, начиная от абстрактного описания объектов и операций на некотором языке высокого уровня. Далее формируются двоичные наборы данных сетевого уровня, которые с помощью протоколов транспортного (и далее пакетного и физического) уровней передаются в сеть для отправки адресату. При получении адресатом предназначенного ему пакета происходит обратное восстановление данных (операций).

Каждый элемент в сети заменяется абстрактной информационной моделью (АИМ), которая рассматривает его как сетевой ресурс. Параметры этого ресурса (объекта информационной модели) передаются средствами используемого протокола (например, CMIP). Информационная модель определяет основные параметры объекта, абстрагируясь от его физической сущности и используя наборы атрибутов, уведомлений и действий.

Для создания информационной модели объекта, который описывается как некоторый класс в терминах объектно-ориентированного подхода, в стандартах TMN используются шаблоны GDMO (Х.722), на смену которым в ближайшем будущем придет язык IDL, используемый для описания данных в системах CORBA и JAVA.

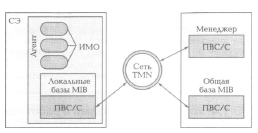


Рис. 1.3.4. Взаимодействие процессов Агент—Менеджер через сеть TMN

Как уже указывалось ранее, в качестве информационной базы данных, откуда Менеджер и (или) Агент получают информацию о структуре и особенностях любого зарегистрированного в сети объекта, используется база данных MIB, которая является ресурсом, разделяемым всеми объектами сети. Все объекты, зарегистрированные в сети, представлены своими информационными моделями (ИМО).

Интерфейс (называемый Q-интерфейсом или Q-адаптером), через который Агент взаимодействует с Менеджером через сеть TMN, представляет собой стек протоколов выхода в сеть CMIP/CORBA, показанный на рисунке 3.4. В его основе лежат следующие принципы:

* использование в качестве транспортного средства для передачи сообщений между Агентом и Менеджером полного семиуровневого стека протоколов, соответствующего модели OSI, в качестве которого могут применяться стеки ISO/OSI или TCP/IP;
* использование для передачи сообщений на прикладном уровне протокола CMIP;
* применение поверх CMIP более содержательных протоколов взаимодействия Агент—Менеджер, конкретизирующих отдельные функции эксплуатационного управления, например контроль ошибок, измерение производительности и т. п.

Так как Менеджер связывается с Агентом при помощи полного транспортного стека, то при сборе данных от встроенных Агентов можно использовать промежуточную сеть передачи данных произвольной сложности. Это обстоятельство является одним из важных компонентов открытости архитектуры TMN. Оно дает возможность объединять любые сети, в том числе и такие, которые не могут переносить в своих основных информационных потоках данные, используемые системой эксплуатационного управления.

Поддержка стандартов TMN и Q-интерфейса декларируется практически всеми ведущими разработчиками платформ эксплуатационного управления: Hewlett-Packard, Digital, Sun, Cabletron, IBM, TTI. К тому же, оборудование новых технологий (SDH, ATM, ADSL, WLL и др.) в настоящее время выпускается со встроенной поддержкой Q-интерфейса.

**Управление отказами в работе сети**

Управлением отказами в сети называется такое управление сетью, которое имеет целью находить и распознавать отказы в сети.

Цели управления отказами: определить, зарегистрировать, уведомить пользователей и, по мере возможности, автоматически разрешить сетевые проблемы, для того чтобы обеспечить эффективное функционирование сети. Поскольку неисправности могут привести к простою или недопустимому снижению производительности, управление отказами в сетевом управлении ISO является наиболее важным элементом.

Управление отказами включает в себя следующие этапы:

* определение симптомов проблемы;
* изолирование и устранение единичной проблемы;
* обнаружение и устранение проблем во всех важных подсистемах;
* запись информации об обнаружении и исправлении проблемы.

Современные средства управлением отказами в ЛВС позволяют прогнозировать, обнаруживать и устранять некоторые виды отказов. Специальные датчики сбора данных о параметрах сетевого оборудовании постоянно информируют систему об уходе этих параметров за установленные пределы. При обнаружении отказа в сети система управления отказами производит соответствующую запись в журнале фиксации отказов, после чего выполняется автоматический и (или) ручной поиск в базе данных решения возникшей проблемы.

Таким образом, инструменты, используемые системой в процессе управления отказами, информируют ее об ошибочных ситуациях, анализируют и указывают причину ошибки, автоматически устраняют ошибочные ситуации. Примером автоматического решения проблемы может служить ПО маршрутизатора, которое способно восстановить прерванный в результате отказа сетевой путь, выбрав альтернативный оптимальный маршрут для передачи пакета и (или) сообщения. Однако этого может и не произойти, если коммутируемая сеть имеет топологию, показанную на рис. 1.3.5, в которой коммутаторы (К) соединены единственным каналом.

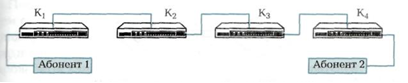


Рис.1.3.5 – Простая коммутируемая сеть

Сеть, представленная на рис. 1.3.6, выгодно отличается от нее наличием параллельных связей между коммутаторами, позволяющими им выбирать альтернативный маршрут для передачи пакетов при выходе из строя любой одной линии связи между коммутаторами.

Повышение уровня связности сети, т. е. создание альтернативных маршрутов, — мощное масштабируемое средство повышения эксплуатационных характеристик сети. Неизбежные дополнительные затраты, как правило, оказываются меньше, чем при простом повышении производительности (за счет применения более сложной технологии канала), а для повышения надежности введение избыточных соединений чаще всего становится единственным практически осуществимым способом достижения цели. При этом не стоит опасаться возможного образования петель в графе топологии резервированной сети, поскольку любой коммутатор и (или) маршрутизатор поддерживает работу специального алгоритма SpanningTree, автоматически устраняющего петли в ячеистой сетевой топологии путем отключения портов, через которые проходит петля.

В настоящее время разработчики ЛВС используют новую технологию резервирования каналов, получившую название «агрегирование портов». Различные производители коммутаторов используют разные термины для реализации этой технологии. Например, компания Cisco (мировой лидер в области сетевых технологий, предназначенных для сети Интернет) использует термин Etherchannel, а компания Brocade (лидер в индустрии производства надежных, высокопроизводительных сетевых решений) использует термин Brocade LAG.

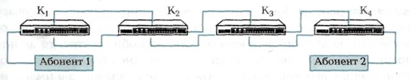


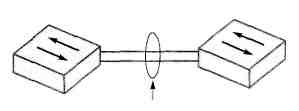
Рис.1.3.6 – Коммутируемая сеть с резервными связями

Рис.1.3.7 – Агрегация портов между двумя коммутаторами

Стандартное решение для агрегирования портов реализовано в протоколе LACP (LinkAggregationControlProtocol). Данный протокол не зависит от производителя коммутационного оборудования и в настоящее время поддерживается почти всеми коммутаторами.

Независимо от производителя все реализации агрегирования портов выполняют одну и ту же задачу по объединению двух и более портов в единый логический порт с повышенной пропускной способностью, резервированием соединений и балансировкой нагрузки между физическими соединениями. Технически коммутаторы соединяются несколькими физическими соединениями для создания единого канала с повышенной пропускной способностью. В качестве примера на рис. 1.3.7 показана агрегация физических соединений между двумя коммутаторами. Если скорость одного физического каналов равна 10 Кбит/с, то скорость агрегированного соединения будет в два раза выше, т. е. 20 кбит/с.

Если просто включить показанную на рис. 1.3.7 пару коммутаторов в действующую сеть, то протокол SpanningTree, который поддерживает каждый из них, воспримет эти соединения как петли и отключит одно дублирующее соединений, оставив активным другое. В связи с этим в паре коммутаторов, использующих агрегированные порты, протокол SpanningTree должен быть отключен и заменен другим — протоколом LACP. Агрегирование портов создает одно логическое соединение, которое может служить как магистралью с удвоенной пропускной способностью, так и в качестве единого соединения (для подключения серверов). При этом коммутаторы и серверы, образующие агрегацию портов, должны использовать единый протокол LACP для совместимости и стабильности работы. Как видим, агрегация портов позволяет резервировать физические соединения: если одно из физических соединений из агрегированного соединения обрывается, то данные могут продолжать передаваться по оставшимся соединениям. Восстановление агрегированного соединения обычно занимает несколько миллисекунд. Поскольку агрегированное соединение может содержать в общем случае N физических соединений, то соединение между коммутаторами будет установлено до тех пор, пока все N физических соединений не оборвутся. Обрывы физических соединений в агрегированном канале обычно не заметны для пользователей. Однако чем меньше физических соединений в агрегированном канале остается, тем большее количество информации требуется передать через оставшиеся в агрегированном канале физические соединения. Чем больше физических соединений находятся в агрегированном канале, тем лучше нагрузка сбалансируется между физическими соединениями.

Системы управления отказами часто используют методы, позволяющие уменьшить риск полной утраты работоспособности системы. Основой подобных мероприятий является резервирование. На практике применяют:

* «холодное» резервирование, при котором запасной модуль, находящийся постоянно на складе, в случае выхода основного модуля монтируется вместо отказавшего устройства;
* «теплое» резервирование, При котором запасной агрегат подключен параллельно основному, но находится в выключенном состоянии и включается автоматически, как только откажет основной агрегат;
* «горячее» резервирование, при котором резервирующий и резервируемый элементы работают параллельно.

С точки зрения времени, требуемого на восстановление работоспособности системы, оптимален вариант с «горячим» резервированием, поскольку он включается практически мгновенно. Однако с точки зрения времени наработки на отказ «горячее» резервирование приводит к преждевременному износу запасных модулей.

Для современных систем (например, коммутаторов) среднее время наработки на отказ составляет сотни тысяч часов непрерывной работы. Отказать может любой элемент сети: линия передачи, образуемая кабелем (витая пара с разъемами 8Р8С, зачастую ошибочно называемыми RJ45, оптоволокно с соответствующими разъемами), порт коммутатора и (или) коммутаторов, плата расширения коммутатора, контроллер плат расширения, процессор коммутации, блок вентилятор, сеть переменного тока.

Для того чтобы обезопасить свою сеть от перебоев электропитания, следует предусматривать источники бесперебойного питания, а если возможны долгосрочные перебои с электропитанием, то и системы резервного энергообеспечения. Чтобы максимально обезопаситься от поломок оборудования, следует резервировать все уязвимые узлы системы и использовать надежное оборудование известных производителей, причем обе рекомендации равнозначны.

Примером горячего резервирования может служить отказоустойчивый сервер Gemini компании ThemisComputer, в котором продублирован каждый компонент. Для распределения задач и процессов используется специализированное ПО и линии связи Ethernet. В подобных системах с двойным резервированием все узлы продублированы сверху донизу — все, от источников питания до питающих проводов, имеется в запасном варианте в каждой половине общего блока.

Каждая половина совершенно независима, со своими собственными системами охлаждения, питания и диагностики, работающими от любого из источников питания. Любая неисправность в какой-либо половине интерпретируется как отказ системы. Это может быть как перегрев поступающего охлаждающего либо вытяжного воздуха, так и выход напряжения питания за границы допуска, невозможность обновить значение сторожевого таймера либо ошибка программного протокола. Любое из этих событий может привести к запуску процедуры отключения соответствующей половины, после чего другая половина берет всю вычислительную нагрузку на себя.

**Управление производительностью и безопасностью**

Управление производительностью. Это вид сетевого управления, которое позволяет следить за нагрузкой сетевых узлов и устройств и, таким образом, находить узкие места в сети. Процессу планирования производительности способствуют проверка сетевых устройств на соответствие предъявляемым к ним требованиям и корректность их использования в инфраструктуре сети. Основные параметры, влияющие на эффективное управление производительностью сети:

* объем данных, передаваемых по сети в единицу времени;
* время реагирования устройств и сервисов в часы пик, равное сумме времени запроса, обработки и ответа;
* процент отклоненных запросов из-за перегрузки сети;
* среднее время между двумя ошибками (доступность сети).

Управление производительностью включает в себя следующие мероприятия:

* сбор статистики использования устройств сети;
* определение порога уведомления;
* тестирование сети;
* составление отчетности.

Задачу сбора статистики использования устройств сети в сети выполняет отдельная подсистема, которая является частью общего программного комплекса по управления сетью. Подсистема накапливает разнообразную информацию о параметрах работы ЛВС, необходимую для решения задач управления сетью. Собственно сбор статистики работы сети предполагает периодическое получение информации о состоянии устройств сети. Данный процесс базируется на использовании протокола SNMP — простого протокола управления сетью. Получаемая информация ограничена управляющей базой, поддерживаемой SNMP-агентом. Все устройства, входящие в состав современных ЛВС, как минимум, поддерживают стандартную управляющую базу MIB2 и базу удаленного мониторинга RMON, что необходимо для систем, построенных но распределенному принципу, реализующих сбор статистики удаленно через сеть.

Использование протокола SNMP в подсистеме сбора статистики работы сети позволяет получить гибкий, универсальный и, главное, стандартизированный подход к получению информации о состоянии устройств сети. Гибкость использования SNMP заключается в расширяемости информационной базы, поддерживаемой устройствами, и в использовании абстракции получения данных, которая позволяет использовать общий подход получения данных, не опираясь на их конкретное значение и интерпретацию. В более продвинутых системах наряду с протоколом SNMP используется протокол управляющих сообщений — ICMP, с помощью которого производится сбор информации о доступности хостов на основе эхо-запросов и данных о состоянии ТСР-и UDP-портов, позволяющих определить работу определенных служб.

Подсистема сбора статистики сети позволяет производить периодический сбор данных о состоянии информационно-вычислительной сети. Собираемые данные задаются в параметрах работы подсистемы. При запуске исполняемого модуля программы производится считывание начальных параметров опроса из конфигурационного файла. Обычно изменение параметров опроса во время работы подсистемы выполняется без ее останова. Для обеспечения универсальности взаимодействия с другими подсистемами передаваемые данные преобразуются в XML-документ, передаваемый через сеть по протоколу передачи гипертекста HTTP. Использование языка XML позволяет существенно упростить протокол обмена данными между подсистемами, упрощается взаимодействие модулей, написанных на разных языках программирования и под разные платформы.

Как правило, подсистема сбора статистики обеспечивает получение данных от некоторого количества устройств сети одновременно. Для получения данных от одного устройства может потребоваться несколько минут, что не должно препятствовать сбору данных с другого устройства. Для решения этой проблемы используется идеология пула потоков, позволяющая выполнять одновременно несколько запросов, не перегружая систему.

Результаты сбора информации о состоянии сети также передаются через сеть подсистеме обработки. Если последняя по каким-либо причинам недоступна, обычно используется очередь, кэширующая передаваемые данные. И только в случае, если наступает переполнение очереди, непереданные данные отбрасываются. Предоставляемые данные используются для решения других задач управления, перечисленных ранее, таких как управление конфигурациями, ошибками, производительностью, безопасностью, учет работы пользователей [50].

**Определение порога уведомления** — функция SNMP-менеджера, которая обеспечивает постоянное тестирование состояния сети в целях определения устройств, не отвечающих на управляющее воздействие. Не отвечающие на запрос SNMP-менеджера устройства классифицируются им как поврежденные в том случае, если превышен установленный заранее порог уведомления, равный числу посланных к нему управляющих воздействий.

В задачи тестирования сети могут входить: построение карты сети, выявление «узких мест» и возможных проблем, способных привести к неработоспособности сети или ее части, выявление причин низкой производительности работы сети, анализ антивирусной защиты сети и ее защищенности от несанкционированного доступа, а также общий анализ топологии и масштабируемости ЛВС. Проведение тестирования позволяет избежать неоправданных расходов на ее последующую модернизацию.

В качестве примера кратко перечислим возможные шаги тестирования типовой ЛВС и используемые для этого программы: построение карты сети и определение скорость каналов (программа 3COM NetworkDirector); снятие статистики загруженности портов с корневого коммутатора сети (программа MRTG); анализ трафика (программа SnifferPro), сканирование внешнего IP-адреса на предмет поиска возможных уязвимостей (программы XSpider).

**Управление безопасностью**. В управлении безопасностью применяются всевозможные средства и системы управления сетью, позволяющие установить, предотвратить и противостоять возможным атакам и другим угрозам безопасности.

Обеспечение безопасности предполагает предварительный сбор информации, которая является критически важной или касается приватности личных данных сотрудников. Затем требуется идентифицировать все каналы доступа, такие как терминальные услуги, FTP-, HTTP-серверы, разделение сетей, и все, что связано с предоставлением доступа к ним, включая такие службы инфраструктуры, как DNS.

Обеспечение безопасности данных осуществляется на разных уровнях:

* на уровне канала передачи данных (использование криптографии);
* на уровне сети (разрешается лишь избранный трафик);
* на уровне приложений, посредством безопасной и процедуры аутентификации.

Средства и методы управления безопасностью сети должны распознавать атаки, направленные на блокировку услуг, т. е. обеспечивать доступность самого персонала к необходимым службам.

Управление безопасностью должно предотвращать возможные атаки, попытки кражи или изменения данных. Для этого система управления безопасностью должна быть оснащена системами контроля и слежения, позволяющими быстро и эффективно отображать использование информации. Системы контроля предупреждают неавторизированный доступ, отслеживают его попытки или атаки и информируют об этом администратора.

По типу механизма слежения инструменты защиты подразделяются на активные и пассивные. Пассивные инструменты позволяют контролировать текущее состояние сети через определенные интервалы времени. Активные инструменты могут непрерывно измерять использование услуг и устройств в реальном времени и реагировать на подозрительные действия путем сообщений или изменения конфигураций.

В функции системы управления безопасностью сети входит также слежение за использованием сетевых ресурсов отдельными пользователями. На основании этой информации можно определить пользовательскую нагрузку сети и при необходимости отрегулировать сетевой трафик, чтобы избежать заторов в сети. Например, следует выделить приоритет VoIP (голосовой) трафику и ограничить трафик, связанный с загрузкой файлов.

## 1.4 Средства мониторинга и анализа локальных сетей

**Средства мониторинга и анализа сетей**

Постоянный контроль функционирования ЛВС, составляющей основу любой корпоративной сети, необходим для поддержания ее в работоспособном состоянии. Контроль — это необходимый первый этап, который должен выполняться при управлении сетью. Вследствие важности этой функции ее часто отделяют от других функций систем управления и реализуют специальными средствами. Такое разделение функций контроля и собственно управления полезно для небольших и средних сетей, для которых установка интегрированной системы управления экономически нецелесообразна. Использование автономных средств контроля помогает администратору сети выявить проблемные участки и устройства сети, а их отключение или реконфигурацию он может выполнять в этом случае вручную.

Процесс контроля работы сети обычно разделяют на два этапа: мониторинг и анализ.

На этапе мониторинга выполняется более простая процедура — процедура сбора первичных данных о работе сети: статистики о количестве циркулирующих в сети кадров и пакетов различных протоколов, состоянии портов концентраторов, коммутаторов и маршрутизаторов и т. п.

Далее выполняется этап анализа, под которым понимается более сложный и интеллектуальный процесс осмысления собранной на этапе мониторинга информации, сопоставления ее с данными, полученными ранее, и выработки предположений о возможных причинах замедленной или ненадежной работы сети.

Задачи мониторинга решаются с помощью программных и аппаратных измерителей, тестеров, сетевых анализаторов, встроенных средств мониторинга коммуникационных устройств, а также Агентов систем управления. Задача анализа требует более активного участия человека и использования таких сложных средств, как экспертные системы, аккумулирующие практический опыт многих сетевых специалистов.

Все многообразие средств мониторинга и анализа сети подразделяется на следующие группы.

1. Агенты систем управления, поддерживающие функции одной из стандартных MIB и поставляющие информацию по протоколу SNMP или CMIP. Для получения данных от Агентов обычно требуется наличие системы управления, собирающей данные от Агентов в автоматическом режиме.

2. Встроенные системы диагностики и управления, выполняемые в виде программно-аппаратных модулей, встраиваемых в коммуникационное оборудование, а также в виде программных модулей, встроенных в ОС.

3. Анализаторы протоколов, представляющие собой программные или аппаратно-программные системы, которые выполняют функции мониторинга и анализа трафика в сетях. Анализаторы протоколов предоставляют возможность собирать данные о работе протоколов всех уровней сети и в большинстве случаев способны производить генерацию тестового сетевого трафика. Анализаторы протоколов имеют большой буфер для сбора пакетов, что позволяет им быстро локализовать причину сбоя в сети, такую как перегрузку сервера и (или) исчезновение пакетов транспортного уровня.

4. Экспертные системы, аккумулирующие знания технических специалистов о выявлении причин аномальной работы сетей и возможных способах их устранения. 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 система помощи. Более сложные экспертные системы представляют собой, так называемые базы знаний, обладающие элементами искусственного интеллекта. Примерами таких систем являются экспертные системы, встроенные в систему управления Spectrum компании Cabletron и анализатора протоколов Sniffer компании Network General. Работа экспертных систем заключается в анализе большого числа событий для выдачи пользователю краткого диагноза о причине неисправности сети.

Анализатор может захватывать и декодировать до нескольких десятков протоколов, применяемых в сетях, ставить логические условия для захвата отдельных пакетов и выполнять полное декодирование захваченных пакетов, т.е. показывать в удобной для специалиста форме вложенность пакетов протоколов разных уровней друг в друга (инкапсуляцию) с расшифровкой содержания отдельных полей каждого пакета.

Кроме того, анализатор сетевых протоколов может использоваться для решения следующих задач:

* изучение работы сети и локализация трудноразрешимых проблем;
* обнаружение и идентификация несанкционированного ПО;
* получение базовых моделей трафика и метрики утилизации сети (здесь термин «метрика утилизации» показывает степень загрузки сети в определенном географическом месте и в определенное время);
* идентификация неиспользуемых протоколов для удаления их из сети;
* генерация трафика для испытания на вторжение в целях проверки системы защиты;
* работа с системами обнаружения вторжений;
* прослушивание трафика, т.е. локализация несанкционированного трафика с использованием, например, беспроводных точек доступа.

5. Многофункциональные портативные устройства анализа и диагностики. В связи с развитием технологии больших интегральных схем появилась возможность производства портативных приборов, которые совмещали бы функции нескольких устройств: кабельных сканеров, сетевых мониторов и анализаторов протоколов.

6. Оборудование для диагностики и сертификации кабельных систем, которое условно подразделяется на четыре основные группы: сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры.

**Принципы локализации неисправностей**

Диагностика сети — это измерение характеристик работы сети в процессе ее эксплуатации (без остановки работы пользователей). Диагностикой сети является, в частности, измерение числа ошибок передачи данных, степени загрузки ресурсов и пр. Диагностика бывает двух типов: упреждающая и реактивная. Основная цель упреждающей диагностики — предотвращение сбоев в работе сети. Упреждающая диагностика должна проводиться в процессе эксплуатации сети ежедневно.

Реактивная диагностика выполняется, когда в сети уже произошел сбой и требуется быстро локализовать источник и выявить причину.

Тестирование сети — это процесс активного воздействия на сеть в целях проверки ее работоспособности и определения потенциальных возможностей по передаче сетевого трафика. Тестирование, в отличие от диагностики, подразумевает отсутствие в сети работающих пользователей. Оно может применяться для решения следующих задач:

* проверка соответствия качества СКС требованиям стандартов;
* определение максимальной пропускной способности сети;
* проверка устойчивости работы конкретных сетевых устройств при различных уровнях нагрузок и различных типах сетевого трафика.

В основе методов разработки тестовых и диагностических программ локализации неисправностей сети лежат следующие принципы.

1. Зависимость от модели OSI. Для проведения диагностики сети администратор должен ясно представлять себе способы размещения сетевых узлов и методы их взаимодействия друг с другом. Основу этих сведений составляют протоколы. Именно знание протоколов лежит в основе успешных действий по анализу и диагностике сетей. Протоколы являются основой:

* подключения к сети новых узлов;
* разделения потока данных на отдельные пакеты;
* обмена пакетами между устройствами в сети.

Эффективной следует признать только ту методологию диагностики сети, которая зеркально отражает модель OSI: анализ начинается с самого нижнего уровня (физического) и, при необходимости, поэтапно продолжается до самого верхнего уровня — уровня приложений. Например, нет смысла начинать поиск низкой производительности сети на уровне приложений файлового сервера, если в физическом сегменте Ethernet клиента наблюдается чрезмерно большое число ошибок CRC (Cyclic Redundancy Code — избыточный циклический код).

Большинство реализаций конкретных сетей не совпадает с моделью OSI в точности, но в любой такой реализации функции, описанные моделью OSI, по крайней мере, принимаются в расчет. Ценность модели OSI в качестве инструмента поиска неисправностей заключается в описании принципов функционирования сети. Другими словами, имея точное представление о том, что делает сценарий, можно точно локализовать проблему

2. Декомпозиция сетевой проблемы. Даже в простом случае сети с двумя узлами существует много аппаратуры и параметров ПО, взаимосвязь между которыми может значительно влиять на эффективность работы сети. Обычно подход к такой сложной проблеме должен начинаться с декомпозиции общей проблемы на более мелкие части и так далее, до нахождения первоисточников проблемы, а затем уже должен выполняться систематический и логический план удаления возможных причин, пока не будет достигнуто ее решение.

3. Выбор правильного инструмента диагностики. Есть существенные различия в способах измерения производительности у разных инструментов тестирования, при этом важно их взаимодействие с тестируемой системой. Существует два класса тестовых систем: генераторы трафика и генераторы транзакций. Генераторы трафика являются источником огромного числа пакетов, которые могут как соответствовать трафику реального сетевого стека, так и отличаться от него. Генераторы транзакций, как минимум, отсылают и принимают реальные транзакции через полноценный работающий сетевой стек OSI. Главное их отличие от генераторов трафика заключается в том, что они реализуют настоящий сетевой стек, в том числе и на прикладном уровне.

При выборе правильного инструмента диагностики ключевым является вопрос: нужна ли для тестирования данной системы работа на четвертом (транспортном) и более высоких уровнях OSI? Устройствам, которые взаимодействуют с потоками транспортного уровня, таким как межсетевые экраны и распределители нагрузки, требуется генератор транзакций. Поскольку эти системы взаимодействуют с потоком транспортного уровня, то и генерировать его нужно соответствующим образом. Такая тестируемая система может вступать во взаимодействие с приложением, содержащим динамический контент. В этом случае искусственный трафик четвертого уровня (и более высокого) не будет должным образом обработан тестируемой системой, так как имитационный трафик предполагает наличие ожидаемых откликов на запросы.

4. Принцип «сверху вниз». Поиск неисправностей следует проводить «снизу вверх», т.е. начиная с физического уровня и заканчивая уровнем приложений. Например, плохая кабельная сеть является причиной 90 % всех сетевых проблем, поэтому так важно начинать диагностику сети именно с физического уровня, используя для этого качественный кабельный тестер. Такие приборы работают быстро и обеспечивают высокую точность. Однако поиск оставшихся 10% ошибок потребует 90% общего времени на восстановление работоспособности сети.

Каждому уровню модели OSI свойственны свои характерные проблемы, обнаруживаемые при сбоях в сети именно на этих уровнях. В таблице 1.4.1 представлены наиболее характерные из них.

5. Документирование сети. Квалифицированный сетевой аналитик всегда начинает анализ сети с полного понимания текущей сетевой среды, что подразумевает документирование сетевой топологии, прикладных программ и используемых протоколов. Трудно переоценить важность точной и подробной документации для сети. Обычно сетевая документация содержится в разрозненных документах, причем даже собранные воедино они не позволяют получить полную картину сети.

Таблица 1.4.1 – Проблемы, обнаруживаемые при сбоях в сети

|  |  |
| --- | --- |
| Наименование уровня | Возможные сетевые проблемы на соответствующем уровне |
| Уровень  приложений | Зацикливание (перекрытие) запросов на чтение (запись) файлов. Долгий поиск ресурсов, замедленная обработка данных клиентом (сервером). Плохое заполнение пакетов данными. Низкая пропускная способность между хостами сети |
| Представительский уровень | Несовместимость протоколов. Некорректные сведения в базе данных MIB протокола SNMP. Замена кодовых таблиц ASCII на EBCDIC |
| Сеансовый уровень | Согласование MTU блока и буфера. Поиск и регистрация ресурсов по логическим именам. Повторная установка соединений |
| Транспортный уровень | Повторные пересылки. Избыточная фрагмента­ция или ее отбрасывание. Превышение длины посылаемого сегмента размера скользящего окна |
| Сетевой уровень | Ошибки CRC. Проблемы маршрутизации (за­держки, отбрасывание пакетов, несогласован­ность MTU). «Широковещательные» штормы |
| Канальный уровень | Ошибки CRC. Конфликты и фрагментация ка­дров. Ошибки линии и пакета. Очистка кольца и аварийная сигнализация. Задержки, отбрасыва­ние пакетов, искажение данных в коммутаторах и мостах. «Штормы» |
| Физический уро­вень | Неисправности и ошибки СКС (соединители, расщепление пары, обрывы, короткое замыкание (КЗ), некорректная длина линии). Отказы портов, концентраторов, внешние высокочастотные помехи. |

Насыщение полосы пропускания наблюдения за работой сети. Очень важна хорошая регистрация ежеминутных изменений сети, но без постоянного обновления всего комплекта документации.

Точная и понятная документация для сети, отражающая все изменения в сети, позволяет успешно управлять оборудованием и эффективно проводить диагностику, причем необходимо заранее выделять рабочее время на поддержание документации на должном уровне.

Не следует подробно отражать на структурной схеме каждый хост в каждом сегменте сети, поскольку редко удается постоянно поддерживать корректность этих сведений, однако необходимо отразить топологию и все коммуникационное оборудование: коммутаторы, маршрутизаторы, серверы, шлюзы и средства защиты сетей. При этом достаточно упрощенных изображений, подчиняющихся общей системе условных обозначений (например, всегда маршрутизатор изображать восьмиугольником, а коммутатор квадратом и т.д.). Внутри этих фигур можно поместить полезную ин-формацию об оборудовании, а рядом — показать IP-адрес, дополненный маской подсети.

6. Входное тестирование. Множество проблем в сети можно избежать, если качественно провести тестирование сети на этапе ее приемки у системного интегратора. Прежде всего – это относится к сертификации кабельного хозяйства на соответствие стандартам и тестированию сетевого оборудования на наличие скрытых дефектов. Правилом хорошего тона для системного интегратора является не только проведение тестирования, но и внесение его данных в паспорт сети, предоставляемый пользователю. Если входное тестирование не проводится, то пользователь может получить сеть со скрытыми дефектами, которые проявятся не сразу, так как на начальных этапах эксплуатации сети нагрузка в ней мала. Дефект может проявиться значительно позже, создав у пользователя впечатление, что он явился следствием каких-то модификаций в сети.

**Нагрузочное тестирование сети**

Нагрузочное тестирование — это вид диагностики сетевой инфраструктуры, позволяющий получить интегральную оценку качества работы сети и локализовать скрытые дефекты. Нагрузочное тестирование, которое также называют стрессовым тестированием, или имитацией трафика, проводится:

* для получения интегральной оценки качества работы модифицируемой (новой) сети и определения запаса ее производительности;
* выявления скрытых дефектов сетевых адаптеров и драйверов;
* измерения производительности и выявления скрытых дефектов активного сетевого оборудования;
* сравнения эффективности различных сетевых архитектур.

|  |  |  |
| --- | --- | --- |
| **Хост имитатор трафика** | Воздействие | **Тестируемое устройство** |
| Отклик |

Рис.4.1.1 – Схема нагрузочного тестирования

Идею нагрузочного тестирования поясняет Рис.4.1.1. хост — имитатор трафика создает в сети диапазон нагрузок с переменной плотностью и составом цифрового потока. Одновременно с этим измеряются скоростные и нагрузочные характеристик 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.

Общие принципы локализации дефектов при проведении нагрузочного тестирования. В качестве основного критерия качества работы сети здесь используется скорость выполнения файловых операций каждым хостом. 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 заключается в том, что скорость файловых операций не очень сложно измерить. Если скорость мала, то, изменяя режим работы станций, легко определить причину этого.

Рассмотрим несколько простых правил, соблюдая которые, можно избежать отсутствия на хостах дефектов.

1. Если хосты работают с сервером по очереди, то скорость выполнения файловых операций каждой станцией должна быть пропорциональна производительности ее компьютера и сетевой карты. Если на каком-то хосте с «быстрой» сетевой картой файловые операции выполняются медленно, то это предмет для изучения.

2. Если рабочие станции работают с сервером по очереди, то скорость выполнения файловых операций каждой станцией не должна быть существенно меньше теоретической пропускной способности коллизионного домена (сегмента) сети, в которой станция расположена. Например, если станция расположена в коллизионном домене Ethernet, ее скорость должна быть в диапазоне 800... 1 150 Кбайт/с.

3. Если рабочие станции работают с сервером по очереди, то число ошибок канального уровня, измеренных в процессе работы каждой станции анализатором сетевых протоколов, должно быть равно нулю.

4. Если все станции работают одновременно, то, как бы сильно ни была загружена сеть, не должно быть станций, скорость работы которых близка к нулю или которые отключаются от сервера.

5. Если все станции работают одновременно и при этом увеличивают интенсивность запросов к серверу, то максимальная производительность всех станций не должна быть существенно ниже теоретической пропускной способности сети.

6. Если все станции работают одновременно и при этом увеличивают интенсивность запросов к серверу, то число ошибок (не путать с коллизиями) канального уровня, измеряемых в ходе теста анализатором сетевых протоколов или SNMP-консолью, должно быть близко к нулю и не должно увеличиваться с ростом утилизации сети.

7. Скорость выполнения операций чтения может отличаться от скорости выполнения операций записи не более чем на 10...30%.

При проведении диагностики сети важно выявить стабильно неадекватную реакцию сети на воздействия тестовых приложений. Если неадекватную реакцию сети можно воспроизвести, значит, можно определить и ее причину и локализовать дефект или «узкое место» сети.

Для проведения нагрузочного тестирования применяются разные тестовые приложения, такие как FTest, SelFTest и т. п. Одновременно с этим могут использоваться различные средства анализа работы сети и серверов (анализаторы протоколов, SNMP- консоли, утилиты сетевых ОС).

Перед проведением тестирования на все хосты проверяемых фрагментов сети устанавливается специальное ПО (FTAgent), которое осуществляет генерацию тестового трафика в соответствии с заданными параметрами. Тестовый трафик создается за счет выполнения файловых операций между Агентами (хостами с установленной программой FTAgent) и каким-либо сервером. Управление работой всех Агентов осуществляется централизованно с одной рабочей станции сети, играющей роль сервера. Агенты выполняют файловые операции с одним общим файлом на сервере либо с индивидуальными файлами на сервере.

Файловые операции — это либо чтение (запись) блока данных фиксированного размера из файла (в файл), либо последовательность операций (файловая транзакция): блокирование файла —> чтение данных из файла -> запись данных в файл —> разблокирование файла. Все файловые операции выполняются в режиме произвольного доступа к файлу.

В ходе выполнения файловых операций Агенты измеряют скоростные и нагрузочные характеристики сети. Скоростные характеристики сети — это скорость выполнения агентами файловых операций с тестовым сервером. Нагрузочные характеристики сети — это производительность, достигнутая Агентами при выполнении файловых операций с тестовым сервером.

Программа FTAgent спроектирована таким образом, что передаваемые ей данные «обходят» кэш-память рабочей станции, на которой она установлена. Это позволяет измерять реальные значения скорости работы сети вместо показателей быстродействия кэш-памяти.

Типы нагрузочных тестов. Проведение нагрузочного тестирования предполагает выполнение нескольких типов тестов. Каждый тест по-разному воздействует на сеть и поэтому диагностирует различные компоненты сети. Типовая последовательность нагрузочных тестов, которая подойдет для большинства случаев, подразумевает выполнение теста:

* FTest by steps в режиме калибровки с нагрузкой только на сеть;
* FTest all stations с нагрузкой только на сеть;
* FTest all stations с нагрузкой на сеть и сервер;
* FTest by steps (нормальный режим) с нагрузкой только на сеть.

Тест FTest by step в режиме калибровки с нагрузкой только на сеть. Обычно нагрузочное тестирование сети целесообразно начинать именно с режима калибровки. В этом режиме все Агенты по очереди выполняют одни и те же файловые операции, с одним тестовым сервером, с одинаковой интенсивностью. Слова «с нагрузкой только на сеть» означают следующее. Параметры теста задаются так, чтобы производительность дисковой системы тестового сервера в ходе выполнения теста не оказывала существенного влияния на измеряемые скоростные характеристики сети.

Цель выполнения теста — локализовать дефекты сети, которые не являются следствием взаимного влияния одних рабочих станций на другие. Это могут быть дефекты активного и (или) пассивного сетевого оборудования, дефекты в системном ПО хостов или сервера, не оптимальные для данной архитектуры сети параметры настройки сетевого оборудования или ПО и т. п. Рекомендуемые параметры теста, которые подойдут для большинства случаев: предлагаемая нагрузка — задается так, чтобы интенсивность, с которой каждый агент будет стараться генерировать трафик, превышала теоретическую пропускную способность коллизионного домена (сегмента) сети, в котором расположен агент, — принять 10 Мбайт/с;

* доля операций чтения — принять 50 %;
* размер файла — принять 64 Кбит;
* размер записи — принять 8 192 байт;
* разделяемый файл и параметр CRC — принять «Нет». Остальные параметры задаются в соответствии с общей логикой работы теста исходя из следующих соображений.

1. Для каждого агента средняя скорость выполнения файловых операций не должна быть существенно меньше теоретической пропускной способности коллизионного домена (сегмента) сети, в котором агент расположен. В большинстве случаев для сетей Ethernet, Half Duplex это значение должно быть в диапазоне 800... 1 150 Кбайт/с.
2. Для каждого агента измеряемые значения скорости выполнения операций чтения-записи и значения производительности должны быть прямо пропорциональны значению индекса производительности компьютера агента и производительности его сетевой карты.
3. Для каждого агента скорость выполнения операций чтения не должна существенно отличаться от скорости выполнения операций записи. Как правило, скорость выполнения операций чтения немного выше (на 5... 10%), чем скорость выполнения операций записи.
4. Утилизация канала связи (порта коммутатора), измеряемая в процессе работы каждого агента анализатором сетевых протоколов, не должна существенно отличаться от измеряемых каждым агентом значений производительности. Как правило, утилизация канала связи должна быть на 5... 10% выше, чем измеряемое значение производительности.

Число ошибок канального уровня, измеренное в процессе работы каждого агента анализатором сетевых протоколов, должно быть равно нулю.

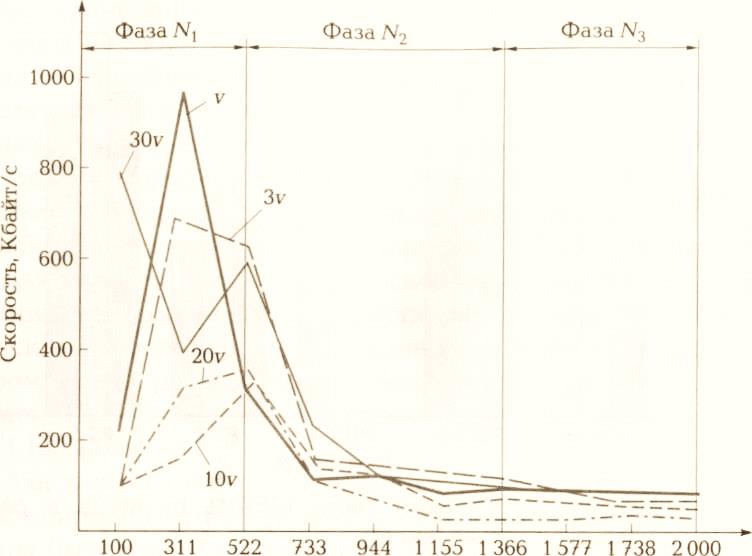
Для проведения нагрузочного тестирования применяются тестовые приложения FTest и SelFTest. Одновременно с этим могут использоваться различные средства анализа работы сети и серверов (анализаторы протоколов, SNMP-консоли, утилиты сетевых ОС и т.п.).

Тест FTest all stations с нагрузкой только на сеть. Этот тест выполняется только после того, как реакция всех агентов в ходе выполнения теста FTest by steps в режиме калибровки была признана адекватной. В процессе выполнения этого теста все агенты одновременно выполняют одни и те же файловые операции, с одним тестовым сервером, постепенно наращивая их интенсивность.

Цели выполнения теста:

1. локализовать дефекты, которые являются следствием высокой нагрузки в сети и (или) взаимного влияния хостов. Это могут быть дефекты активного сетевого оборудования, дефекты в системном ПО хостов и (или) сервера, неоптимальные для данной архитектуры сети параметры настройки активного сетевого оборудования или ПО и т. п.;
2. локализовать «узкие места» сети (без учета дисковой системы сервера);
3. измерить общую производительность сети (без учета дисковой системы сервера).

При задании параметров для этого теста необходимо учесть, что минимальная и максимальная предлагаемые нагрузки, а также число шагов тестирования являются взаимосвязанными параметрами. Значения параметров задаются так: на первом шаге теста общая загрузка сети не должна превышать 10% теоретической пропускной способности (ТПС) сети, а на последнем — должна составлять 150...200 % ТПС сети; не менее трех последних шагов теста должны соответствовать нагрузке на сеть, превышающей 100 % ТПС сети, и один шаг выполняется при нагрузке 30...40% ТПС сети. Остальные параметры теста можно принять, как в предыдущем тесте.



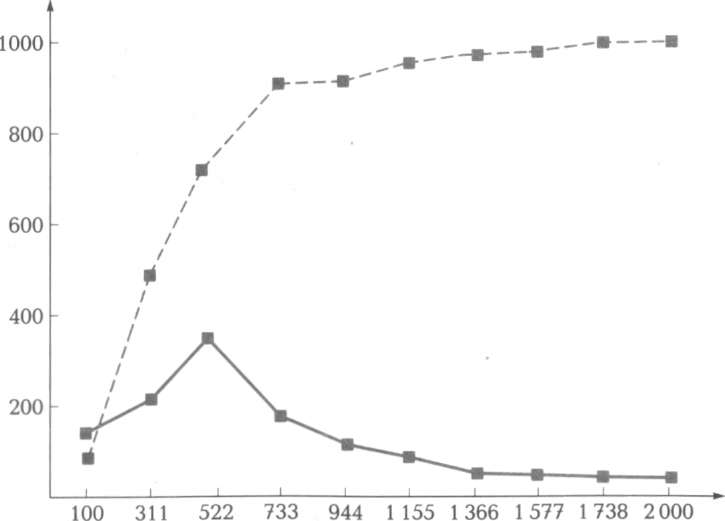
Предлагаемая нагрузка L, Кбайт/с

Рис.4.1.2 – Зависимость скорости чтения от нагрузки на сеть Ethernet

На рисунках 4.1.2, 4.1.3 приведены графики изменения скорости выполнения файловых операций от величины нагрузки на сеть. Здесь v, с-1, — минимальная скорость чтения пакетов Агентами. Штриховая линия на рисунке 3.3.3 показывает зависимость производительности сети от величины предлагаемой нагрузки на сеть, а сплошная — зависимость средней скорости работы агентов от того же аргумента. Анализируя приведенные графики, можно отметить следующую закономерность.

В фазе N1 в соответствии с рисунком 4.1.2, пока предлагаемая нагрузка на сеть низкая, значения скоростей Агентов могут «прыгать». При некоторой нагрузке (здесь это L1 = 522 Кбайт/с) значения скоростей всех Агентов достигают значения, после которого только уменьшаются (фаза N2). Уменьшение скорости происходит до того момента, когда при определенном значении нагрузки L2 скорость всех агентов стабилизируется на некотором постоянном, минимальном значении (здесь — на уровне L2= 1 366 Кбайт/с). В фазе N3 значения скоростей стабилизированы на минимальном значении.

Большой разброс скоростей в фазе N1 объясняется следующими причинами. При низкой нагрузке на сеть производительность канала связи не оказывает существенного влияния на значения скоростей, так как он еще не загружен. Однако сетевые ОС имеют следующую особенность. Чем ниже интенсивность запросов (предлагаемая нагрузка), тем меньше ресурсов сетевая ОС сервера выделяет для обслуживания этих запросов. Этим объясняется большой разброс значений скоростей у разных агентов и то, что скорости могут «прыгать». При этом для некоторых агентов в фазе N1 можно наблюдать рост значений скорости с увеличением предлагаемой нагрузки, а для некоторых — снижение скорости. Однако усредненное значение скорости по всем агентам, как правило, растет (как видно из рисунка 4.1.3 средняя скорость выполнения операций чтения на первых трех шагах теста растет с 154,7 до 381 Кбайт/с).



Предлагаемая нагрузка I, Кбайт/с

Рис.4.1.3 – Зависимость производительности сети и средней скорости чтения (записи) всеми агентами от нагрузки на сеть.

Значение нагрузки, равное I1, соответствует такой интенсивности запросов, при которой сетевая ОС уже выделяет достаточно ресурсов, но канал связи еще не настолько загружен, чтобы оказывать существенное влияние на скорость выполнения файловых операций. Этим объясняется максимальное значение усредненной по всем агентам скорости на последнем шаге фазы N, (как видно из рисунка 3.3.3, максимальное значение усредненной скорости достигается при значении предлагаемой нагрузки, равном 522 Кбайт/с). Интересно, какое значение производительности сети и какое значение утилизации канала связи соответствуют максимальному значению усредненной скорости? Очевидно, что значение утилизации канала связи в этой точке не должно быть выше рекомендуемого для конкретного типа сети. Например, для сети Ethernet на основе разделяемого канала связи рекомендуемое значение — 35...40%. Из рисунка 3.3.3 видно, что 522 Кбайт/с предлагаемой нагрузки соответствует производительность, равная 713 Кбайт/с. Учитывая, что тестировалась сеть, состоящая из одного коллизионного домена, это соответствует более чем 60 % утилизации канала связи сети. Следовательно, сервер и канал связи плохо сбалансированы друг с другом по производительности.

Снижение скоростей в фазе N2 объясняется тем, что производительность канала связи начинает ограничивать скорость выполнения файловых операций. Чем больше предлагаемая нагрузка, тем ниже усредненное значение скорости. Значение L2 соответствует максимальной производительности тестируемой сети. Таким образом, можно измерить, какова максимальная производительность тестируемой сети. Если производительность компьютеров не хуже производительности канала связи сети, то утилизация канала связи в точке L2 должна быть 100% (как видно из рисунка 3.3.3, максимальная скорость тестируемой сети равна 1 048 Кбайт/с, что соответствует близкой к 100% утилизации канала связи сети Ethernet).

Фаза N3 соответствует нагрузке, при которой канал связи или сервер полностью загружены, поэтому скорости постоянны и минимальны. При тестировании коммутируемых сетей значения скоростей могут оставаться постоянными в течение всего теста. Это объясняется фиксированной полосой пропускания, которую имеет каждый агент в коммутируемой сети.

При анализе результатов теста FTest all stations обязательно учитывается архитектура сети. Коммутируемая сеть будет вести себя отлично от сети, построенной на основе разделяемого канала связи. Поэтому основное правило заключается в следующем. Все Агенты, которые находятся в одинаковых условиях и имеют идентичную конфигурацию компьютера, должны работать приблизительно одинаково. Не должно быть агентов, которые без особых на то оснований работают быстрее или медленнее, чем другие. Нужно учитывать следующее:

а) независимо от нагрузки в сети не должно быть агентов, скорость которых близка к нулю или которые в ходе теста отключаются от сервера;

б) значение производительности, соответствующее предлагаемой нагрузке 12 не должно быть существенно меньше теоретической пропускной способности сети.

Число ошибок (не коллизий) канального уровня, измеряемое в ходе теста анализатором сетевых протоколов, не должно увеличиваться с ростом предлагаемой нагрузки и должно быть близко к нулю.

Тест FTest all stations с нагрузкой на сеть и сервер. Он выполняется только после того, как в ходе выполнения теста FTest all stations с нагрузкой только на сеть работа всех Агентов признана адекватной. В процессе выполнения теста FTest all stations все Агенты одновременно выполняют одни и те же файловые операции, с одним тестовым сервером, постепенно наращивая их интенсивность.

Единственное отличие данного теста от предыдущего заключается в том, что в данном тесте производительность дисковой системы сервера будет оказывать существенное влияние на скоростные характеристики Агентов.

Цели выполнения этого теста:

а) определение баланса производительности сервера и производительности остальных компонент сети;

б) локализация дефектов и «узких мест» на сервере, следствием которых может быть отключение рабочих станций от сервера или крах операционной системы сервера.

Методика задания параметров в данном тесте практически полностью соответствует методике задания параметров в тесте FTest all stations с нагрузкой только на сеть. Более того, все параметры, за исключением параметра «размер файла», рекомендуется принять, как в тесте FTest all stations — с нагрузкой только на сеть. Параметр «размер файла» следует задавать таким, чтобы его значение, как минимум, в два-три раза превышало размер оперативного запоминающего устройства (ОЗУ) на сервере.

При анализе результатов данного теста можно увидеть, что скорость выполнения файловых операций каждым Агентом может резко меняться во всем диапазоне предлагаемых нагрузок. Более того, при повторном выполнении одного и того же теста скорости выполнения файловых операций одним и тем же Агентом могут отличаться друг от друга. Это объясняется, с одной стороны, взаимным влиянием Агентов при доступе к диску сервера, а с другой — принципом работы дисковой системы сервера. Дело в том, что, обрабатывая запросы от рабочих станций, дисковая система сервера оптимизирует число обращений к диску. В результате этого запросы от рабочих станций обслуживаются не обязательно в том порядке, в каком они поступают на сервер.

В одном случае быстрее могут обслуживаться запросы одного Агента, в другом случае — другого. По этой причине следует анализировать не скорость выполнения файловых операций, а производительность при выполнении файловых операций.

В данном тесте основной интерес представляет суммарное значение производительности по всем Агентам, измеренное на последнем шаге теста. Это значение, как правило, меньше значения производительности, измеренного в ходе выполнения теста FTest all stations с нагрузкой только на сеть. Разница между этими значениями характеризует степень сбалансированности по производительности дисковой системы сервера, с одной стороны, и остальных компонент сети — с другой. Чем меньше разница, тем лучше сбалансированы эти компоненты.

В целях проверки сбалансированности по производительности канала связи и сервера целесообразно с помощью анализатора сетевых протоколов измерить утилизацию канала связи при максимальной нагрузке на сеть. Поскольку производительность дисковой системы сервера, как правило, ниже производительности канала связи сети, в данном тесте именно сервер, скорее всего, будет «узким местом» сети. Чем ближе утилизация канала связи к 100% при максимальном значении предлагаемой нагрузки, тем ближе производительность сервера к производительности канала связи. Чаще всего это значение составляет 50...60 %.

При анализе результатов данного теста следует обратить внимание также на следующее:

* в ходе теста агенты не должны отключаться от сервера;
* производительность Агентов при выполнении ими операций записи не должна быть существенно ниже производительности при выполнении операций чтения.

Максимальная производительность сети должна быть приблизительно равна NU, где N — теоретическая пропускная способность сети; U — утилизация канала связи, выраженная в долях.

Тест FTest by steps (нормальный режим) с нагрузкой только на сеть. Под нормальным режимом понимается выполнение теста в режиме, отличном от режима калибровки. В этом случае на каждом следующем шаге теста автоматически добавляется один агент, т.е. число одновременно работающих Агентов постепенно увеличивается. Данный тест имеет смысл выполнять только в том случае, если в ходе выполнения теста FTest by steps с нагрузкой только на сеть анализатором протоколов или SNMP-консолью было зафиксировано большое число ошибок передачи данных, в то время как в ходе выполнения теста FTest by steps (режим калибровки) ошибок зафиксировано не было. Такая ситуация свидетельствует о том, что ошибки передачи данных являются следствием взаимного влияния агентов.

Измеряя число ошибок передачи данных в ходе выполнения данного теста, можно легко определить, при начале работы какого именно Агента в сети начинают появляться ошибки передачи данных.

**Программные средства диагностики**

Все ПС диагностики компьютерной сети подразделяются на две группы:

1) утилиты, встроенные в операционную систему;

2) специализированные диагностические программные продукты, известные как сетевые утилиты.

Утилиты, встроенные в операционную систему, являются исполняемыми операторами, запускаемыми из командной строки ОС. Рассмотрим назначение указанных команд и работу наиболее информативных из них:

netstat — отображает статистику протокола и текущих сетевых подключений tcp/ip;

ping — проверяет наличие связи с указанным узлом;

tracert — выводит имена и IP-адреса всех маршрутизаторов, через которые проходят пакеты от локального компьютера к указанному узлу;

ipconfig — выводит сведения о текущей конфигурации протокола IP и может осуществлять базовое конфигурирование этого протокола;

nslookup — обращается с запросом к DNS-серверу;

netsh — показывает различные параметры настроек сети. Получить подробную справку по каждой из этих команд можно, набрав в командной строке соответствующую команду, содержащую в поле операндов символы «/» и «?». Например, справка для встроенной утилиты ping будет показана системой после выполнения команды «ping /?». Практика показывает, что чаще других используются утилиты ping и tracert.

Утилита ping отправляет запрос указанному узлу сети и фиксирует время между отправкой запроса и получением ответа, т. е. позволяет определить время отклика интересующего сервера. Понятно, что чем оно меньше, тем обмен данными с этим сервером производится быстрее.

Утилита tracert выполняет отправку тестового пакета узлу сети, указанному в поле операндов. Утилита отображает информацию обо всех промежуточных маршрутизаторах, через которые прошел пакет на пути к запрошенному узлу, а также минимальное, максимальное и среднее время отклика каждого из них. Это позволяет оценить «расстояние», которое прошел пакет, и на каком участке возникают наибольшие задержки, связанные с передачей данных.

Рассмотрим подробнее смысл результатов, выдаваемых утилитами ping и tracert. Отсутствие отклика от удаленного сервера на введенную команду ping или tracert может свидетельствовать о том, что сервер в данный момент недоступен или же администратор сервера заблокировал эхозапросы. По сути, команда ping и является эхозапросом по протоколу ICMP, на который указанный в команде адрес должен дать эхоответ — именно его и может заблокировать администратор. Если время отклика удаленных хостов слишком велико и не зависит от месторасположения хостов, то локальный хост подключен к провайдеру с ошибками. Слишком «длинный» путь до удаленного сервера (т.е. большое количество промежуточных маршрутизаторов на пути соединения с сервером) часто приводит к замедлению связи с ним. Если это критично, то имеет смысл попытаться поискать варианты сокращения длины маршрута. Например, в случае игровых серверов можно сделать выбор в пользу тех, которые находятся как можно ближе к серверу провайдера. Если утилиты показывают, что тестовые пакеты не проходят дальше сервера провайдера, то, вероятно, провайдер выполняет плановые профилактические работы.

Очень полезной встроенной утилитой является также команда ipconfig, примеры применения которой иллюстрирует таблица 4.1.1

Применение утилит ping, tracert и ipconfig технически не всегда удобно, поскольку для их запуска необходимо открывать окно командной строки и вводить команду с параметрами, которые нужно либо запоминать, либо каждый раз обращаться к справке.

Таблица 4.1.1 – Команды утилиты ipconfig

|  |  |  |
| --- | --- | --- |
| № п/п | Команда | Описание выполнения |
| 1 | ipconfig | Отображает краткую информацию о теку­щей конфигурации протокола IP |
| 2 | ipconfig /all | Отображает полную информацию |
| 3 | ipconfig /renew | Обновляет сведения для всех адаптеров |
| 4 | ipconfig/renew EL' | Обновляет сведения для адаптеров, имя которых начинается с букв EL |
| 5 | ipconfig/release \*EL?1\* | Освобождает ip-адреса адаптеров с име­нами, подходящими под шаблон \*EL?1\*, Например: EL-1, mELilada |

Например, чтобы выяснить путь прохождения пакетов до хоста www.3dnews.ru, требуется в окне командной строки набрать и ввести команду tracert www.3dnews.ru. Результат работы команды, представленный далее, показывает, что хосты разделяют восемь узлов:

С: \Users\naza>tracert www.3dnews.ru

Трассировка маршрута к www.3dnews.ru (195.90.131.231) с максимальным числом прыжков 30:

1 <1 мс <1 мс <1 мс vpn237-10.msk.corbina.net

(85.21.0.237)

2 \* \* \* Превышен интервал ожидания для запроса.

3 1 ms 1 ms 1 ms rti-bb-be4.corbina.net

(195.14.54.149)

4 2 ms 3 ms 3 ms m9-crs-2-be8.corbina.net

(195.14.62.86)

5 2 ms 2 ms 1 ms m9-br-be3.corbina.net

(195.14.62.85)

6 35 ms 1 ms 1 ms Rostelecom-2.corbina.net

(83.102.145.134)

7 2 ms 1 ms 1 ms 188.254.31.98

8 2 ms 2 ms 2 ms Belyaevo.Rosnet.Net

(212.5.174.2)

9 2 ms 2 ms 2 ms ceta.3dnews.ru

(195.90.131.231)

Трассировка завершена.

Применение сетевых утилит позволяет преодолеть неудобство обращения со встроенными утилитами, поскольку обычно они имеют дружественный оконный интерфейс.

Сетевые утилиты — это внешние самостоятельные программные модули и (или) пакеты программ, выполняющие функции специализированных диагностических программных продуктов. Например, программа WinMTR, доступная на сайте, является аналогом консольной утилиты tracert и применяется для трассировки маршрута пакета в сети с одновременным определением потерь данных на межсетевых узлах. Программа запускается от имени администратора. Преимуществом утилиты WinMTR являются простота в использовании, отсутствие инсталлятора и возможность выполнения с любого носителя. Для выполнения теста необходимо в поле Host указать имя хоста, например serfock. ru, и нажать кнопку Start. Тест выполняется приблизительно со скоростью 100 пакетов в минуту, что достаточно для получения картины состояния сети.

В колонке Hostname программа выведет IP-адреса маршрутных узлов от хоста-инициатора теста до тестируемого хоста, т. е. будет произведена трассировка маршрута прохождения сигнала. По полученному списку адресов видно, сколько пакетов отправлено (принято) (Sent/Recv), с какими задержками (Best/Avrg/Worst/Last) и процентом потерь (Loss%) на каждом из узлов маршрута. Здесь Best/Avrg/Worst/Last — соответственно минимальное, среднее, максимальное, последнее время задержки пакета в миллисекундах.

Другой распространенной и доступной на сайте диагностической программой, не требующей установки, является программа Tcpdump. Эта программа переводит интерфейс ЭВМ в режим приема всех пакетов, пересылаемых по сетевому сегменту, в котором находится хост — инициатор запуска программы. Программа Tcpdump отбирает и отображает на экране пакеты, посылаемые и получаемые хостом. Критерии отбора могут варьироваться, что позволит проанализировать выполнение различных сетевых процедур. В качестве параметров при обращении к программе могут использоваться наименования протоколов, номера портов и т.д. Например, в результате выполнения команды tcpdump-q на консоль по каждому захваченному пакету будет выведена строка, содержащая минимум информации вида 16: 53 : 18.339465 IP ns3.corbina.net.53 > naza-PK.63089 UDP, length 89

Как видим, строка содержит лишь имя протокола (UDP), сетевые имена, показывающие, откуда (ns3.corbina.net) и куда (naza- РК) шел пакет, номера портов (53 и 63089) и количество переданных данных (length 89). Программа для запуска также требует прав администратора.

Пакет программ Essential NetTools представляет еще один пример сетевой утилиты, которая предназначена для диагностики сети и выявления проблем в ее безопасности. Инструменты программы Essential NetTools могут быть использованы не только для нужд диагностики сетевыми администраторами, но и рядовыми пользователями для наблюдения за любым сетевым соединением. В состав программы входит мощный инструмент PortScan — так называемый сканер портов, который кроме операции «пингования» любого хоста в сети, производит поиск активных ТСР-портов в тестируемой сети. Сканер PortScan кроме имени и МАС-адреса хоста показывает все открытые порты, список активных устройств, подключенных в данный момент к сети, а также дополнительную информацию, с помощью которой администратор может определить какие из служб — HTTP, FTP, SMB, ISCSI и (или) SMTP — задействованы на данном хосте. С помощью сканера портов PortScan можно также узнать реальную скорость Интернета. Сохранить все результаты работы по анализу сети PortScan позволяет в удобном формате .xml. Программа работает во всех версиях Windows; она портативная и не требует установки на жесткий диск.

**Номенклатура и особенности работы тест-программ**

В отличие от программ мониторинга сети, которые выполняет постоянное наблюдение за компьютерной сетью, администраторы сети периодически вынуждены решать повседневные задачи, устраняя относительно несложные, но в то же время наиболее распространенные проблемы локализации дефектов в объектах сетевой инфраструктуры и оценивая производительность серверов и качество каналов связи. Для этих целей они используют так называемые тест-программы. Номенклатура тест-программы достаточно обширна, о чем свидетельствует далеко не полный список их наименований, приведенный в таблице 4.4.2

Таблица 4.1.2 – Номенклатура тест-программы

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № п/п | Имя программы | № п/п | Имя программы | № п/п | Имя программы |
| 1 | Active Administrator | 10 | LAN Tornado 1.0 | 19 | Ping  Terminal 2.5 |
| 2 | AnetTest 1.0-1 | 11 | Local Pinger 1.03 |
| 3 | CheckHost  1.5 + 3 | 12 | MyVoIPSpeed  Server | 20 | Ping 1.0 build 56 |
| 21 | PingMaster 0.9 |
| 4 | Connection | 13 | Network  Tools 1.0 | 22 | Port Sweep  Demo 2.40 |
| Checker |
| 5 | Desktop Pinger  1.0 | 14 | NetQuality 3.12 | 23 | Roadkil's ComTest 1.1 |
| 15 | Net Runner 1.0 |
| 6 | Expert Website  Monitor | 16 | Network Spy 2.0 | 24 | RoboTest 2.0.7 |
| 17 | Paessler SNMP  Tester | 25 | TansuTCP 2.1 |
| 7 | Flexiblesoft  Ping 2.0 | 26 | TrafficEmulator |
| 18 | Performance | 27 | Winsock Tester  0.0.6 |
| 8 | Graph-A-Ping  1.0.10 | Pinging |
|  |  |  |  |
| 9 | Jac-Ping 1.0 |  |  |  |  |

Широкое распространение тестовых программ объясняется их невысокой стоимостью, удобством в эксплуатации и хорошей эффективностью. В большинстве случаев результаты тестирования сети, будь то определение скорости обмена информацией между компьютером и сетевым ресурсом, локализация участков уязвимости сети и другие, тест-программы выводят не только в цифровом, но и в графическом виде. Как правило, тест-программы применяются для локализации дефектов и «узких мест» в локальных и в распределенных сетях. Типовыми функциями, которые они выполняют, являются измерение, оценка и контроль производительности работы сетевого оборудования. Рассмотрим назначение наиболее распространенных тест-программ.

Essential NetTools — это мощный пакет, предназначенный для диагностики сети и выявления проблем в ее безопасности.

Инструменты Essential NetTools могут быть использованы не только для нужд диагностики сетевыми администраторами, но новыми пользователями для наблюдения за любым сетевым соединением.

DoSHTTP — это программа проверки Web-серверов на пригодность к эксплуатации в реальной сети. Одновременно DoSHTTP может тестировать несколько серверов. Тестирование производительности программа DoSHTTP выполняет, «забрасывая» Web-сервер потоком пакетов с разными скоростями, и по результатам теста оценивает уровень защиты Web-сервера и его ПО.

PingPlotter — диагностический инструмент для локализации неисправностей в сети. PingPlotter использует комбинацию инструментов, позволяющих выполнять сбор данных в течение заданного интервала времени. Этим интервалом могут быть часы, дни или недели. Выявленные в результате анализа собранных данных потенциальные проблемные участки программа локализует, указывая путь к ним графическими средствами.

Nsauditor Network Security Auditor — это сетевой сканер, служащий для осуществления диагностики и мониторинга сетевых компьютеров на предмет обнаружения возможных проблем в системе безопасности, а также для проверки уровня защиты сети от всех потенциальных уязвимостей, которые хакер может применить для взлома сети.

LanHelper — программа проверки и сканирования офисных и домашних сетей. Программа имеет точный и быстрый сканер, вы-дающий информацию об IP- и МАС-адресах и позволяющий детально и удобно просматривать данные удаленного компьютера с Web-браузером в режимах просмотра HTML-документов. Кроме того, программа LanHelper позволяет отключать или перезагружать, а также планировать периодическое и (или) отложенное сканирование удаленных компьютеров.

Особенности работы тест-программ рассмотрим на примере проведения оценочных тестов программой SelFTrend. Свободная версия программы доступна для загрузки на сайте www.prolan.ru/ selftrend.

Программа позволяет измерять, оценивать и контролировать производительность работы сетевого оборудования и сетевых сервисов, включая:

* измерение времени реакции файловых сервисов;
* съем SNMP-статистики о работе активного сетевого оборудования;
* получение статистической информации о работе серверов MS Windows;
* получение в режиме реального времени информации о работе сети;
* оповещение о возникающих в сети сбоях посылкой сообщений администратору сети и запуском внешних программ.

Отличительной особенностью программы SelFTrend является реализованный в ней метод пороговых значений, называемый в документации по программе методом светофора. Его суть заключается в следующем. Значения измеряемых характеристик автоматически сравниваются с пороговыми значениями, хранящимися в специальном файле, который называется «модуль знаний». На основании результатов сравнения формируется и выводится на экран интегральная оценка состояния того компонента сети, характеристики которого она измеряет. На экране эта оценка имеет вид светофора. Если значения измеряемых характеристик в норме, то «светофор» горит зеленым светом. Если пороговые значения превышены, то, в зависимости от величины превышения, «светофор» будет выдавать соответствующий сигнал светофора: мигающий желтый, желтый, мигающий красный, красный.

Среди комплекса оценочных тестов программы приведем четыре:

* 1. оценка состояния серверов MS Windows;
  2. оценка состояния коммутаторов Ethernet;
  3. интегральная оценка производительности файлового сервиса сети;
  4. интегральная оценка качества IP-канала в сети VoIP.

Первые три теста ориентированы на тестирование локальных сетей, а четвертый — на тестирование распределенных сетей.

Рассмотрим выполнение первого теста «Оценка состояния серверов MS Windows», который позволяет определить, соответствует ли производительность серверов требованиям используемых в сети приложений. Работа теста основана на автоматическом контроле статистической информации о работе серверов MS Windows NT4/2000/XP. После своего запуска программа SelFTrend предлагает ввести имена серверов, которые должны тестироваться, а также тип ОС MS Windows, которая установлена на этих серверах.

После запуска теста программа подключается к тестируемым серверам и с заданной периодичностью начинает контролировать основные характеристики их работы. Значение каждой характеристики оценивается соответствующим счетчиком. Контролируемые характеристики и диапазоны разрешенных значений соответствующих им счетчиков указаны в таблице 4.1.3 В содержательном плане приведенные характеристики означают следующее.

Память (доступно байт) — это объем оперативной памяти на сервере, которая доступна операционной системе в текущий момент времени.

Обмен «память <-» диск» (страниц/с) — это среднее число страниц в секунду, которое ОС сервера была вынуждена прочитать с диска и (или) записать на диск, так как требуемых страниц не оказалось в оперативной памяти сервера в тот момент, когда они потребовались приложению или ОС.

Файл подкачки — если объем этого файла на диске исчерпан, то ОС не сможет запустить новую задачу и будет динамически его расширять, что приведет к резкому падению производительности сервера и «светофор» предупредит, что необходимо увеличить размер файла подкачки.

Процессор (общий процент загруженности процессора) — это процент времени, который приходится на выполнение процессорами сервера полезной работы. Если значение счетчика, отвечающего за эту характеристику, в течение продолжительного времени превышает 85%, то это свидетельствует о недостаточной производительности процессоров сервера. В этом случае следует заменить процессоры более мощными либо переместить часть задач на другие компьютеры.

Таблица 4.1.3 – Характеристика оценки серверов

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Характеристика | Сигнал «светофора» | |
| Зеленый | Красный |
| 1 | Память (доступно) | > 64 Мбайт | < 4 Мбайт |
| 2 | Обмен «память<-»диск» (страниц/с) | < 40 | > 120 |
| 3 | Файл подкачки (общий процент использования) | < 60 | > 90 |
| 4 | Процессор (общий процент загруженности процессора) | < 30 | > 85 |
| 5 | Кэш (процент запросов на получение данных) | > 80 | < 20 |
| 6 | Физический диск (процент активности диска при чтении (записи)) | < 5 | > 25 |
| 7 | Физический диск (процент активности диска при чтении (записи)) | <20 | >50 |
| 8 | Система (время работы системы, с) | > 600 | < 600 |

Кэш (процент запросов на получение данных) — это процент запросов на получение данных, которые уже находятся в оперативной кэш-памяти сервера, поэтому обращение к диску не требуется. Обращения к диску существенно увеличивают время выполнения запросов и, следовательно, снижают производительность работы сервера.

Физический диск (процент активности диска при чтении (записи)) — это процент времени, которое тратится дисковыми устройствами сервера на обработку запросов на чтение (запись) данных. В случае выхода этой характеристики за пределы, установленные счетчиком, рекомендуется установить на сервере более быстрые диски или переместить активно используемые файлы (например, файлы БД и (или) подкачки) на другие диски.

Система (время работы системы, с) — общее время работы сервера, прошедшее с момента его последней перезагрузки. Считается, что сервер должен перезапускаться как можно реже, поэтому новая перезагрузка (< 10 мин) вызывает мигающий желтый сигнал «светофора».

**Диагностика неисправностей средств сетевых коммуникаций**

**Введение в диагностику кабельных систем**

Кабельные системы являются основой построения каналов для передачи и приема информации в сетях. Они всегда проектируется на основе иерархического принципа, благодаря чему получили название «структурированные кабельные системы». Любая перспективная СКС на этапе подготовки к эксплуатации должна быть протестирована специальным оборудованием для выявления тех или иных дефектов и на соответствие заданным характеристикам. От результатов проверки зависит качество и долговечность СКС. Основной практический интерес при тестировании СКС имеют линии связи на основе витых пар и оптики, чаще других использующиеся для построения кабельных систем. Для облегчения проектирования и обслуживания СКС на них разработаны стандарты: международный ISO/IEC 11801: 2002-Е (далее — международный).

Стандарты призваны обеспечить взаимозаменяемость и универсальное качество СКС наряду с ее доступностью и грамотным использованием. В частности, стандарты телекоммуникационной инфраструктуры зданий должны обеспечить работу разнотипного оборудования любых производителей, создание СКС на этапе строительства зданий и их длительную эксплуатацию.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № п/п | Частота, МГц | Максимально допустимые значения потерь ARL, дБ | | | |
| Класс С | Класс D | Класс Е | Класс F |
| 1 | 1 | 15,0/15,0 | 17,0/19,0 | 19,0/21,0 | 19,0/21,0 |
| 2 | 16 | 15,0/15,0 | 17,0/19,0 | 18,0/20,0 | 18,0/20,0 |
| 3 | 100 |  | 10,0/12,0 | 12,0/14,0 | 12,0/14,0 |
| 4 | 250 |  |  | 8,0/10,0 | 8,0/10,0 |
| 5 | 600 |  |  |  | 8,0/10,0 |

Таблица 4.1.4 – Категории и классы кабельной системы

Категории и классы кабельной системы приведены в таблице 3.5. Классификации по производительности в международном и американском стандартах отличаются друг от друга.

Международный стандарт определяет классы приложений (от А до F), которые могут работать по данной системе, а американский — специфицирует системы по максимальной частоте передаваемых сигналов (категории 3...7). Поэтому для определения СКС используются как категории, так и классы.

Стандарты определяют среду передачи, параметры разъемов, линии и канала, в том числе предельно допустимые длины, способы подключения проводников, топологию и функциональные элементы СКС.

Реальная кабельная линия всегда имеет неоднородности, которые приводят к отражению электромагнитной волны в процессе прохождения сигнала по кабелю. Обратные потери ARL, дБ, — мера величины отражения сигналов, вызываемого несоответствием импедансом компонентов кабельной системы. Этот параметр определяется как отношение мощности основного сигнала к мощности обратного потока энергии.

Максимально допустимые стандартом ISO-11801 значения потерь ARL, ДБ, В формате канал/стационарная линия приведены в таблице 4.1.4

Наиболее распространенной причиной возникновения обратных потерь является различие волнового сопротивления у компонентов кабельного канала (розетка, патчпанель, кабель и т.д.). Поэтому рекомендуется подбирать оборудование одного производителя, обладающее одинаковыми (специально подобранными) характеристиками. Также неоднородность может возникнуть в случае нарушения шага скрутки. Это может быть следствием брака при производстве либо ошибки монтажников при протяжке кабеля, надлома жилы или слишком сильного изгиба.

Тестирование кабельных систем. Конечные пользователи и проектировщики сетей постоянно планируют более высокие скорости передачи данных, возможности передачи большего количества данных, а также способность сети к гибкой и удобной пере конфигурации.

Таблица 4.1.5 – допустимые значения потерь.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № п/п | Частота, МГц | Максимально допустимые значения потерь ARL, дБ | | | |
| Класс С | Класс D | Класс Е | Класс F |
| 1 | 1 | 15,0/15,0 | 17,0/19,0 | 19,0/21,0 | 19,0/21,0 |
| 2 | 16 | 15,0/15,0 | 17,0/19,0 | 18,0/20,0 | 18,0/20,0 |
| 3 | 100 |  | 10,0/12,0 | 12,0/14,0 | 12,0/14,0 |
| 4 | 250 |  |  | 8,0/10,0 | 8,0/10,0 |
| 5 | 600 |  |  |  | 8,0/10,0 |

До 20% высокоскоростных СКС, как правило, не обеспечивают возможного быстродействия, что является результатом некачественной их реализации. Это особенно хорошо заметно на примерах высокоскоростных систем, в состав которых входят Fast Ethernet, коммутируемые LAN, Gigabit Ethernet.

СКС не существует, пока не проведено ее тестирование. Тестирование СКС определено международным стандартом в трех видах:

1) приемочное тестирование (ПТ) — позволяет принять СКС к эксплуатации, если она сделана в соответствии с рекомендациями стандарта по структуре, топологии и изготовлению и состоит из компонентов с известными характеристиками, отвечающих заранее установленным категориям;

2) тестирование на соответствие (ТС) — позволяет объявить соответствующей стандарту ISO/IEC 11801: 2002(E) кабельную систему, которая содержит не только известные по характеристикам компоненты, но и такие компоненты, характеристики которых заранее неизвестны;

3) эталонное тестирование (ЭТ) — применяется как средство тестирования моделей каналов и линий в лабораторных условиях с помощью лабораторного оборудования, а также как средство для сравнения результатов измерений, полученных с помощью лабораторного оборудования, с результатами, полученными «полевым» измерительным оборудованием. Эталонное тестирование моделей каналов и линий в лабораторных условиях используется также для проверки тех параметров, которые не могут быть протестированы в полевых условиях.

Параметры, измеряющиеся в соответствии с международным стандартом, в таблице 4.1.5 отнесены к одной из трех категорий:

1) информативные («И») — могут измеряться по согласованию с заказчиком СКС;

2) расчетные («Р») — рассчитываются по измеренным параметрам;

3) обязательные («О») — измеряются обязательно.

Из таблицы 4.1.6 видно, что при приемочном тестировании обязательными параметрами для измерений являются только карта соединений и непрерывность проводников. Однако убедиться в качестве остальных параметров, определяемом именно монтажом, можно только их измерением, поэтому если приемку проводит заказчик, то фактически производится не «приемочное тестирование», а «тестирование на соответствие», даже если соблюдены условия приемочного тестирования.

Таблица 4.1.6 – Тестирование параметров измерений

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Параметр | Тестирование | | |
| ПТ | тс | эт |
| 1 | Возвратные потери *ARL* | И | о | о |
| 2 | Затухание на ближнем конце NEXT | И | о | о |
| 3 | Суммарное переходное затухание на ближнем конце | Р | р | р |
| 4 | Защищенность на ближнем конце | И | о | о |
| 5 | Суммарная защищенность на ближнем конце | И | р | р |
| 6 | Нормированное переходное затухание на дальнем конце | И | о | о |
| 7 | Суммарное переходное затухание на дальнем конце | Р | р | р |
| 8 | Сопротивление петли по постоянному току | И | о | о |
| 9 | Задержка сигнала | Р | о | о |
| 10 | Перекос задержки | Р | о | о |
| 11 | Длина канала, линии | И | и | о |
| 12 | Карта соединений | О | о | о |
| 13 | Непрерывность проводников, экранов, КЗ и обрывы | О | о | о |

Основным инструментом для оперативного тестирования кабельных систем, реализованных на основе витых пар, являются кабельные сканеры.

Одна из наиболее удобных и важных функций тестирования кабельных систем — автоматизация процесса проведения измерений и интерпретация полученных результатов. Во время общего теста (режим Autotest) в течение нескольких секунд последовательно, без вмешательства оператора, измеряется ряд необходимых для проверки параметров. Результаты измерений сравниваются с требованиями стандартов, после чего выдается заключение в виде: «выполняется/не выполняется». Время автотеста составляет около 10...20 с. Многие сканеры поддерживают голосовую связь во время тестирования, что очень удобно при тестировании распределенной СКС.

Практические рекомендации по тестированию СКС. Правила использования полевых тестеров определены их подробными инструкциями, которая должна быть изучена досконально. Однако приведенные далее рекомендации следует учитывать при пользовании любым из этих приборов.

1. При проведении тестирования необходимо представлять, по каким критериям проводится тестирование. Как правило, полевые тестеры имеют режим «Автотест», в котором могут использоваться американский, международный или другие стандарты, поэтому необходимо однозначно выбрать стандарт и набор параметров, подлежаoих измерению.

2. Необходимо точно знать скорость распространения сигнала в том кабеле, из которого сделана линия, и на котором проводятся измерения. Для кабелей скорость распространения сигнала обязательно указывается в спецификации, а полевые тестеры, как правило, хранят библиотеку этих значений для конкретных типов изделий. Скорость распространения сигнала по кабелю принято характеризовать параметром NVP, который указывается в долях от скорости света. В четырех парных кабелях значения NVP находятся в пределах от 0,6 до 0,8. Тестеры обычно имеют функцию калибровки NVP, которая позволяет на образце данного кабеля известной длины определить этот параметр. Минимальная длина кабеля при этом должна быть более 15 м; чем она больше, тем лучше, поскольку точность в значении NVP будет определять точность измерения длины полевым тестером.

3. Необходимо прокалибровать прибор именно при выбранных критериях перед началом измерений.

4. Тестовые шнуры и измерительные адаптеры изнашиваются в процессе эксплуатации и погрешности прибора возрастают. Поэтому стандарт IEC 61935-1 настоятельно рекомендует владельцу тестера создать «эталонную» линию и периодически проверять по ней свой прибор.

Особенности проверки электрической подсистемы СКС. Тестирование электрической подсистемы СКС выполняется с помощью рефлектометра, принцип действия которого основан на анализе сигнала, отраженного от различных неоднородностей в линии при ее зондировании мощными импульсами тока небольшой длительности.

Электрическая волна, возбуждаемая в тестируемой линии импульсным генератором рефлектометра, при распространении в линии отражается в обратном направлении от всех точек неоднородностей. Анализатор приемника контролирует как момент прихода отраженного сигнала, так и изменение его формы во времени. Результат работы анализатора может быть представлен на дисплее графически, в виде так называемой рефлектограммы, или же в табличной форме. По времени задержки между зондирующим и приходящим импульсом рассчитывается расстояние до неоднородности, и его значения выводятся на экран.

Рефлектограммы для электрических кабелей получили широкое распространение в сетях городской и междугородной связи. Из-за трудностей анализа начального участка они эффективны только в процессе тестирования кабелей магистральных подсистем и поэтому не получили широкого распространения в технике СКС. При тестировании кабельных систем здания их роль успешно выполняют кабельные сканеры, реализующие функции рефлектометра.

Особенности тестирования оптоволоконных сетей. Процедуры тестирования оптоволоконных линий и каналов СКС, построенных в соответствии с международным стандартом, определены международным техническим документом ISO/IEC TR 14763-3, в котором указаны следующие характеристики СКС, подлежащие проверке:

* целостность оптоволокон;
* длина линий и каналов;
* задержка оптических сигналов;
* ослабление оптических сигналов.

Целостность оптоволокон разрешается определять любым прибором, начиная от любого простого источника света и заканчивая оптическими рефлектометрами. В СКС, где длины внутри объектовых кабелей не превышают 100 м, для этой цели удобно использовать недорогие (250 долл. США) определители обрывов.

Длина линий и каналов определяется по длине кабелей СКС или рефлектометром.

Задержка оптических сигналов определяется расчетным путем по известным значениям длины линий и группового показателя преломления оптоволокна, обычно указываемого производителем кабеля. Как правило, задержка сигналов в оптоволокне составляет 5 нс/м.

Ослабление оптических сигналов при наладочных измерениях можно измерять относительно недорогими оптическими тестерами, содержащими источник света и измеритель мощности. При ответственных измерениях, имеющих целью установить соответствие инсталлированной СКС международному стандарту, необходимо применять качественные приборы, отличающиеся от простых оптических тестеров гарантированной спектральной шириной источника излучения, стабильностью и точностью прибора.

**Оборудование для проверки кабельных систем**

Оборудование для проверки кабельных систем. Оно подразделяется на четыре группы: сетевые анализаторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры. При этом для каждого вида проверок, приведенных в таблице 4.1.7, необходимо применять только соответствующее этому виду оборудование.

Сетевые анализаторы — это эталонные измерительные инструменты для диагностики и сертификации кабелей и СКС. Примером сетевого анализатора может служить устройство HP 85 компании Hewlett-Packard.

Сетевые анализаторы являются интеллектуальными устройствами, способными работать на физическом, канальном, а иногда и на сетевом уровнях. В их состав входят высокоточный частотный широкополосный генератор и узкополосный приемник, позволяющие измерять на приемной паре амплитудно-частотную характеристику, перекрестные наводки, затухание, суммарное затухание, параметр NEXT.

Кроме того, с их помощью можно измерять среднюю интенсивность общего трафика сети и среднюю интенсивность потока пакетов с определенным типом ошибки. Сетевой анализатор представляет собой лабораторный прибор больших размеров, достаточно сложный в обращении, стоимостью более 20 ООО долл. США.

Далее рассмотрены портативные диагностические устройства, доступные практически каждому администратору ЛВС.

Таблица 4.1.7 – Виды операций тестирования

|  |  |  |
| --- | --- | --- |
| № п/п | Вид контрольной операции | Оборудование |
| 1 | Эталонное тестирование кабелей разных категорий | Сетевой анализатор |
| 2 | Проверка кабеля на отсутствие физи­ческого обрыва | Тестеры |
| 3 | Диагностика медных кабельных систем | Кабельные сканеры |
| 4 | Сертификация СКС на соответствие определенному стандарту. Диагно­стика СКС | Портативные устройства для сертификации СКС |

Кабельные сканеры используются для диагностики медных кабельных систем. Основное назначение кабельных сканеров — измерение электрических и механических параметров кабелей: длины кабеля, параметра NEXT, затухания, импеданса, схемы разводки пар проводников, уровня электрических шумов в кабеле. Точность измерений, произведенных этими устройствами, ниже, чем у сетевых анализаторов, но вполне достаточная для оценки соответствия кабеля стандарту.

Для определения местоположения неисправности кабельной системы (обрыва, короткого замыкания, неправильно установленного разъема и т.д.) используется метод отраженного импульса. Суть этого метода заключается 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 почти отсутствует.



(а) (б)

Рис.4.1.1 – Кабельный сканер PentaScanner (а) и кабельный тестер (б)

Точность измерения расстояния зависит от того, насколько точно известна скорость распространения электромагнитных волн в кабеле, которая задается в процентах от скорости света в вакууме. Современные сканеры содержат в себе электронную таблицу данных об этом параметре для всех основных типов кабелей, что дает возможность пользователю после калибровки сканера устанавливать их самостоятельно. На рисунке 4.1.2, а представлен современный многофункциональный сканер семейства моделей PentaScanner компании Microtest, который применяется для сертификации кабельных систем категории 5. Он предназначен для поиска неисправностей кабельной системы и представляет собой недорогой и простой в использовании прибор, позволяющий быстро определить неисправность кабельной системы. Кабельный сканер PentaScanner содержит несколько частотных генераторов и узко-полосных приемников, графический дисплей на жидких кристаллах и флэш-память для записи результатов тестирования и новых версий ПО. Как элемент питания PentaScanner использует аккумуляторные батареи, работающие без подзарядки до 10 ч. Прибор содержит разъемы для прямого присоединения к кабелю.

Для измерения перекрестных наводок между витыми парами (NEXT) источник сигналов — Super Injector (прибор, поставляемый в комплекте с PentaScanner) — подсоединяется к передающей паре и начинает передавать в нее сигналы различной частоты. Приемник сигналов подключается к приемной паре и измеряет сигнал, наведенный в ней, сравнивая его со стандартными величинами. Преимуществом узкополосного приемника в PentaScanner является измерение чистого NEXT с отфильтровыванием всех наводок и электрического шума. Для измерения затухания PentaScanner использует Super Injector+ в качестве удаленного источника сигналов, генерирующего серию сигналов различной частоты. Сканер PentaScanner в этот момент измеряет амплитуду этих сигналов на другом конце кабеля.

Кабельный тестер, показанный на рисунке 3.6.2.1, б, — это наиболее простой и дешевый прибор для диагностики витой пары. Он позволяет определить непрерывность кабеля, не указывая места сбоя. Кабельный тестер этого типа показывает только минимальное соответствие характеристик канала связи заложенным в него требованиям. Этот тип кабельного тестера служит для повышения эффективности монтажа проводки и оперативного обнаружения неисправностей.

Оборудование для проверки оптоволоконных СКС. Оно очень разнообразно. Рассмотрим назначение отдельных его представителей.

Измеритель оптической мощности используется для измерения оптической мощности сигнала и в паре со стабилизированным оптическим излучателем применяется для измерения затухания в кабеле. Основным показателем качества измерителя является тип примененного в нем фотодиода. Наилучшие характеристики имеет фотодиод на основе арсенида галлия.

Анализатор затухания — это комбинация оптического измерителя мощности и источника оптического сигнала. Выпускается он в виде набора из измерителя, излучателей на разных длинах волн и комплекта оптических интерфейсов, показанных на рисунке 4.1.2



Рис. 4.1.2 – Комплект оптических интерфейсов

Оптические аттенюаторы используются для моделирования потерь в оптической линии при стрессовом тестировании сети, при измерении коэффициента ошибок, калибровке и проверке измерителей мощности, тестировании оптоэлектронных и электрооптических преобразователей, анализе допустимых потерь оптического сигнала на всем пути от передатчика до приемника (эти потери называются оптическим бюджетом линии).

В оптических аттенюаторах используются различные методы внесения затухания: осевое и радиальное смещение, использование фильтров и призм. Для согласования излучающего и приемного торцов световодов применяются согласующие узлы, фокусирующие излучение.

Основными характеристиками оптических аттенюаторов являются: точность, линейность, уровень возвратных потерь, повторяемость установления затухания, разрешение, остаточное вносимое затухание.

Оптические рефлектометры являются наиболее информативными и мощными средствами тестирования волоконно-оптических линий.

На рисунке 4.1.3 показан оптический рефлектометр OptiFiber Pro, позволяющий обнаруживать, идентифицировать и измерять эффекты отражения и потерь в многомодовых и одномодовых волоконно-оптических линиях. Номинальная предельная дальность измерений составляет 35 км при длине волны 1 300 нм в многомодовых оптических линиях и 130 км при длине волны 1 550 нм в одномодовых оптических линиях.

Большинство рефлектометров имеет встроенное ПО для автоматического определения и анализа участков аномального затухания и разрывов. Все, что требуется от специалиста, — это подключить устройство к кабельной линии и нажать кнопку, а затем ознакомиться с результатами измерений. Благодаря применению рефлектометра можно быстро находить дефекты на линии связи и иметь представление об их характере, чтобы заранее знать, какие меры предпринять для их устранения. Современные рефлектометры имеют очень высокий уровень точности. Оптические рефлектометры имеют следующие особенности:

* за один цикл они позволяют измерять целый ряд параметров (длину, затухание и местонахождение неоднородности);
* допускают выполнение измерений с одного конца кабеля;
* высокие требования к качеству ввода излучения в тестируемое волокно;
* достаточно малое время получения рефлектограммы — около 30с.

Оптический локатор — это упрощенный вариант рефлектометра. Принцип его действия идентичен работе рефлектометра, а упрощение достигнуто за счет отказа от графического дисплея и применения более простого ПО. Функция «визуализатор дефектов» является одной из наиболее полезных функций оптического локатора. Визуализатор дефектов предназначен для выявления близких к концу кабеля (не более 5 км) обрывов и других дефектов, волоконных световодов методом просветки. Основой прибора является лазер красного свечения. При подключении визуализатора к волокну в месте повреждения наблюдается красное свечение.

Идентификаторы кабеля применяют для неразрушающего тестирования его целостности, проверки маркировки кабеля, подтверждения наличия или отсутствия сигнала в линии, определения вида модуляции, а также для ввода-вывода оптического сигнала через изгиб кабеля.



Рис. 4.1.3 – Оптофоны

Последняя возможность эффективно используется для организации связи по проложенному кабелю, когда идентификаторы кабеля используются в комплекте с оптическими разговорными устройствами. Идентификаторы удобны для пошагового прохода (трассировки) оптического кабеля.

Анализатор возвратных потерь измеряет суммарный уровень отражения во всей линии, включая кабель, оптические интерфейсы и разветвители. Возвратные потери приводят к понижению отношения сигнал/шум в аналоговых системах и увеличению параметра ошибки в цифровых системах передачи. В качестве источника сигнала обычно используется лазерный диод в режиме и непрерывного излучения, а в качестве измерителя мощности отраженного сигнала — измерители оптической мощности. Очень важна стабильность источника сигнала, поскольку спектральная нестабильность источника приводит к удвоению ошибки измерения за счет отражения.

Оптические разговорные устройства (оптофоны), представленные на рисунке 3.6.2.3, обеспечивают голосовую связь по оптическому кабелю при его прокладке и тестируют его работоспособность. Голосовая оптическая связь обеспечивает взаимодействие между бригадами, производящими укладку кабеля. В полудуплексных оптофонах режим передачи переключается вручную или активируется голосом. В полнодуплексных оптофонах прием и передача осуществляются одновременно на двух разных длинах волн или применяется временное разделение сигналов на одной длине волны.

Динамический диапазон современных оптофонов достигает 60 дБ, что позволяет разговаривать на расстоянии до 150 км.

## 1.5 Организация профилактических работ на объектах сетевой инфраструктуры

Техническое обслуживание (ТО) - это комплекс организационно-технических мероприятий и работ, производимых на объекте и направленных на поддержание в рабочем или исправном состоянии оборудования (программного обеспечения (ПО)) технических систем в процессе их использования по назначению с целью повышения надежности и эффективности их работы.

Основными задачами Технического обслуживания систем являются:

* определение качественного состояния оборудования, кабельных сетей и проверка их работоспособности (в том числе ПО);
* своевременное выявление и устранение недостатков, снижающих эффективность работы систем и приводящих к возникновению отказов аппаратуры (ПО);
* предупреждение отказов оборудования (ПО), увеличение межремонтных сроков эксплуатации и сроков службы оборудования;
* проверка и доведение до установленных норм параметров оборудования систем, линейно-кабельных и распределительных устройств;
* ликвидация последствий воздействия на оборудование неблагоприятных климатических и других условий эксплуатации;
* подготовка оборудования к сезонной эксплуатации;
* проверка укомплектованности механизмов, аппаратуры, наличия инструментов и пополнение ЗИП;
* анализ и обобщение сведений результатов выполненных работ, разработка мероприятий по совершенствованию форм и методов Технического обслуживания, эксплуатации систем;
* техническая консультативная поддержка эксплуатирующего персонала и руководителей по любым вопросам, связанным с эксплуатацией систем в целях эффективного использования.

Техническое обслуживание — это комплекс мероприятий, направленных на поддержание аппаратуры в исправном состоянии, контроль ее параметров и обеспечение профилактического ремонта.

Организация технического обслуживания средств вычислительной техники (СВТ) включает в себя не только типовые системы технического и профилактического обслуживания, периодичность и организацию работ и материально-техническое обеспечение, но и системы автоматизированного контроля и диагностирования, системы автоматического восстановления, а также различные виды программного, аппаратного и комбинированного контроля, микро диагностику и диагностические программы общего и специального назначения. С этими и другими понятиями нам и предстоит

далее познакомиться.

Техническое обслуживание СВТ включает в себя следующие этапы (рис. 1.1):· обслуживание аппаратного обеспечения (АпОб) средств ВТ и сетей:

– профилактику АпОб,

– диагностику АпОб,

– ремонт АпОб;

Порядок планирования и проведения мониторинга компьютерных сетей и порядок организации работ по техническому сопровождению корпоративной компьютерной сети

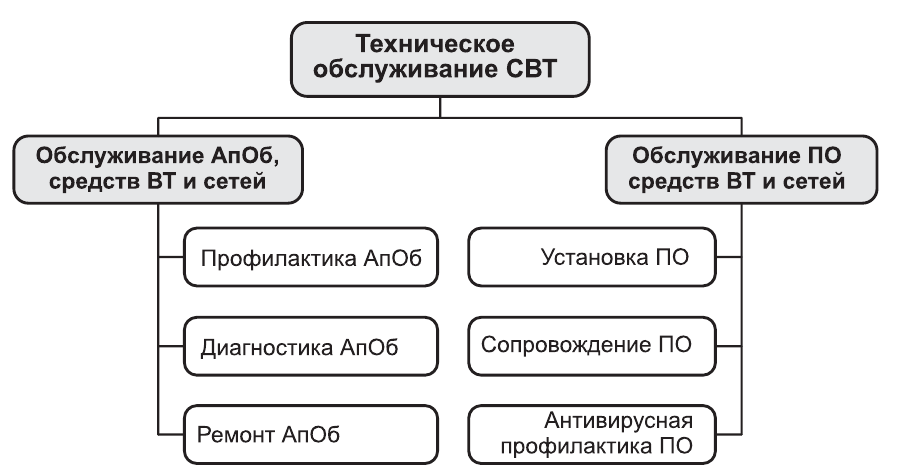


Рис. 5.1.1 Техническое обслуживание СВТ· обслуживание программного обеспечения (ПО) средств ВТ и сетей:

– установку ПО,

– сопровождение ПО,

– антивирусную профилактику.

Все виды работ, связанные с профилактикой (уход за внешним состоянием, уборку пыли внутри корпуса ПК), пользователь СВТ обычно может провести сам. Кроме того, на предприятиях существуют специалисты (если предприятие небольшое) или даже целые информационные отделы, обслуживающие весь комплекс имеющихся СВТ. Они также выполняют работы по диагностированию и ремонту аппаратных средств в случае их отказа.

Классификация регламентов технических осмотров, технические осмотры объектов сетевой инфраструктуры

Обслуживанием ПО обычно занимаются системные администраторы.

ТО СВТ, в соответствии с ГОСТ 28470-90, можно также подразделить на следующие виды:

* регламентированное;
* периодическое;
* с периодическим контролем;
* с непрерывным контролем.

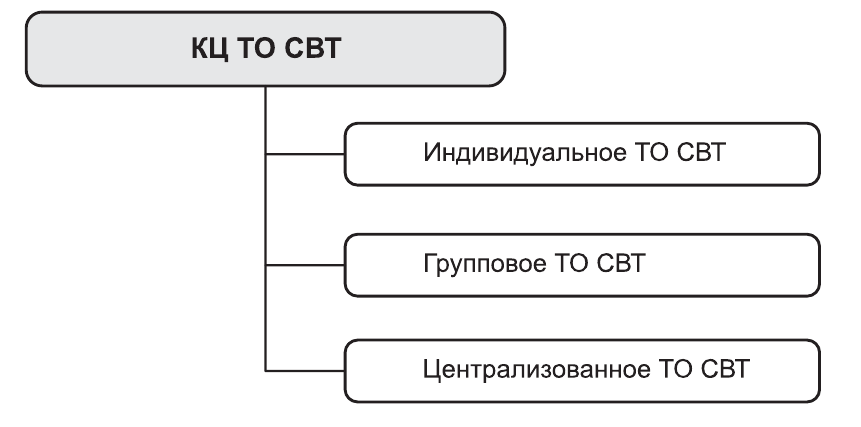


Рис. 5.1.2. Типовая система ТО СВТ

При индивидуальном обслуживании каждое устройство обеспечивается полным комплектом сервисной аппаратуры и тестовых программ, запасным инструментом и соответствующим обслуживающим персоналом, которые совместно должны обеспечивать заданное время восстановления устройства.

При групповом обслуживании несколько рабочих станций и соответствующих периферийных устройств обслуживаются силами и средствами персонала информационно-технических отделов (АСУ, АИС и т. д.) или сервисных центров; структура состава оборудования при этом та же, что и при индивидуальном обслуживании, но с включением дополнительной аппаратуры и приспособлений.

Централизованное техническое обслуживание СВТ осуществляется сетью региональных центров обслуживания и их филиалов, которые в централизованном порядке производят:

* монтажно-наладочные работы и ввод в эксплуатацию любого вида аппаратуры;
* устранение сложных отказов, возникающих в процессе
* эксплуатации СВТ;
* централизованный ремонт типовых элементов замены
* и электромеханических устройств в ремонтных органах;
* оказание помощи обслуживающему персоналу предприятий по вопросам материального обеспечения и совершенствования эксплуатации, повышение их квалификации;
* управление процессом обслуживания СВТ на основе данных учета и анализа;
* ввод в эксплуатацию существующих и разрабатываемых операционных систем (ОС), пакетов прикладных
* программ (ППП), тестового программного обеспечения

и т.д.**Комплекс организационно-технических мероприятий; выявление и своевременная замена элементов инфраструктуры**

1. Мониторинг аппаратного обеспечения

Мониторинг работоспособности аппаратных компонентов КС осуществляется в процессе их обслуживания и при проведении работ по техническому обслуживанию оборудования. Наиболее существенные компоненты системы, имеющие встроенные средства контроля работоспособности (серверы, активное сетевое оборудование), должны контролироваться постоянно.

2. Мониторинг парольной защиты

Мониторинг парольной защиты и контроль надежности пользовательских паролей предусматривают:

* установление сроков действия паролей;
* периодическую (не реже 1 раза в месяц) проверку пользовательских паролей.

3. Мониторинг попыток несанкционированного доступа

Предупреждение и своевременное выявление попыток несанкционированного доступа осуществляется с использованием средств операционной системы, специальных программных средств и предусматривает:

* фиксацию неудачных попыток входа в систему в системном журнале;
* протоколирование работы сетевых сервисов;
* выявление фактов сканирования определенного диапазона сетевых портов в короткие промежутки времени с целью обнаружения сетевых анализаторов, изучающих систему и выявляющих ее уязвимости.

4. Мониторинг производительности

Мониторинг производительности КС производится по обращениям пользователей в ходе обслуживания систем и при проведении профилактических работ.

5. Системный аудит

1. Системный аудит производится администратором информационной безопасности ежеквартально и в особых ситуациях. Он включает проведение обзоров безопасности с занесением записей в Журнал обзоров безопасности, тестирование системы, контроль внесения изменений в системное программное обеспечение.
2. Активное тестирование надежности механизмов контроля доступа производится путем осуществления попыток проникновения в систему (с помощью автоматического инструментария или вручную).
3. Пассивное тестирование механизмов контроля доступа осуществляется путем анализа конфигурационных файлов системы.
4. Внесение изменений в системное программное обеспечение осуществляется с условием обязательного документирования изменений в соответствующем журнале; уведомлением каждого сотрудника, которого касается изменение; рассмотрением претензий в случае, если внесение изменений повлекло причинение вреда; разработкой планов действий в аварийных ситуациях для восстановления работоспособности системы, если внесенное в нее изменение вывело ее из строя.

6. Антивирусный контроль

Для защиты объектов вычислительной техники необходимо использовать антивирусные программы:

* резидентные антивирусные мониторы, контролирующие подозрительные действия программ;
* утилиты для обнаружения и анализа новых вирусов.

К использованию допускаются только лицензионные средства защиты от вредоносных программ и вирусов или сертифицированные свободно распространяемые антивирусные средства.

При подозрении на наличие не выявленных установленными средствами защиты заражений следует использовать Live CD с другими антивирусными средствами.

Запуск антивирусных программ должен осуществляться автоматически по заданию, централизованно созданному с использованием планировщика задач (входящим в поставку операционной системы либо поставляемым вместе с антивирусными программами).

Устанавливаемое (изменяемое) на серверы программное обеспечение должно быть предварительно проверено на отсутствие компьютерных вирусов и вредоносных программ. Непосредственно после установки (изменения) программного обеспечения сервера должна быть выполнена антивирусная проверка.

7. Анализ попыток взлома инцидентов

Если администратор информационной безопасности подозревает или получил сообщение о том, что система подвергается атаке или уже была скомпрометирована, то он должен установить:

* факт попытки несанкционированного доступа (далее - НСД);
* продолжается ли НСД в настоящий момент;
* кто является источником НСД;
* что является объектом НСД;
* когда происходила попытка НСД;
* как и при каких обстоятельствах была предпринята попытка НСД;
* точка входа нарушителя в систему;
* была ли попытка НСД успешной;
* определить системные ресурсы, безопасность которых была нарушена;
* какова мотивация попытки НСД.

8. Порядок проведения резервного копирования

1.  Для предотвращения потери данных из-за сбоев оборудования, уничтожения оборудования, программных ошибок, неправильных действий персонала и других возможных причин утери информации предусмотрена система регулярного резервного копирования данных. Такое резервное копирование позволяет в случае возникновения ошибки и потери информации вернуться к ближайшей работоспособной копии.

2. Резервное копирование критически важной информации и информации, размещенной на серверах, выполняется на предназначенные для этих целей сервера, ленточные накопители и оптические носители.

3. Резервное копирование проводится автоматически в установленные промежутки времени (ночью, 1 раз в сутки).

4. На объектах вычислительной техники пользователей не предусматривается резервного копирования системной информации, но в целях сохранности важных документов пользователю желательно проводить архивирование и хранение данных документов на оптических дисках (CD-R).

**Программа профилактических мероприятий на объектах сетевой инфраструктуры. Правила эксплуатации технических средств сетевой инфраструктуры. Методы активного профилактического обслуживания. Пассивные профилактические меры**

Профилактическое обслуживание представляет собой ряд мероприятий, направленных на поддержание СВТ в рабочем состоянии в течение определенного промежутка времени и на продлевание технического ресурса СВТ.

Период проведения профилактических работ является необходимым и достаточно продолжительным этапом обеспечения рабочего состояния СВТ. Сокращение сроков проведения профилактического обслуживания обычно негативно влияет на отказоустойчивость СВТ.

Планово-профилактические работы представляют собой совокупность мероприятий, направленных на поддержание СВТ в исправном состоянии, предупреждение сбоев и отказов при работе СВТ. Объем планово-профилактических

работ зависит от технического состояния СВТ и от квалификации инженерно-технического персонала. Продолжительность и периодичность таких работ определены заводами изготовителями в соответствующих инструкциях по эксплуатации.

Сущность профилактических работ сводится к следующему: при подготовке СВТ к решению соответствующих задач обязательно проверяется исправность не только СВТ, но и их составных частей с помощью специально подготовленных задач или тестовых программ с известными ответами (например, при подключении принтера обязательно распечатывается пробная страница — приветствие).

Текущее ТО СВТ предусматривает комплекс настроечных и ремонтных работ, направленных на восстановление утраченных свойств или работоспособности СВТ путем замены или восстановления их составляющих.

В настоящее время типовое профилактическое обслуживание можно подразделить (рис. 1.3) на:

* ежедневную профилактику;
* еженедельную профилактику;
* ежемесячную профилактику;
* полугодовую профилактику;
* ежегодную профилактику.

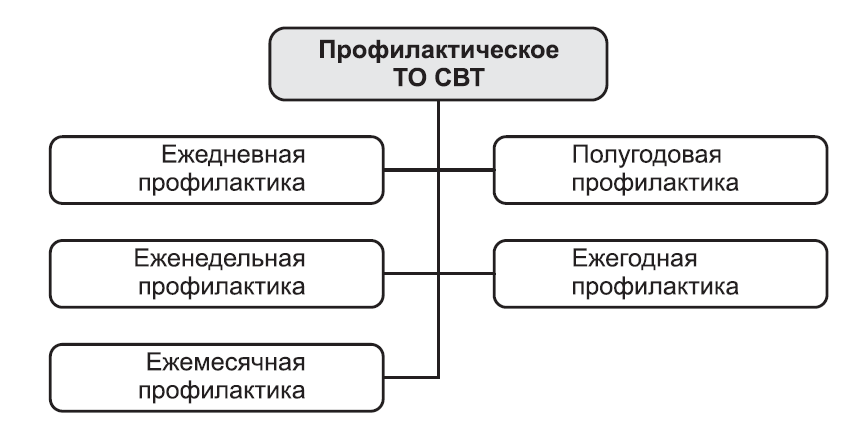


Рис. 5.1.3. Типовое профилактическое обслуживание

Подробное описание профилактических работ обычно дается в инструкциях по эксплуатации СВТ, прилагаемых заводами-изготовителями. В этих инструкциях также содержатся указания о возможных неисправностях СВТ.

Тщательное проведение планово-профилактических работ заметно уменьшает риск появления неисправностей. Однако оперативность нахождения и устранения неисправностей в значительной степени зависит от квалификации и опыта обслуживающего персонала.

**Профилактические мероприятия**

Существуют два типа профилактических мероприятий: активные и пассивные.

При активном профилактическом обслуживании выполняются операции, основная цель которых — продлить срок безотказной работы компьютера. Они сводятся в основном к техническому обслуживанию как всей системы, так и отдельных ее компонентов.

Под пассивной профилактикой обычно подразумеваются меры, направленные на защиту компьютера от внешних неблагоприятных воздействий — таких как перегрев или переохлаждение, перепады напряжения, различные электростатические помехи и т. д.

**Активная профилактика**

Частота проведения активных профилактических мероприятий зависит от местоположения компьютеров и качества их компонентов. Такие мероприятия могут проводиться от одного раза в неделю до одного раза в год, в зависимости от интенсивности использования СВТ.

При проведении активной профилактики необходимо соблюдать следующие меры предосторожности.

1. Перед чисткой необходимо полностью обесточить устройство, отключив его от источника тока. Подключение и отключение системного блока персонального компьютера (ПК) от питающей сети во включенном состоянии не допускается. Подключение и отключение внешних устройств (кроме рассчитанных на подключение по интерфейсу USB или IEEE 1394) к системному блоку, находящемуся во включенном состоянии, не допускается. Повторное включение системного блока ПК следует проводить не ранее чем через минуту после выключения. Во время работы не открывайте корпус блока питания во избежание удара электрическим током, не засовывайте в него посторонние предметы.

2. Чтобы было легче работать внутри компьютера, необходимо обеспечить достаточное освещение.

3. Если активная профилактика устройства проводится впервые и до этого пользователь не разбирал устройство, то при отключении от источника питания и отсоединении проводов или плат расширения лучше отметить положение разъемов и подсоединительных гнезд, чтобы затем вновь правильно подсоединить провода и платы. Все компоненты устройства, не предназначенные для самостоятельной замены, обычно имеют специальные наклейки, удаление или повреждение которых влечет за собой прекращение гарантии на устройство.

4. Лучше не применять при чистке жидкие средства и аэрозоли, заменив их на слегка увлажненный кусок ткани. Слегка намочив ткань в растворе (три части воды, одна часть моющего средства) и отжав ее, протрите корпус компьютера, клавиатуру и внешнюю поверхность корпуса монитора (экран протирается специальными салфетками), а также все периферийные устройства, не допуская попадания раствора внутрь этих устройств.

Головки дисководов можно чистить, используя промышленно выпускаемый набор чистящих средств, специально предназначенных для этой цели. Такие наборы включают в себя «дискеты», обработанные составом для неабразивного удаления загрязнений, которые скапливаются на головках во время их обычной работы. Не следует пытаться чистить головки дисковода щеткой! Вы можете рассогласовать головки, что приведет дисковод в нерабочее состояние.

5. Во избежание повреждения изделия необходимо использовать только те запасные части, которые предусмотрены его производителем.

6. Во время профилактики устройство должно быть размещено на устойчивой подставке или на столе, так как в результате опрокидывания или падения оно может получить серьезные повреждения.

7. Используйте запястный браслет, подключенный заземляющим кабелем к шасси заземленного компьютера. Такой браслет представляет собой гибкую полоску с минимальным сопротивлением 1 МОм ± 10% и с заземляющим проводом. Чтобы обеспечить надежное заземление, надевайте браслет так, чтобы он плотно прилегал к коже.

8. Используйте переносной набор, в который входит складной рабочий коврик для отвода электростатического заряда.

9. Обращайтесь с компонентами и платами компьютера осторожно. Не прикасайтесь к компонентам и соединениям на плате. Берите плату за края или металлические крепежные выступы. Держите такие компоненты, как микропроцессорная схема, за края, а не за выводы.

10. Не загораживайте вентиляционные отверстия, предназначенные для циркуляции воздуха и предотвращения перегрева устройства. Продувочные вентиляторы, установленные на шасси системного блока, охлаждают блок питания и сам компьютер при втягивании воздуха через отверстия в корпусе и его выбросе через выпускные отверстия на задней стороне корпуса. Однако вентилятор втягивает в компьютер также пыль и другие частицы, вызывая тем самым нарост загрязнений, что приводит к росту температуры внутри компьютера и мешает нормальной работе различных компонентов системы. Чтобы избежать этого, рекомендуется содержать рабочее место в чистоте, чтобы уменьшить количество пыли и грязи вокруг компьютера.

Обычный пылезащитный футляр для монитора или клавиатуры также уменьшает накопление пыли и грязи внутри этих устройств, когда они не используются. Однако независимо от наличия защитных футляров время от времени необходимо чистить монитор и клавиатуру. Для удаления пыли из гнезд и других отверстий на компьютере и между клавишами на клавиатуре можно использовать фен или пылесос.

11. Перед подключением устройства необходимо убедиться в соответствии значений напряжения и тока подсоединяемого источника энергии.

12. В целях электробезопасности подключение должно производиться в розетку, снабженную контактом с неплавким заземленным проводником.

13. Электрический шнур должен быть расположен так, чтобы никто не наступал на него. Механические нагрузки на электрический шнур изделия также не допускаются.

14. Штепсельная розетка должна быть расположена рядом с устройством и быть легко доступной.

15. При проведении профилактических мероприятий необходимо соблюдать инструкции, указанные на корпусе изделия.

16. Если устройство не будет использоваться в течение долгого времени, то оно должно быть отключено от основного источника электрического тока во избежание повреждения в результате перенапряжения.

При возникновении следующих ситуаций устройство должно быть обесточено и подвержено активным профилактическим мероприятиям:

* повреждены кабели или разъемы;
* внутрь изделия попала жидкость;
* устройство было подвержено воздействию влаги;
* при обычной работе устройство дает сбои;
* в случае падения изделия и механических повреждений корпуса и других частей;
* изделие имеет очевидные признаки дефекта.

К мерам активной профилактики относится не только чистка устройства, но и сохранение данных. Любой пользователь, даже достаточно опытный, может нечаянно удалить необходимые файлы. Кроме того, при достаточно продолжительном использовании возможен отказ жестких дисков компьютера. Чтобы избежать потери данных, необходимо регулярно делать резервные копии файлов, содержащих нужную информацию. Частота, с которой должны выполняться резервные копии, зависит от объема необходимых данных, содержащихся на диске. Многочасовое повседневное использование систем требует постоянного обновления копий, в отличие от систем, в которых файлы изменяются редко. В среднем резервное копирование постоянно меняющихся данных можно проводить один раз в неделю. В случае отказа дисков или повреждения важных файлов резервные копии избавят вас от потери рабочего времени в течение целого дня. Для гарантии от потери данных желательно хранить копии еженедельных и ежемесячных резервных записей в отдаленном от компьютера и безопасном месте.

Кроме резервного копирования, для сохранения скорости и надежности работы жесткого диска необходимо раз в месяц проводить его дефрагментацию.

Также раз в месяц можно:

* обновлять все антивирусные базы;
* обновлять драйверы для видеоадаптеров, звуковых плат, модемов и других устройств;
* создавать заново загрузочный диск ОС.

**Пассивная профилактика**

Под пассивной профилактикой подразумевают создание приемлемых для работы СВТ общих внешних условий:

* поддержание постоянной температуры и влажности помещения;
* избавление СВТ от электростатического напряжения;
* при необходимости — защита от различного рода излучений;
* поддержание в порядке элементов локальной сети и т. п.

Колебания температуры неблагоприятно сказываются на состоянии СВТ, вызывая, например, окисление контактов, выход из строя различных микросхем, жестких дисков и т. д. Для нормальной работы СВТ необходимо поддержание постоянной температуры. Для любых электронных устройств, в том числе и для компьютеров, в прилагаемой инструкции по эксплуатации указывается допустимый диапазон температур. Эксплуатационные характеристики компьютера и принтера представлены в табл. 1.5.1-1.5.3.

Таблица 1.5.1

**Требования к условиям окружающей среды для работы и хранения струйных принтеров**

|  |  |  |
| --- | --- | --- |
| Характеристики | В процессе печати | При хранении и в режиме ожидания |
| Температура | от 15 до 32,5 °С | от -20 до 40 °С |
| Относительная  влажность | от 10 до 80% | от 10 до 90% |

Таблица 1.5.2

**Требования к условиям окружающей среды для работы и хранения лазерных принтеров**

|  |  |  |
| --- | --- | --- |
| Характеристики | В процессе печати | При хранении и в режиме ожидания |
| Температура | от 7,5 до 35 °С | от 0 до 35 °С |
| Относительная  влажность | от 5 до 90%  (без конденсации) | от 35 до 85%  (без конденсации) |

Для нормальной работы компьютера необходимо избегать его близкого расположения к системам отопления, радиаторам и прочим нагревательным устройствам; относительная влажность воздуха должна составлять от 10 до 90% при тем­пературе 25 °С; массовая концентрация пыли в воздухе не должна превышать 0,75 мг/м . В воздухе не допускается наличие паров кислот и щелочей, вызывающих коррозию. После транспортировки при отрицательных температурах любые компоненты СВТ должны быть выдержаны в нор­мальных климатических условиях в транспортной упаков­ке не менее 6 часов.

Таблица 1.5.3

**Требования к условиям окружающей среды для работы и хранения компьютеров**

|  |  |  |
| --- | --- | --- |
| Характеристики | В процессе работы в закрытых отапливаемых помещениях | При  хранении |
| Температура | от 5 до 35 °С (оптимально 20 ± 5 °С) | от -30 до 60°С |
| Относительная влажность | 10-90%  (оптимально 60 ± 15%) | 5-95% |
| Атмосферное давление | от 84 до 107 КПа | от 84  до 107 КПа |
| Напряженность внешнего магнитного поля | не более 200 А/м | не более 200 А/м |
| Запыленность окружающего воздуха согласно ГОСТ 16325-76 | не более 0,75 мг/м3 | не более 0,75 мг/м3 |
| Электропитание ПК осуществляется от однофазной сети переменного тока напряжением | от 187 до 242 В при частоте 50 Гц |  |
| Сопротивление заземляющего контура | не более 4 Ом (согласно Правилам устройства электро­установок) |  |

Компьютерные системы особенно чувствительны к пере­падам напряжения в сети переменного тока. Повышенное, пониженное или нестабильное напряжение может привести к потере данных или вызвать выход из строя электронных компонентов. Чтобы избежать этих проблем, компьютер и периферийные устройства должны быть надлежащим обра­зом заземлены. При этом необходимо использовать только за­земленные розетки питания и соответствующие кабели, при­лагаемые к компьютеру в стандартной упаковке (с третьим контактом заземления). Кроме того, следует убедиться, что все кабели находятся в исправном состоянии и не имеют видимых повреждений. Не наступайте на них и не пережимайте кабели посторонними предметами.

Перед подключением СВТ необходимо проверить номинальные напряжения, на которые рассчитаны блоки питания компьютерных и периферийных устройств. Они должны соответствовать напряжению питания в вашей местности. (В большинстве европейских стран, в том числе и в России, используется напряжение 230 В/50Гц.)

Не следует использовать одну и ту же электроцепь для работы компьютеров и таких приборов, как кухонные электроприборы, копировальные устройства, кондиционеры, пылесосы, обогревательные приборы, электроинструменты, любое другое оборудование с электроприводом.

Кроме перечисленных приборов, большую опасность для нормального энергообеспечения компьютера вносят броски напряжения или длительные перерывы в энергоснабжении, вызванные грозами. По возможности старайтесь во время грозы выключать компьютер и другие периферийные устройства и отсоединять их от электросети.

При длительном перерыве в энергоснабжении отключите компьютер и вытащите вилку сетевого шнура из розетки. Оставив компьютер включенным, вы рискуете повредить его в тот момент, когда ток будет подан снова: другие приборы, оставленные включенными в этом помещении, могут создать значительный скачок напряжения; кроме того, нередки случаи ошибочной подачи в электросеть более высокого напряжения но сравнению с номинальным.

Существует ряд специальных приборов, таких как сетевые фильтры, источники бесперебойного питания и линейные стабилизаторы, которые защищают СВТ от проблем с перебоями в электропитании — скачков напряжения, нестабильного напряжения и пропадания напряжения в сети.

Указания по проведению профилактических работ

1. Профилактические работы проводятся строго в соответствии с установленным графиком. График проведения профилактических работ на серверах на следующий месяц составляется администратором.

2. Администратор ЛС обязан включить в график все периодические профилактические работы, независимо от необходимости их проведения.

3. Профилактика целостности операционной системы, сетевого взаимодействия, проверка работы сервисов и служб проводятся в рабочем порядке, поскольку в подавляющем большинстве случаев не требуют перезагрузки серверов.

4. Профилактика баз данных, проверки на наличие вирусов, обновлений системы и серверных приложений, проверка отказоустойчивости системы, профилактика работоспособности дисковой и файловой подсистем, остановки сервера для чистки и вентиляции проводятся в рабочее время с учетом времени минимальной загрузки серверов.

5.  Профилактические работы на серверах, требующие длительного (более 1 часа) отключения и способные повлиять на рабочие процессы в организации, проводятся в выходные дни.

6. Процедуры, необходимые для проведения профилактических работ, включают в себя:

* анализ журналов событий серверов: проводится ежедневно для выявления ошибок, связанных с функционированием базовых компонентов серверного аппаратно-программного комплекса;
* анализ отчетов системы безопасности: проводится ежедневно с целью выявления соответствия политик доступа к ресурсам локальной сети путем просмотра журналов системы безопасности серверов и программ, отвечающих за безопасность информационных потоков с оценкой соответствия доступа пользователей к ресурсам организации;
* проверка работоспособности почтовых служб и служб Интернет: проводится ежедневно с целью поддержания возможности получения пользователями оперативной информации из внешних источников;
* анализ Интернет-трафика: проводится ежедневно с целью предотвращения нецелевого использования Интернет-ресурсов;
* анализ возможностей доступа пользователей к сетевым ресурсам: проводится ежедневно с целью определения возможности совместного доступа к различным сетевым ресурсам и выполнения пользователями их должностных обязанностей;
* просмотр отчетов служебных программ: проводится с целью проверки работоспособности пользовательских приложений, установленных на сервере;
* проверка сетевого взаимодействия: производится еженедельно в начале рабочей недели и включает в себя краткий анализ журналов событий и графиков загрузки сети;
* проверка работы служб: проводится еженедельно на каждом из работающих серверов, находящихся в ЛС;
* проверка наличия обновлений операционной системы и серверных приложений: проводится еженедельно с целью поддержания работоспособности аппаратно-программного комплекса на должном уровне и сохранения безопасности использования внешних источников информации;

Перечень профилактических работ

Профилактические работы включают в себя:

* анализ журналов событий серверов (ежедневно);
* анализ отчетов системы безопасности (ежедневно);
* анализ изменения состава групп безопасности в AD (Active Directory);
* выявление попыток несанкционированного доступа к ресурсам;
* выявление попыток несанкционированного изменения уровня доступа к ресурсам;
* проверку работоспособности почтовых служб и служб Интернет (ежедневно);
* анализ Интернет-трафика (ежедневно);
* анализ возможностей доступа пользователей к сетевым ресурсам (ежедневно);
* просмотр отчетов служебных программ (ежедневно);
* проверку сетевого взаимодействия (1 раз в неделю);
* проверку работы сервисов и служб (1 раз в неделю);
* проверку наличия обновлений операционной системы и серверных приложений (1 раз в неделю);
* профилактику баз данных (1 раз в неделю);
* антивирусную профилактику сервера (1 раз в неделю);
* проверку целостности операционной системы (1 раз в 2 недели);
* принудительную проверку отказоустойчивости системы (1 раз в 2 недели);
* профилактику дисковой и файловой подсистем на сервере (1 раз в 2 недели);
* профилактическую остановку сервера (1 раз в 2 недели);
* составление отчета доступа к Интернет-ресурсам (1 раз в месяц);
* профилактические работы на объектах вычислительной техники (выполняются пользователем, по необходимости при помощи сотрудников ООВТ ЦСИТ).

К профилактическим работам на объектах вычислительной техники относятся:

* проверка обновления клиентских приложений (по необходимости);
* проверка времени последнего обновления антивирусных баз (1 раз в неделю);
* выявление попыток несанкционированной установки приложений пользователем (ежедневно);
* удаление временных и устаревших копий файлов (по необходимости);
* выполнение прочих работ, непосредственно связанных с работоспособностью объектов вычислительной техники (по необходимости).

# Способы резервного копирования данных. Принцип работы хранилищ данных. Средства резервного копирования и восстановления данных. Проведение регулярного резервирования

**Резервное копирование денных**

Хранение информации — это процесс поддержания исходной информации в виде, обеспечивающем выдачу данных но запросам конечных пользователей в установленные сроки. Процесс храпе­ния связан с необходимостью накопления и долговременного хра­нения данных, необходимостью комплектации первичных данных до их обработки, обеспечением их актуальности, целостности безопасности, доступности. Хранение информации осуществляется на машинных носителях в виде информационным массивов, где данные располагаются по установленному в процессе проектирования группировочному признаку. Хранение информации в на­стоящее время реализуется при использовании концепций базы данных и хранилища данных (ХД).

База данных представляет собой совокупность взаимосвязанных данных, используемых несколькими пользователями и храня­щихся с регулируемой избыточностью. Хранимые данные не за­висят от программ пользователей, а для их модификации приме­няется общий управляющий метод реализуемый системой управления базой данных на основании запросов пользователей. База данных вместе с СУБД образуют так называемый банк дан­ных. В содержательном плане банк данных — это система, пред­ставляющая определенные услуги по хранению и поиску данных определенной группе пользователей по определенной тематике.

Хранилище данных — это база, хранящая данные, агрегирован­ные по многим измерениям.

Наряду с термином «хранилище данных» используют также равноценные термины: Dala Warehouse, «склад данных». «инфор­мационное хранилище». Основное отличие ХД от БД — агрегиро­вание данных. Данные из ХД никогда не удаляются, а его пополнение происходит путем формирования новых агрегатов данных зависящих от старых. Доступ к ХД осуществляется на основе многомерного куба или гиперкуба, координаты осей которого являются по сути индексами, указывающими точное положение информации в хранилище.

Любая современная СУБД предоставляет пользователю средства резервного копирования, позволяющие восстанавливать базу данных в случае ее разрушения. Резервное копирование — периодически выполняемая процедура получения копии базы данных и ее файла журнала (а также, возможно, программ) на носителе, хранящемся отдельно от системы. Обычно резервные копии базы данных (и ее файла журнала) создаются с некоторой установленной периодичностью в местах, обеспеченных необходимой защитой. В случае аварийного отказа резервная копия и зафиксированная в файле журнала оперативная информация используются для восстановления базы данных до последнего согласованного состояния [44, 8].

Процедура создания и обслуживания файла журнала, содержащего сведения обо всех изменениях, внесенных в базу данных с момента создания последней резервной копий, и предназначенного для обеспечения эффективного восстановления системы в случае ее отказа, называется процедурой ведения системного журнала БД. Средства оперативного обслуживания системного журнала также предоставляет СУБД пользователю. Если в отказавшей системе функция ведения системного журнала не использовалась, то базу данных можно будет восстановить только до того состояния, которое было зафиксировано в последней созданной резервной копии. Все изменения, внесенные в базу данных после создания последней резервной копии, будут потеряны.

Основной проблемой восстановления работоспособности ЛВС после отказа является восстановление хранимых данных. Отказ многих аппаратных компонентов ЛВС (процессора, памяти, контроллеров, внешних устройств, телекоммуникационного оборудования и самой сетей передачи данных), как правило, нарушает целостность хранимых данных. Поэтому подготовка к восстановлению данных является важнейшим элементом планов работ по восстановлению работоспособности ИС. Такая подготовка включает в себя:

• изготовление резервных копий данных (резервное копирование);

• тренировки персонала по восстановлению данных;

• хранение резервных копий.

Резервное копирование следует осуществлять настолько часто, насколько допустима потеря части данных после их восстановления из последней резервной копии; например, если резервное копирование осуществляется один раз в сутки, то средний потерянный объем изменений данных — это изменения, сделанные за 12 ч работы ИС, а в худшем варианте — за все 24 ч. Резервное копирование может быть длительным процессом. Во время изготовления резервной копии работать с БД нельзя. Поэтому для резервного копирования следует принимать все возможные меры, снижающие время изготовления копии:

а) уменьшать объем копируемых данных;

б) повышать производительность оборудования, на котором изготавливаются копии;

в) использовать ПО, которое позволяет изменять данные, не затрагивающие целостность резервной копии (например, уже полностью скопированные).

Тренировки персонала должны быть регулярными, обеспечивающими автоматизацию навыков администраторов по восстановлению данных. Дело в том, что восстановление данных может занимать часы и требовать от администратора действий, выполняемых в строго определенной последовательности. Нарушение такой последовательности может приводить к повторению процедуры восстановления с ее начала, снова вызывая простой ИС.

Хранение резервных копий зависит от вида носителей. Например, магнитные носители следует хранить в размагниченном металлическом сейфе (шкафу), а оптические диски можно хранить в любом непрозрачном контейнере. При использовании трех копий еще одна копия хранится в том же здании, где будет происходить восстановление данных, но в помещении, отдаленном от того помещения, где эксплуатируется ИС. На любых носителях обычно изготавливаются не менее двух резервных копий (как правило, три), одна из которых хранится в помещении, в котором предстоит восстановление данных, а другая — в другом здании, желательно не ближе 10... 15 км (на случай стихийного бедствия или теракта).

До недавнего времени хранение данных было лишь малой частью компьютерной инфраструктуры на предприятиях. По мере роста объемов и ценности увеличивалась и значимость данных, а их хранение стало одной из важнейших составляющих современного центра обработки данных. Если в самом начале XXI в. объемы средств, вкладываемых в системы хранения данных, примерно соответствовали объемам средств, тратившихся на сами серверы, то в настоящее время объем средств, вкладываемых в системы хранения данных, существенно превысил аналогичный объем для серверов (примерно 15% против 85%). Правда, теперь к стоимости самого оборудования прибавляется стоимость средств для управления данными.

Можно сказать, что хранение данных стало ключевым ресурсом современных информационных технологий, и важность этого ресурса постоянно растет.

Фундаментальные правила резервного копирования данных.

Резервное копирование, в отличие от других видов копирования данных (зеркалирование, снэпшоты и репликация данных), является стратегическим компонентом защиты данных [8]. Поэтому независимо от используемой технологии резервного копирования необходимо придерживаться определенных правил, выполнение которых облегчает проведение резервного копирования, причем, как показывает практика, соблюдать их требуется неукоснительно и комплексно. Это позволит выполнять резервное копирование без каких-либо затруднений, укладываясь в выделенное временное окно. Итак, при организации и (или) оптимизации существующей системы резервного копирования необходимо соблюдать следующие правила:

1. Предварительное планирование. Все компоненты инфраструктуры резервного копирования должны учитываться в процессе планирования, а все приложения, серверы и тенденции увеличения емкости первичных хранилищ данных не должны оставаться без внимания. Правильное планирование позволяет составить более полное представление о потребностях и особенностях работы приложений с точки зрения защиты данных. Приложения баз данных, где присутствуют разделенные «зеркала» (копии данных на других компьютерах) и приложения, работающие в файловой среде, в которой нет дополнительной защиты данных, требуют разных стратегий и подходов к резервному копированию. Аналогично большое корпоративное приложение, развернутое на нескольких серверах и предполагающее сложную взаимозависимость данных для обеспечения последующего восстановления, будет требовать соответствующей синхронизации резервного копирования [62].

2. Установление жизненного цикла и календаря операций. Эффективная работа системы резервного копирования требует ежедневного выполнения определенных заданий. Однако есть не менее важные задания, которые выполняются еженедельно, ежемесячно, ежеквартально и ежегодно. Задания с коротким циклом большей степени являются тактическими, а задания с большим циклом — стратегическими. В среде эффективного резервного копирования все задания должны быть задокументированы и выполняться согласно расписанию, причем ежедневно должны решаться следующие задачи:

• мониторинг заданий и отчеты о сбоях и успешном выполнении;

• анализ и разрешение проблем;

• манипуляции с лентами и управление библиотекой;

• расписание выполнения заданий.

Еженедельные и ежемесячные задания включают в себя:

• анализ производительности;

• тенденции изменения объемов и планирование этих изменений;

• рассмотрение и анализ методики резервного копирования;

• проверку возможности восстановления;

• планирование развития архитектуры.

Документируя эти задания, необходимо убедиться, что они выполняются в полном соответствии с расписанием.

3. Ежедневный обзор логов процесса резервного копирования. Это необходимая ежедневная задача. Затраченное на это время, в конечном счете, приведет к надежно работающей системе резервного копирования. Проблемы при резервном копировании, как правило, возникают лавинообразно. Один-единственный сбой может повлечь за собой целую последовательность, на первый взгляд, даже не связанных между собой событий. Например, задание резервного копирования может либо «зависнуть», либо не запуститься из-за того, что нужный привод магнитных лент не был освобожден предыдущим заданием. Это предшествующее задание сохраняло сервер приложений, на котором одновременно шел незапланированный ресурсоемкий процесс. Выполнение данного процесса не позволило закончить резервное копирование в установленный расписанием срок. Ответственный системный администратор своевременно не информировал администратора резервного копирования, чтобы он мог внести соответствующие изменения в расписание процессов. Для того чтобы определить, является ли некоторое состояние причиной или следствием чего-то другого, может потребоваться немало опыта и усилий, а сам процесс будет напоминать детективное расследование. Естественно, для успешного решения возникающих проблем необходима согласованная работа системных, сетевых администраторов и администраторов баз данных.

4. Защита базы данных резервного копирования или каталога. Все приложения резервного копирования ведут свою базу данных или каталог, необходимые для последующего восстановления сохраненных данных. Ясно, что потеря каталога влечет за собой потерю сохраненных данных. Хотя некоторые приложения резервного копирования имеют механизмы корректного чтения лент и индексов, для восстановления этого может оказаться недостаточно. Более того, каталог должен рассматриваться как критически важное приложение баз данных. Желательно иметь его зеркальную копию или, по крайней мере, хранить в RAID-системе (Redundant Array of Intelligent/Independent Drives). RAID-системы автоматически дублируют все хранящиеся данные и ведут мониторинг локальных сбоев, что делает систему более устойчивой. Кроме того, желательно убедиться в том, что каталог сохраняется согласно расписанию и без ошибок.

5. Ежедневное определение временного окна резервного копирования. Ошибки, связанные с временным окном резервного копирования, не оставляют соответствующих сообщений в отчетах, так как на самом деле это нормальный и успешно завершившийся процесс резервного копирования. Поэтому часто проблема остается незамеченной. Если задания начинают приближаться или выходить за пределы отведенного временного окна, это является признаком приближения к предельной емкости системы или наличия «узких мест» в производительности. Своевременное обнаружение таких признаков может избавить от последующих более крупных сбоев системы.

6. Локализация и сохранение «внешних» систем и томов. ПО резервного копирования предоставляет отчеты о ежедневных сессиях резервного копирования, куда включается информация только об известных ему серверах. Рассматривать только их и полагаться только на них рискованно. «Внешние» (например, купленные) системы, которые участвуют в работе, но не включены в схему резервного копирования, оказываются вне поля зрения ИТ-подразделения и некоторое время могут работать с собственным резервным копированием. Но рано или поздно возможен сбой, приводящий к потере данных. Тогда специалисты ИТ-подразделения получают запрос восстановления данных на системе, о которой им ничего не известно. Как правило, такие системы попадают в поле зрения ИТ-служб слишком поздно. Решение этой проблемы может оказаться трудоемким и займет много времени. Потребуются регулярный просмотр и мапирование (определение соответствия) новых сетевых адресов, фильтрация не связанных с задачей адресов, идентификация местоположения и владельцев таких узлов и внесение соответствующих изменений в политику резервного копирования.

7. Максимально возможная централизация и автоматизация резервного копирования. Ключом к успешной защите данных является их целостность. Проблема «внешних» систем является хорошим примером нарушения целостности данных, возникающим из-за нецентрализованного управления резервным копированием. Нередко операции резервного копирования для Windows- и Unix-серверов происходят независимо. Помимо того что это неэффективно, подобная организация предполагает разные наборы процедур и разные стратегии резервного копирования для разных платформ. По географическим соображениям функции резервного копирования могут быть действительно распределены по удаленным офисам, но, принимая во внимание качество современных коммуникаций, выгода от такой децентрализации небольшая.

По мере увеличения сложности инфраструктуры резервного копирования для выполнения повторяющихся операций желательно применять средства автоматизации. Рассмотрим, например, трудоемкую задачу ежедневного изучения журналов (логов) выполнения операций. Автоматизация позволит генерировать сигналы тревоги при появлении в них заранее определенных ошибок и избавит персонал от утомительной рутинной работы по их поиску в соответствующих журналах (логах).

8. Создание и поддержка отчетов об открытых проблемах. Оценка качества резервного копирования поможет улучшить его инфраструктуру. Например, наличие журнала открытых (нерешенных на данный момент) проблем может способствовать оптимизации процесса резервного копирования. В любом случае отчеты, детализирующие открытые проблемы, будут указывать частоту и количество появления новых и закрытия старых проблем, что, в свою очередь, многое говорит об общем состоянии системы резервного копирования. Простой отчет о тенденциях с соответствующими данными может открыть фундаментальные проблемы и помочь выработать их решение.

9. Резервное копирование должно быть включено в процесс контроля изменений системы. Среда резервного копирования по своей природе достаточно динамична. Изменение системы резервного копирования тоже происходит динамично. Резервное копирование должно входить в процесс стратегического планирования, а на операционном уровне — стать частью процесса контроля изменений системы. Происходит много непредусмотренных перебоев резервного копирования по вине коммутационной топологии сетей хранения данных, или в связи с изменениями в зонировании, или в связи с появлением «узких мест», возникающих в результате изменения конфигурации системы резервирования данных. Они могут и должны быть устранены. Если в инфраструктуре резервного копирования необходимо наличие ежемесячного перерыва для проведения апгрейдов или регламентных тестов, то такое временное окно не должно пересекаться с аналогичным перерывом в работе остальных систем. При внесении изменений в систему существует повышенная потребность в восстановлении данных, когда файлы сохраняются, а новые устанавливаются. Если инфраструктура резервного копирования остановлена для планового обслуживания, то данные не смогут быть восстановлены в нужное время. Инфраструктура резервного копирования — это производственная система, как одно из важнейших используемых приложений требующая поддержки и внимания ничуть не меньше остальной производственной среды.

Категории резервируемых данных. Обычно резервное копирование выполняется для того, чтобы можно было восстанавливать либо отдельные файлы, либо целиком файловые системы. Первый вариант позволяет удовлетворить типичный запрос на восстановление файла, когда пользователь случайно удаляет файл и просит восстановить его из последней копии. Второй вариант спасает, когда «рушится» вся система. Данные, которые обрабатываются и хранятся в типичной компьютерной системе, подразделяются на две категории: к первой категории относятся данные, которые практически никогда не изменяются; ко второй категории относятся постоянно изменяемые данные. Поскольку резервная копия — это снимок, копируемый в определенный момент времени, то чем чаще данные меняются, тем чаще следует выполнять их резервное копирование.

Например, данные, представляющие ОС, обычно меняются только во время обновлений, установки исправлений ошибок и каких-либо изменений в соответствии с задачами пользователя. Сам процесс установки ОС довольно прост, а применение исправлений и процедуры настройки хорошо документированы и легко воспроизводимы. Поэтому вместо резервирования ОС можно в \ случае аварии просто переустановить ее, используя дистрибутивную копию. Однако если есть хоть малейшее сомнение в том, что при новой установке удастся полностью воссоздать окружение изначальной системы, лучше выполнить резервное копирование ОС, хотя делать его можно гораздо реже, чем резервную копию полезных данных.

Резервные копии ОС также могут пригодиться, когда потребуется восстановить всего несколько системных файлов (например, в случае ошибочного удаления). Похожая ситуация складывается с данными, представляющими прикладное ПО, которые меняются либо при установке, либо при обновлении, либо при удалении программ.

Другой вид данных — данные приложений. Они меняются так же часто, как часто запускаются связанные с ними приложения. В зависимости от определенного приложения это может означать, что изменения происходят ежесекундно или один раз в квартал — по-видимому, так же часто нужно производить их резервное копирование. Наконец, данные пользователей постоянно меняются в соответствии с характером работы организации.

Определив эти и другие категории данных, администратор отдела резервирования данных должен хорошо представить себе, какие резервные копии необходимо делать, чтобы защитить данные пользователей. При этом нужно иметь в виду, что большинство программ резервного копирования работает с данными на уровне каталога или файловой системы. Другими словами, структура каталогов системы предприятия влияет на то, как будет выполняться резервное копирование. Поэтому следует выбирать оптимальную структуру каталогов в новой системе и группировать файлы и каталоги в соответствии с их предназначением.

Типы резервного копирования. Чтобы правильно настроить резервное копирование, необходимо знать, что существуют три типа резервного копирования: полные, добавочные и разностные копии.

Полная копия — это копия, при которой на резервном носителе сохраняется каждый файл, подлежащий резервированию. Если копируемые данные никогда не меняются, то все создаваемые полные копии будут одинаковыми. Это объясняется тем фактом, что при создании полной копии не проверяется, был ли файл изменен со времени последнего копирования, и, таким образом, на носитель записываются все файлы независимо от того, были они изменены или нет. Именно по этой причине полные копии не делаются постоянно — все файлы уже записаны на резервный носитель. Ежедневное копирование 100 Гбайт данных, когда возможно, изменяются только 10 Мбайт, противоречит здравому смыслу, поэтому в данном случае будет применен механизм добавочных копий.

При создании добавочных копий файла сначала проверяется время изменения файла и сравнивается со временем последнего копирования. Если время изменения более раннее, значит, файл не был изменен после последнего копирования и в этот раз его можно пропустить. С другой стороны, если дата изменения файла более поздняя, чем дата последнего копирования, значит, файл был изменен и его следует включить в резервную копию.

Добавочные копии используются в сочетании с регулярными полными копиями (например, полные копии делаются еженедельно, а добавочные — ежедневно). Основное преимущество добавочных копий заключается в том, что они выполняются гораздо быстрее, чем полные; основной недостаток — в том, что для восстановления нужного файла может потребоваться просматривать несколько добавочных копий, пока он не будет найден. При восстановлении всей файловой системы необходимо восстановить последнюю полную копию и все последующие добавочные копии. Именно с целью исключить необходимость восстановления всех копий по очереди был разработан разностный метод резервного копирования данных.

Разностные копии похожи на добавочные тем, что они включают в себя только измененные файлы. Разностные копии являются накопительными: файл, измененный однажды, будет включаться во все последующие разностные копии (имеется в виду до следующей полной копии). Это значит, что каждая разностная копия содержит все файлы, измененные со времени последней полной копии, что позволяет выполнить полное восстановление, восстановив только последнюю полную и последнюю разностную копии.

Стратегия резервного копирования с разностными копиями обычно похожа на стратегию с добавочными копиями: за одним периодическим полным циклом копирования следуют несколько более частых разностных циклов. Эффект такого использования разностных копий заключается в том, что со временем разностные копии немного вырастут (если в интервале времени между полными копиями меняются разные файлы). Таким образом, разностные копии находятся где-то между добавочными и полными копиями с точки зрения использования резервных носителей и скорости копирования, а также быстроты восстановления файла или всей файловой системы (так как приходится просматривать (восстанавливать) меньше копий).

Резервный носитель. В настоящее время на практике в качестве резервных носителей используются магнитная лента и магнитный диск. Несомненными преимуществами магнитных лент являются их невысокая стоимость и достаточно большой объем. Однако последовательный доступ к ленточному накопителю часто приводит к недопустимым временным затратам, идущим на поиск требуемого файла из резервного архива. Что касается накопителей на магнитных дисках, то в прошлом они никогда не использовались в качестве резервного носителя. Однако в настоящее время цена хранения данных на дисках упала до такой отметки, когда хранение резервных копий на дисках имеет большое практическое значение. Главной причиной для использования дисков в качестве резервных носителей является то, что они — самые быстрые из существующих носителей данных.

Сама по себе сеть не может являться резервным носителем, но в сочетании с технологиями хранения она может оказаться очень полезной. Например, если взять высокоскоростное сетевое подключение к удаленному центру данных с дисковыми хранилищами большого объема, то можно получить хороший вариант резервирования данных.

Архитектуры систем хранения данных. Совершенствование сетевых технологий сопровождалось развитием инфраструктуры систем хранения данных. При изменении требований к этим системам улучшались и технологии записи и чтения магнитных лент, для которых резервное копирование, архивирование и иерархическое хранение данных в настоящее время являются основными областями применения. Развитие технологии хранения данных привело к упрощению организации совместного пользования устройствами, увеличению пропускной способности соединений, оптимизации поддержки работоспособности и лучшему масштабированию. В настоящее время известны следующие виды архитектур хранения данных:

* прямое подключение системы хранения данных к серверу — Direct Attached Storage (DAS), показанное на рис. 1.5.4, а;
* подключение автономной системы хранения данных к сети — Network Attached Storage (NAS), показанное на рис. 1.5.5;
* инфраструктура блочного хранения данных, построенная на базе высокоскоростной сети — Storage Area Network (SAN), показанная на рис. 1.5.7, 1.5.8.

Целостность данных в системе прямого подключения к серверу (DAS) обеспечивается известной технологией RAID. Однако такое Решение подойдет для ограниченного числа рабочих станций. Действительно, совместное использование конечных вычислительных ресурсов ограничивает количество одновременно подключенных машин к серверу числом портов в устройстве хранения, причем сервер оказывается перегруженным функциями работы с файлами.

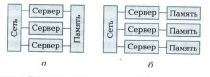


Рис. 1.5.4. Варианты DAS-архитектур с одним (а) и парком [б] серверов



Рис. 1.5.5. Минимальная NAS-архитектура хранения данных

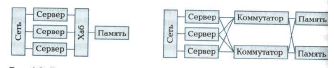


Рис. 1.5.7. Первая минималь- Рис. 1.5.8. Современная минимальная

ная SAN-архитектура SAN-архитектура хранения данных

хранения данных

Кроме того, вынесение хранения данных за пределы компьютеров на сервер не является гарантией их полной защищенности и постоянной доступности по той причине, что в случае «падения» сервера данные становятся недоступными.

Частично проблемы производительности могут быть решены парком серверов (например, разделенные по типу обрабатываемых запросов), каждый из которых нагружает отдельное устройство хранения, как это показано на рис. 4.1.4, б. Однако и у этой схемы начинаются трудности, когда возникает необходимость разделять данные между серверами или объем занимаемой памяти оказывается неравномерным.

Очевидно, что в таких условиях DAS не отвечает требованиям масштабируемости и отказоустойчивости. По этой причине были предложены другие варианты архитектур хранения данных: NAS и SAN [46].

NAS-технология, в отличие от DAS-схемы, созданная в соответствии с концепцией выделенного файл-сервера, снимает нагрузку с универсального сервера, что повышает его производительность при работе с приложениями.

Основное конструктивное отличие NAS-серверов от универсальных серверов заключается в том, что в NAS-серверах есть только системный блок (файл-сервер) и множество «расшаренных» папок для доступа клиентов. NAS — это всего лишь устройство для файлового обмена в IP-сети. Минимальная конфигурация HAS показана на рис. 5.4.5

Характерной особенностью NAS-серверов является также их независимость от ОС и работа под управлением ОС, оптимизированных для работы с файлами в сетевом окружении. Многие современные NAS-серверы работают со встроенными ОС MS Windows, Unix, Linux или собственной ОС от производителя. Взаимодействие NAS-сервера с ЛВС осуществляется через стандартные сетевые протоколы. Технология NAS кроме обеспечения заметного снижения загрузки сервера приложений, простоты установки и эксплуатации обладает следующими преимуществами по сравнению с технологией DAS:

* позволяет гибко распределять ресурсы дисковой системы и устройств резервного копирования, добавляя эти ресурсы туда, где они наиболее необходимы, причем общий объем доступной информации может достигать многих терабайт;
* данные с NAS-сервера можно всегда скопировать на магнитную ленту стриммера, подключенного к NAS;
* реализует совместный доступ к данным с множества платформ, работающих под управлением различных ОС (Windows, Linux, Unix, NetWare и MacOS), причем функционирование NAS-сервера не зависит напрямую от сервера ЛВС и установленной на нем ОС;
* в NAS-серверах применяется специализированная ОС, оптимизированная для обработки и передачи данных, что обеспечивает высокую производительность и надежность их работы;
* возможность доступа к данным NAS-сервера при отключенном (или отказавшем) основном сервере.

Недостатком технологии NAS является так называемый конфликт сетевого трафика. При применении технологии NAS локальная сеть используется как для обмена данными между серверами приложений и устройствами хранения, так и для передачи пользовательского трафика на рабочие станции. Хотя NAS-СеРверы и освобождают системные ресурсы серверов ЛВС от за-Аач управления хранением, но не разгружают полностью сетевой тРафик, так как обмен данными между серверами приложений(или клиентскими ПК) и NAS-серверами осуществляется в той же ЛВС. Это ведет к тому, что высокая нагрузка на сеть с ограниченной пропускной способностью может существенно увеличить время отклика.

SAN является высокоскоростной коммутируемой сетью передачи данных, которая позволяет соединить серверы, рабочие станции, дисковые массивы и ленточные библиотеки в единую систему. Соединение происходит по протоколу Fibre Channel, который обеспечивает оптимизированный и быстрый обмен данными между элементами сети на расстоянии от нескольких метров до сотен километров.

Первая SAN-архитектура была предложена в конце 1980 гг. В качестве коммутирующего устройства она использовала хаб, как показано на рис. 5.4.6. Принцип ее работы был аналогичен методу CSMA/CA: каждый раз, когда какой-либо узел собирался выполнить операцию ввода-вывода, он посылал блокирующий пакет, оповещая всех о начале передачи. Когда пакет возвращался отправителю, узел получал полный доступ для проведения операции. По окончанию операции все узлы оповещались об освобождении канала и процедура повторялась. Однако ближайшее рассмотрение данной архитектуры показывает, что она кроме проблемы с пропускной способностью, аналогичной архитектуре DAS, имеет еще одну: в каждый момент времени только один клиент может выполнять операцию ввода-вывода. Кроме того, использование 8-битной адресации в этой архитектуре накладывало ограничение на количество устройств в сети — 127, что не"позволяло ей конкурировать с архитектурой DAS.

В настоящее время на смену первой архитектуры SAN пришла архитектура FC (Fibre Channal), показанная на рис. 5.4.7, которая вместо хаба использует несколько коммутаторов, поэтому данные предаются здесь не по разделяемому каналу, а по индивидуальным каналам. Как и в сети Ethernet, на базе этих коммутаторов можно построить множество топологий.

Основные преимущества архитектуры FC:

* общий объем памяти может расти не только за счет увеличения емкости существующих блоков памяти (storage), но и за счет добавления новых;
* каждый хост может работать с любым устройством хранения, а не только со своим, как в случае с DAS;
* сервер имеет несколько «путей» получения данных, поэтому при правильно построенной топологии, даже после выхода из строя одного из коммутаторов, система остается работоспособной;
* система позволяет разграничивать доступ серверов к ресурсам;
* в основном решена проблема с пропускной способностью, так как операции резервного копирования не оказывают влияния на всю сеть.

Еще одно преимущество SAN-архитектуры — она позволяет построить множество различных решений в зависимости от задачи. Например, если установить на один из серверов специальную ОС, то можно реализовать gateway-реализацию NAS-архитектуры со всеми ее дополнительными преимуществами, перечисленными ранее. Таким образом, в рамках решения для одного предприятия могут сочетаться и DAS-, и NAS- и SAN-архитектурные решения резервного хранения данных.

Недостатком SAN-архитектуры является ее высокая цена, поэтому она еще мало распространена за пределами ведущих предприятий [47].

**Принципы работы и компоненты хранилищ данных**

Хранилища данных — это процесс сбора, отсеивания и предварительной обработки данных в целях представления результирующей информации пользователям для статистического анализа и аналитических отчетов. Автор концепции ХД, Ральф Кинболл, описывал его как «место, где люди могут получить доступ к своим данным». Он же сформулировал основные требования к хранилищам данных:

* поддержка высокой скорости получения данных из хранилища;
* поддержка внутренней непротиворечивости данных;
* возможность получения и сравнения данных;
* наличие удобных утилит просмотра данных хранилища;
* полнота и достоверность хранимых данных;
* поддержка качественного процесса пополнения данных.

Часто всем перечисленным требованиям удовлетворить не удается, поэтому для реализации ХД используют несколько продуктов: одни продукты — это средства хранения данных, другие — средства их извлечения и просмотра, третьи — средства пополнения ХД. Типичное ХД, как правило, отличается от реляционной БД по трем позициям:

* обычная БД помогает пользователям только изменять данные, тогда как ХД предназначены для принятия решений;
* обычная БД подвержена постоянным изменениям с заданной периодичностью (ежечасно, ежедневно, ежемесячно), причем пополнение данными происходит без изменения прежней информации, находящейся уже в хранилище;
* обычная БД чаще всего является источником данных попадающих в хранилище, кроме того, ХД может пополняться за счет внешних источников.

Принципы построения ХД. Информация, которая загружается в хранилище, должна интегрироваться в целостную структуру, от-: вечающую целям анализа данных. При этом минимизируются несоответствия между данными из различных ОС — в ХД данные именуются и выражаются единым образом. Данные в ХД интегрированы на множестве уровней: на уровне ключа, атрибута, на описательном, структурном уровнях и т. д.

Хранилища можно рассматривать как набор моментальных снимков состояния данных — можно восстановить картинку на любой момент времени. Атрибут времени всегда явно присутствует в структурах данных хранилища.

Попав однажды в ХД, данные уже никогда не изменяются, а только пополняются новыми данными. Новые данные по мере поступления обобщаются с уже накопленной информацией в ХД.

Основные компоненты ХД. Использование технологии ХД предполагает наличие в системе следующих компонентов:

* источники данных;
* реляционное хранилище;
* средства переноса и трансформации данных;
* средства доступа и анализа данных;
* OLAP-хранилища;
* метаданные.

Данные из различных источников собираются, очищаются, интегрируются и помещаются в реляционное хранилище, где они уже доступны для анализа средствами построения отчетов. Затем данные подготавливаются с использованием средств переноса и трансформации данных для OLAP-анализа, который реализуется применением средств доступа и анализа данных. При этом они могут быть загружены в специальную базу данных (OLAP-хранилища) или оставаться в реляционном хранилище.

Важнейшим элементом хранилища являются метаданные, т.е. данные о структуре, размещении, трансформации данных, которые используются любыми процессами хранилища. Метаданные включают в себя каталог хранилища и правила преобразования данных при загрузке их из внешних БД. Метаданные могут быть востребованы для различных целей (например, для извлечения и загрузки данных, обслуживании хранилища и запросов). Метаданные для различных процессов могут иметь различную структуру, т.е. для одного и того же элемента данных могут существовать несколько вариантов метаданных.

Хранилища данных являются структурированными. Они содержат базовые данные, которые образуют единый источник для обработки данных во всех системах поддержки принятия решений. Элементарные данные, присутствующие в хранилище, могут быть представлены в различной форме. ХД очень велики, поскольку содержат интегрированные и детализированные данные.

Эти характеристики являются общими для всех ХД. Несмотря на то что хранилища обладают общими свойствами, разные типы хранилищ имеют свои индивидуальные особенности.

Для работы с ХД используются специальные СУБД, к которым предъявляются следующие требования:

* высокая производительность загрузки данных;
* возможность обработки данных на уровне загрузки;
* наличие средств управления качеством данных;
* высокая производительность запросов;
* широкая масштабируемость по размеру и количеству пользователей;
* возможность организации сети хранилищ данных;
* наличие средств администрации хранилищ данных;
* поддержка интегрированного многомерного анализа;
* расширенный набор функциональных средств запросов.

Хранилище данных — это компьютерная система, главной целью разработки которой является информационное обеспечение компьютерной поддержки принятия решений по всем или основным видам деятельности организации.

OLAP-технология анализа данных

OLAP (OnLine Analytical Processing) — это технология комплексного многомерного анализа данных. В 1993 г. эта технология была описана Эдгером Коддом, который связал ее с концепцией ХД. Назначение систем класса OLAP — предоставить пользователям гибкий, интуитивно понятный и простой доступ к данным в ХД. Наличие такого доступа позволяет отказаться от использования предопределенных отчетов, делает пользователей независящими от администраторов баз данных и программистов. В основе концепции OLAP лежит принцип многомерного представления данных. Данные представляются в виде многомерного куба, причем пользователь может быстро свернуть или развернуть данные по любому измерению этого куба.

Для построения ХД используется СУБД — MS SQL-сервер, которая удовлетворяет всем перечисленным ранее требованиям, начиная от высокой производительности и заканчивая расширенным набором функциональных средств запросов пользователей к ХД.

OLAP — это совокупность концепций, принципов и требований, лежащих в основе программных продуктов, облегчающих пользователям доступ к данным. Кубы OLAP представляют собой по сути метаотчеты, разрезая которые по измерениям, пользователь фактически получает интересующие его обычные двумерные отчеты. Преимущества кубов очевидны — данные необходимо запросить из реляционной СУБД всего один раз — при построении куба. Самих отчетов в ХД по сути дела не существует — они формируются «на лету» и материализуются в виде файла на компьютере вызвавшего этот отчет пользователя, который может просто просмотреть его на своем ПК, после чего удалить и (или) распечатать.

В хранилище данных информация хранится в измерениях и процессах. Измерение — это объект анализа, который может характеризоваться свойствами, присущими только ему и имеет уникальный идентификатор. Процесс представляет собой звезду, в центре которой хранятся факты, а лучи являются измерениями. Рассмотрим сказанное на примере. Пусть в ХД присутствуют данные только по процессу «Сделка», который содержит измерения: «И1 — номер клиента», «И2 — состояние сделки», «ИЗ — причина отказа», «И4 — менеджер, курирующий сделку», «И5 — дата сделки». Дополнительными и з м е р е н и я м и являются: «И6 — источник информации, способствующий сделке», «И7 — номер покупаемого товара», «И8—номер региона» и «И9 — сфера деятельности клиента». Кроме того, в ХД присутствуют следующие факты: «Ф1 — объем сделки» и «Ф2 — сумма сделки».

Если бы в ХД по «Сделке» присутствовали только три измерения, например «номер клиента», «дата сделки» и «состояние сделки, причем каждое измерение содержало бы только по два значения («объем» (О) и «сумма» (С)), то графически OLAP-куб такого хранилища можно было бы представить в виде обычного куба, показанного на рис. 1.5.8. В нашем случае не три измерения, а девять, причем по каждому из них количество «координат» — переменное число. Изобразить такой куб на плоскости можно, показав его проекцию из 9-го измерения, однако наглядность такой проекции будет нулевая. Более нагляден куб в виде графа, показанного на рис. 1.5.8. В данном случае ХД представляется двумя «звездами» с центрами соответственно в вершинах «Объем» и «Сумма» сделки. «Плоский» или двумерный отчет «Дата/Состояние», который построит OLAP-модуль по запросу пользователя, представляет табл. 1.5.4

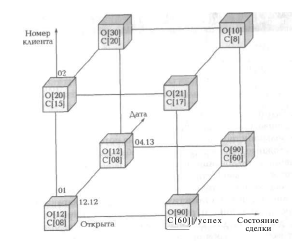


Рис. 1.5.8 Пример OLAP-куба

Перечислим основные требования, предъявляемые к программным продуктам, реализующим OLAP-технологию обработки данных в ХД.

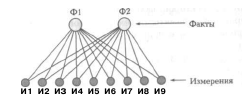


Рис. 1.5.9. Модель OLAP-куба в виде двудольного графа

Таблица 1.5.4

|  |  |  |
| --- | --- | --- |
| Дата | Состояние | |
| Открыта | Успех |
| 02.12 | 25/19 | 2/2 |
| 03.12 | 80/50 | 100/60 |

1. Fast (быстрый). Это свойство означает, что система должна обеспечивать ответ на запрос пользователя в среднем за 5 с; при этом большинство запросов обрабатываются в пределах 1 с, а самые сложные запросы должны обрабатываться в пределах 20 с. Недавние исследования показали, что пользователь начинает сомневаться в успешности запроса, если он занимает более 30 с.

2. Analysis (аналитический). Система должна справляться с любым логическим и статистическим анализом, характерным для бизнес-приложений, и обеспечивает сохранение результатов в виде, доступном для конечного пользователя. Средства анализа могут включать в себя процедуры анализа временных рядов, распределения затрат, конверсии валют, моделирования изменешг организационных структур и некоторые другие.

3. Shared (разделяемый). Система должна предоставлять широ кие возможности разграничения доступа к данным с одновременной работы многих пользователей.

4. Multidimensional (многомерный). Система должна обеспечивать концептуально многомерное представление данных, включая полную поддержку множественных иерархий.

5. Information (информация). Мощность различных программных продуктов характеризуется количеством обрабатываемых входных данных. Разные OLAP-системы имеют разную мощность: передовые OLAP-решения могут оперировать в 1 000 раз большим количеством данных по сравнению с самыми маломощными OLAP-системами. При выборе OLAP-инструмента следует учитывать целый ряд факторов, включая дублирование данных, требуемую оперативную память, объем дискового пространства, эксплуатационные показатели, интеграцию с информационными хранилищами и т. п.

В настоящее время в мире разработано множество программных продуктов, реализующих OLAP-технологии. Чтобы легче было в них ориентироваться, используют классификации OLAP-продук-тов: по способу хранения данных для анализа и по месту нахождения OLAP-машины.

## Аудит сетевой инфраструктуры

**Порядок проведения аудита локальной вычислительной сети**

Локальная сеть – это группа из нескольких компьютеров, соединенных посредством кабелей или радиоканалов, используемых для передачи информации между компьютерами. Для соединения компьютеров в локальную сеть необходимо сетевое оборудование и программное обеспечение.

Локальная сеть предоставляет возможность совместного использования оборудования. Оборудование, программы и данные информации объединяют одним термином: ресурсы. Можно считать, что основное назначение локальной сети – доступ к ресурсам. Часто дешевле создать локальную сеть и установить один принтер на все подразделение, чем приобретать по принтеру для каждого рабочего места. Файловый сервер сети позволяет обеспечить совместный доступ к программам. В локальной сети удобнее реализовывать администрирование ресурсов, контролировать ход работ над проектами в сети проще, чем иметь дело со множеством автономных компьютеров.

Прежде чем проводить работы по развитию локальной сети или проектированию новой сети, следует провести анализ состояния и характеристик существующей локальной сети (аудит сети).

Анализ состояния и характеристик (аудит) локальной сети – это комплекс мероприятий, направленных на выяснение текущего состояния дел в локальной сети образовательного учреждения (количество и размещение компьютеров и сетевого оборудования, выявление характеристик компьютеров и установленного программного обеспечения, определение структуры кабельной системы), поиск и идентификацию «узких мест». По результатам аудита готовится отчет, описывающий текущее положение дел и содержащий рекомендации по дальнейшей модификации или эксплуатации локальной сети.

В каких случаях проводится аудит локальной сети?

Аудит локальной сети целесообразно проводить в следующих случаях:

1) перед модернизацией сети, чтобы можно было спроектировать новую сеть на основе объективных данных;

2) после модернизации сети, чтобы убедиться, что локальная сеть была реализована адекватно требованиям образовательного процесса;

3) для оценки качества сервиса. Например, чтобы убедиться, что провайдер сети Интернет выполняет взятые на себя обязательства по качеству предоставляемого сервиса (пропускная способность канала, время задержки, доступность канала и т.п.);

4) при передаче функций администрирования локальной сети другому лицу или организации.

Порядок проведения аудита локальной сети

Вне зависимости от объекта обследования проведение аудита включает три основных этапа:

1. постановка задачи и уточнение границ работ;
2. сбор данных. Инвентаризация сети;
3. анализ данных и подготовка отчета.
4. Постановка задачи и уточнение границ работ

На данном этапе проводятся организационные мероприятия по подготовке проведения аудита:

1) уточняются цели и задачи аудита;

2) подготавливается и согласовывается техническое задание на проведение аудита.

# Сбор данных. Инвентаризация сети

Инвентаризация сети на этом этапе обычно совмещается с интервьюированием персонала заказчика, предполагается осмотр активного и пассивного оборудования, сбор конфигурационной и операционной информации, измерение различных параметров сети.

Сбор данных может включать следующие типовые работы:

1. интервьюирование пользователей ЛС ОУ (педагогических и административных работников ОУ, использующих в своей работе ЛС);
2. документальное обследование (анализ представленных документов);
3. визуальное обследование инфраструктуры, инвентаризацию сети;
4. инструментальное обследование (приборные измерения):
5. – нагрузочное (стрессовое) тестирование локальной сети;
6. – нагрузочное тестирование каналов связи распределенной сети;
7. – мониторинг «здоровья» сети и сетевых сервисов;
8. – оценка качества канала связи с Интернет;
9. оценку состояния информационной безопасности ЛС;
10. сбор конфигурационной и операционной информации.

Детальный перечень выполняемых работ обычно определяется в техническом задании на аудит.

# Автоматизация инвентаризации сети

Для сокращения затрат на сбор информации при проведении инвентаризации сети удобно использовать специальные программы. Одной из таких доступных и бесплатных программ является программа Hardware Inspector Client / Server.

Программа Hardware Inspector Client / Server предназначена для автоматизированного учета компьютеров, а также заявок от пользователей. Уникальность программы заключается в возможности вести учет не просто текущего состояния параметров компьютера, а всей истории жизни каждого устройства. С помощью программы Hardware Inspector Client / Server можно решать широкий круг задач.

Основные возможности программы Hardware Inspector Client / Server:

Клиент-серверная технология. Позволяет работать с единой базой данных как в локальной сети, так и через Интернет. Отличается высокой устойчивостью к повреждениям данных, высокой скоростью работы и повышенной защищенностью информации.

Детальный учет устройств. На каждое устройство заводится паспорт, в котором отражается информация о его покупке, технических параметрах, истории его перемещений по рабочим местам и обслуживания.

Детальный учет лицензий на программное обеспечение. На каждую лицензию заводится паспорт, в котором отражается информация о ee покупке, параметрах, истории ее перемещений по рабочим местам.

Учет заявок от пользователей. Встроенный учет заявок от пользователей. История сообщений в заявке, прикрепляемые файлы и прочее. Возможность совместной работы с веб-интерфейсом.

Учет расходных материалов. Программа позволяет вести учет поступления на склад и выдачи расходных материалов, а также планирование их потребности на основе статистики расхода за прошлые периоды.

Наглядная иерархия подразделений и рабочих мест. «Дерево» рабочих мест организации может отображаться в двух разрезах: организационное представление (оргструктура) и территориальное (карта).

Визуализация компьютеров на поэтажных планах. Расположение рабочих мест на планах помещений предприятия помогает визуальному восприятию размещения компьютеров в сети. Наглядно показаны сетевые соединения, благодаря которым возможны переходы по этажам и кабинетам.

Проведение работ по обслуживанию устройств и рабочих мест. В программе ведется учет любых работ по обслуживанию устройств и рабочих мест: ремонт, профилактика и прочее. Фиксируются все обстоятельства работ, на основе чего могут строиться отчеты по выполненным работам IT-отделом и его сотрудниками.

Программы, автоматизирующие инвентаризацию сети, приведены на.

Инвентаризация компьютеров. Механизм инвентаризации с использованием штрих-кодов показывает реальное наличие устройств на рабочих местах. Автоматизация и контроль процедуры проведения плановой инвентаризации оборудования.

Аудит рабочих мест. Этот инструмент проведения инвентаризации выявляет отклонения информации в базе данных от реального состояния конфигурации. Многоуровневая проверка уникальности каждого устройства позволяет сразу определить его статус, выполнить импорт или перемещение.

Большой набор отчетов: "Паспорт устройства", "Паспорт рабочего места", "Паспорт лицензии", "Список инвентарных номеров", "Список IP-адресов", "Полный перечень оборудования", "Выполненные работы за пе-риод времени" и прочее. Отчеты могут экспортироваться в PDF, MS Word, MS Excel, OpenOffice и другие форматы. При этом пользователь может самостоятельно настраивать шаблоны во встроенном визуальном дизайнере, а также создавать свои собственные отчеты.

Незарегистрированная копия программы HardwareInspectorClient/Server не ограничена по количеству рабочих мест и не имеет срока жизни БД. В качестве ограничения в некоторых формах и отчетах в случайном порядке вместо данных отображается текст [DEMO VERSION]. Кроме того, через 2 месяца использования к серверу одновременно сможет подключиться только один оператор.

# Анализ данных и подготовка отчета

При анализе полученных при инвентаризации сети данных проводится проверка собранных данных на полноту и корректность, формирование выводов и рекомендаций, оформление результатов. В ходе анализа может быть принято решение о сборе дополнительных данных. Этап анализа данных и оформления результатов может включать следующие типовые работы:

1. Проверка и анализ собранных данных.

2. Анализ структуры сети.

3. Анализ конфигурационных файлов.

4. Подготовка эксплуатационной документации.

5. Подготовка отчета об аудите.

Для сбора данных о компьютерах, их характеристиках и установленном программном обеспечении целесообразно использовать специальные программы. В Интернете можно найти бесплатные и условно-бесплатные программы, позволяющие автоматизировать процесс сбора данных инвентаризации и составления отчетов. Некоторые полезные программы для инвентаризации сети приведены на компакт-диске.

Результатом аудита является создание пакета документов, содержащего детализированные данные о локальной сети образовательного учреждения, а также рекомендации по улучшению качества работы и повышению эффективности функционирования сети.

Основным отчетным документом является отчет об аудите. Он включает описание текущего состояния сети, выводы о соответствии локальной сети образовательного учреждения решаемым образовательным задачам, рекомендации по модернизации и развитию сети.

# Эксплуатационная документация по локальной сети

Эксплуатационная документация по локальной сети образовательного учреждения может быть представлена совокупностью следующих документов.

1. Документы, описывающие структуру локальной сети (ЛС):
2. Поэтажный план здания с указанием:

– компьютерных классов;

– кабинетов с компьютерной аппаратурой (административных, учебных, лаборантских и др.);

– помещения серверной;

– элементов компьютерных сетей (провода и др.);

– сетей 220 В (щиты, проводка, розетки, линии заземления).

1. Для каждого компьютерного класса, каждого кабинета с аппаратурой, серверной – отдельные схемы с указанием размещения в них:

– аппаратуры (компьютеры, ноутбуки, тележки мобильного класса, сетевое оборудование);

– линий локальных сетей (ЛС);

– сетей 220 В (проводка, розетки, линии заземления).

1. Описание среды передачи данных:

– кабельной системы (схема прокладки кабеля по зданию);

– схемы прокладки кабеля оптоволоконной сети и её оборудования (при наличии в ОУ);

– системы радиосвязи – WiFi (схема зон охвата помещений здания) (при наличии в ОУ).

1. Описания подключения компьютеров к сетевому оборудованию и связь сетевого оборудования между собой (подключение с точностью до порта сетевого оборудования).
2. Описание адресного пространства ЛС: какие IP-адреса какими компьютерами используются при фиксированной адресации или какой диапазон IP-адресов выделен для DHCP для организации ЛС (адреса ПК в компьютерном классе, ПК учителей, администрации, бухгалтерии), для выхода в Интернет.
3. Документы учета технических средств информатизации ЛС:

– компьютеров (серверов, ПК, ноутбуков);

– сетевого оборудования (концентраторов, коммутаторов и маршрутизаторов);

– проекторов;

– интерактивных досок.

1. Документы учета программного обеспечения, установленного на компьютерах ЛС:

– операционных систем;

– антивирусных ПО;

– офисных программ;

– программ для работы с графической информацией;

– программно-педагогических средств, установленных на компьютерах пользователей ЛС и серверах;

– другого ПО.

1. Документы, подтверждающие лицензионную чистоту программного обеспечения:
2. Лицензии;
3. Документация по ПСПО;
4. Голограммы.
5. Документы по организации доступа к сети Интернет:
6. Приказ по ОУ на организацию доступа к Интернету с указанием ответственного лица.
7. Схема подключения ЛС к Интернету с указанием портов сетевого оборудования, IP-адресов, шлюза (при его использовании).
8. Документы по организации контентной фильтрации.
9. Документы по организации учета интернет-трафика.
10. Документы по организации доступа учителей и учеников к Интернету вне занятий.
11. Должностные инструкции для администратора и пользователей сети.
12. Документы по обеспечению безопасной работы в локальной сети:
13. Документы по организации антивирусной защиты.
14. План резервирования и восстановления информации.
15. Документы по организации защиты персональных данных в автоматизированной информационной системе.
16. Документация по технике безопасности.

# Анализ состава и лицензионной чистоты программного обеспечения

В первую очередь следует оценить лицензионную «чистоту» ПО Microsoft.

Управление лицензиями Microsoft в образовательных организациях

Зачем нужно управлять лицензиями Microsoft в образовательной организации? Чтобы ответить на этот вопрос, нужно прежде всего понять, что же такое лицензии на программное обеспечение и зачем они нужны.

Для работы с любым программным обеспечением необходимо получить право на его использование. Такое право обычно предоставляет лицензионное соглашение. Нужно ясно понимать, что именно соглашение дает право устанавливать программный продукт и работать с ним. Само по себе наличие оригинального «лицензионного» дистрибутива при отсутствии соглашения не дает права на использование данного продукта.

Существует несколько вариантов приобретения права на использование программного обеспечения Microsoft.

* 1. Коробочные (FPP) продукты (лицензии)

Данный тип лицензий рассчитан на индивидуального пользователя и представляет собой красочную упаковку, содержащую лицензионный сертификат, документацию и носитель с дистрибутивом. Этот продукт предназначен для розничной продажи и не подразумевает какие-либо дополнительные специальные условия при приобретении образовательной организацией. К тому же данный тип лицензии несет ряд ограничений по использованию продукта, устраивающих индивидуального пользователя, но не предоставляющих дополнительных возможностей, необходимых организации.

Вывод: Такой тип лицензии не лучшим образом может удовлетворить требования образовательной организации и к тому же оказывается дорогим при неоднократных закупках лицензий.

* 1. Лицензии на предустановленное программное обеспечение (OEM)

Программное обеспечение Microsoft может поставляться вместе с компьютером в предустановленном виде. В данном случае о наличии лицензии свидетельствует сертификат подлинности, наклеенный на корпус компьютера. Такие версии продуктов, предназначенные для поставки вместе с аппаратным обеспечением, называются OEM-версиями продуктов.

Основной отличительной особенностью OEM-версий является то, что они «привязаны» к компьютеру, на который были первоначально установлены, и не могут быть перенесены на компьютер, служащий заменой старого, или на другой ПК. Так же как и коробочные лицензии, данный вариант рассчитан на индивидуального пользователя, и права использования продукта в определенной степени ограничены, что не всегда подходит для организации.

Вывод: Данный тип лицензии является оптимальным вариантом приобретения базовой лицензии на операционную систему Windows в составе новых ПК. Весь необходимый функционал для операционной системы, а также любые другие продукты Microsoft (MicrosoftOffice, серверные продукты и т.д.) будет дешевле и удобнее получить в рамках Академических программ лицензирования.

* 1. Академические программы лицензирования

Купив одну коробку с программным продуктом, пользователь имеет право установить программу только на один компьютер. Однако в органи-зациях, как правило, один и тот же продукт используется на нескольких

компьютерах. В этом случае наиболее выгодный способ приобретения ли-цензий – Академические программы лицензирования Microsoft.

Покупая продукты по программам академического лицензирования, плата осуществляется только за лицензионные права. Носители для установки продукта либо предоставляются бесплатно, либо могут быть заказаны отдельно. Один носитель может быть использован в качестве эталона для установки, что позволяет не только сократить расходы на приобретение, но и устранить сложности, связанные с развертыванием продукта на нескольких ПК в организации. Помимо всего прочего, лицензии, доступные в рамках таких программ, дают возможность использовать не только текущие, но и предыдущие версии программного обеспечения в количестве, соответствующем количеству приобретенных в рамках соглашения лицензий. Так называемое право «Downgrade». Это право дает, например, возможность перейти от операционной системы WindowsVista к операционной системе Windows XP или от пакета программ Office 2007 к пакету Office 2003. Право использования программных продуктов в данном случае подтверждается бумажным свидетельством (сертификатом) или подписанными документами соглашения, оформленного на Ваше образовательное учреждение.

Вывод: Академические программы являются оптимальным решением для образовательных организаций в случаях, когда планируется приобретение лицензий WindowsUpgrade (расширение прав использования базовых лицензий на операционную систему, а также в случаях приобретения всех других продуктов Microsoft (MicrosoftOffice, серверные продукты и т.д.) при первоначальной закупке 5 и более лицензий. Кроме того, данные программы подразумевают специальный, существенно сниженный уровень цен для образовательных и академических организаций (таблица 1.6.1).

Таблица 1.6.1 – Процесс управления лицензиями

|  |  |
| --- | --- |
| Для этого нужно начать работы по организации управления, для начала текущими версиями ПО, имеющимися в образовательном учреждении. Такие работы можно организовать самостоятельно или прибегнуть к помощи партнерской организации, специализирующейся на данных видах работ. | В случае если в ОУ решили наладить процесс управления лицензиями самостоятельно, можно рекомендовать организовать его, распределив все мероприятия на несколько шагов: |
| 1 этап Сбор необходимой начальной информации. | |
| 2 этап Проведение инвентаризации установленного программного обеспечения. | |
| 3 этап Сопоставление лицензий и программного обеспечения. | |
| 4 этап Разработка стратегического подхода и практических процедур для использования программного обеспечения. | |
| 5 этап Разработка плана управления лицензиями. | |

Этап 1: Сбор необходимой начальной информации

Этот этап носит подготовительный характер, в процессе его осуществления необходимо собрать информацию, требуемую для внедрения управления лицензиями в организации.

Информация включает в себя ответы на следующие вопросы:

1. Какое количество персональных компьютеров используется в организации, объединены ли они в сеть?
2. Какое количество серверов?
3. Какое на них установлено программное обеспечение?
4. Кто отвечает за закупку и эксплуатацию программного обеспечения?

Реализация всех этапов технологии управления лицензиями потребует определенного времени и усилий не только со стороны персонала отдела информационных технологий, руководящего состава, но и рядовых работников. Поэтому настоятельно рекомендуется составить и разослать внутри организации разъяснительную записку относительно целей проводимой работы. Понимание необходимости данной работы всеми сотрудниками организации способно значительно сократить сроки внедрения технологии управления лицензиями в организации.

Этап 2: Проведение инвентаризации установленного программного обеспечения

Проведение инвентаризации программного обеспечения является вторым этапом в процессе управления лицензиями. Существуют два способа инвентаризации программного обеспечения:

* ручная инвентаризация;
* автоматическая инвентаризация;

Ручная инвентаризация. Пользователь может провести инвентаризацию вручную, просмотрев жесткие диски всех компьютеров и зафиксировав всю информацию в виде отчета. Одним из простых способов является использование опции AddorRemovePrograms.

Автоматическая инвентаризация. Для автоматической инвентаризации ПО на компьютерах и серверах организации можно использовать специальные программы. Каталог продуктов для инвентаризации ПО и управления лицензиями содержит полный перечень всех типов программ. В дополнение для выявления всех основных установленных продуктов Microsoft можно использовать программу Microsoft Software Inventory Analyzer (MSIA). Эти автоматизированные средства существенно упрощают процесс инвентаризации. С помощью MSIA или программы из каталога продуктов для инвентаризации ПО и управления лицензиями можно проводить инвентаризацию ПО как для автономно работающих компьютеров, так и для подключенных к локальной сети. При анализе автономно работающих компьютеров нужно установить соответствующие программы на каждом из них. Большая часть специальных программ для инвентаризации ПО автоматически генерирует инвентаризационные отчеты. После инвентаризации ПО всех компьютеров организации необходимо поместить всю собранную информацию в один отчет.

Этап 3: Сопоставление лицензий и программного обеспечения

После того как стало известно, какие программные продукты установлены на компьютерах организации, наступило время сопоставить установленное программное обеспечение с имеющимися лицензиями.

Перед тем как приступить к выполнению данного этапа, необходимо понять, какие документы являются подтверждением лицензии на каждый тип программного продукта, используемого организацией.

Поиск лицензионной документации. Сначала необходимо связаться с лицом, ответственным за приобретение или состояние программного обеспечения в ОУ. Если организация участвует в одной из программ корпоративного лицензирования Microsoft, то можно получить лицензионную документацию на специализированных сайтах. Если пользователь не может отыскать необходимую лицензионную документацию, он может обратиться за помощью к поставщикам оборудования или в Комитет по образованию.

Хранение лицензионной документации. Хранить всю лицензионную документацию необходимо в надежном месте, рекомендуется использовать сейф.

Сравнение данных. После того как вся лицензионная документация собрана, нужно зафиксировать информацию в виде отчета. Затем сравнить его с отчетом по инвентаризации программного обеспечения, подготовленным на этапе 2; подойдет даже суммарный отчет, использованный на этапе 2. При сравнении легко выяснить, какие программные продукты лицензированы, а какие нет.

Если образовательное учреждение располагает избыточным количеством лицензий, то это означает неэффективное использование ПО. Соответствующие программные продукты следует установить на дополнительных компьютерах так, чтобы количество лицензий было равно количеству установок. Если в ОУ наблюдается недостаток лицензий, то необходимо приобрести дополнительные лицензии (таблица 1.6.2).

Таблица 1.6.2 – План управления лицензиями

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Программное обеспечение | Количество установок | Общее количество лицензий | Избыток или недостаток лицензий | |
| Office 2003 | 22 | 24 | -2 | |
| Office 2007 | 32 | 32 | | 0 |
| Windows XP | 10 | 12 | | -2 |
| Windows 2000 | 40 | 37 | | +3 |

Этап 4: Разработка стратегического подхода и практических процедур

Выбор и последующее использование надлежащих стратегий и процедур для использования программного обеспечения и его лицензирования являются важнейшей частью технологии управления лицензиями в целом.

Стандартизация используемого программного обеспечения. Одним из ключевых процессов, проводимых на этом этапе, является процесс стандартизации. Существенную выгоду могут получить ОУ, которые проведут у себя стандартизацию компьютеров и используемых программ. Например, это может выглядеть так: внутренний стандарт ОУ предусматривает "Рабочий компьютер для учителя – тип 1", который состоит из настольного компьютера, монитора и установленного программного обеспечения; "Рабочий компьютер для учителя-предметника – тип 2" – это ноутбук с определенными возможностями для расширения и конкретным набором программ, стандарт компьютера для администрации ОУ, бухгалтеров, учеников.

Необходимо, чтобы в ОУ имелось описание всех приведенных ниже стратегий и процедур. Если имеется вся документация, то следует провести ее оценку и при необходимости сделать соответствующую корректировку.

Стратегия приобретения программного обеспечения. Централизованное приобретение программного обеспечения позволит сэкономить денежные средства за счет использования скидок при лицензировании большого количества однотипных программ.

Система централизованного приобретения может помочь ОУ в:

1. упрощении поиска лицензионных документов и экономии времени за счет хранения всех лицензий и соглашений в одном месте;
2. уменьшении затрат при приобретении надлежащего типа лицензии;
3. эффективном размещении программных ресурсов, согласовании финансовой сметы на программное обеспечение с реальными нуждами;
4. максимально эффективном использовании программного обеспечения за счет потенциально многократного использования или перераспределения программного обеспечения между отделами.

Стратегия приобретения программного обеспечения может обеспечить достижение всех вышеуказанных целей при условии выполнения следующих процедур:

1. централизация полномочий и документирование при приобретении нового программного обеспечения;
2. приобретение программного обеспечения только у надежных торговых партнеров;
3. хранение лицензионной документации (оригинальные CD, сертификат подлинности, лицензионное соглашение с конечным пользователем, оригинал руководства для пользователя и товарные чеки) в надежном месте;
4. инвентаризация имеющихся программных средств на регулярной основе с целью обеспечения надлежащего лицензирования.

Контроль нового программного обеспечения. Для гарантированного включения данных о новом программном обеспечении следует разработать и включить в инвентаризационный отчет ОУ систему действий, которые должны быть выполнены при поступлении нового программного продукта.

Система действий должна охватывать:

1. хранение оригинальной документации, включая транспортную накладную;
2. хранение оригинальной упаковки;
3. корректировку базы или хранилища инвентаризационной информации.

Процессом контроля программных средств часто пренебрегают, однако только указанные выше действия могут гарантировать точное ведение базы данных с информацией о ПО в организации.

Стратегия использования программного обеспечения. Стратегия использования программного обеспечения должна включать те нормы и положения, которые приняты в организации при загрузке, инсталляции и дальнейшем использовании лицензионных программных средств.

Следует учесть, что:

1. проверка сроков действия условий каждой лицензии для обеспечения надлежащего использования программного продукта;
2. разработка процесса санкционированной инсталляции программного обеспечения (т. е. выделение одного сотрудника, ответственного за установку программных средств);
3. контроль деятельности, связанной с инсталляцией программ или загрузкой программных средств через Интернет.

Важно, чтобы все сотрудники ОУ четко представляли все допустимые и недопустимые действия по отношению к программным и аппаратным средствам. Таким способом возможно исключить попадание вирусов в систему, уменьшить число обращений в службу технической поддержки, а следовательно, обеспечить эффективное использование программного обеспечения.

Чрезвычайный план для программных средств. Важно провести анализ самых неблагоприятных сценариев. Чрезвычайный план включает те процедуры, которые будет выполнять организация в случае чрезвычайной ситуации.

Чрезвычайный план должен содержать информацию по защите и восстановлению программных средств. Пункты плана должны охватывать:

1. регулярное создание копий;
2. хранение копий всех программных средств на CD в сейфах в специально охраняемых помещениях;
3. хранение всей лицензионной документации в сейфах в специально охраняемых помещениях (в случае непрерывного использования информации следует изготовить копии документов, а оригиналы хранить в безопасном месте).

Этап 5: Разработка плана управления лицензиями

Конечным этапом процесса управления лицензиями является разработка плана действий, предусматривающих дальнейшее развитие.

Анализ потребностей в программных средствах. Чрезвычайно важно определить те программные продукты, в которых пользователи (ученики, учителя и административные работники) нуждается для выполнения всех задач по организации образовательного процесса и управления ОУ. Кроме того, целесообразно провести опрос учителей и административных работников: какие программные средства необходимы, а какие не используются в рабочем процессе? Выполнять данную процедуру можно один или два раза в год. На основании проведенного опроса можно создать таблицу, которая отражала бы соотношение между профессиональной компетентностью сотрудника и его потребностью в программном обеспечении. После выполнения этого анализа можно провести списание и деинсталляцию неиспользуемых в работе программных продуктов и предоставить пользователям программное обеспечение, которое действительно может потребоваться в рабочем процессе.

Обучение: как использовать программные продукты. Если ОУ имеет соответствующие ресурсы, можно организовать повышение квалификации в области обучения профессиональному использованию программных продуктов. Обучение может оказаться наиболее эффективно для новых программных продуктов, которые никогда ранее в ОУ не применялись. Повышение квалификации можно организовать и на базе соответствующих городских или районных учреждений.

Надлежащее обучение обеспечит максимальную отдачу от использования нового программного продукта и сократит число обращений в службу технической поддержки из-за неверного использования программного обеспечения.

Снижение затрат на поддержку. К основным направлениям сокращения затрат на поддержку программного обеспечения можно отнести следующие:

1. сокращение числа приложений и устройств, требующих технической поддержки, с заменой их стандартизированными приложениями и системами (осуществляется соответствующим техническим персоналом);
2. отказ от использования заказных "самодельных" решений – расходы на их поддержку могут существенно превосходить расходы на лицензирование. Кроме того, при возникновении проблем с использованием лицензионных программных продуктов специалисты технической службы могут связаться с поставщиком, тогда как в случае эксплуатации "самодельных" программных продуктов какие-либо консультации исключены.

График инвентаризации. Следует установить периодичность проведения инвентаризации программных средств с последующим обновлением хранящейся информации. График проведения инвентаризации определяется масштабами ОУ и количеством компьютеров, периодами поставки нового программного обеспечения и темпами развития локальной сети.

С помощью технологии управления лицензиями можно в реальном времени проводить мониторинг вновь установленного ПО на компьютерах, подключенных к локальной сети, и создавать соответствующие отчеты по инвентаризации ПО.

Полностью изучив и внедрив поэтапный метод использования технологии управления лицензиями, руководитель ОУ и администраторы локальной сети обладают всей информацией о состоянии дел с имеющимся в организации программным обеспечением и точно знают, что необходимо приобрести и как максимально эффективно использовать программные ресурсы.

# 1.6 Диагностика неисправностей технических средств и сетевой инфраструктуры сети

# Модернизация ПК

Основная задача модернизации – расширение возможностей.

Пользователям требуется повысить скорость, производительность, увеличить количество места на диске, получить возможность применять дополнительные функции, словом – улучшить работу компьютера. Основные преимущества, которые можно получить от модернизации компьютера:

1. модернизированный ПК имеет необходимые вам компоненты;

2. благодаря модернизации ПК работает быстрее и эффективнее выполняет текущие задачи;

3. модернизация избавляет от трудностей, связанных с заменой ПК.

Появление в конфигурации компьютера обновленных компонентов, таких, как монитор с большим размером экрана, вместительный жесткий диск, мощная видеокарта или удобный манипулятор, делает общение с компьютером более приятным и продуктивным. Однако, выбирая комплектующие для модернизации, не следует забывать о том, что некоторые устройства могут оказаться несовместимыми друг с другом, а при выходе из строя источника питания в этом придется винить только себя.

Замену старого компьютера на новый можно сравнить с переездом на новую квартиру. Необходимо:

1. выделить нужные файлы;

2. перенести их на новый компьютер;

3. убедиться, что не утеряно ничего необходимого;

4. уничтожить информацию на старом жестком диске.

Неудивительно, что гораздо проще добавить в компьютер новый компонент, чем преодолевать вышеперечисленные трудности.

1. Планирование модернизации

Когда компьютер перестает функционировать должным образом,

вернуть его работу в нормальное русло можно лишь путем обновления комплектующих. В этой главе мы расскажем о необходимости разработки стратегии модернизации, выясним, какая стратегия соответствует вашим задачам и материальным возможностям. Вы найдете рекомендации о том, как избежать лишних затрат при обновлении компьютера, и увидите, как удачно спланированное обновление способно превратить устаревшую систему в мощное и современное вычислительное средство.

Существуют два способа планирования модернизации:

1. на основе задач, которые должен выполнять компьютер;

2. на основе средств, которые можно вложить.

Приняв решение модернизировать компьютер, человек хочет получить максимум выгоды, поэтому необходимо подсчитать затраты и прикинуть, какие именно комплектующие нужны.

Успешная модернизация позволяет ликвидировать «узкие места» в вашей системе в результате чего появляется возможность использования нового программного и аппаратного обеспечения, а также улучшается качество выполнения текущих задач.

Как правило, «узкие места» можно ликвидировать одним из следующих способов:

1. обновить видеокарту;

2. увеличить объем оперативной памяти;

3. повысить быстродействие процессора;

4. повысить скорость соединения с Интернетом.

Аппаратные и программные возможности расширяются за счет установки обновленной версии операционной системы, увеличения объема оперативной памяти и приобретения таких комплектующих как:

* процессора с частотой 3 ГГц или выше (может потребоваться обновление материнской платы);
* материнской платы со встроенным ускоренным графическим портом PCI Ex 16x и портами USB 3.0;
* плат USB 3.0 и Sata3;
* сетевого адаптера Ethernet 100/1000;

Для того чтобы расширить возможности системы по решению задач,

нужно выполнить следующее:

1. определить, какие задачи система должна выполнять;

2. оценить возможности текущего аппаратного обеспечения и ОС;

3. модернизировать те компоненты, которые не удовлетворяют

полученным в результате оценки требованиям.

Бюджет модернизации:

1. бюджет менее 2000 рублей

За такие деньги можно приобрести что-нибудь из следующего списка:

* Новая клавиатура.
* Новая мышь.
* Клавиатура и мышь одновременно.
* Игровые манипуляторы.
* Оперативная память (RAM).
* Устройство flash-памяти.
* Концентратор USB.

2. бюджет менее 4000 рублей

За эти деньги можно серьезно улучшить конфигурацию машины и

производительность системы. Достаточно выбрать что-нибудь из

следующего списка:

* Жесткий диск.
* Комбинированный дисковод CD-RW/DVD.
* Звуковая карта.
* Динамики.
* Беспроводной доступ в Интернет.
* Операционная система.

3. бюджет менее 6000 рублей

За эти деньги можно значительно улучшить производительность и

возможности своей машины чем-нибудь из следующего списка:

* Материнская плата и процессор.
* 21- или 23-дюймовый монитор.
* Высокопроизводительный ЗD-ускоритель.

4. бюджет свыше 6000 рублей

С такими деньгами есть два пути: создать список модернизируемых

компонентов из перечисленных выше либо воспользоваться одной из

следующих альтернатив:

* Широкополосный доступ в Интернет.
* Сканеры, цифровые камеры, струйные и лазерные принтеры.
* Процессор, материнская плата или другие важные узлы компьютера.

2. Оценка состояния компьютера

Наиболее простым способом оценки системы по возрасту является

«правило трех лет»: если в течение этого срока конфигурация компьютера не меняется, его модернизация становится экономически невыгодной.

Данное правило не относится к внешним устройствам, так как их Эффективный возраст системы определяется максимальным возрастом одной из трех перечисленных ниже компонентов:

1. материнская плата/ процессор;

2. оперативная память;

3. видеокарта.

Указанные компоненты оказывают наибольшее влияние на

производительность компьютера.

3 способа оценки состояния компьютера:

1. анализ информации, выводимой компьютером при загрузке;

2. использование специального программного обеспечения;

3. визуальное обследование системы.

Просмотр и анализ комплектации компьютера

Есть простой способ определить правильность комплектации компьютера программно. Существует ряд программ, позволяющих узнать модели комплектующих скрытых от глаз покупателя. Ведущими в этой области являются программы Everest и SiSoft Sandra. Однако можно обойтись и без них. Операционная система Windows позволяет делать то же самое своими встроенными утилитами для этого достаточно выполнить следующие действия:

1. Проверка процессора и оперативной памяти

Найдите ярлычок «Мой компьютер», который расположен на «Рабочем

столе» либо в меню «Пуск» и нажмите на него правой кнопкой мыши. В

появившемся меню выберите строку – «Свойства».

Теперь перед нами открылось окно с информацией о нашей ОС,

пользователе ПК и оборудовании – процессоре и оперативной памяти.

2. Затем в окне слева: Диспетчер устройств или Дополнительные

параметры, закладка Оборудование, Диспетчер устройств:

Здесь мы можем просмотреть информацию о жестких дисках, звуковых

и видео устройствах.

3. Эту и другую информацию можно получить другим способом.

Открываем меню «Пуск» и выбираем пункт «Выполнить». В открывшемся окошке пишем «dxdiag» и нажимаем «Enter». Соглашаемся с тем, что программа просканирует оборудование, нажав кнопку «Да». В открывшемся окне мы также можем проверить процессор, память и видеокарту.

Не все системы легко поддаются модернизации. Проблемы, с которыми

можно встретиться при модернизации:

1. уникальная конструкция системы;

2. материнская плата устаревшего типа;

3. память устаревшего типа;

4. процессор устаревшего типа;

5. недостаточное количество PCI-разъемов;

6. недостаточное количество разъемов и отсеков под накопители.

3. Выбор комплектующих для модернизации с учетом задач, решаемых компьютером после модернизации

Выбор задач для компьютера после модернизации. Существуют разные виды модернизаций.

Модернизация для любителей игр:

Эта модернизация подразумевает приобретение следующих компонентов:

1. Игровой контроллер;

2. Монитор;

3. Процессор, материнская плата, оперативная память

4. Вентиляторы;

5. Аудиосистема;

6. Оптические накопители.

Модернизация для работы с цифровым видео:

Эта модернизация подразумевает приобретение следующих

компонентов:

1. Цифровая видеокамера;

2. Порт IEEE-1394;

3. Аппаратное обеспечение для оцифровки аналогового видео;

4. Программы для редактирования видео;

5. Дисковод для записи DVD;

6. Операционная система.

Модернизация для работы с цифровым фото:

Эта модернизация подразумевает приобретение следующих

компонентов:

1. Сканер;

2. Монитор

3. Цифровой фотоаппарат;

4. Устройства для хранения цифровых фотографий;

5. Устройства ввода;

6. Принтер;

7. Процессор, материнская плата, оперативная память;

8. Операционная система.

Модернизация для широкополосного доступа в Интернет:

Эта модернизация подразумевает приобретение следующих

компонентов:

1. Сетевой адаптер;

2. Домашняя компьютерная сеть;

3. Технология широкополосного доступа.

Модернизация для прослушивания цифровой музыки:

Эта модернизация подразумевает приобретение следующих

компонентов:

1. Устройство для хранения оцифрованного звука;

2. Переносной MP3-плеер;

3. Звуковая карта и динамики.

Модернизация для создания web-сайтов и программирования:

Эта модернизация подразумевает приобретение следующих

компонентов:

1. Монитор;

2. Программируемая клавиатура.

**Обоснование модернизации сети**

Аналитические данные помогают обосновать необходимость модернизации сети при ее низкой производительности, но перспектива достижения новых бизнес-целей способствует этому еще больше.

Эта потребность оказывается особенно настоятельной при обращении предприятий к электронной коммерции. Однако, как правило, модернизация сети является сложной и дорогостоящей задачей, и к тому же ее осуществление может потребовать временного отключения имеющихся сервисов и привести к снижению продуктивности пользователей, вызывая дополнительные затраты.

Прежде чем браться за модернизацию сети, ее необходимо обосновать. Вместо того чтобы устанавливать новые штуковины всякий раз при очередном изменении технологии или предложении поставщика, лучше, может быть, подождать, пока у пользователей созреет в этом необходимость или когда новая система позволит сократить затраты?

К сожалению, универсальной формулы для обоснования модернизации сети не существует. «Планирование развития сети и обоснование ее модернизации — это скорее искусство, чем наука», — считает Дэвид Ринас, президент DJR Communications, консалтинговой компании в области планирования сетевых сервисов и управления проектами.

В данной статье я постараюсь объяснить некоторые из приемов этого искусства и методов этой науки, а также перечислить объективные показатели необходимости модернизации. Иногда невозможно сказать, бизнес определяет технологию, или наоборот. Часто процесс модернизации сети складывается под действием обеих тенденций. Я начну с рассмотрения технических причин и продолжу коммерческими выкладками.

**Технические причины**

Потребность в увеличении скорости является, вероятно, наиболее распространенной причиной модернизации сети. Она может привести к обновлению оборудования, например маршрутизаторов или самих каналов. Если производительность сети недостаточна, то первое, что следует сделать, — выяснить уровень загруженности каналов.

В качестве эмпирического правила обычно принимается, что емкость канала или интерфейса следует увеличить, когда уровень его загруженности достигает 70%. Если пропускная способность канала достаточна, то причина может лежать в адекватной производительности оборудования.

Прежде всего внимание следует обратить на старое оборудование, в частности мосты между локальными сетями. В этом случае наилучшим решением будет замена оборудования, а не его модернизация.

Однако часто появление узких мест является следствием увеличения трафика или нагрузки на такие системы, как серверы или маршрутизаторы, ранее обеспечивавшие нормальную производительность. Ответ на вопрос, что лучше — модернизировать или заменить такие системы, зависит от стоимости каждого из решений и его влияния на поддерживаемые сервисы. Рассмотреть следует оба пути, чтобы определить, какого рода модернизация наиболее оправдана.

Например, отключение сервера на выходные для увеличения объема оперативной памяти или установки еще одной сетевой платы не приведет к заметным простоям, будет стоить недорого и практически всегда оправдано. Однако когда модернизация имеет более существенные последствия для непрерывности сервиса, скажем, при переводе локальной сети от компактной магистрали на базе концентратора/маршрутизатора к коммутируемой среде, то такое решение должно иметь веские основания — желательно, чтобы оно подкреплялось планом реализации.

Кроме того, неадекватная производительность может быть связана с длительной задержкой в сети. Причиной задержки может стать медленное оборудование или каналы либо неэффективность сетевых протоколов или прикладных сервисов, например медленная обработка сообщений сервером SMTP.

Эти проблемы реально решить посредством модернизации, но сам процесс может оказаться весьма извилистым и занять много времени. Обоснование часто сводится к анализу экономических выгод «а стоит ли это делать», с учетом как бизнес-целей, так и удобства работы.

В других случаях задержка может быть связана с необходимостью преобразования форматов, обеспечения межсетевой защиты и контроля доступа или даже с большими расстояниями между конечными точками. Функции защиты и преобразование форматов предполагают аппаратную реализацию. В этом случае стоимость модернизации будет трудно обосновать без анализа экономических выгод.

Задержку при передаче вследствие географической удаленности, скажем через Атлантику или через спутники, устранить невозможно — если только вы не найдете сеть быстрее скорости света.

Необходимость внесения изменений в сеть может быть вызвана и другими причинами, в частности потребностью обеспечения взаимодействия между сетями и системами при слиянии двух компаний. В этом случае все определяется требованиями бизнеса.

Другим побудительным мотивом может стать необходимость ликвидации периодических или хронических проблем в функционировании сети или при управлении ею. Такую модернизацию обычно можно обосновать улучшением сервиса и сокращением затрат на обслуживание и управление сетью.

Стимулом для модернизации может также стать желание получить новые возможности администрирования. Упрощение обслуживания сети является веским основанием для приобретения административного инструментария, такого, как программное обеспечение для инвентаризации настольных систем. Чтобы еще более подкрепить его, модернизацию можно увязать с такими осязаемыми выгодами, как оптимизация закупок.

Необходимость стандартизации вычислительной среды для реализации планируемых приложений или сервисов также может потребовать модернизации. В этой ситуации обоснование обычно не составляет проблем: стандартная среда позволит оптимизировать закупки, снизить затраты на обслуживание и обучение и упростить предоставление требуемых сервисов.

Наконец, необходимость выполнения сертификационных требований или решения спорных вопросов, выявленных при аудите сети, также может потребовать модернизации. Со все большим распространением корпоративных сетей Extranet, сервисов удаленного доступа, VPN и меж организационного взаимодействия эти специальные требования становятся достаточно типичными. В подобной ситуации потребность в модернизации вызывается и обосновывается стремлением выглядеть в глазах других «безопасным» и надежным партнером.

«Если аудит выявит в сети проблему, то ее потребуется устранить, но это может повлечь за собой необходимость модернизации и дальнейшие расходы», — говорит Эрик Деспрес, директор по сетевым сервисам в компании GENet, занимающейся управлением сетями правительственных учреждений Канады.

Часто модернизация одного элемента сети вызывает необходимость модернизации связанных с ним элементов инфраструктуры сети. Например, если локальная сеть модернизируется до Ethernet на 100 Мбит/с и на всех пользовательских системах устанавливаются соответствующие сетевые платы, то это может потребовать также и модернизации сервера.

По словам Деспреса, один из примеров того, как может возникнуть потребность в такого рода связанной модернизации, можно найти в предлагаемых классах QoS для сетей на базе IP. С появлением в результате увеличения емкости сети возможности реализации новых приложений, которым необходимы гарантии на QoS, провайдерам услуг «потребуются более мощные средства измерения и контроля для «раскрашивания» IP-пакетов в соответствии с ожиданиями отправителя в отношении QoS», — говорит Деспрес. В этом случае обоснованием может служить необходимость выполнения соглашений об уровне сервиса (Service Level Agreement, SLA).

Однако реализация QoS в существующей сети приведет к увеличению на 20% накладных расходов при передаче трафика и заметно скажется на общей производительности межсетевых устройств. Переход к современной, более эффективной межсетевой инфраструктуре позволяет компенсировать эти потери, обеспечив при этом поддержку QoS и общее улучшение обслуживания.

# 1.7 Восстановление сети после аварии

Быстрое восстановление работоспособности сетей в распределенных системах управления является весьма актуальной задачей. Ее успешное решение имеет непосредственное отношение к минимизации производственного ущерба, связанного с вынужденным простоем оборудования. Перечень и последовательность процедур, необходимых для восстановления нормального функционирования системы после наступления чрезвычайных обстоятельств, обычно устанавливает «План восстановления функционирования системы», который должен быть подготовлен заранее и утвержден руководством организации, эксплуатирующей любые ОСИС [1].

Основная цель реализации плана заключается в обеспечении быстрого и полного восстановления устойчивого функционирования информационной системы. Как правило, план предусматривает решение следующих задач:

1) определение порядка действий, процедур и ресурсов, необходимых для восстановления функционирования системы или обеспечения ее устойчивого функционирования в резервном варианте размещения технических средств и персонала;

2) определение штатного состава и основных обязанностей персонала оперативного штаба и аварийных групп из числа сотрудников предприятия по реализации мероприятий плана восстановления;

3) определение порядка координации действий оперативного штаба по реализации плана с другими структурами (пожарные, медперсонал, полиция, спасатели и др.), которые будут привлекаться к ликвидации последствий чрезвычайных событий, вызвавших нарушение нормального функционирования системы.

Все мероприятия по выполнению плана распределяются по трем этапам:

• этап уведомления/активации плана;

• собственно этап восстановления;

• этап воссоздания системы/деактивации плана.

Задачи, решаемые на этапе уведомления/активации плана, — своевременная идентификация наступления чрезвычайных условий, обнаружение нанесенных системе повреждений, оценка ущерба, прогноз возможности восстановления функционирования системы и принятие решения о необходимости активации плана восстановления системы.

Задачи, решаемые на этапе восстановления, — восстановление функционирования системы по временной схеме (с использованием резервных средств и помещений), проведение комплекса работ по полному восстановлению работоспособности системы в объеме обычных условий.

Задачи, решаемые на этапе воссоздания системы/деактивации плана, — полное восстановление нормальной работы системы и деактивация плана восстановления, возврат к нормальному функционированию.

Пренебрежение к организационным и стратегическим решениями в области ИТ-безопасности дает немедленный отрицательный эффект: значительно (в разы) возрастает число компьютерных атак на корпоративные ИТ-системы и случаев взлома систем информационной безопасности компании. Целью хакерской атаки обычно является хищение коммерческой информации и финансовое мошенничество, однако в Москве, по опросам специалистов, эти позиции составляют лишь 3 и 6% от общего числа хакерских атак. Эксперты полагают, что масштабы проблемы намного существеннее, а низкий процент объясняется тем, что современные хакеры искусно скрывают следы. Только в Москве ущерб от электронных мошенников оценивается правоохранительными органами в 12—15 млн долл, в месяц.

Основной принцип планирования восстановления предполагает наличие заранее подготовленного помещения, которое выполняет функции резервного центра размещения технических средств системы. Персонал системы формирует необходимую информационно вычислительную среду на основе технических средств резервного центра для восстановления функционирования системы по резервному варианту размещения в период действия плана восстановления. Кроме того, резервный вариант размещения используется в течение всего времени, необходимого для восстановления функционирования системы по прежнему (либо новому) месту размещения.

При разработке плана восстановления, как правило, применяются следующие основные допущения и посылки:

• технические средства неработоспособной системы могут быть восстановлены по прежнему месту размещения не ранее чем через 12 ч;

• заранее определен ключевой персонал, осведомленный о действиях в аварийных обстоятельствах и своих обязанностях в процессе восстановления работоспособности системы;

• системы контроля, аварийного оповещения и ликвидации последствий аварий должны находиться в работоспособном состоянии;

• все элементы системы (в том числе и в резервном помещении) обеспечены непрерывным энергопитанием не менее чем на 30 мин с момента выхода из строя основной энергосистемы, после чего они подключаются к дизель-генератору с трехсуточным запасом топлива;

• актуальные резервные копии прикладного ПО и данных не должны быть повреждены и должны быть доступны в резервном офисе;

• необходимое для восстановления системы оборудование должно быть доступно в резервном офисе;

• договоры на техническое обслуживание аппаратных средств, обновление ПО и услуги провайдеров связи включают положения, необходимые для реализации плана восстановления функционирования системы.

Перечислим основные требования к политике организации схемы послеаварийного восстановления сети:

1) при недоступности аппаратно-программных систем, расположенных в центральном офисе организации, более 6 ч должен быть организован резервный офис с соответствующими ресурсами для восстановления нормального функционирования системы по резервному варианту;

2) все пункты выполнения плана должны быть изложены в соответствующих инструкциях в отделах организации, привлекаемых к реализации плана, причем ревизия документов должна проводиться не реже одного раза в год и модифицироваться по мере необходимости;

3) персонал, ответственный за систему, должен быть заранее обучен выполнять процедуры плана восстановления;

4) все положения плана и практические возможности персонала по его реализации в части восстановления функционирования системы должны проверяться в ходе учений и тренировок не реже одного раза в год.

Эффективный план обеспечения бесперебойной деятельности является относительно недорогой формой страхования компаний от последствий возможных бедствий, и затраты на него должны рассматриваться как составляющая необходимых издержек на поддержание нормальной деятельности организации.

Организация работ по восстановлению ЛВС

Руководители организации или компании являются хранителями ее интересов. Они должны применять качественные методы управления, которые обеспечат получение прибыли, должное качество продукции и услуг, стабильность и развитие организации в интересах заказчиков, служащих и инвесторов. Если нештатная ситуация может поставить под вопрос само существование организации, то вряд ли ее руководство справляется со своими обязанностями.

При отсутствии эффективного «Плана обеспечения бесперебойной деятельности организации в случае нештатных ситуаций» могут возникнуть следующие проблемы и опасности:

• прерывание деятельности организации, которое влечет за собой неспособность обслуживания имеющихся заказчиков, потерю перспектив для бизнеса, уменьшение существующего круга заказчиков, утрату престижа и потерю конкурентоспособности;

• финансовый ущерб из-за невозможности обрабатывать счета дебиторов, штрафов за задержку платежей, упущенных скидок, неспособности обновлять балансы счетов и потерянных или неучтенных продаж;

• юридическая ответственность за невыполнение обязательств по контрактам;

• прекращение деятельности организации.

Под планированием бесперебойной деятельности организации в случае нештатных ситуаций понимается «выявление и защита критически важных бизнес-процессов и ресурсов, необходимых для поддержания деятельности организации на нужном уровне, а также разработка процедур, которые обеспечат выживание организации при нарушении ее нормальной деятельности».

Для обеспечения бесперебойной деятельности необходимо учитывать все взаимосвязанные внешние и внутренние функции, в том числе ручные методы учета и обработки информации. Целями проекта по составлению плана, обеспечивающего бесперебойность и восстановление деятельности организации в случае бедствий, являются:

1) оценка бизнес-процессов, которая обеспечит разработку плана с помощью хорошо структурированной и всеобъемлющей методологии;

2) разработка экономичного и работоспособного плана, который обеспечит бесперебойность критически важных бизнес-процессов в случае серьезного нарушения деятельности организации;

3) минимизация последствий любого бедствия для организации. Основным координирующим и управляющим органом по реализации плана восстановления функционирования системы (далее — Плана) является оперативный штаб. Возглавляет деятельность штаба координатор по вопросам восстановления — руководитель организации или его заместитель.

Штаб обычно размещается в рабочем кабинете координатора и оборудуется средствами связи и обмена информацией, способными обеспечить бесперебойное взаимодействие членов штаба с руководителями подразделений, руководителями аварийных групп, организациями и структурами, привлекаемыми для ликвидации последствий чрезвычайной ситуации. В состав оперативного штаба, как минимум, входят:

• начальники структурных подразделений организации;

• начальник отдела защиты информации;

• оперативный дежурный (секретарь).

Все члены штаба снабжаются средствами мобильной связи. Список номеров телефонов членов штаба, руководителей аварийных групп и дежурных служб, а также городских аварийных служб находится у каждого члена штаба. В схеме оповещения персонала должны быть предусмотрены варианты их информирования для рабочего и нерабочего времени. В задачу штаба входит оценка ущерба, необходимых для восстановления нормального функционирования ресурсов и времени, а также координация действий персонала.

Штаб взаимодействует и координирует свои действия с оперативными штабами других организаций и служб, связанных с ликвидацией последствий чрезвычайной ситуации. В ходе реализации Плана выполняются сгруппированные по категориям мероприятия:

• анализ повреждений — оценка повреждений, подготовка прогноза восстановления и предложений по активации Плана;

• подготовка к развертыванию аппаратно-программной системы по резервному варианту (подготовка рабочих мест для прибывающего персонала, телефонной связи и компьютерной сети, обеспечение резервного электропитания подключаемой техники идр.);

• развертывание системы по резервному варианту, предусматривающее использование резервных копий данных, находящихся в резервном центре;

• аварийное сопровождение системы — поддержание работы технических средств в здании организации, попавшем в зону чрезвычайной ситуации, возможно более долгое время до момента задействования резервного варианта функционирования системы;

• восстановление — проведение необходимых мероприятий совместно с представителями других организаций (пожарные, полиция, спасатели и др.) по локализации и устранению последствий событий, повлекших выход из строя системы;

• эвакуация носителей информации ограниченного распространения и оборудования системы из здания, попавшего в зону чрезвычайной ситуации.

Проведение начальной стадии работ по восстановлению функционирования системы регламентирует «Порядок уведомления о чрезвычайных событиях», который делится на фазы:

• получение сигнала о чрезвычайной ситуации;

• развертывание оперативного штаба;

• принятие решения на активацию Плана и доведение его до всех задействованных в нем подразделений.

Получение сигнала о чрезвычайной ситуации. Эксперты отмечают, что информация о чрезвычайной ситуации может быть как срочной (начавшийся пожар, прорыв системы водоснабжения, внезапное отключение электричества, теракт, нападение и т.д.), так и долгосрочной (приближение наводнения, радиационного или химического облака, штормовое предупреждение, оперативные данные о готовящемся террористическом нападении и т.п.).

В любом случае координатор должен уточнить источник информации и убедиться в ее истинности, прежде чем принимать решение о развертывании оперативного штаба. При получении информации координатор (оперативный дежурный) должен в специальном журнале зафиксировать время поступления информации и ее источник (фамилию передавшего информацию, телефон или другой источник ее поступления). При поступлении срочной информации координатор немедленно оповещает о ее получении руководство, членов оперативного штаба и руководителей подразделений.

Вся оперативная информация о чрезвычайной ситуации и ее развитии должна стекаться, как правило, в оперативный штаб. Учитывая конфиденциальный характер, в полном объеме с данной информацией может быть ознакомлено руководство организации и члены оперативного штаба. Выдача кому-либо другому информации о чрезвычайной ситуации без разрешения координатора категорически запрещается.

Развертывание оперативного штаба. Приняв решение об активации Плана, координатор доводит необходимую информацию до членов оперативного штаба. В сообщении должны быть указаны время и место сбора его членов.

Должно быть предусмотрено несколько вариантов размещения оперативного штаба: основной — в рабочем кабинете координатора; запасной — вне помещений организации; резервный — в микроавтобусе, автофургоне и т.д. Каждый член штаба должен знать, какие документы и технические средства он обязан иметь при себе на случай объявления чрезвычайной ситуации. При созыве членов штаба в рабочее время они (или замещающие их лица) прибывают в указанное место незамедлительно. При созыве членов штаба в нерабочее время должно учитываться время на их сбор и перемещение в указанное место.

В схеме оповещения членов оперативного штаба должны быть указаны точный адрес, телефон, наличие личного транспортного средства. В случае невозможности прибытия члена штаба на личном транспорте должен быть предусмотрен вариант его доставки служебным или частным автотранспортом. По прибытии члены штаба вводятся в курс дела, им обеспечивается доступ ко всей необходимой информации. Каждому члену штаба определяется его рабочее место, которое должно быть оснащено необходимыми средствами связи.

Решение на активацию Плана координатор принимает лично на основании результатов анализа, проведенного группой анализа повреждений, а также выводов и рекомендаций членов оперативного штаба. С этой целью каждый член штаба дает ситуации оценку, в которой приводит свое видение проблемы (активировать ли План в складывающейся обстановке) и кратко его аргументирует. В докладах членов штаба и руководителя группы анализа повреждений должна быть отражена следующая информация:

• возможная причина инцидента;

• характер повреждений (затронутая физическая область и состояние физической инфраструктуры, состояние и функциональные возможности оборудования и инвентаря, включая перечень элементов, подлежащих восстановлению);

• прогноз развития инцидента, потенциал для возможного углубления (расширения) его последствий, могущих привести к увеличению разрушений или повреждений в системе;

• примерное время на восстановление работоспособности системы;

• предложения по активации Плана.

На принятие решения накладываются серьезные ограничения. Так, решение координатором об активации Плана должно быть принято в течение не более 30 мин с момента получения им информации об инциденте. Принятое решение не обсуждается. План должен быть активирован в обязательном порядке, если анализ повреждений говорит о том, что на восстановление работоспособности необходимо более 6 ч, при этом существует опасность физического разрушения инфраструктуры и системы или реальная угроза жизни и здоровью персонала.

Если нанесенный системе ущерб может быть устранен за время не более 6 ч, то координатор вправе не активировать План, а поручить устранение неисправностей соответствующим специалистам в рабочем порядке. Координатор также может принять решение о привлечении аварийно-спасательных служб города для локализации и ликвидации последствий чрезвычайного происшествия.

И при активировании Плана и при его деактивации решение об этом доводится до руководства и всех привлекаемых к реализации Плана структур.

Возврат к нормальному функционированию системы. По завершении восстановительных мероприятий руководитель работ по анализу повреждений готовит отчет о готовности системы к возврату в первоначальное состояние и возможности деактивации Плана.

Решение о деактивации Плана принимается координатором на основании информации, полученной по результатам анализа ситуации. Принятое решение докладывается руководству организации.

После получения сигнала по деактивации Плана персонал аварийных групп выполняет мероприятия по приведению системы в исходное состояние. Для этих целей, как правило, привлекается тот же персонал, что и для выполнения работ по активации Плана. О результатах выполнения работ каждый сотрудник докладывает своему непосредственному начальнику, а тот — координатору.

После восстановления нормального функционирования системы по первоначальному варианту руководители структурных подразделений проводят подробный разбор и анализ действий подчиненных в ходе выполнения работ по Плану. Результаты разбора и анализа передаются координатору. На основании полученных материалов он составляет подробный отчет для руководства организации о произошедшем событии, принятых мерах и их эффективности, понесенных убытках. При необходимости вырабатываются и докладываются предложения по совершенствованию инфраструктуры на случай повторения подобных ситуаций.

Изменившийся характер угроз заставляет обратить внимание на те сферы обеспечения устойчивого функционирования систем, которые еще несколько лет назад не были столь актуальными. Среди документов, регламентирующих работу системы в чрезвычайной ситуации, основное место занимает план функционирования. Сегодня наличие подобного документа стало обязательным для всех предприятий и организаций.

Планирование восстановления работы системы

Планированию восстановления данных после сбоя в последнее время уделяется все более серьезное внимание со стороны руководства предприятий. Причиной здесь является масса значительных природных катаклизмов, катастроф, произошедших объективно и/ или по вине человека, а также все более строгих правил и законов, предписывающих защищать и сохранять данные — самый незаменимый актив компании, уступающий место, пожалуй, только квалифицированному персоналу.

Рассмотрим с практической точки зрения содержание компонентов планирования восстановления данных. Собственно методология планирования восстановления данных в консалтинговых компаниях представляется неким сложным и извилистым процессом, известным только нескольким привилегированным практикам. Однако на самом деле методология планирования восстановления данных — это простое применение здравого смысла, за которым следует прагматический план проекта, подобный методологии разработки жизненного цикла систем.

Анализ.

Планирование восстановления данных должно начинаться с этапа непосредственной инициации проекта. Это широкое понятие включает в себя сбор команды для проекта (можно включить в нее собственных и привлеченных со стороны экспертов по данной тематике), а также формулировку целей плана и бюджета. Важным моментом является разработка и применение единых шаблонов для копирования/восстановления данных, обязательных к применению во всех отделах организации, включая инструкции по использованию стандартного ПО, такого как электронная почта, обработка текста и электронные таблицы, управляемые элементы БД. Основная задача — добиться того, чтобы все члены команды подавали документы в одном и том же формате, что облегчит последующее объединение и анализ данных.

Сбор данных — следующий этап анализа ситуации. Он включает в себя сбор информации о внутренних приложениях, инфраструктуре, рисках внешних воздействий. В рамках этапа осуществляется сбор информации о рисках сбоев в работе и методах восстановления данных, используемых другими компаниями. Данные распределяются по категориям и собираются в «информационном складе», в котором сотрудники, работающие над последующими стадиями планирования, могут быстро найти нужную информацию. Также необходимо собрать информацию о том, сколько будет стоить компании простой системы, влияющий на все бизнес-процессы, через 24, 48 и 72 ч, как в денежном эквиваленте, так и в виде нематериальных затрат (потеря доверия потребителей и пр.).

Анализ рисков включает в себя назначение приоритетов для восстановления данных бизнес-процессов, приложений и инфраструктуры, используемой для их поддержки. Частично это попытка предсказать потери компании от перерыва в работе приложений. На основе таких факторов, как начисленные денежные потери от сбоя, данная оценка назначается для каждого бизнес-процесса, а также связанных с ним приложений и инфраструктуры.

Сценарий «выявления потерь», направляющий разработку плана, также формулируется в рамках данной задачи. Идеальным решением было бы выбрать для плана сценарий полной потери основного оборудования, объединив материальные и нематериальные издержки, понесенные после 24, 48 и 72 ч после катастрофы. Это создает весьма убедительную картину при обсуждении финансирования плана, что важно, если учесть, что впоследствии менеджеры могут сократить планируемый бюджет. В конечном счете создаваемый план должен отвечать наихудшему сценарию, но он также должен обладать модульной структурой, чтобы гибко реагировать на менее серьезные случаи сбоев.

По окончании первой стадии планировщики обращаются к стратегиям по логистике восстановления данных, приложений, сетей и рабочих сред конечных пользователей в случае сбоя. Философия, лежащая в основе построения стратегий, проста — устранить те возможности возникновения сбоя, которые можно устранить, и минимизировать влияние тех возможностей возникновения сбоя, устранить которые нельзя.

Постановка задач восстановления данных после сбоя. Большинство задач этой фазы включают разработку стратегий и логистики восстановления после сбоя инфраструктуры и данных, необходимых для критически важных приложений. Каждая из задач требует рассмотрения множества альтернативных вариантов, что помогает построить наиболее эффективную стратегию в рамках ограничений бюджета.

В случае если стратегия предполагает значительные затраты, ее необходимо строго обосновать перед руководством. Поэтому актуальной является задача поиска такой стратегии, которая не только решает вопросы по восстановлению сети после аварии, но и приносит пользу для повседневной деятельности организации.

Например, консолидация хранилищ в сети Fibre Channel для совместного использования ленточной библиотеки обеспечивает улучшенную защиту данных по сравнению с существующей системой. Однако это дорогое приобретение. Альтернативными могут быть решения: а) консолидация серверов, позволяющая снизить затраты на покупку лицензионного ПО, либо б) продление срока службы существующих ленточных устройств. Только когда затраты на каждое решение будут хорошо обоснованы, с ними можно выходить к руководству предприятия.

Актуален следующий практический вопрос, вытекающий из ограниченности бюджета на восстановление: выбрать ли систему, позволяющую избежать катастрофы, или разрабатывать стратегию восстановления данных?

Задача выбора «безаварийных» систем фокусируется на разработке технологий, помогающих определить условия или события, которые могут привести к катастрофе, с последующей их нейтрализацией. Безаварийные системы (включая ПО по управлению, контроль безопасности, датчики пожарной сигнализации и т.д.) не только помогают предотвратить сбои в сети, но могут также спасти жизнь персоналу компании.

Разработка стратегии восстановления данных является актуальной альтернативой задаче выбора «безаварийных» систем. Защита данных ограничена только одной стратегией — избыточностью. Чтобы защитить информацию от потери или разрушения, данные необходимо дублировать.

Способ дублирования данных находится в спектре между резервированием «диск—лента» и зеркальным копированием «диск- диск». В этот спектр попадает все возрастающее число вариантов выбора, представленных отраслью хранения данных в качестве комплексов решений. Рисунок 4.9 демонстрирует спектр современных решений по защите данных, организованных по целевому критерию: «время на резервирование» против «времени на восстановление».

В данном многообразии решений отражается весь спектр продуктов, представленных отраслью хранения данных и отвечающих на проблемы времени и стоимости защиты данных.

Существует множество характеристик программных продуктов, предназначенных для снижения времени на резервное копирование, относящихся к группе «данные для копирования на ленту»: добавочное резервное копирование, «горячее» резервное копирование, а также средства резервирования «диск—диск», имитирующие ленту (DDT). Однако существуют и другие технологии, предназначенные для снижения стоимости зеркалирования данных с диска на диск, например дублирование «диск—диск», многоцелевое и сетевое кэширование, основанное на программном и аппаратном обеспечении, и др.

Таким образом, можно говорить о множестве альтернатив, удовлетворяющих многим средам и бюджетам, а также о множестве вариантов выбора способа резервного копирования данных при планировании. Если компания обладает ограниченными финансовыми ресурсами для планирования восстановления данных, средства лучше потратить на комбинацию решений.

Не стоит минимизировать важность планирования для восстановления приложений (и хост платформ), сетей и данных конечных пользователей. Чем больше способов защиты вы можете спланировать заранее для этих важных направлений восстановления данных, тем лучше.

Однако, как убедились во многих компаниях, даже если тщательно разработанные схемы восстановления сетей, систем и рабочих пространств пользователей становятся жертвой незапланированных событий или сбоев, восстановление этих элементов можно провести достаточно быстро. Но данные невозможно заменить, если они не были заранее продублированы!

После того как все стратегии были сформулированы и задокументированы, наступает последняя стадия проекта планирования, которая включает:

• создание команд по восстановлению и их обучение;

• тестирование плана;

• реализацию процесса управления изменениями.

Последний пункт позволяет собрать результаты тестов и обеспечить обратную связь для ранее созданного информационного склада. Это позволит обновить план и учесть в нем все изменения, произошедшие в бизнесе и ИТ-инфраструктуре.

Выполнение.

К этому моменту должны быть закончены все организационно-подготовительные мероприятия: подписаны контракты с поставщиком; экипирован необходимым компьютерным и сетевым оборудованием и хранилищами собственный центр резервных данных и рабочее пространство пользователей, что поможет обеспечить правильное выключение систем; данные компании продублированы и проверены.

В этой точке фактически начинается наиболее важная часть в проекте планирования. Успешное решение задач последнего, третьго этапа даст гарантию, что план будет активирован и выполнен тогда, когда это необходимо, и обеспечена полная синхронизация процедуры восстановления данных с требованиями компании.

Стадия выполнения включает составление документации для плана или, по крайней мере, блок-схемы процесса принятия решений, которые покажут менеджерам все необходимые шаги, которые необходимо мгновенно предпринять в случае аварии или критического положения. На этом этапе важно понять, что план, который составлен и написан на бумаге, служит в меньшей степени сценарием для восстановления данных и в большей степени учебным пособием и руководством для тестирования.

После разработки возможностей восстановления данных следует тщательно задокументировать, что должно произойти, когда вам необходимо оповестить всех тех, кто будет принимать участие в восстановлении данных, об их ролях и обязанностях. Не существует никаких указаний насчет того, сколько должно быть команд и сколько человек должно входить в каждую из них. Здравый смысл — лучшее руководство в данном случае. Хороший вариант — спросить менеджеров отделов или бизнес-подразделений, кого, по их мнению, необходимо привлечь к работе по восстановлению данных: выбрать ответственное лицо и дублера. ИТ-отдел обязательно должен выбрать значительное число сотрудников.

Обучение состоит из представления стратегий и процедур. Обучайте команды тому, что им необходимо делать в случае аварии, однако необходимо также детально описать обстановку, чтобы члены команды понимали, как на их работу будут влиять и как их работа повлияет на работу других команд. Внимательно выслушивайте замечания, так как они помогут вам определить те требования, на которые вы, возможно, не обратили внимания.

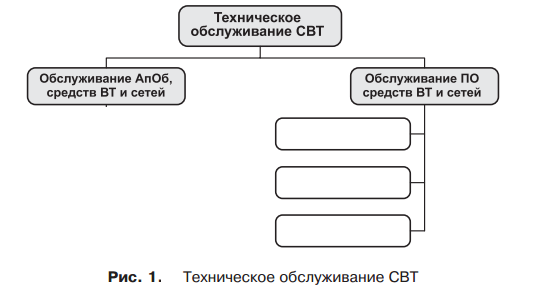
Команды также участвуют в тестировании, что является таким же учебным упражнением, как и репетиция активации плана. Существует множество способов тестирования, и по этой теме консультантами по планированию восстановления данных написано огромное количество книг. Предпочтительным является неразрушающее тестирование, т.е. тесты, которые не влияют и не мешают повседневной работе компании.

Одной из возможных стратегий является критический анализ. Команды собираются вместе, и им предлагается сценарий. Затем команды определяют, что им понадобится сделать, и рассуждают о возможных препятствиях, с которыми они могут столкнуться, и что понадобится для их преодоления в плане ресурсов и времени, причем весь процесс должен быть задокументирован.

Еще одной стратегией может быть использование времени, которое отведено вам для тестирования, если вы заключили контракт с поставщиком средств восстановления после аварии. Постарайтесь восстановить данные, системы и сетевые операции и убедитесь, что у вас есть все необходимые ресурсы и отведенного вам времени достаточно. Результат этого теста также должен быть задокументирован, поскольку он напрямую демонстрирует эффективность плана и возможные слабые места из-за недостаточной синхронизации с текущими изменениями в работе организации.

# Вопросы и упражнения

1. Перед вами, схема этапов технического обслуживания СВТ (рис. 1). Впишите этапы второй ветви: Обслуживание ПО СВТ и сетей.



1. В каких случаях проводится аудит локальной сети?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. При каком виде обслуживания каждое устройство обеспечивается полным комплектом сервисной аппаратуры и тестовых программ, запасным инструментом и соответствующим обслуживающим персоналом, которые совместно должны обеспечивать заданное время восстановления устройства?
2. При централизованном техническом обслуживании СВТ
3. При групповом обслуживании
4. При индивидуальном обслуживании
5. При каком профилактическом обслуживании выполняются операции, основная цель которых — продлить срок безотказной службы компьютера (т.е. выполняются операции по чистке и смазке всех основных элементов, переустановке микросхем, перестыковке разъемов и переформатированию жестких дисков)?
6. пассивном
7. активном
8. Диалоговое окно какой программы на рисунке – 1?
9. CPUCooL9
10. SiSoftware Sandra
11. Lavalys Everest
12. PC Wizard

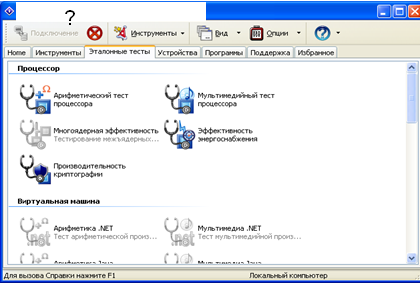


Рисунок - 1

1. Диалоговое окно какой программы на рисунке – 2?
2. CPUCooL9
3. SiSoftware Sandra
4. Lavalys Everest
5. PC Wizard

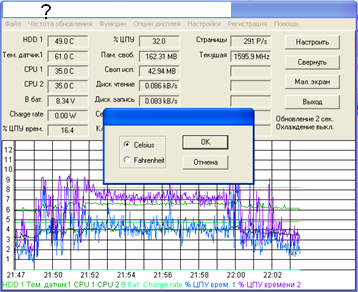


Рисунок- 2

1. Какая программа позволяет получить информацию об аппаратных компонентах и программном обеспечении компьютера, а также протестировать производительность оборудования? Выделить все варианты ответов.
2. POST (Power-On Self Test)
3. CPUCooL9
4. SiSoftware Sandra
5. Lavalys Everest
6. PC Wizard
7. Какую неисправность определила программа POST, выдав звуковой сигнал в виде, серии коротких сигналов?
8. Неисправна системная плата
9. Неисправен адаптер дисплея
10. Неисправна планка оперативной памяти
11. В сети установлена следующая неисправность: Нет доступа к Internet. Установите причину.
12. В сети используются различные имена рабочей группы
13. Служба доступа к файлам и принтерам сети не установлена
14. Параметры TCP/IP заданы неверно
15. Как проверить качество связи компьютера с сервером?
16. Достаточно использовать команду ping из командной строки, введя в качестве параметра IP-адрес сервера, если время ответа менее 0,1 мкс, то все нормально
17. Достаточно использовать команду ping из командной строки, введя в качестве параметра IP-адрес сервера, если время ответа менее1 мкс, то все нормально
18. Достаточно использовать команду ping из командной строки, введя в качестве параметра IP-адрес сервера, если время ответа менее10 мкс, то все нормально
19. Достаточно использовать команду ping из командной строки, введя в качестве параметра IP-адрес сервера, если время ответа менее100 мкс, то все нормально
20. Диалоговое окно какой программы на рисунке – 3?
21. LanSpy
22. NetView
23. LanScope
24. LanShutDown

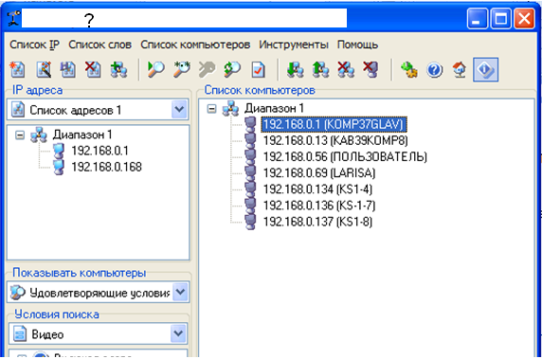


Рисунок - 3

1. Какая из ниже перечисленных программ является многопотоковым сканером ресурсов NetBios (разделяемых) и FTP, которая сканирует заданные диапазоны адресов и определяет доступность ресурсов(чтение, запись), позволяет искать ресурсы с заданным именем (Music, Video и т. п.), определяет наличие установленных сервисов (FTP, HTTP) на удаленном хосте?
2. LanSpy
3. LanScope
4. LanShutDown
5. NetView
6. Укажите название эталонных измерительных инструментов для диагностики и сертификации кабелей и кабельных систем, которые содержат высокоточный частотный генератор и узкополосный приемник (передавая сигналы различных частот в передающую пару и измеряя сигнал в приемной паре, можно измерить затухание в линии и ее характеристики).
7. Кабельные сканеры
8. Сетевые анализаторы
9. Приборы для сертификации кабельных систем
10. Тестеры
11. Что изображено на рисунке 4?
12. Схема зависимости точек отказа для пользовательского сервиса «Электронная почта»
13. Схема процедуры восстановления пользовательского сервиса
14. Схема зависимости точек отказа для пользовательского сервиса «Печать документов»
15. Схема зависимости точек отказа для пользовательского сервиса «Доступ в Интернет»

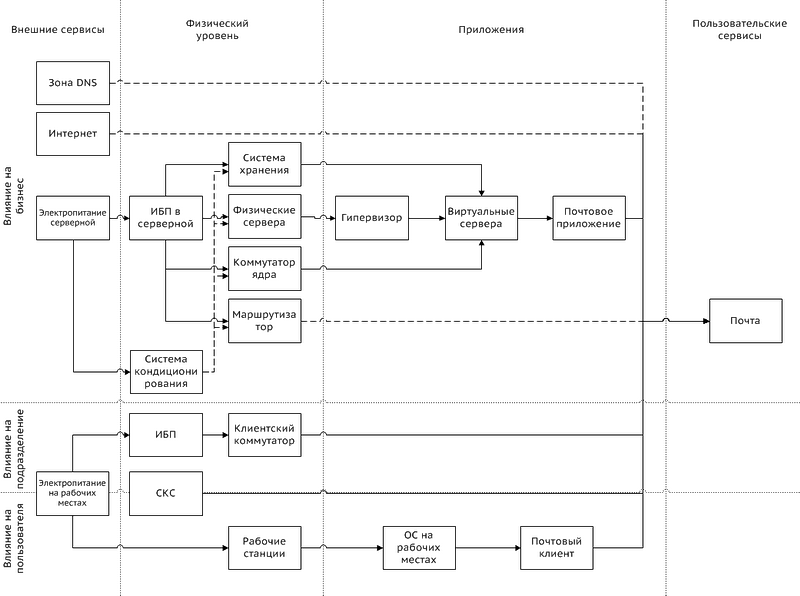


Рисунок – 4

1. На рисунке 5 схема подкючения сети 10.15.2.0 к Интернету через сервер. Выберите правильный ответ настроек сетевого адаптера, смотрящего во внешнюю сеть и сетевого адаптера второй сети
2. Настройки сетевого адаптера, смотрящего во внешнюю сеть - IP-адрес: 192.168.1.7; маска подсети: 225.225.225.0; шлюз: 195.34.32.116; Предпочитаемый DNS – сервер: 192.168.1.1; Альтернативный DNS – сервер: 195.34.32.116. Настройки сетевого адаптера второй сети - IP-адрес: 10.15.2.7; маска подсети: 225.225.225.0; шлюз: отсутствует; Предпочитаемый DNS – сервер: 192.168.1.1; Альтернативный DNS – сервер:отсутствует.
3. Настройки сетевого адаптера, смотрящего во внешнюю сеть - IP-адрес: 192.168.1.7; маска подсети: 225.225.225.0; шлюз: 10.15.2.0; Предпочитаемый DNS – сервер: 192.168.1.1; Альтернативный DNS – сервер: 195.34.32.116. Настройки сетевого адаптера второй сети - IP-адрес: 10.15.2.7; маска подсети: 225.225.225.0; шлюз: отсутствует; Предпочитаемый DNS – сервер: 195.34.32.116; Альтернативный DNS – сервер: отсутствует.
4. Настройки сетевого адаптера, смотрящего во внешнюю сеть - IP-адрес: 192.168.1.7; маска подсети: 225.225.225.0; шлюз: 192.168.1.1; Предпочитаемый DNS – сервер: 192.168.1.1; Альтернативный DNS – сервер: 195.34.32.116. Настройки сетевого адаптера второй сети - IP-адрес: 10.15.2.7; маска подсети: 225.225.225.0; шлюз: отсутствует; Предпочитаемый DNS – сервер: 195.34.32.116; Альтернативный DNS – сервер:отсутствует.

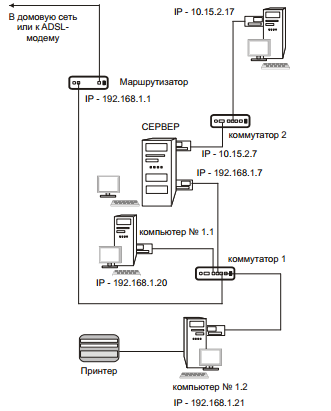


Рисунок - 5

Сформулировать ответы на следующие вопросы:

1. Как повысить эффективность работы жесткого диска?
2. Какие звуковые сигналы издает компьютер при включении в случае исправности и неисправности?
3. В каких допустимых диапазонах температур могут эксплуатироваться и хранится компьютеры?
4. Для чего предназначена сервисная плата HD-tester?

Ситуационная задача:

1. Есть ЛВС. СерверWindows 2003 Server SP1. КлиентыWindows XP

Pro SP2 (Celeron 1700/128). Используется коммутаторDLink DES 1226G.

При обмене информацией между компьютерами происходят потери дан-ных18—20%. Перезагрузка сервера и компьютеров не помогает. Укажите, возможные причины этого.

# Cписок литературы

1. А. В. Назаров, В. П. Мельников, А. И. Куприянов, А. Н. Енгалычев Эксплуатация объектов сетевой инфраструктуры. Учебник для [профессионального образования](http://www.chitai-gorod.ru/catalog/books/seria.php?Seria=%CF%F0%EE%F4%E5%F1%F1%E8%EE%ED%E0%EB%FC%ED%EE%E5%20%EE%E1%F0%E0%E7%EE%E2%E0%ED%E8%E5) / А. В. Назаров — Издательство: Академия, 2014: - 368 с.: ил.
2. Логинов М. Д. Техническое обслуживание средств вычислительной техники : учебное пособие / М. Д. Логинов, Т. А. Логино-ва. — М. : БИНОМ. Лаборатория знаний, 2010. — 319 с. :ил.
3. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для ВУЗов. / Олифер В.Г., Олифер Н.А. 4-е издание СПб: Питер, 2010 – 943 с.: ил.
4. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. / В.Г. Олифер, Н.А. Олифер 2-е издание СПб: Питер, 2001 – 672 с.: ил.
5. Поляк-Брагинский А. В. Локальные сети. Модернизация и поиск неисправностей: / Поляк-Брагинский А. В 2-е изд., перераб. и доп. — СПб.: БХВ-Петербург, 2009. — 832 с.: ил. — (Системный администратор)