Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 1 (104)/2002

Особенности планирования корпоративных сетей (стр. 2)

«Техосмотр» сети передачи данных (стр. 12)

СЕТЕВЫЕ ТЕХНОЛОГИИ

Особенности планирования корпоративных сетей

Юрий Наумов

СОДЕРЖАНИЕ

Введение

Корпоративная сеть — сложная система, включающая множество самых разнообразных компонентов: серверные комплексы, рабочие станции, системное и сетевое программное обеспечение, базы данных, активное и телекоммуникационное оборудование, структурированную кабельную систему. Основная задача состоит в том, чтобы эта громоздкая и весьма дорогостоящая система как можно лучше справлялась с теми функциями, которые на нее возлагаются.

Для поддержания сети в состоянии, соответствующем требованиям времени, необходимо внедрение разнообразных современных технических, технологических и организационных новшеств. Без таких изменений корпоративная сеть быстро устареет и не сможет функционировать так, чтобы эффективно выполнять все возложенные на нее задачи.

Рост, развитие и стремительное распространение сетевых технологий, заставляет пересмотреть устоявшиеся годами подходы к проектированию корпоративных сетей.

Сетевые технологии, разработанные за последнее время, подготовили фундамент для выполнения корпоративными сетями ряда задач, которые ранее решались при помощи отдельных систем. При помощи интеграции функций корпоративной сети с функциями таких подсистем, как корпоративная телефония, обработка факсимильных сообщений, видеоконференцсвязи и т.д., можно достигнуть значительной экономии накладных расходов, сконцентрировавшись на использовании сети в качестве единой информационной системы предприятия. Как следствие, на корпоративную сеть возлагается ответственность за выполнение всех информационных функций, которые составляют основу нормальной работы современного предприятия. Поэтому требования, предъявляемые к надежности функционирования сети, безопасности и целостности корпоративных данных, ужесточаются.

С ростом сложности и увеличением размера корпоративных систем обостряются проблемы их поддержки и сохранения средств, инвестированных в сетевую инфраструктуру. Главный вопрос состоит в том, позволит ли существующая инфраструктура корпоративной сети внедрять в дальнейшем новые технологии, и насколько существенные затраты потребуются для этого. В том случае, если при проектировании сети было уделено достаточное внимание гибкости ее архитектуры и заложен необходимый резерв для будущих применений, при внедрении новых приложений не будет возникать значительных проблем. Необходимая для этого гибкость закладывается на этапе планирования корпоративной сети, предшествующем проектированию.

Вторая важнейшая задача, решаемая на этапе планирования корпоративной сети, связана с происходящими качественными изменениями технологий, которые можно определить как "виртуализацию" сетевых ресурсов и средств сети. Логика функционирования корпоративной сети, построенной на основе современных технологий, не зависит от физической архитектуры. Это позволяет сделать сеть максимально гибкой, но только в том случае, если этим вопросам также было уделено соответствующее внимание на этапе планирования.

Планирование сети состоит в нахождении компромисса между потребностями предприятия, его финансовыми возможностями и возможностями сетевых и информационных технологий сегодня и в будущем.

При планировании сети необходимо принять решения по четырем группам вопросов:

- Какие новые решения и продукты являются стратегически важными? Какие решения в данных областях являются перспективными?
- Каким образом новые решения и продукты нужно внедрять в существующую сеть? На какие этапы необходимо разделить процесс перехода на новые решения и продукты, как обеспечить максимально безболезненное взаимодействие новых и старых компонентов сети?
- Как правильно выбрать внешних исполнителей при внедрении новых решений и продуктов? Как выбрать интеграторов, производителей и поставщиков программных и аппаратных продуктов, провайдеров услуг территориальных сетей?
- Как организовать процесс обучения сотрудников при переходе к использованию новых технологий и продуктов?

Таким образом, планирование современной корпоративной сети является ключевым этапом ее создания.

Этапы построения и эксплуатации сети

При современных темпах развития сетевых технологий корпоративные сети постоянно находятся в состоянии трансформации, как из-за внедрения новых задач, так и в связи с ростом размеров сети и количества пользователей. В таких условиях становится проблематично определить, как в дальнейшем совершенствовать сетевую инфраструктуру, и есть ли в этом необходимость.

Создание корпоративной сети (или ее модернизация) начинается с этапа планирования, на котором определяются задачи, которые будет призва-

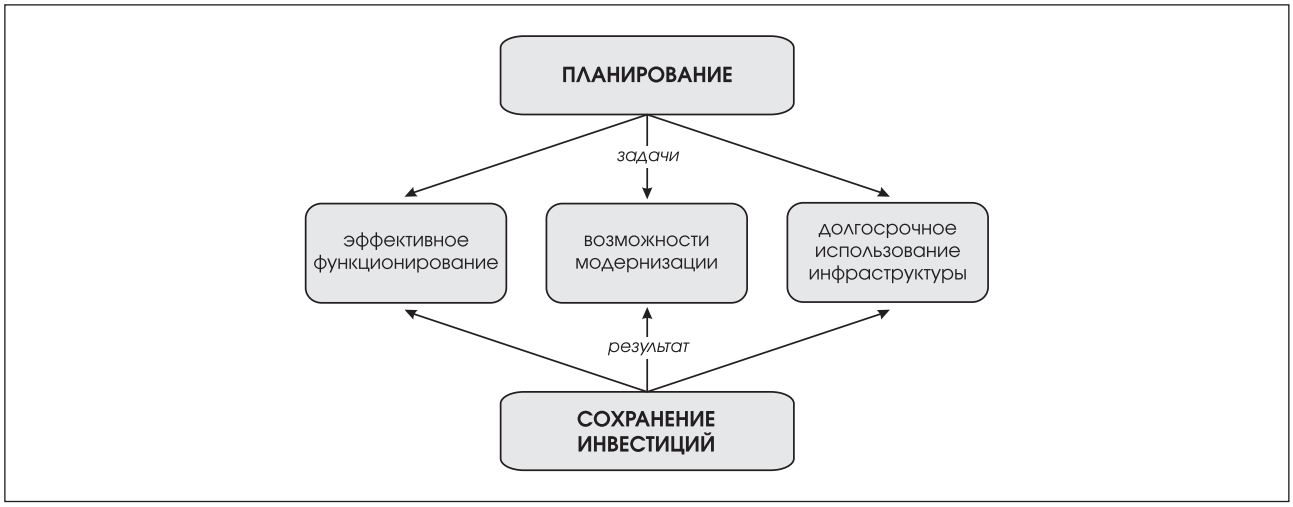

Рис. 1. Планирование сети

на решать сеть, составляется логическая структура сети с учетом дальнейшего роста, как количественного, так и качественного. Нельзя построить (модернизировать) хорошую корпоративную сеть без ясного понимания всех целей предприятия, без четкого плана достижения этих целей. Если модернизируется существующая сетевая инфраструктура, то этапу планирования должно предшествовать проведение аудита сети. Это необходимо для рационального использования имеющихся ресурсов и приведения сетевой инфраструктуры в соответствие текущим задачам бизнеса.

При проведении аудита сети необходимо:

- собрать нужную информацию и проанализировать текущее состояние сети и ее компонентов, что позволит выявить проблемы, требующие решения;
- подготовить документацию, нужную для эксплуатации сети;
- определить возможности модернизации сети и оценить выгоды от ее проведения.

Опыт проведения работ по аудиту сетей свидетельствует о том, что задача аудита носит не только технический характер: результатом аудита является выявление технических и технологических (эксплуатационных) проблем, оказывающих негативное влияние на бизнес-процессы. Задачи бизнеса с течением времени могут изменяться, а сетевая инфраструктура подвержена изменениям постоянно. Поэтому целесообразным является периодическое проведение аудита, вне зависимости от того, нуждается ли сеть в модернизации.

На основании работ, проведенных на этапе планирования, выполняется проектирование корпоративной сети: определяется ее физическая конфигурация. Реализация проекта состоит в построении сети и наложении на физическую инфраструктуру логической схемы функционирования, определенной при планировании.

В процессе эксплуатации сети часто возникает необходимость производить какие-либо незначительные изменения или внедрять прикладные системы. По мере накопления такого рода изменений корпоративная сеть перестает соответствовать тому, что было описано в документации, составленной при вводе сети в эксплуатацию. В результате сеть перестает функционировать в оптимальном режиме, часто могут возникать какие-либо аварийные ситуации. Внедрение некоторых прикладных задач или увеличение количества пользователей сети могут потребовать архитектурных изменений. Это предопределяет необходимость модернизации, которая начинается с проведения аудита корпоративной сети.

Таким образом, жизненный цикл корпоративной сети, проиллюстрированный на рис. 2, состоит из следующих этапов:

- планирования корпоративной ЛВС;
- проектирования;
- реализации проекта;
- периода эксплуатации сети;
- модернизация.

Современные корпоративные сети нуждаются в периодической модернизации как для решения вновь возникающих задач, так и для поддержания инфраструктуры в работоспособном состоянии. Кроме этого, постоянно уделяемое внимание не позволит корпоративной сети устареть морально. В противном случае сеть может потребовать дорогостоящего вмешательства, которое к тому же парализует рабочие процессы пользователей.

Требования к современным корпоративным сетям и их реализация

Традиционные требования, которые предъявляют пользователи к современным корпоративным сетям, следующие:

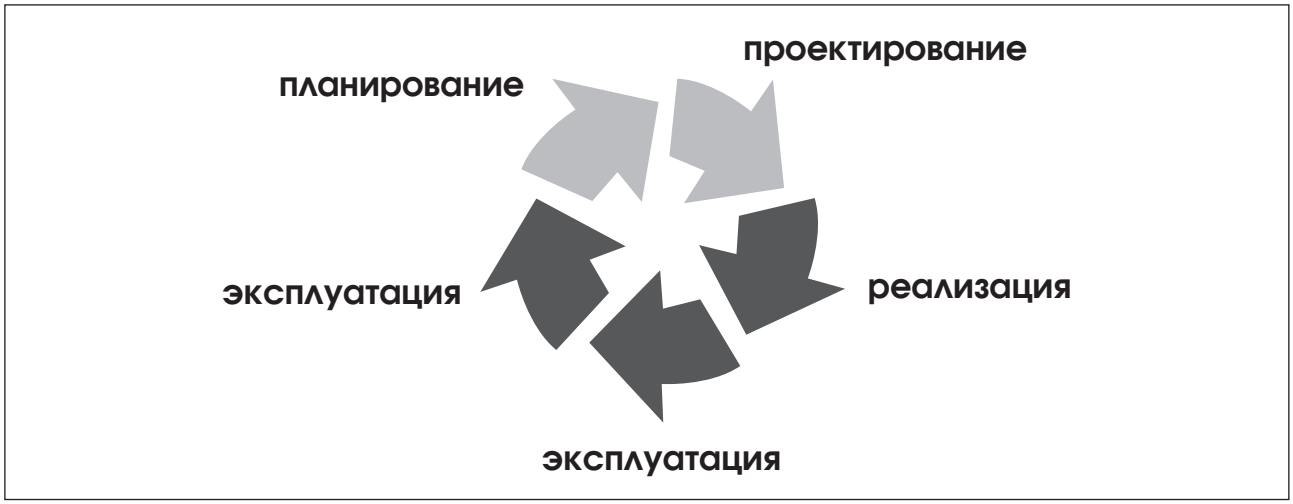

Рис. 2. Этапы жизненного цикла корпоративной сети

- высокая производительность;
- высокая доступность сетевых ресурсов и служб;
- обеспечение необходимого уровня безопасности;
- возможность управления ресурсами.

Эти требования в настоящее время ужесточились и трансформировались. Высокая производительность сети необходима для нормального функционирования приложений, порождающих неоднородный трафик. Доступность сетевых служб — ключевое условие успешного функционирования всего предприятия, учитывая исключительную важность функций сети и необходимость в своевременном доступе к информации. Повышенные требования к безопасности данных в первую очередь вызваны увеличением числа критических задач, выполнение которых зависит от работы корпоративной сети. По той же причине централизованное управление сетевыми службами рассматривается как обязательная подсистема, позволяющая динамически распределять ресурсы сети по мере необходимости.

Производительность сети

Требования прикладных задач к пропускной способности сети вызвали необходимость расширения полосы передачи данных до уровня гигабитных скоростей. Технология **Gigabit Ethernet** предоставляет возможность решить проблему пропускной способности и достигла стадии развития, на которой возможно использовать Gigabit Ethernet на уровне доступа конечных пользователей к сети. Однако увеличение пропускной способности сети решает задачу лишь отчасти. С одной стороны, возможный совокупный трафик пользователей сети к общему сетевому ресурсу может вызвать значительную утилизацию канала и потерю пакетов, вне зависимости от пропускной способности сети. Другим узким местом является взаимодействие локальных сетей в рамках корпоративной сети и доступность территориально-распределенных сетевых служб.

Во многих реальных ситуациях корпоративные сети не требуют полного перехода на более скоростные технологии передачи трафика. Другими словами, если загрузка сети близка к пределу пропускной способности, это не обязательно означает необходимость перехода на новую технологию передачи. В таких случаях, в первую очередь, нужно проанализировать направления информационных потоков и переконфигурировать сеть для максимальной оптимизации маршрутов передачи данных. Поспешные выводы о необходимости модернизации сети могут стать причиной ненужных расходов.

Утилизация среды передачи данных на грани максимума пропускной способности может привести к полной остановке работы сети: несколько сбойных пакетов требуют повторной передачи, проброс следующих пакетов задерживается, а продолжающие поступать на максимальной скорости пакеты не принимаются коммутаторами и сбрасываются, снова вызывая необходимость повторной передачи. Наконец, экспоненциальный рост числа повторяемых пакетов останавливает передачу новых данных. Именно такая ситуация складывалась несколько лет назад на магистралях национальных операторов связи в США, и это парализовывало работу Интернет на многие часы. Избежать подобных критических ситуаций из-за превышения пропускной способности каналов можно при использовании средств фильтрации и определения приоритетов передачи трафика.

Передаваемый трафик является разнородным: данные приложений, передача голоса, видео и других типов данных нуждаются в различных условиях передачи. Например, голосовой трафик критичен ко времени задержки в процессе передачи, однако, точность передачи не является опреде-

ляющим критерием, так как определенный уровень ошибок не оказывает влияния на качество воспроизведения голосовых сообщений. При передаче данных требования противоположны: отсутствие ошибок — обязательное условие, но определенная задержка пакетов на маршруте допустима. Эти требования относятся как к процессу передачи трафика между территориально-распределенными ЛВС, так и должны соблюдаться при передаче данных внутри ЛВС.

Фильтрация трафика и передача данных по приоритетам осуществляется при использовании технологии обеспечения качества обслуживания (**QoS – Quality of Service**). Набор средств, составляющих технологию гарантированного качества обслуживания (QoS), позволяет обеспечить контроль над потоками данных в сети. Рациональное использование полосы пропускания основано на обеспечении привилегированных условий проброса трафика критичных приложений или приложений с высокими требованиями к передаче данных за счет низкоприоритетного сетевого трафика.

Помимо использования QoS применяются специализированные подсети, решающие конкретные сетевые задачи. Трафик, порождаемый этими приложениями не подвержен влиянию со стороны прочих сетевых служб из-за использования выделенной подсети. Как правило, отдельные подсети применяются для обеспечения информационного обмена между корпоративными серверами (т.н. серверные сети), для организации процедур резервного копирования и для задач управления сетью. В любом из перечисленных вариантов применение выделенной сети основано на одном из двух соображений: критичность передаваемых данных или их огромный объем.

Технологии обеспечения качества обслуживания используются и при обеспечении взаимодействия ЛВС в составе территориально-распределенной корпоративной сети. Так как в абсолютном большинстве случаев при организации дальней связи используются ресурсы операторов услуг связи, обеспечение качества обслуживания осуществляется оператором. Необходимость планирования при этом не исчезает: результатом работ по планированию межсетевого взаимодействия является заключение с оператором определенного соглашения об уровне обслуживания (**SLA – Service Level Agreement**).

Магистральные каналы операторов связи на уровне агрегации трафика и уровне ядра сети имеют достаточную пропускную способность: каналы, которые могут быть предоставлены корпоративным абонентам, по своей пропускной способности сопоставимы со скоростями современных ЛВС. Проблему, как правило, составляет относительно низкоскоростной доступ к сети оператора связи (последняя миля).

Для построения ядра сети операторами связи сегодня широко применяется высокоскоростной транспортный протокол – технология уплотненного спектрального мультиплексирования (**DWDM – Dense Wavelength Division Multiplexing**). Технология DWDM позволяет, заменив установленное оборудование на оборудование DWDM, без организации новых оптоволоконных каналов, добиться скоростей передачи, во много раз превышающих скорости передачи данных в сетях SDH/SONET. DWDM имеет несколько реализаций. Относительно дешевый вариант DWDM, специально созданный для сетей масштаба города (**MAN – Metropolitan Area Network**), может быть использован в качестве технологии доступа ЛВС к сети оператора дальней связи.

В больших корпоративных сетях может быть использован один из двух других вариантов DWDM – **Long Haul** или **Ultra Long Haul**, расстояние передачи для которых составляет, соответственно, 600 и 2000 км без электрической регенерации сигнала.

Кроме того, что технология DWDM предоставляет новый уровень скоростей для связи между ЛВС, которые сравнимы со скоростями передачи данных в самих ЛВС, DWDM позволяет осуществлять обмен данными для приложений, которые по той или иной причине не могут быть наложены поверх стека протоколов TCP/IP. Например, при организации распределенных серверных ферм используются такие технологии передачи трафика, как **Fibre Channel**, **ESCON** или закрытые протоколы. Наложение трафика Fibre Channel и ESCON поверх IP-сети невозможно, и задача может быть решена при помощи DWDM. В результате территориально-распределенные центры обработки информации могут обладать высочайшей степенью надежности благодаря резервированию в режиме online. Помимо этого, используя закрытые протоколы, можно организовать связь, обладающую большой степенью защищенности.

В корпоративных сетях малых и средних предприятий решаются задачи, подобные задачам крупных предприятий, используются аналогичные прикладные системы. Основное отличие состоит в объеме передаваемого трафика. Характер трафика имеет те же особенности: неоднородность, чередование пиковых нагрузок и простоев. Технологии, используемые в малых и средних сетях, обладают теми же возможностями и особенностями, что и технологии, применяемые для построения крупномасштабных корпоративных сетей. Однако с экономической точки зрения применение дорогостоящих сетевых технологий и оборудования не является оправданным. Организация взаимодействия между ЛВС может быть осуществлена с помощью технологии дальней связи по Ethernet (**LRE – Long Reach Ethernet**), расстояние передачи для которой составляет до 100 км.

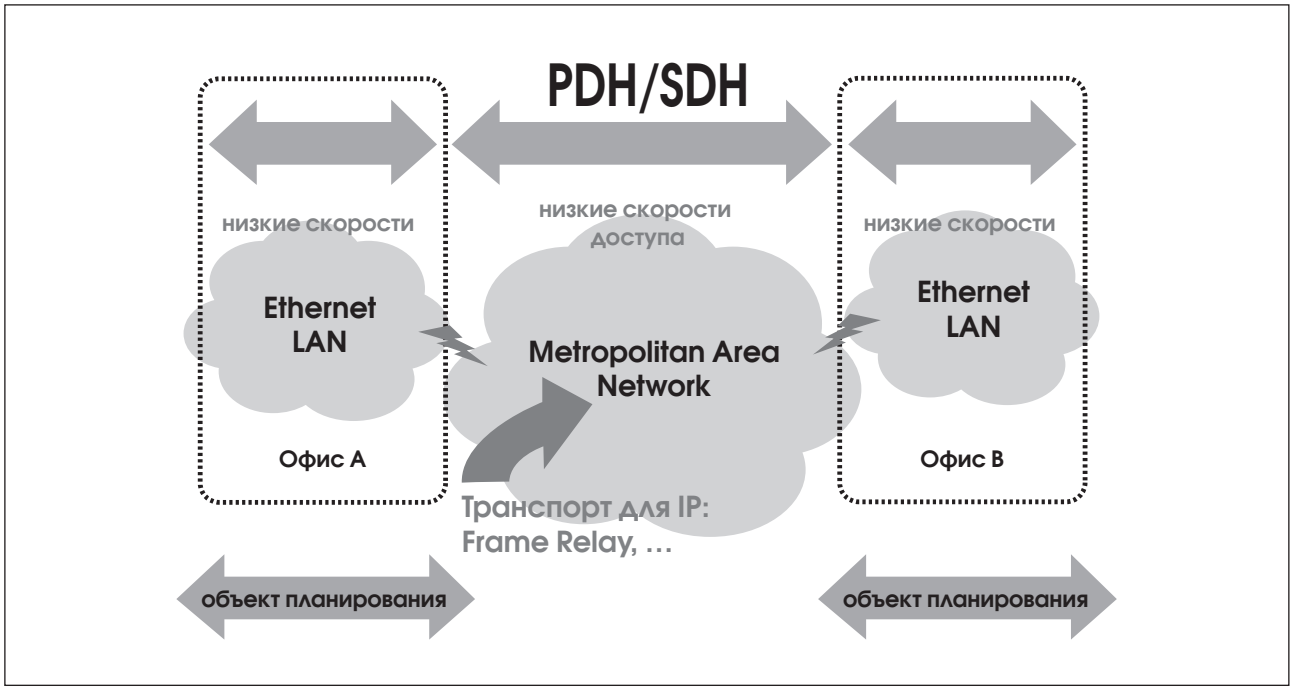

Рис. 3(а). Традиционные объекты планирования корпоративной сети

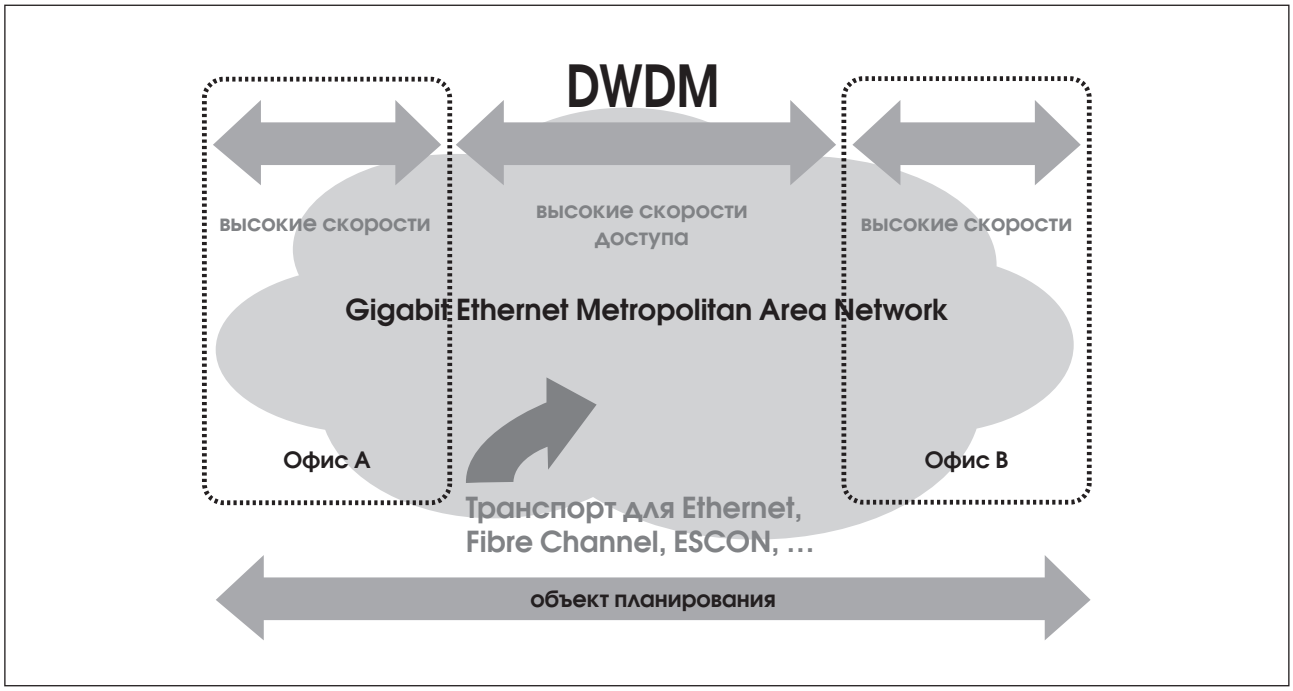

Рис. 3(б). Объект планирования современной корпоративной сети

Доступность ресурсов

Надежность работы корпоративной сети обеспечивается резервированием всех ее важнейших компонентов и устранением единых точек отказа, но этого не вполне достаточно для достижения требующегося уровня доступности. При возникновении сбоя первоочередной задачей является восстановление функциональности сетевых служб. Например, при выходе из строя какого-либо маршрутизирующего устройства требуется произвести настройки для введения в работу резервного оборудования. Это может занять значительное время, в течение которого нормальная работа сети будет нарушена. Автоматическое восстановление является наиболее предпочтительным решением. В настоящее время большинство крупных корпоративных сетей строится по схеме с маршрутизирующими коммутаторами в центре. В таких сетях обычно организуются виртуальные сети (VLAN), с маршрути-

зацией между ними, и предусмотрены избыточные связи между устройствами. Применение виртуальных подсетей исключает возможность использования протоколов обеспечения отказоустойчивости второго уровня (модели OSI), таких как **Spanning Tree**. Для обеспечения отказоустойчивости в современных сетях разработаны технологии уровня маршрутизации (третий уровень модели OSI), например, протокол VRRP (**Virtual Router Redundancy Protocol**), позволяющий выполнить необходимую при аварии переконфигурацию автоматически. Протокол VRRP регламентирует процесс переноса функций маршрутизации от одного устройства к другому при отказе первого. При использовании этого протокола резервный маршрутизатор включается в работу автоматически. При этом никаких дополнительных настроек на рабочих станциях делать не требуется. Следует заметить, что VRRP и виртуальный маршрутизатор — это понятия, относящиеся к интерфейсам, а не к устройствам. Поэтому для обеспечения отказоустойчивости всегда необходимо настраивать несколько виртуальных маршрутизаторов, относящихся к разным подсетям. Применение протокола VRRP позволяет существенно снизить время самовосстановления сети после аварии. Еще одним важным свойством протокола VRRP является поддержка функции распределения нагрузки — назначая рабочим станциям в качестве шлюзов различные виртуальные маршрутизаторы можно обеспечить балансировку нагрузок на маршрутизаторы сети.

Управление сетью

В современных корпоративных сетях на каждое устройство возложен целый ряд функций, работоспособность которых необходимо контролировать. Кроме этого, динамическое распределение сетевых ресурсов также требует применения централизованных систем управления и выделенной подсети управления.

Современные системы управления постепенно превращаются из пассивного средства наблюдения за состоянием сети в активный инструмент обеспечения качества обслуживания (QoS). Для увеличения производительности важнейших бизнес-приложений необходимо использовать решения на основе правил системной политики. Такие решения обеспечивают активный мониторинг сети, контроль выполнения соглашений об уровне обслуживания (SLA) и интеграцию с различными сетевыми операционными системами для управления трафиком индивидуальных пользователей.

Объект планирования

Требования, предъявляемые к современным корпоративным сетям, определяют объект планирования при построении сети. Объектами планирования являются не только ЛВС в составе корпоративной информационной системы, но и средства взаимодействия всех составляющих корпоративной сети. Изменение задач планирования корпоративных сетей проиллюстрированы на рис. 3(а) и 3(б).

Планирование корпоративных сетей

Планирование виртуальных подсетей

Решение задачи планирования подразумевает разработку логической структуры функционирования сети. На этом этапе необходимо разделить сеть на виртуальные подсети (VLAN) таким образом, чтобы это деление соответствовало инфраструктуре и бизнес-процессам предприятия. К планированию виртуальных подсетей следует также подойти с точки зрения разграничения доступа пользователей к ресурсам сети и корпоративным данным. Задача планирования VLAN является, с одной стороны, задачей разделения информационной инфраструктуры по предъявляемым требованиям и, с другой стороны, по функциональному назначению (рис. 4).

Средства обеспечения надежности

Ранее обеспечение необходимого уровня надежности выполнялось на физическом уровне (L2), средствами являлись такие протоколы как **Spanning Tree**. Эти средства были допустимы до тех пор, пока логическая структура сети являлась повторением ее физического строения — виртуальные подсети не использовались. Использование механизма VLAN, функционирующего на третьем уровне OSI — L3, позволило отделить логику работы сети от ее физического представления. Соответственно, средства обеспечения надежности физического уровня непригодны для сетей с использованием VLAN. С применением маршрутизирующих коммутаторов (L3) в качестве ядра сети средством обеспечения надежности сети стало совместное использование VRRP (или HSRP — Hot Standby Redundancy Protocol) с одним из протоколов маршрутизации. Например, OSPF. Сложность схемы обеспечения надежности многократно возросла и требует предварительного планирования и разработки планов устранения аварийных ситуаций.

Планирование QoS

Механизм обеспечения качества обслуживания должен функционировать согласно выработанной на этапе планирования политике, которая основывается на приоритетах задач и пользователей корпоративной сети. Первый этап планирования

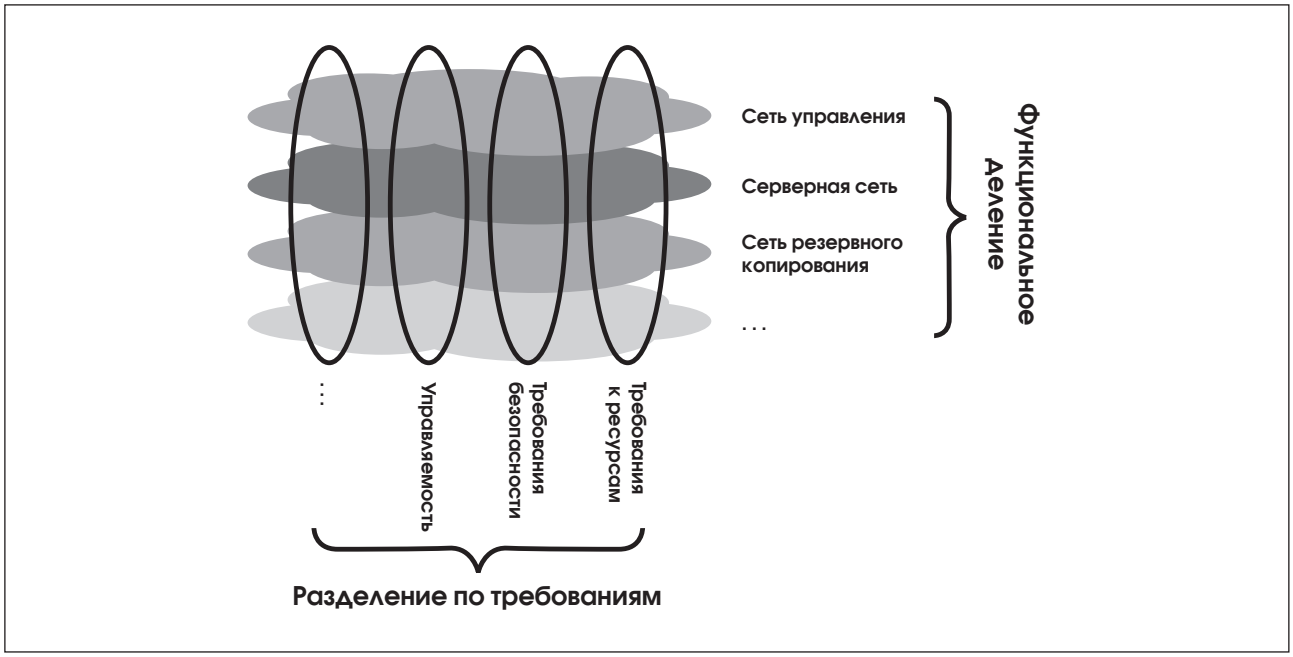

Рис. 4. Планирование виртуальных подсетей

QoS — формализация задач, которые будет выполнять информационная инфраструктура. Для полученного набора задач составляется набор приоритетов, отражающий потребности прикладных систем и пользователей в сетевых ресурсах (рис. 5).

Требования к СКС

Структурированные кабельные системы, согласно требованиям прикладных задач, должны планироваться с учетом достаточного резерва для будущих применений, особенно это относится к оптоволоконной части СКС. Под необходимым резервом подразумевается не только увеличение числа возможных соединений, но и увеличение пропускной способности.

С учетом требований надежности СКС должна иметь достаточное количество ресурсов для создания резервных соединений, в том числе оптоволоконных. Задача планирования СКС состоит в определении текущих потребностей и прогнозирования будущих нужд.

Недостаток ресурсов СКС может вызвать значительные расходы в связи с тем, что прокладывание дополнительного кабеля в существующие магистрали почти всегда затруднено, если вообще возможно.

Условия эксплуатации

Создание определенных удовлетворяющих эксплуатационным нормам условий функционирования сети является обязательным требованием, предъявляемым к проектируемым объектам.

Современное серверное и сетевое оборудование, образующее сегодня ядро корпоративных информационных систем, способно обеспечить исключительно высокий уровень надежности. Однако его эксплуатация предъявляет весьма жесткие требования к помещениям, в которых оно располагается.

С одной стороны, надежность работы серверного и сетевого оборудования сильно зависит от внешних условий — качества электропитания, запыленности, температурного и влажностного режимов.

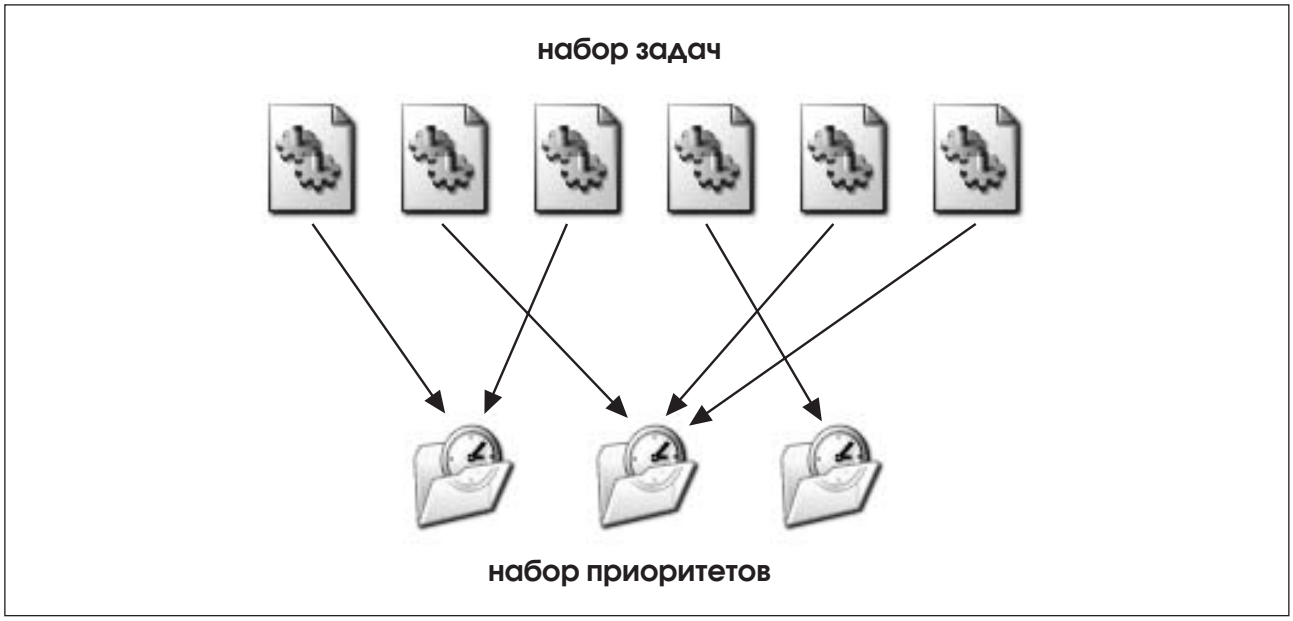

Рис. 5. Планирование политики QoS

С другой стороны, стоимость оборудования, размещенного в серверном помещении, и хранящихся на нем данных может быть весьма высокой и требующей принятия специальных мер для обеспечения их сохранности.

Наконец, в серверном помещении на ограниченной площади размещаются десятки единиц вычислительной техники и сетевого оборудования. За счет этого плотность и сложность коммуникаций оказывается на порядок выше, чем в других помещениях. Так как в процессе эксплуатации оборудование может многократно перемещаться, добавляться, удаляться и перекоммутироваться, то только принятие специальных мер позволит не допустить, чтобы через короткое время серверное помещение не превратилось в путаницу кабелей, удлинителей и временных соединений.

Решением поставленных задач является построение серверной комнаты — специализированного помещения, оборудованного инженерными подсистемами коммуникаций, охраны и жизнеобеспечения.

Подсистемы жизнеобеспечения включают:

- подсистему гарантированного электропитания критического оборудования;
- подсистему общего электропитания для технических средств, не требующих гарантированного бесперебойного электроснабжения;
- подсистему кондиционирования для обеспечения климатических условий эксплуатации оборудования;
- подсистему основного и резервного электрического освещения.

Охранные подсистемы, обеспечивающие сохранность оборудования и ограничение доступа к данным:

- подсистема пожарной сигнализации и пожаротушения;
- охранная сигнализация, подсистема контроля доступа и видеонаблюдения — для обеспечения регламентированного доступа к оборудованию и визуального контроля событий;
- укрепленные входные двери и окна.

Подсистемы коммуникаций:

- подсистема закладных и кабельных каналов — для защиты и упорядоченной прокладки слаботочных и силовых линий;
- кабельная подсистема — для формирования единой среды передачи информации;
- подсистема серверной сети — для обеспечения высокопроизводительного, защищенного обмена между серверами, и высоконадежного информационного обмена между пользователями и серверами;
- подсистема внутренней телефонии для обеспечения голосовой связи с персоналом, находящимся в серверной комнате.

Выделение специализированного серверного помещения обеспечивает необходимый уровень безопасности и контроля доступа к общим информационным ресурсам и оборудованию. Сами подсистемы проектируются с учетом возможного наращивания количества серверов и их подключений к ЛВС. Необходимая в процессе эксплуатации реконфигурация подсистем может проводиться без нарушения работы корпоративной сети.

Назначение серверных помещений, а также практика их проектирования и построения показывает, что некоторые из инженерных подсистем являются ключевыми. Набор ключевых компонентов серверных помещений включает кабельную

подсистему (в том числе закладные и кабельные каналы), систему гарантированного электропитания, систему кондиционирования. Остальные подсистемы серверного помещения не оказывают непосредственного влияния на условия эксплуатации сетевого и серверного оборудования и выбираются по усмотрению заказчика.

Выводы

Задача планирования сети заключается в оценке имеющихся на сегодня решений, предвидении того, что станет доступным и необходимым завтра, и объединении этих решений в эффективно функционирующую сеть. Только компания-интегратор, имеющая большой практический опыт, сможет профессионально спланировать и построить или модернизировать корпоративную сеть, учитывая всю специфику данной работы.

Учитывая трудоемкость планирования корпоративных сетей и особую важность тщательного выполнения задач планирования, а также тесную связь между корпоративной информационной системой и бизнес-процессами предприятия-заказчика, очевидно, что участие заказчика в процессе планировании сети необходимо.

Приложение. Разработка контракта с интегратором

Каждое решение в области построения корпоративных сетей индивидуально ввиду различий задач бизнеса, расположения объектов и многих других факторов. В соответствии с этим, каждый контракт на построение сети должен отражать особенности конкретного проекта. Однако требуется обратить должное внимание на основные моменты, характерные для любого контракта.

В контракте приводятся взаимные обязательства между компанией-интегратором и заказчиком. Контракт устанавливает и определяет детали гарантий, обслуживания, оплаты, лицензирования продуктов, определяет права собственности и условия поставок. Контракт является своего рода "страховым полисом" для сети заказчика.

Контракт формализует предложения интегратора. В нем юридически устанавливаются термины для приемки оборудования и программного обеспечения, оговариваются виды обслуживания, документации, сроки внедрения сети, создания проекта сети и ее реализации, цены и порядок тестирования.

Типовые пункты контракта включают:

- **Сетевое оборудование, системное программное обеспечение и приложения**

  В контракте перечисляются количество и характеристики сетевого и коммуникационного оборудования, которое должно быть установлено. Контракт фиксирует условия окружающей среды в офисах, где будет установлено оборудование, включая требования к температуре, влажности, и требования к электрическим параметрам.

- **Обслуживание**

  Если необходимо, чтобы обслуживание корпоративной сети производилось компанией-интегратором, это должно быть зафиксировано в контракте, включая количество технических специалистов, обслуживающих сеть предприятия, и гарантированное время обслуживания. Обсуждению подлежит и следующий вопрос: относится ли контракт на обслуживание и к обслуживанию сетевой аппаратуры, коммуникационных средств, системного программного обеспечения и приложений.

- **План внедрения решения**

  Включает в контракт сроки поэтапного внедрения.

- **Документация**

  Контракт должен определять состав документации. Для успеха любого проекта чрезвычайно важно правильное ведение документации. По окончании работ заказчику необходим исчерпывающий отчет с исчерпывающими данными о функционировании и правилах эксплуатации сети. Интегратор должен предоставить полную информацию для того, чтобы сотрудники компании-заказчика смогли самостоятельно решать возникающие проблемы в будущем.

- **Реализация решения**

  Контракт описывает технические спецификации проекта сети. Контракт должен содержать информацию о том, какие компоненты будут связаны и каким образом. Следует основывать эту часть контракта на технических аспектах предложений интегратора.

- **Тестирование**

  Инсталляционные и приемочные испытания являются очень важными, но часто поверхностными элементами периода анализа требований и заключения контракта. Инсталляционные испытания являются основными, они гарантируют, что сетевые компоненты работают по отдельности и все вместе. Приемочные испытания гарантируют, что система, построенная интеграторами, отвечает всем техническим и бизнес-требованиям.

- **Стоимость**

  Контракт определяет стоимость, сроки согласований стоимости и сроки оплаты.

«Техосмотр» сети передачи данных

Сергей Андронов

Поддержание сети передачи данных в состоянии эффективного функционирования - одна из главных задач, стоящих перед руководителями IT-подразделений любой компании.
Ведь не секрет, что по мере того, как компании становятся более технологичными, они попадают все в большую зависимость от своих IT-инфраструктур.
Определить соответствие возможностей сети передачи данных уровню поставленных перед нею задач главная цель аудита.

Зачем нужен сетевой аудит?

Одним из способов регулярного контроля состояния сети, своевременного документирования изменений, происходящих в ней, фиксирования ее текущего состояния и определения адекватности сети решаемым с ее помощью задачам, является сетевой аудит или сетевое обследование.

Одной из наиболее важных и сложных задач, решаемых при проведении сетевого аудита, является определение и согласование характеристик эффективности.

Опыт показывает, что под термином «эффективность» Заказчики понимают различные (прямые и косвенные) характеристики функционирования сети.

В одном случае показателем эффективности может быть скорость обмена данными между двумя рабочими станциями, а в другом — стоимость аренды каналов связи.

Именно поэтому задача определения и согласования характеристик эффективности является одной из первоочередных при проведении сетевого аудита.

Под термином «сетевой аудит» понимается системный процесс исследования и документирования сети с целью выявления возможностей повышения эффективности функционирования сети. Аудит не решает проблемы, возникающие в сети, результатом аудита, в первую очередь, является выработанный на основе обследования, согласованный перечень рекомендаций.

Сразу следует отметить, что специфика российского рынка сложила устойчивый стереотип термина «аудит», вызванный, в первую очередь, понятием «финансовый аудит». В отличие от финансового аудита, сетевой аудит содержит процесс обследования, а не процесс контроля со стороны фискальных органов власти.

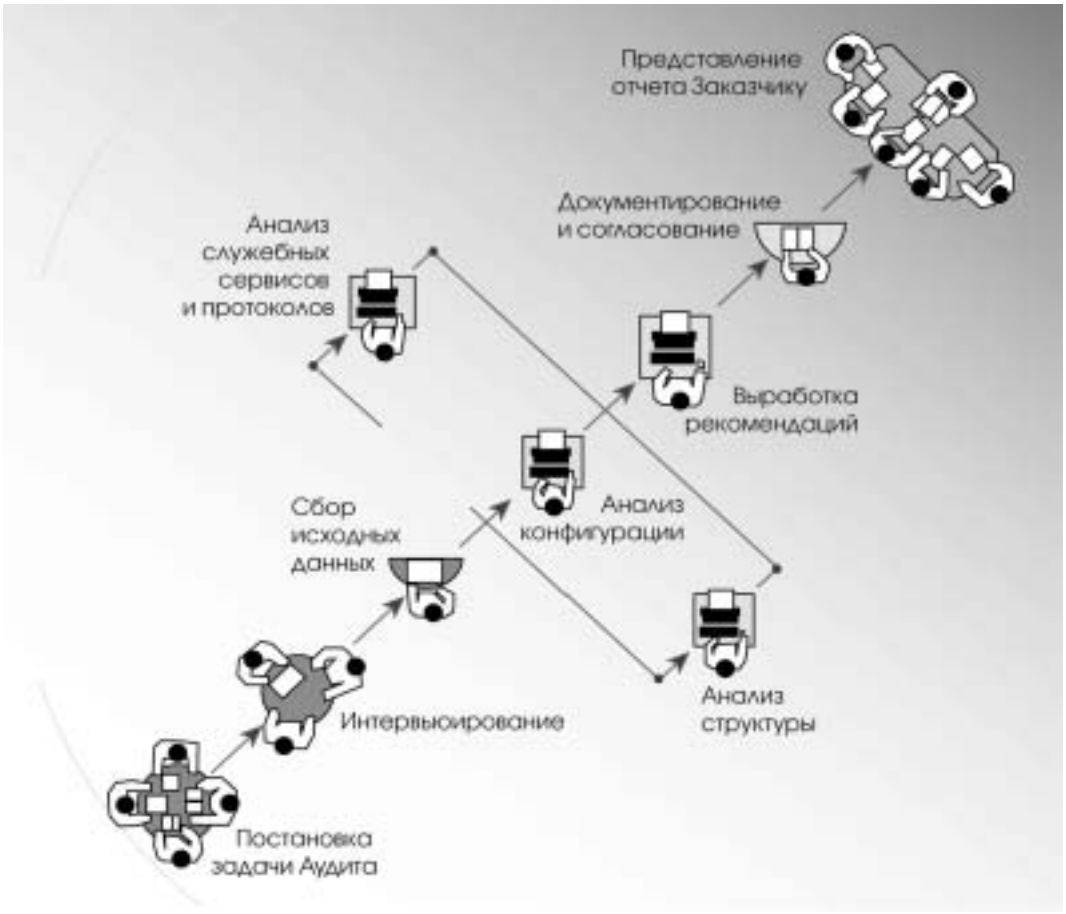

Рис. 1. Этапы Аудита

Шаг за шагом

Эффективность функционирования сети определяется комплексом технических и нетехнических характеристик. К техническим характеристикам относятся следующие:

- производительность, как отдельных устройств в сети, так и определенного комплекса логических сетевых узлов, сложным образом взаимодействующих между собой;
- надежность компонентов сети, которая, в свою очередь, может быть рассмотрена, как надежность отдельных устройств сети или как надежность неких логических схем, (например, схемы доступа к центральным серверам или сетевым сервисам);
- механизмы ухода от единых точек отказа;
- управляемость оборудования или сетевых сервисов.

Спектр нетехнических оценок эффективности работы сети более широк и менее формализован. В подобные оценки, например, могут входить такие понятия, как обоснование вложенных в сеть инвестиций или ожидаемое улучшение работы сотрудников компании.

Таким образом, одним из самых сложных и продолжительных технических этапов является этап формализации задачи проведения сетевого аудита (формализации термина эффективность) или в терминах процедуры сетевого аудита — этап подготовки к обследованию (сокращенный перечень всех этапов проведения сетевого аудита приведен в приложении). На этом этапе помимо привлечения экспертного, технического и административного (если мы говорим о не технических оценках эффективности) персонала компании-аудитора, требуется максимально плотная работа специалистов Заказчика с исполнителем работ.

После завершения формирования основных параметров оценки эффективности с Заказчиком, требуется в обязательном порядке согласовать методики (сценарии) проведения обследования, поскольку доступ к персоналу или оборудованию Заказчика должен быть регламентирован.

Среди наиболее часто применяющихся методов обследования можно выделить следующие:

- интервьюирование персонала Заказчика;

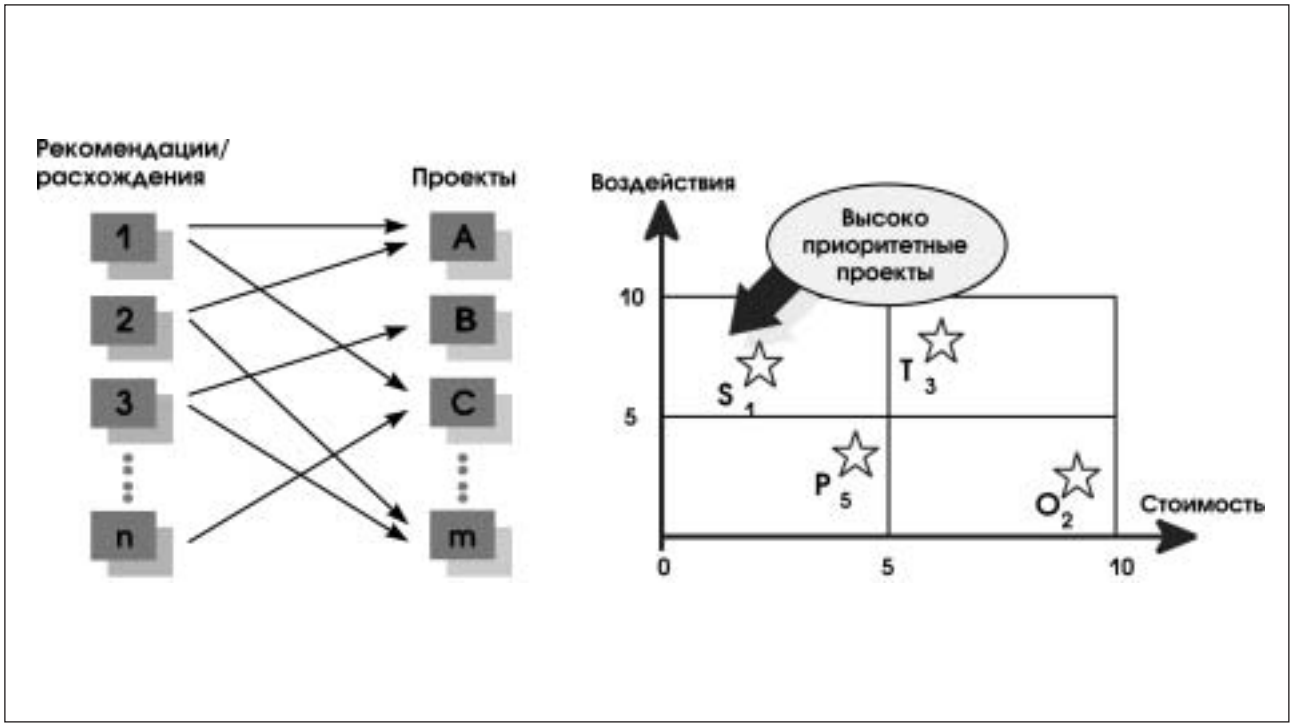

Рис. 2. Реализация рекомендаций

- ознакомление с конфигурациями и журналами работы оборудования;
- ознакомление с рабочей документацией и эксплуатационной документацией, имеющейся у заказчика.

Для большинства случаев проведений обследования, сценарии сбора информации уже существуют, и только 20-30% сценариев необходимо доработать для полной ориентации на конкретного клиента. Примером могут служить «опросные листы», используемые при интервьюировании персонала. Усредненная оценка доработки этих «опросных листов» составляет около 20%.

Процедура позиционирования сценариев, их согласование и планирование проведения также входит в стадию подготовки к обследованию. Сам же процесс сбора информации (этап обследования) является менее интеллектуальным и обычно требует привлечения инженерного состава исполнителя. Отличительная черта этапа обследования — использование инженерным составом максимального набора аппаратно-програмных средств сбора данных в сети (аппаратно-программные анализаторы, сетевые зонды и т.д)

К самым распространенным ошибкам этапа обследования можно отнести ситуацию, когда компания-аудитор доверяет Заказчику самостоятельно собрать большую часть информации по обследованию сети (конфигурационные файлы оборудования, результаты интервью, схемы соединений, данные об информационных потоках в сети и т.д.). Опасность заключается в том, что Заказчик, которому компания-аудитор доверяет провести такие работы, может по разным причинам выполнить их некачественно, но главное сознательно или несознательно «подтасовать» факты, как заказчику кажется, в свою пользу. Именно поэтому все сведения, полученные от Заказчика должны в обязательном порядке перепроверяться. Фальсифицированные исходные данные могут не только запутать процесс их анализа, но и прямым образом повлиять на результаты аудита.

Проверка и перепроверка полученных данных — основное правило этапа обследования.

Продолжительность этапа обследования сильно коррелируется с проводимыми в процессе обследования сценариями, так, например, сбор информации о характере информационных потоков в сети может занимать от одного дня до недели.

Следующим этапом является анализ полученных в процессе обследования данных и подготовка отчета. В отчет обязательно входят следующие разделы:

- Вводная часть, содержащая постановку задачи и описание текущей ситуации на основе собранных в ходе обследования данных.
- Анализ. В этом разделе изложена методика, по которой обрабатываются данные, и показано, как ее применение позволяет сделать выводы о причинах возникновения проблем в сети.

- Выводы. Приводятся выявленные в результате анализа причины, приводящие к возникновению проблем, решения которых ожидает Заказчик после исполнения рекомендаций аудита.
- Рекомендации. В этом разделе содержатся описания действий, которые необходимо совершить для решения проблем Заказчика. Это могут быть как технические мероприятия (перенастройка оборудования, установка дополнительного оборудования), так и организационные мероприятия (например, заключение сервисного контракта). Предоставляется план реализации рекомендаций.

Отчет готовится высококвалифицированными специалистами по аудиту сетей и сетевыми инженерами-проектировщиками. Все данные, входящие в отчет, в обязательном порядке согласовываются с Заказчиком.

Специфика изложения Вводной части Отчета позволяет Заказчику, помимо всего прочего, получить техно-рабочую и эксплуатационную документацию, отражающую текущее состояние сети.

При правильной постановке задачи, в процессе проведения сетевого аудита Заказчик может получить полный комплект проектной документации на сеть.

Это, в первую очередь, интересно компаниям, в которых этап построения сетей происходил минуя этап проектирования (для большей массы российских предприятий это характерно), или сетевое проектирование было выполнено не в полном объеме, или эксплуатационная документация существенно устарела или велась не полностью.

Итак, рекомендации, направленные на повышение эффективности функционирования сети получены, однако, не стоит забывать, что конечный приоритет по реализации рекомендаций, прогнозируемый эффект, расстановка акцентов на той или иной группе рекомендаций могут быть выполнены только самим Заказчиком. Именно поэтому конечный отчет, полученный в результате аудита, должен быть согласован и оговорен с Заказчиком. Не редки случаи, когда в процессе согласования Отчета оценки эффективности функционирования сети изменились. В этом случае этапы формирования оценок эффективности, подготовки к обследованию, обследования и подготовки отчета необходимо повторить.

Завершающим этапом проведения аудита является планирование дальнейших работ, связанных с реализацией рекомендаций. Наибольшее предпочтение следует уделять рекомендациям, выполнение которых влечет максимальный эффект при минимальной стоимости реализации. (рис. 2)

Процедура проведения сетевого аудита в мировой практике не нова. Во всем мире сетевой аудит является одним из ключевых процедур оценки адекватности сети решаемым с ее помощью задачам. Спланированное и периодическое проведение аудита, а также реализация рекомендаций, полученных в его результате, позволит не только повысить эффективность функционирования сетей Заказчика, но и получить актуальный набор эксплуатационной документации на сеть, обосновать потраченные инвестиции, усилить административную позицию IT-службы.

Приложение

В данном разделе приведены основные административные и технические этапы сетевого аудита, ориентировочные сроки и трудозатраты, необходимые для их проведения (рис. 1).

Этап 0. Постановка задачи

На этом этапе клиент изъявляет свое желание провести аудит информационной системы или, что бывает чаще, жалуется на проблемы вида «сеть работает, как мне кажется, хорошо, потому что все лампы зеленые, а приложения работают медленно». Самое важное, что должен понимать Заказчик на этом этапе — то, что аудит не решает проблем в сети, проблемы решаются при соблюдении рекомендаций, выработанных в ходе аудита.

Этап 1. Предварительное обследование

Данный этап обычно длится 1-2 чел./дня, в его ходе определяется вероятность успешного проведения аудита сети, даются ориентировочные временные оценки проведения аудита и принимается решение о проведении работ.

Этап 2. Заключение договора

В договоре оговаривается, что работы по аудиту завершаются отчетом, содержащим рекомендации, при соблюдении которых ожидается решение проблем заказчика с сетью, повышение эффективности ее функционирования.

Этап 3. Подготовка к обследованию

На этом этапе проводится выбор и согласование с Заказчиком методик обследования, подготовка и адаптация необходимых ресурсов, оп-

ределяются оценки эффективности функционирования сети.

Основными методами обследования являются:

- Интервьюирование сотрудников заказчика.
- Ознакомление с конфигурациями и журналами работы оборудования.
- Ознакомление с рабочей документацией, имеющейся у заказчика.

Данный этап требует привлечения высококвалифицированных специалистов Заказчика.

Продолжительность этапа составляет от 3 до 5 чел/дней.

Этап 4. Обследование

На этом этапе проводится интервьюирование сотрудников Заказчика, ознакомление с конфигурациями оборудования, журналами его работы, документацией на сеть.

Часть работ по сбору конфигурационных данных может быть передана сотрудникам Заказчика, однако все сведения, сообщенные заказчиком, должны быть перепроверены в обязательном порядке.

Время проведения зависит от методик, выбранных на этапе 3.

Этап 5. Анализ и выдача рекомендаций

На этом этапе проводится анализ собранных на предыдущих этапах данных и составляется отчет. В отчет должны входить следующие разделы:

- Вводная часть.
- Анализ.
- Выводы.
- Рекомендации.

Отчет готовится высококвалифицированными специалистами по аудиту сетей. Продолжительность этапа не более 5-7 рабочих дней.

Этап 6. Обсуждение рекомендаций, планирование дальнейших действий

На этом этапе проводится обсуждение рекомендаций и планируются дальнейшие работы, связанные с реализацией этих рекомендаций.

На этом этапе может проводиться бюджетное планирование, составление краткосрочных, среднесрочных и долгосрочных планов модернизации сети, планирование приобретения дополнительного оборудования, планирование заключения сервисных контрактов.

Следует отметить, что при необходимости (например, при выявлении новых параметров эффективности) процесс сбора данных и их анализа может быть повторен (возврат на этап 3).

Продолжительность определяется Заказчиком.

Этап 7. Заключение договоров

На этом этапе заключаются договоры на проектные работы, поставку оборудования, пуско-наладку оборудования, сопровождение систем. Договоры должны быть направлены на исполнение рекомендаций, выданных в отчете, составленном после завершения этапа 6.

Этап 8. Реализация договоров

Проводятся работы, предусмотренные договорами, заключенными на этапе 7. Следует отметить очередность реализации рекомендаций, выработанных в результате аудита. В первую очередь, это должны быть проекты, имеющие минимальную стоимость и оказывающие максимальное воздействие на информационную систему Заказчика.

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания Джет Инфо Паблишер

Главный редактор: Дмитриев В.Ю. *(vlad@jet.msk.su)*
Россия, 103006, Москва, Краснопролетарская, 6
тел. (095) 972 11 82, 972 13 32
факс (095) 972 07 91
email: JetInfo@jet.msk.su
http://www.jetinfo.ru

Подписной индекс по каталогу Роспечати 32555