Корпоративная сеть

3.1 Понятие и свойства корпоративной сети

Термин «корпоративная» («enterprise-wide networks» сеть масштаба предприятия) отражает с одной стороны величину сети, так как корпорация это крупное, многофилиальное, территориально раздробленное предприятие. С другой стороны, этот термин несет в себе смысл объединения, то есть корпоративная сеть это сеть, получившаяся в результате объединения нескольких, как правило, разнородных сетей.

Появление корпоративных сетей это хорошая иллюстрация известного философского постулата о переходе количества в качество. При объединении отдельных сетей крупного предприятия, имеющего подразделения в различных городах и странах, в единую сеть, многие количественные характеристики объединенной сети часто превосходят некоторый критический порог, за которым начинается новое качество. При этом число пользователей и компьютеров может измеряться тысячами, число серверов превышать несколько сотен, число записей в базе данных несколько миллионов, а расстояния между сетями могут оказаться такими, что использование глобальных связей становится необходимостью.

Кроме того, непременным атрибутом такой сложной и крупномасштабной сети является гетерогенность нельзя удовлетворить потребности тысяч пользователей с помощью однотипных элементов и однородных структур. В корпоративной сети обязательно будут использоваться различные типы компьютеров от мейнфреймов до персоналок, 3-5 типов операционных систем, с десяток различных коммуникационных протоколов, несколько СУБД и множество других приложений. Превышение количественными изменениями некоторой критической массы и породило новое качество корпоративную сеть.

Термин «корпоративность» связывает описанный вид сетей с принадлежностью их одному предприятию, причем крупному. Этот признак не является главным, а просто отражает тот факт, что крупномасштабная, гетерогенная и хорошо интегрированная сеть чаще всего получается в результате усилий предприятия при объединении своих отдельных сетей в единую информационную систему. Поэтому, если сеть обладает отмеченными выше

особенностями, но не принадлежит одной корпорации, то ее все равно можно назвать корпоративной.

Корпоративные сети возникли не на пустом месте. Сначала на предприятиях создавались небольшие локальные сети, используемые только небольшой группой сотрудников так называемые сети рабочих групп, затем они вырастали в сети отделов и кампусов (площадок).

Сети рабочих групп и отделов используются небольшой группой сотрудников, решающих общие задачи, например таких, как ведение бухгалтерского учета или осуществление маркетинговой деятельности. Главной целью сетей отделов является разделение ресурсов, таких как приложения, данные, лазерные принтеры и, возможно, низкоскоростные модемы. Обычно сети отделов имеют один или два файловых сервера и не более чем 30 пользователей. Сети отделов, как правило, не разделяются мостами на подсети (сегменты). Даже когда сети отделов соединены в корпоративную сеть, большая часть трафика локализуется в сети отдела, потому что именно в ней выполняется большая часть работы. Как правило, пользователи в 80% случаев обращаются к локальным ресурсам, а в 20% случаев - к удаленным ресурсам. Основными признаками сети рабочей группы или отдела являются однородность и небольшой масштаб.

Сети рабочих групп и отделов обычно создаются на основе какой либо одной сетевой технологии Ethernet, Token Ring, или, если в рабочей группе происходит обмен большими объемами информации (например, мультимедийными файлами), то высокоскоростные протоколы, такие как FDDI, Fast Ethernet или 100VG-AnyLAN.

Такая сеть обычно использует одну или максимум две сетевые ОС. Чаще всего это сеть с выделенным сервером NetWare или Windows NT/2000/2003, или же одноранговая сеть. Все пользователи рабочей группы или отдела пользуются СУБД одного типа, чаще всего настольными СУБД типа FoxPro, Access, dBase, Paradox, пользующимися файловым сервером для хранения разделяемых данных.

Сети отделов не требуют сложного управления, так как решаемые на этом уровне задачи поддержания сети относительно просты. В функции администратора входит добавление новых пользователей, устранение простых отказов, инсталляцию новых узлов и установку новых версий программного обеспечения. Сложные задачи, такие как установка принципиально нового программного обеспечения, выполняются консультантами или

представителями фирм- поставщиков. Средства управления сетей отделов хорошо отработаны и разнообразны, так же, как и сами сети отделов, уже давно применяющиеся и достаточно отлаженные. Такой сетью может управлять сотрудник, посвящающий обязанностям администратора только часть своего времени. В большинстве случаев администратор сети отдела не имеет специальной подготовки, но чаще всего он является тем человеком в отделе, который лучше всех разбирается в компьютерах и само собой получается так, что он занимается администрированием сети.

Пользователи и администраторы сетей отделов вскоре осознают, что они могут улучшить эффективность своей работы путем получения доступа к информации других отделов своего предприятия. Если сотрудник, занимающийся продажами, может получить доступ к характеристикам конкретного продукта и включить их в презентацию, то эта информация будет более свежей, и будет оказывать большее влияние на покупателей. Если отдел маркетинга может получить доступ к характеристикам продукта, который еще только разрабатывается инженерным отделом, то он может быстро подготовить маркетинговые материалы сразу же после окончания разработки.

Итак, следующим шагом в эволюции сетей является объединение локальных сетей нескольких отделов в единую сеть здания или группы зданий. Такие сети называют сетями кампусов.

Сети кампусов соединяют несколько сетей отделов внутри отдельного здания или внутри одной территории предприятия. Эти сети являются все еще локальными сетями, хотя и могут покрывать территорию в несколько квадратных километров. Сервисы такой сети включают взаимодействие между сетями отделов, доступ к базам данных предприятия, доступ к факс-серверам, высокоскоростным модемам и высокоскоростным принтерам.

Сети кампусов могут простираться на несколько километров, но при этом глобальные соединения не требуются. Сети кампусов имеют *позвоночник (backbone)* или главную сеть, и подсети, подобные ребрам. Для повышения производительности предприятия иногда используют маршрутизаторы, однако чаще подсети присоединяются к позвоночнику с помощью мостов или быстродействующих многопортовых мостов коммутирующих концентраторов (switching hubs).

В сети кампуса в каждом отделе осуществляется администрирование своими серверами, но сотрудники отдела

получают доступ к некоторым файлам и ресурсам сетей других отделов. Услуги, предоставляемые сетями кампусов, не ограничиваются простым разделением файлов и принтеров, а часто включают доступ и к серверам других типов, например, к факс-серверам и к серверам высокоскоростных модемов. Важным сервисом, предоставляемым сетями кампусов, стал доступ к корпоративным базам данных, независимо от того, располагаются ли они на серверах баз данных или на миникомпьютерах.

Именно на уровне сети кампуса начинаются проблемы интеграции. В общем случае, в отделах уже выбраны компьютеры и приложения (а, следовательно, и сеть), которые подходят им наилучшим образом. Однако, то, что подходит отделу продаж, может не подойти, например, отделу разработчиков. Типы компьютеров, сетевых операционных систем, сетевого аппаратного обеспечения могут отличаться в каждом отделе. Например, инженерный отдел может использовать операционную систему UNIX и сетевое оборудование Ethernet, отдел продаж может использовать операционную среду Novell и оборудование Token Ring. Очень часто сеть кампуса соединяет разнородные компьютерные системы, в то время как сети отделов используют однотипные компьютеры. Часто сети кампусов оказываются соединенными случайным образом. Например, два отдела, которые работают вместе, могут соединить свои компьютерные системы, а уже затем к ним захочет присоединиться третий отдел. Отсюда вытекают сложности управления сетями кампусов. Администраторы должны быть в этом случае более квалифицированными, их нужно специально обучать. В случае сбоев и отказов администратору уже недостаточно проверить надежность соединения разъема. Нужны более изощренные средства оперативного управления сетью.

Корпоративная сеть это объединения сетей нескольких кампусов. Многие существующие методы и подходы к решению традиционных задач сетей меньших масштабов для корпоративной сети оказались непригодными. На первый план вышли такие задачи и проблемы, которые в сетях рабочих групп, отделов и даже кампусов либо имели второстепенное значение, либо вообще не проявлялись.

Например, простейшая для небольшой сети задача ведения учетной информации о пользователях выростает в сложную проблему для сети масштаба предприятия. Использование глобальных связей заставило специалистов по локальным сетям выйти в новый для них мир телекоммуникаций. Особое значение приобрели задачи

преодоления гетерогенности в сети появились многочисленные шлюзы, обеспечивающие согласованную работу различных ОС и сетевых системных приложений. Для обеспечения совместной работы в сети различных коммуникационных протоколов стали широко использоваться многопротокольные маршрутизаторы и транслирующие мосты.

Расширился и круг услуг, предоставляемых конечному пользователю: кроме традиционных сервисов локальных сетей разделения файлов и принтеров в набор сервисов корпоративной сети обычно входят почтовая служба, средства коллективной работы, поддержка удаленных пользователей, факс-сервис, обработка голосовых сообщений, организация видеоконференций и пр. и пр.

Важное значение приобретает время реакции приложений в корпоративной сети при динамичном рынке для успешной борьбы с конкурентами решения необходимо принимать в реальном масштабе времени, что требует соответствующей организации корпоративной сети и ее приложений, в том числе СУБД, способной оперативно отрабатывать запросы к данным (поддержка режима On Line Transaction Processing, OLTP). В то же время в большой корпоративной сети обеспечить хорошее время реакции особенно сложно. Этому мешает высокая интенсивность потока запросов, создаваемых сотнями и тысячами сотрудников корпорации, необходимость производить поиск данных в базах колоссальных размеров, невысокая скорость глобальных линий связи между отделениями корпорации, замедление скорости взаимодействия в шлюзах, согласующих неоднородные компоненты различных подсетей.

Корпоративные сети состоят из продуктов, часть из которых можно назвать корпоративными. Понятие «корпоративности» продукта включает в себя несколько аспектов, среди которых важнейшими являются:

- масштабируемость, то есть способность одинаково хорошо работать в большом диапазоне различных количественных характеристик сети,
- совместимость с другими продуктами, то есть способность работать в сложной гетерогенной среде интерсети в режиме plug-and-play.

Очевидно, в корпоративной сети могут использоваться не только продукты класса корпоративных, но и продукты уровня отделов и рабочих групп. Корпоративные продукты используются на

магистрали сети, там, где они организуют разделение ресурсов между большим количеством пользователей, в пределе между всеми пользователями корпорации. Продукты же рабочих групп предоставляют свои ресурсы в основном только членам своей рабочей группы, поэтому их производительность, надежность и другие свойства могут быть гораздо более скромными, чем у корпоративных продуктов. Поэтому в одной и той же сети успешно справляются со своими обязанностями и СУБД Access компании Micosoft, работающая на персоналках и СУБД Oracle, работающая на суперсерверах компаний Digital, Hewlett-Packard или Tricord.

Корпоративные сети хорошо справляются со своими обязанностями не только из-за того, что включают корпоративные аппаратные и программные продукты, но и за счет особой организации и наличия специфических компонент, отсутствующих в небольшой сети. Рассмотрим некоторых специфических особенностей некоторых служб и подсистем корпоративной сети.

Подобно большой организации, корпоративная сеть нуждается в централизованном хранении как можно более полной справочной информации о самой себе (начиная с данных о пользователях, серверах, рабочих станциях и кончая данными о кабельной системе). Естественно организовать эту информацию в виде базы данных специального системного назначения. Данные из этой базы могут быть востребованы многими сетевыми системными приложениями, в первую очередь системами управления и администрирования. Кроме этого, такая база полезна при организации электронной почты, систем коллективной работы, службы безопасности, службы инвентаризации программного и аппаратного обеспечения сети, да и для практически любого крупного бизнес- приложения, в том числе и СУБД. Чем больше возможностей по хранению данных об элементах сети предоставляет справочная служба сетевой операционной системы, тем меньше потребности в отдельной системе администрирования СУБД. Хотя пока потребность в последней сохраняется, и в одной корпоративной сети одновременно работает несколько администраторов каждый из них администрирует свой слой сети коммуникационное оборудование, серверы, операционные системы, базы данных и т.п.

База данных, хранящая справочную информацию, предоставляет все то же многообразие возможностей и порождает все то же множество проблем, что и любая другая крупная база данных. Она позволяет осуществлять различные операции поиска,

сортировки, модификации и т.п., что очень сильно облегчает жизнь, как администраторам, так и пользователям. Но за эти удобства приходится расплачиваться решением проблем распределенности, репликации и синхронизации.

В идеале сетевая справочная информация должна быть реализована в виде единой базы данных, а не представлять собой набор баз данных, специализирующихся на хранении информации того или иного вида, как это часто бывает в реальных операционных системах. Например, в Windows NT имеется по крайней мере пять различных типов справочных баз данных. Главный справочник домена (NT Domain Directory Service) хранит информацию о пользователях, которая используется при организации их логического входа в сеть. Данные о тех же пользователях могут содержаться и в другом справочнике, используемом электронной почтой Microsoft Mail. Еще три базы данных поддерживают разрешение низкоуровневых адресов: WINS устанавливает соответствие Netbios-имен IP-адресам, справочник DNS сервер имен домена оказывается полезным при подключении к Internet, и наконец, справочник протокола DHCP используется для автоматического назначения IP-адресов компьютерам сети. Ближе к идеалу находятся справочные службы, поставляемые фирмой Banyan (продукт Streettalk III) и фирмой Novell (NetWare Directory Services), предлагающие единый справочник для всех сетевых приложений.

Наличие единой справочной службы для сетевой операционной системы один из важнейших признаков ее корпоративности. Важным свойством любого корпоративного приложения является поддержка такой справочной службы, то есть возможность пользоваться имеющимися в ней данными о пользователях, серверах и принтерах и не заводить своих собственных дублирующих справочников. В этом случае администратор имеет дело с одним хранилищем и одним представлением пользователей и ресурсов системы, и ему не приходится заводить одного и того же пользователя в нескольких справочниках например, операционной системы, СУБД и почты, что неминуемо приводит к путанице.

Другим характерным примером специфики корпоративных сетей является подход к построению и поддержке распределенных приложений. Сетевые распределенные приложения строятся, как известно, в модели клиент-сервер. При этом, в небольших сетях наибольшее распространение получила двухзвенная схема этой

модели: на сервере выполняется часть приложения, связанная с выполнением запросов к базе данных и к файловому сервису, а на клиентских машинах часть, реализующая логику обработки данных приложения, а также организующая интерфейс с пользователем. Большинство современных корпоративных систем управления базами данных представляют собой классический пример двухзвенной модели клиент-сервер: клиентская часть генерирует запросы на поиск данных в некоторой стандартной форме, чаще всего на языке SQL, и реализует логику обработки данных, а СУБД отрабатывает получаемых от клиентов запросы, осуществляя поиск данных в своих таблицах. Именно этот вариант модели клиент-сервер часто считается единственно возможным, а файловому серверу отказывают в титуле "клиент-сервер", хотя на самом деле здесь есть и клиент, и сервер, просто распределение функций между ними иное сервер выполняет централизованное хранение и поиск файлов, а клиент все остальное. Закрепление титула "клиент-сервер" за СУБД, выполняющей на сервере функции поиска записей, имеет основание - при этом резко сокращается трафик между клиентскими и серверными компьютерами, а также уменьшаются требования к вычислительной мощности клиентских компьютеров, правда, только для приложений с простой логикой обработки данных.

Однако, в корпоративных сетях обязательно имеются и сложные приложения, требующие для реализации логической обработки данных большой вычислительной мощности. Для них более подходящей является многозвенная схема, позволяющая разделить приложение на большее число частей. Например, приложение будет выполняться более эффективно, если освободить файл-сервер от выполнения запросов к базе данных и перенести СУБД на отдельный, более мощный компьютер. Из этих же соображений часто оказывается целесообразным перенести обработку логики приложения с персональных компьютеров также на отдельный компьютер большой вычислительной мощности - *сервер приложений*, так как вычислительная часть общих для корпорации программных систем может быть слишком емкой и неподъемной для рабочих станций клиентов.

Сервер приложений должен базироваться на мощной аппаратной платформе (мультипроцессорные системы, часто на базе RISC-процессоров, специализированные кластерные архитектуры). ОС сервера приложений должна обеспечивать высокую производительность вычислений, а значит поддерживать

многонитевую обработку, вытесняющую многозадачность, мультипроцессирование, виртуальную память и наиболее популярные прикладные среды. В этом отношении сетевую ОС NetWare трудно отнести к корпоративным продуктам, так как в ней отсутствуют почти все требования, предъявляемые к серверу приложений. В то же время хорошая поддержка универсальных приложений в Windows NT собственно и позволяет ей претендовать на место в мире корпоративных продуктов.

При построении распределенных приложений важным является способ взаимодействия частей *синхронный или асинхронный*. Синхронный способ, при котором часть приложения, выдавшая запрос, блокируется на время его выполнения, а серверная часть, получив запрос, должна немедленно заняться его выполнением, мало подходит для корпоративных приложений. Так как из-за больших расстояний (нередко с включением глобальных связей) время выполнения запроса может оказаться слишком большим, то клиентская часть приложения может быть приостановлена на долгое время, с другой стороны, большая интенсивность и случайный характер потока запросов может дезорганизовать работу сервера.

Поэтому корпоративные приложения эффективнее строить с применением асинхронной связи между отдельными частями. В этом случае необходимо иметь дополнительную службу (относящуюся к так называемому классу middleware), которая принимала бы запросы от клиентской части приложения, вела бы очередь таких запросов (желательно на диске для повышения отказоустойчивости) и планировала бы загрузку сервера. Асинхронный способ взаимодействия предъявляет менее жесткие требования к устойчивости физической связи между клиентом и сервером, что особенно важно для коммутируемых глобальных каналов, которые в общем случае всегда могут разделять части приложений в корпоративной сети. Примерами продуктов, которые поддерживают асинхронную передачу сообщений между клиентами и серверами, являются системы DECmessage Q от Digital Equipment, Message Express от Momentum Software и Copernicus от New Paradigm Software.

В корпоративных сетях для связи клиентских и серверных частей приложений используются и ряд других средств, относящихся к классу middleware, а не только упомянутые средства асинхронной обработки сообщений (message-oriented midleware, MOM). Широко используемые в сетевых операционных системах и сетевых утилитах

средства удаленного вызова процедур RPC также относятся к классу middleware. Кроме того, в этот класс входят мониторы обработки транзакций (transaction processing monitors, TP), осуществляющие прием потока запросов транзакций от клиентов и осуществляют балансировку этих потоков при передаче их на серверы баз данных, постановку их в очередь, архивацию и восстановление после сбоев. Перспективным, но пока еще не нашедшими практического воплощения являются средства брокеров запроса объектов (object request broker, ORB), которые работают подобно средствам асинхронной обработки запросов, но только с привлечением концепции объектно-ориентированной технологии.

Использование средств класса middleware в корпоративных сетях связано с необходимостью упорядочить хаотический поток запросов от огромного числа клиентов к большому количеству серверов, создать некоторые регулирующие эти потоки механизмы, подобно регулировщикам движения на оживленных городских магистралях.

Важную роль в обеспечении необходимых свойств корпоративной сети играет структура транспортной системы и ее согласованность.

Транспортная система корпоративной сети должна обеспечивать:

- передачу пакетов через разнородные сети с совершенно различными принципами организации транспортных операций,
- многоуровневое иерархическое построение (наличие магистрали сети, к которой присоединяются транспортные артерии нижних уровней),
- хорошую структуризацию за счет разделения сети на подсети небольшого размера с регулярными связями,
- поддержку быстрых протоколов, таких как FDDI, Fast Ethernet для устранения узких мест.

Объединение транспортных потоков отдельных сетей в корпоративной сети происходит за счет использования общего для всех сетей магистрального протокола сетевого уровня модели OSI, который правильнее было бы назвать межсетевым.

Введение сетевого уровня позволяет соединять сети, в которых работают различные протоколы канального уровня, при этом при передаче пакета из сети в сеть пакет сетевого уровня освобождается от оболочки канального уровня одного вида и заменяется оболочкой канального уровня другого вида. Информацией, на основе которой

делается эта замена, является номер сети и номер узла в сети, которая не меняется при переходе пакета из сети в сеть.

К сожалению, существует большого количество протоколов сетевого уровня, равно как и протоколов канального уровня. Все они решают одну задачу, но несколько разными способами, поэтому сетевым интеграторам и администраторам приходится в больших сетях иметь дело одновременно с несколькими сетевыми протоколами. Очень популярными протоколами сетевого уровня, использующимся для объединения сетей, входящих в корпоративную сеть, является протоколы IP и Novell IPX.

Протоколы сетевого уровня не являются протоколами только локальных сетей. С их помощью можно создавать интерсети, включающие как локальные, так как и глобальные сети. В каждой из этих сетей действуют свои правила внутренней доставки пакетов, а их совместная работа становится возможной благодаря наличию общего протокола сетевого уровня.

В последнее время роль объединяющего протокола сетевого уровня все чаще выполняет сетевой протокол IP, ведущий свое происхождение от сети Internet и операционной системы Unix. Для этого протокола существуют стандарты его использования над всеми основными протоколами канального уровня локальных сетей, таких как Ethernet, Token Ring, FDDI, Fast Ethernet и 100VG- AnyLAN, а также над протоколами глобальных сетей X.25, frame relay, PPP. Уже имеется спецификация для использования IP над протоколами таких перспективных сетей как ATM так называемая спецификацией Classical IP. Важным достоинством IP является его высокая эффективность при работе на относительно низкоскоростных глобальных линиях связей. Протокол IPX фирмы Novell был изначально разработан для объединения небольшого числа локальных сетей, поэтому он расточительно использует полосу пропускания линий связи и не так хорошо работает на магистралях корпоративных сетей, как IP, хотя Novell в последнее время предпринимает немало усилий для улучшения своего стека коммуникационных протоколов.

Структуризация транспортной подсистемы корпоративной сети и ее иерархическое многоуровневое построение это взаимосвязанные понятия. Структуризация это деление крупной системы на отдельные взаимосвязанные подсистемы, а иерархическое многоуровневое дерево это наиболее часто используемый тип структурирования транспортных связей в корпоративной сети.

Сеть, предоставленная самой себе, имеет свойство разрастаться хаотически. Такая стихийно создаваемая сеть плохо управляема и подвержена частым сбоям и отказам. Проблемы ранних сетей Ethernet, которые росли таким образом, хорошо известны: отсутствие технического обоснования проводимых изменений, их неполная документированность приводили к слишком большим затратам сил и времени на поиск причин возникающих отказов и сбоев. Масштабные же системы нужно особенно тщательно планировать и структурировать, выбирая для каждой сети соответствующие типы кабельных систем, протоколы и устройства соединения сетей повторители, мосты, маршрутизаторы и шлюзы.

Целью вычислительной сети является предоставление пользователям доступа ко всем ресурсам сети. Но не всем пользователям нужен постоянный доступ ко всем ресурсам. В большинстве случаев им нужен доступ к ресурсам сети их отдела, и только изредка - доступ к удаленным ресурсам. Поэтому сеть предприятия часто реализуется как совокупность подсетей. Большинство сетей разрабатывается на основе структуры с позвоночником, к которому через мосты и маршрутизаторы присоединяются подсети. Эти подсети обслуживают различные отделы. Подсети могут делиться и далее на сегменты для обслуживания рабочих групп.

Деление сети на подсети уменьшает общий трафик, повышает гибкость, увеличивает защиту данных и облегчает управление сетью:

- *Сегментация уменьшает общий сетевой трафик.* При достижении трафиком границы 30%-40% от полной пропускной способности, пользователи сети Ethernet начинают чувствовать значительное уменьшение производительности сети из-за постоянных коллизий. В сетях Token Ring также при достижении трафиком границы 20%-30% от предельной пропускной способности, конкуренция за доступ к кольцу начинает приводить к заметным задержкам.
- Пользователи взаимодействуют в основном с пользователями и ресурсами своего отдела. Здесь применимо правило 80/20 около 80% трафика является локальным, а 20% идет в удаленные сегменты. Путем сегментации сети на подсети отделов можно значительно уменьшить трафик, проходящий через всю сеть, и тем самым повысить производительность сети.
- *Подсети увеличивают гибкость сети.* При построении сети как совокупности подсетей каждая подсеть может быть адаптирована

к специфическим потребностям рабочей группы или отдела. При этом эти подсети могут взаимодействовать.

? *Подсети повышают безопасность данных.* Помещая пользователей на различные физические сегменты можно запретить доступ к некоторым ресурсам. Это уменьшает частоту появления пользовательских ошибок и внутреннего разрушения данных. С помощью сегментации можно обеспечить, например, циркуляцию трафика только в пределах финансового отдела. Устанавливая различные логические фильтры на мосты и маршрутизаторы, можно контролировать доступ к ресурсам. Мосты обеспечивают минимум средств управления доступом, маршрутизаторы обладают большими возможностями.

? *Подсети упрощают управление сетью.* Побочным эффектом уменьшения уровня трафика и повышения безопасности данных является упрощение управляемости сети. Проблемы локализуются внутри сегмента. Как и в случае структурированной кабельной системы проблемы одной подсети не оказывают влияния на другие подсети. Подсети образуют логические домены управления сетью.

Сети должны проектироваться на двух уровнях: физическом и логическом. Логическое проектирование определяет места расположения ресурсов, приложений и способы доступа пользователей к ресурсам. Физическое проектирование определяет точное задание типов устройств (марку и модель), мест прокладки кабеля, типов глобальных сервисов (протокол, тип передающей среды, типы модемов и т.д.). Соотношение между логическим и физическим уровнями проектирования в некотором смысле аналогично соотношению между функциональной и принципиальной электрическими схемами. Например, использование повторителя создает в сетях стандартов 10Base-T, 10Base-F и Token Ring физические сегменты отрезки кабеля, соединяющие по схеме "точка-точка" станции. Однако логически эти отрезки представляют по прежнему один сегмент, моноканал в случае Ethernet и логическое кольцо для сетей Token Ring. Применение же мостов, маршрутизаторов и шлюзов приводит к появлению логических сегментов, локализующих трафик внутри себя.

Как уже было сказано выше, наиболее часто встречающейся структурой коммуникационных связей в корпоративной сети является многоуровневая иерархическая структура. В чистом виде такая структура часто используется на уровне сетей кампусов, когда в корне сети располагается мощный модульный корпоративный

концентратор, выполняющий функции и маршрутизатора и моста и коммутатора по отношению к подключенным к нему сегментам сетей. Магистраль кампуса может в этом случае образовываться внутренней высокопроизводительной шиной корпоративного концентратора с пропускной способностью в несколько гигабит в секунду. Сети, подключаемые к центральному концентратору, образуются с помощью концентраторов масштаба отделов и рабочих групп.

Для объединения сетей кампусов глобальными связями используются, как правило, более нерегулярные структуры например, ячеистая структура, отражающая географию отделений корпорации и интенсивность трафика между ними. Но и здесь часто выделяется центральная, наиболее скоростная сеть, которая служит магистралью всей корпоративной сети, а сети остальных отделений присоединяются к ней менее скоростными линиями.

Особую важность приобретают для корпоративной сети вопросы *безопасности данных*. С одной стороны, в крупномасштабной сети объективно существует больше возможностей для несанкционированного доступа из-за децентрализации данных и большой распределенности «законных» точек доступа, из-за большого числа пользователей, благонадежность которых трудно установить, а также из-за большого числа возможных точек несанкционированного подключения к сети. С другой стороны, корпоративные бизнес-приложения работают с данными, которые имеют жизненно важное значение для успешной работы корпорации в целом. И для защиты таких данных в корпоративных сетях применяется весь спектр имеющихся средств защиты - избирательные или мандатные права доступа, сложные процедуры аутентификации пользователей, программная и аппаратная шифрация, локализация трафика и т.п.

Те же причины обуславливают и повышенные требования к высокой готовности и отказоустойчивости системы. Основные средства достижения этих свойств избыточность аппаратуры и данных на всех уровнях: кабельных связей, источников питания, процессоров, компьютеров, маршрутизаторов, репликация баз данных, кластеризация вычислений.

Как можно заметить, каждое из этих свойств корпоративной сети может быть важно и для сети небольшого масштаба. Например, можно найти такую область применения, для которой и для небольшой локальной сети очень важны требования безопасности данных и высокой готовности. Но для небольших сетей эти

требования могут быть важными или не очень, в зависимости от характера выполняемых ею задач. Для корпоративных же сетей выполнение этих требований обязательно всегда.

Создать крупномасштабную гетерогенную среду для проверки свойств корпоративности не только сложно, но и накладно. Поэтому существуют специальные лаборатории, которые занимаются тестированием и сертификацией продуктов на предмет пригодности их для работы в корпоративной сети. В частности, такие услуги и потребителям и производителям оказывает американская фирма The Tolly Group, которая с помощью специального оборудования может создавать сложную гетерогенную среду, соответствующую требованиям заказчика, и испытывать в ней новое оборудование или программную систему. Клиентами The Tolly Group являются компании-призводители, заинтересованные в получении лого "Enterprise Ready", причем не только новички, завоевывающие рынок, но и такие гранды как Cisco, IBM, Motorola-Codex, 3Com, Wellfleet и многие другие.

3.2 Архитектура Intranet, иерархия протоколов

Intranet это изолированная от Internet или скрытая за брандмауэром внутренняя корпоративная сеть и выполняющиеся в ней приложения на базе Internet. Сеть Intranet способна обеспечить оперативную доставку информации, поддерживать внутрикорпоративные коммуникации и даже предоставить доступ к центральной базе данных с настольных систем пользователей вне зависимости от компьютерной платформы или типа используемой сети. Помимо обеспечения внутренних коммуникаций Intranet дает возможность организовать взаимодействие с удаленными пользователями и мобильными сотрудниками, помогая поддерживать контакт с центральным офисом компании и ее филиалами.

Сети Intranet имеют модульную многоуровневую архитектуру. Верхние уровни используют сервисы нижних уровней. Вместе сетевой и платформенный уровни образуют инфраструктуру внутренней сети. Уровень приложений и уровни системного обслуживания предоставляют услуги конечному пользователю и обеспечивают автоматизацию производственных функций.

Сетевой уровень самый низкий уровень архитектуры. Состоит он из сетевого оборудования и логических компонентов ПО. Физическую сеть образуют такие компоненты как кабели, концентраторы, коммутаторы и маршрутизаторы. Логические

компоненты включают протоколы передачи данных, контроля ошибок, и управления потоками данных и маршрутизации. Вычислительные платформы, как клиентов, так и серверов составляют платформенный уровень архитектуры Intranet. Клиентами могут быть настольные ПК и рабочие станции, а также иные устройства пользователей.

3.2.1 Модель OSI

В модели OSI, называемой также моделью взаимодействия открытых систем (Open Systems Interconnection - OSI) и разработанной Международной Организацией по Стандартам (International Organization for Standardization - ISO), средства сетевого взаимодействия делятся на семь уровней, для которых определены стандартные названия и функции.

Эта модель содержит в себе по сути 2 различных модели:

- горизонтальную модель на базе протоколов, обеспечивающую механизм взаимодействия программ и процессов на различных машинах;
- вертикальную модель на основе услуг, обеспечиваемых соседними уровнями друг другу на одной машине.

В горизонтальной модели двум программам требуется общий протокол для обмена данными. В вертикальной соседние уровни обмениваются данными с использованием интерфейсов API.

Рассмотрим коротко основные функции уровней модели OSI.

Физический уровень (Physical Layer) выполняет передачу битов по физическим каналам, таким, как коаксиальный кабель, витая пара или оптоволоконный кабель. На этом уровне определяются характеристики физических сред передачи данных и параметров электрических сигналов.

Канальный уровень (Data-Link Layer) обеспечивает передачу кадра данных между любыми узлами в сетях с типовой топологией либо между двумя соседними узлами в сетях с произвольной топологией. В протоколах канального уровня заложена определенная структура связей между компьютерами и способы их адресации. Адреса, используемые на канальном уровне в локальных сетях, часто называют MAC-адресами.

Сетевой уровень (Network Layer) обеспечивает доставку данных между любыми двумя узлами в сети с произвольной топологией, при этом он не берет на себя никаких обязательств по надежности передачи данных.

Транспортный уровень (Transport Layer) обеспечивает передачу данных между любыми узлами сети с требуемым уровнем надежности. Для этого на транспортном уровне имеются средства установления соединения, нумерации, буферизации и упорядочивания пакетов.

Сеансовый уровень (Session Layer) предоставляет средства управления диалогом, позволяющие фиксировать, какая из взаимодействующих сторон является активной в настоящий момент, а также предоставляет средства синхронизации в рамках процедуры обмена сообщениями.

Уровень представления (Presentation Layer) . В отличии от нижележащих уровней, которые имеют дело с надежной и эффективной передачей битов от отправителя к получателю, уровень представления имеет дело с внешним представлением данных. На этом уровне могут выполняться различные виды преобразования данных, такие как компрессия и декомпрессия, шифровка и дешифровка данных.

Прикладной уровень (Application Layer) – это в сущности набор разнообразных сетевых сервисов, предоставляемых конечным пользователям и приложениям. Примерами таких сервисов являются, например, электронная почта, передача файлов, подключение удаленных терминалов к компьютеру по сети.

3.2.2 Структура стека TCP/IP

Параллельно с моделью OSI существует разделение протоколов в соответствии со стеком TCP/IP. ***Transmission Control Protocol/Internet Protocol*** (TCP/IP) – это промышленный стандарт стека протоколов, разработанный для глобальных сетей. Лидирующая роль стека TCP/IP объясняется его следующими свойствами:

- Это наиболее завершенный стандартный и в то же время популярный стек сетевых протоколов, имеющий многолетнюю историю;
- Почти все большие сети передают основную часть своего трафика с помощью протокола TCP/IP;
- Это метод получения доступа к сети Internet;
- Этот стек служит основой для создания intranet-корпоративной сети, использующей транспортные услуги Internet и гипертекстовую технологию WWW, разработанную в Internet;
- Все современные операционные системы поддерживают стек TCP/IP;

- Это гибкая технология для соединения разнородных систем, как на уровне транспортных подсистем, так и на уровне прикладных сервисов;
- Это устойчивая масштабируемая межплатформенная среда для приложений клиент-сервер.

Так как стек TCP/IP был разработан до появления модели взаимодействия открытых систем ISO/OSI, то, хотя он также имеет многоуровневую структуру, соответствие уровней стека TCP/IP уровням модели OSI достаточно условно. Протоколы TCP/IP делятся на 4 уровня.

Самый нижний (***уровень IV***) соответствует физическому и канальному уровням модели OSI. Этот уровень в протоколах TCP/IP не регламентируется, но поддерживает все популярные стандарты физического и канального уровня: для локальных сетей это Ethernet, Token Ring, FDDI, Fast Ethernet, 100VG-AnyLAN, для глобальных сетей – протоколы соединений "точка-точка" SLIP и PPP, протоколы территориальных сетей с коммутацией пакетов X.25, frame relay.

Следующий уровень (***уровень III***) – это уровень межсетевого взаимодействия, который занимается передачей пакетов с использованием различных транспортных технологий локальных сетей, территориальных сетей, линий специальной связи и т. п.

В качестве основного протокола сетевого уровня (в терминах модели OSI) в стеке используется протокол **IP**, который изначально проектировался как протокол передачи пакетов в составных сетях, состоящих из большого количества локальных сетей, объединенных как локальными, так и глобальными связями. Поэтому протокол IP хорошо работает в сетях со сложной топологией, рационально используя наличие в них подсистем и экономно расходуя пропускную способность низкоскоростных линий связи. Протокол IP является дейтаграммным протоколом, то есть он не гарантирует доставку пакетов до узла назначения.

К уровню межсетевого взаимодействия относятся и все протоколы, связанные с составлением и модификацией таблиц маршрутизации, такие как протоколы сбора маршрутной информации **RIP** (Routing Internet Protocol) и **OSPF** (Open Shortest Path First), а также протокол межсетевых управляющих сообщений **ICMP** (Internet Control Message Protocol). Последний протокол предназначен для обмена информацией об ошибках между маршрутизаторами сети и узлом - источником пакета. С помощью специальных пакетов ICMP сообщается о невозможности доставки пакета, о превышении

времени жизни или продолжительности сборки пакета из фрагментов, об аномальных величинах параметров, об изменении маршрута пересылки и типа обслуживания, о состоянии системы и т.п.

Следующий уровень (***уровень II***) называется основным. На этом уровне функционируют протокол управления передачей **TCP** (Transmission Control Protocol) и протокол дейтаграмм пользователя **UDP** (User Datagram Protocol). Протокол TCP обеспечивает надежную передачу сообщений между удаленными прикладными процессами за счет образования виртуальных соединений. Протокол UDP обеспечивает передачу прикладных пакетов дейтаграммным способом, как и IP, и выполняет только функции связующего звена между сетевым протоколом и многочисленными прикладными процессами.

Верхний уровень (***уровень I***) называется прикладным. За долгие годы использования в сетях различных стран и организаций стек TCP/IP накопил большое количество протоколов и сервисов прикладного уровня. К ним относятся такие широко используемые протоколы, как протокол копирования файлов FTP, протокол эмуляции терминала telnet, почтовый протокол SMTP, используемый в электронной почте сети Internet, гипертекстовые сервисы доступа к удаленной информации, такие как WWW и многие другие. Остановимся несколько подробнее на некоторых из них.

Протокол пересылки файлов **FTP** (File Transfer Protocol) реализует удаленный доступ к файлу. Для того, чтобы обеспечить надежную передачу, FTP использует в качестве транспорта протокол с установлением соединений – TCP. Кроме пересылки файлов протокол FTP предлагает и другие услуги. Так, пользователю предоставляется возможность интерактивной работы с удаленной машиной, например, он может распечатать содержимое ее каталогов. Наконец, FTP выполняет аутентификацию пользователей. Прежде, чем получить доступ к файлу, в соответствии с протоколом пользователи должны сообщить свое имя и пароль. Для доступа к публичным каталогам FTP-архивов Internet парольная аутентификация не требуется, и ее обходят за счет использования для такого доступа предопределенного имени пользователя Anonymous.

В стеке TCP/IP протокол FTP предлагает наиболее широкий набор услуг для работы с файлами, однако он является и самым сложным для программирования. Приложения, которым не требуются все возможности FTP, могут использовать другой, более экономичный протокол – простейший протокол пересылки файлов **TFTP** (Trivial

File Transfer Protocol). Этот протокол реализует только передачу файлов, причем в качестве транспорта используется более простой, чем TCP, протокол без установления соединения – UDP.

Протокол **telnet** обеспечивает передачу потока байтов между процессами, а также между процессом и терминалом. Наиболее часто этот протокол используется для эмуляции терминала удаленного компьютера. При использовании сервиса telnet пользователь фактически управляет удаленным компьютером так же, как и локальный пользователь, поэтому такой вид доступа требует хорошей защиты. Поэтому серверы telnet всегда используют как минимум аутентификацию по паролю, а иногда и более мощные средства защиты, например, систему Kerberos.

Протокол **SNMP** (Simple Network Management Protocol) используется для организации сетевого управления. Изначально протокол SNMP был разработан для удаленного контроля и управления маршрутизаторами Internet, которые традиционно часто называют также шлюзами. С ростом популярности протокол SNMP стали применять и для управления любым коммуникационным оборудованием - концентраторами, мостами, сетевыми адаптерами и т.д. и т.п. Проблема управления в протоколе SNMP разделяется на две задачи.

Первая задача связана с передачей информации. Протоколы передачи управляющей информации определяют процедуру взаимодействия SNMP-агента, работающего в управляемом оборудовании, и SNMP-монитора, работающего на компьютере администратора, который часто называют также консолью управления. Протоколы передачи определяют форматы сообщений, которыми обмениваются агенты и монитор.

Вторая задача связана с контролируемыми переменными, характеризующими состояние управляемого устройства. Стандарты регламентируют, какие данные должны сохраняться и накапливаться в устройствах, имена этих данных и синтаксис этих имен. В стандарте SNMP определена спецификация информационной базы данных управления сетью. Эта спецификация, известная как база данных MIB (Management Information Base), определяет те элементы данных, которые управляемое устройство должно сохранять, и допустимые операции над ними.

3.3 Виды Intranet приложений

Web-технология позволяет реализовать коллективный доступ к разнообразной информации, работающей в организации.

Информация, размещаемая на сервере, может принадлежать к следующим группам:

- общая политика компании;
- цели компании;
- списки товаров;
- списки контактных адресов и телефонов;
- разнообразная отчетная информация, предоставляемая на любом уровне с разграничением доступа к ней;
- планы и т.д.

Основой технологий Web является язык HTML, который допускает достаточно легкую конвертацию практически любой информации в его гипертекстовый вид. Так, текстовые процессоры, электронные таблицы и СУБД, при приложении незначительных усилий, могут сохранять информацию в таком формате. Кроме того, существуют программы, конвертирующие формат RTF в HTML.

При коллективном использовании информации вам просто не обойтись без баз данных и других хранилищ, если вы хотите обеспечить надежное управление информацией. Точно так же, как обычные плоские файлы не соответствуют потребностям большинства современных бизнес-приложений, так и структурированные каталоги HTML и графика не отвечают нуждам эффективного управления системой знаний в корпоративных сетях Intranet. Услуги по обработке транзакций становятся необходимыми по мере того, как сеть Intranet организации усложняется и начинает привлекаться к выполнению все большего числа жизненно важных для организации функций. С помощью этих услуг вы можете управлять и выполнять распределенные транзакции в разнородной вычислительной среде. Средства доступа к корпоративным базам данных могут быть организованы с помощью практически любых языков программирования (C, Perl, Basic и т.п.) с использованием стандартного интерфейса CGI.

Очень часто Intranet используют в качестве платформы для корпоративных телефонных каталогов. Издание телефонного каталога, впрочем, как и бюллетеня новостей, может стоить довольно дорого, особенно с увеличением размера компании. Размещение телефонного каталога в Intranet позволяет сократить эти затраты; информация может храниться в базе данных, ее легко искать и обновлять. Дополнительную информацию, в частности, о местонахождении, номерах факсов и телефонов, а также организационные диаграммы добавить не составляет труда.

Некоторые компании имеют даже программное обеспечение, с помощью которого пользователь может набрать телефонный номер и послать сообщение на алфавитно-цифровой пейджер прямо со страницы Web в Intranet.

Ни одна из компаний в своей работе не может обойтись без бланков и форм, но, к сожалению, большинство компаний по-прежнему используют одни и те же многочастные формы, с которыми они работают уже долгие годы. Intranet позволяет передавать электронные копии форм, после чего их нетрудно распечатать. В то же время с помощью Intranet формы можно заполнять интерактивно, т. е. так, что их вообще не нужно печатать. Специалисты компании могут написать программы, извлекающие всю информацию из форм и передающие ее непосредственно в базу данных или на мэйнфрейм, избавляя сотрудников от необходимости многократно вводить одну и ту же информацию.

Еще одной реализацией являются поисковые механизмы и агентские услуги, предоставляющие эффективные средства для извлечения и фильтрации данных из информационных ресурсов Intranet. Элементами такого рода службы являются механизмы поиска с использованием естественного языка и автоматизированные агенты для мониторинга и фильтрации информационных ресурсов. Это могут быть поисковые механизмы на базе одного и множества серверов, информационные роботы и средства перемещения в Web.

Протокол пересылки файлов FTP (File Transfer Protocol) реализует удаленный доступ к файлу. Для того, чтобы обеспечить надежную передачу, FTP использует в качестве транспорта протокол с установлением соединений - TCP. Кроме пересылки файлов протокол FTP предлагает и другие услуги. Так, пользователю предоставляется возможность интерактивной работы с удаленной машиной, например, он может распечатать содержимое ее каталогов. Наконец, FTP выполняет аутентификацию пользователей. Прежде, чем получить доступ к файлу, в соответствии с протоколом пользователи должны сообщить свое имя и пароль. Для доступа к публичным каталогам FTP-архивов Internet парольная аутентификация не требуется, и ее обходят за счет использования для такого доступа предопределенного имени пользователя Anonymous.

Электронная почта является новым видом обмена сообщениями. Главным преимуществом такого способа пересылки является оперативность. Если для доставки обычной почты требуется как минимум несколько дней, то доставка электронной почты

осуществляется в секунды. Получить ответ из любой точки земного шара можно за несколько минут, не говоря уж об обмене сообщениями внутри одной организации, в том числе, с сотрудниками, подключенными к системе по удаленному доступу.

Кроме этого, с помощью электронной почты можно пересылать не только текстовые сообщения, но и прикреплять различные файлы, например, графику, мультимедийные файлы и т.д.

В последнее время появилось много приложений для коллективной работы. Это средства анализа, проектирования и разработки программного обеспечения, финансовых структур, баз данных и др. Такие системы значительно облегчают процесс управления коллективной работой. Они могут содержать в себе информацию о

- членах команды разработчиков с указанием участков проекта, которыми они занимаются (для обеспечения связи между отдельными частями проекта);
- текущем состоянии проекта и отдельных его частей;
- спецификациях продуктов, общий вид интерфейса с пользователем, расписание проекта, планы и т.д.
- ключевые точки проекта.

Кроме этого, такие системы предусматривают блокировку отдельных модулей проекта, над которыми ведется работа, в них поддерживается система версий и ревизий с указанием имени разработчика, даты и предоставлением другой информации.

Благодаря Intranet число личных встреч для контроля за выполнением корпоративного проекта может быть значительно сокращено, а кроме того, эта инфраструктура позволяет информировать участников проекта о результатах работы их коллег.

Комплексные приложения с групповым способом общения включают группы новостей с возможностью прямого обмена информацией между различными членами группы и предоставлением доступа к определенной информации для пользователей вне группы. Группы новостей - это не просто электронная почта. Группы новостей позволяют получать сообщения, предварительно выбирая их из общей группы сообщений по различным признакам. Пользователи подписываются на интересующие их группы новостей и могут получать информацию о появляющихся новостях. В случае, если та или иная новость заинтересует пользователя, он может заказать сообщение полностью и получить его как обычное письмо по электронной почте.

Большинство средних и крупных организаций ежедневно или ежемесячно выпускают бюллетень новостей. Хотя компьютеры упрощают эту задачу, общепринятые методы распространения подобных материалов по-прежнему требуют значительных затрат времени, не говоря уж о расходе бумаги и средств на копирование и рассылку бумажных документов. Распространение бюллетеня новостей компании через Intranet не только сокращает затраты на рассылку, но и позволяет подготовить более информативную и эффектную публикацию, включив, к примеру, мультимедийные вставки, что невозможно сделать на бумаге. Бюллетень информации с видео- и аудиофрагментами выглядит значительно более привлекательно.

Зачастую общие внутрикорпоративные материалы, к примеру информация о привилегиях, расписание выплат, меню кафетерия и списки рабочих мест, рассылаются в виде уведомлений всем сотрудникам или вывешиваются на доске объявлений в центральном офисе. Возможность обратиться к этой информации непосредственно с настольной системы делает ее не только более оперативной и доступной, но и своевременной, а ее распространение в итоге обходится компании значительно дешевле.

Огранизуемые внутри организации форумы позволяют получать ответы на неразрешенные вопросы в том случае, если один из сотрудников знает или находит решение. Это еще один способ обмена информацией, не требующий личных встреч, а организованный с рабочего места сотрудника.

Объединение Intranet с коммерческими телекоммуникационными системами открывает путь к управлению настольными телефонными системами. Intranet сможет запоминать и набирать номера, а также поддерживать такие функции телефонии, как селекторные совещания. Включение идентификатора пользователя сделает информацию о звонящем доступной еще до того, как сотрудник снимет телефонную трубку. В ближайшем будущем сеть в сочетании с Intranet станет телефонной системой, связывающей все подразделения компании, поддерживающей проведение аудио- и видеоконференций в любом помещении компании.

3.4 Анализ существующей системы при построении Intranet

Чтобы найти оптимальное решение для Intranet, вы должны рассмотреть внутреннюю сеть с точки зрения применения ее в

деятельности вашей организации, т. е. сравнить текущие и потенциальные функции и услуги Intranet с задачами и планами организации в целом. Ваша цель - выявить те направления деятельности, которые выиграют от применения технологии Intranet (поставка изделий, обслуживание клиентуры, связь между сотрудниками и т. д.).

Определив производственные выгоды, следует подумать, как применить технологию в каждой конкретной области деятельности, чтобы эти выгоды стали реальными. Вот где важна оценка технологии Intranet. Учет и анализ аппаратных и программных средств, применяемых в инфраструктуре системы, поможет определить, насколько они подходят для приложений Intranet. Оценка технологии должна проводиться с позиций ваших требований к Intranet в отношении, например, масштабируемости, производительности, назначения, безопасности и управления; результаты такого анализа могли бы быть использованы при планировании архитектуры и технологии, реализация которых позволила бы получить намеченные выгоды.

Анализ топологии сети

Возможно, первое, что следует проанализировать, так это такую составляющую инфраструктуры организации, как сеть. Определите топологию существующей сети вашей организации, а именно: какие технологии применяются на магистрали, в локальных и территориальных сетях, установите применяемые в этих сетях протоколы и приходящуюся на каждый из них долю активности сети. Следует замерить загрузку сети на нормальном и пиковом уровнях, с тем чтобы установить распределение нагрузки и узкие места сети, а также другие проблемы со связью, которые могут возникнуть из-за дополнительного трафика вследствие активности пользователей Intranet.

Используемое пространство IP адресов

Занимаясь оценкой технологии, важно также учитывать, планируется ли подключение Intranet к Internet. Для того чтобы сетевой узел мог работать в Internet, он должен иметь уникальный IP-адрес. Такие адреса выдаются Центром сетевой информации Internet (InterNIC). Если ваша компания уже использует протокол TCP/IP в своей внутренней сети, но не подключена к Internet, то может оказаться, что ее узлам были присвоены IP-адреса, на которые не получено разрешение InterNIC. Тогда в случае подключения вашей организации к Internet такие IP-адреса могут вступить в конфликт с

теми, что уже были выданы центром InterNIC другим компаниям. В такой ситуации вы должны либо присвоить узлам зарегистрированные адреса, либо скрыть их с помощью брандмауэра и виртуальной частной сети.

Если ваша компания до сих пор этого не сделала, запросите (даже не имея намерений подключиться в ближайшем будущем к Internet) у InterNIC подходящий блок адресов, а также имя собственного домена. Имена доменов товар дефицитный; компании быстро расхватывают желанные имена и адреса. И, готовясь к расширению в будущем, ваша организация должна придерживаться принятых правил адресации и наименования.

Роль защиты сети и ее укрепление

В ходе оценки технологии надлежит определить, насколько надежна защита сети и как ее можно укрепить в связи с введением Intranet. Обычно сеть Intranet подсоединяется к Internet через брандмауэр, защищающий Intranet от нападений со стороны Internet. Брандмауэр представляет собой интегрированную систему сетевой безопасности, благодаря которой одну сеть можно легко подключить ко многим, причем первая останется закрытой и недоступной извне.

Если у вашей организации еще нет определенной политики относительно брандмауэра, то разработайте ее. Однако учтите, что установка брандмауэра предполагает компромисс между защитой и управляемостью. Кроме того, маршрутизаторы должны иметь списки прав доступа для защиты сети, а агенты по мониторингу и аудиту выдавать предупреждения в случае возникновения каких-либо проблем. Результатом такой оценки сети будет схема, в которой имеющаяся сетевая среда встроена в новую структуру Intranet.

Эксплуатируемые организацией системы

Далее, обратите внимание на эксплуатируемые вашей организацией системы. Проанализируйте вычислительные технологии настольных систем, рабочих станций и серверов, обращая особое внимание на их способность работать с IP-трафиком. После анализа их операционных систем, типов аппаратного обеспечения и функций сервера (например, электронная почта, печать, файлы, приложения и т. д.) вы сможете составить более четкое представление относительно того, насколько они впишутся в IP-среду сети Intranet.

Вам потребуется также принять решение относительно систем и процедур управления модернизацией, распространением и лицензиями на ПО. Поскольку TCP/IP - жизненно важный компонент новой сетевой стратегии, ваши системы должны поддерживать эти

протоколы в их новейшей версии для Intranet. Совместимость систем электронной почты - одна из главных забот в разнородных системах. Продумайте вопрос об использовании интегрированной системы, если таковая еще не реализована.

Наличие Web-активов

Наконец, определите, какими Web-активами ваша организация располагает (включая наличные серверы и браузеры Web) на предмет емкости и возможности связи со всеми корпоративными узлами, IP-возможностей и производительности при каждодневной эксплуатации. При необходимости, если того требуют новый трафик и подключение сетей, не использующих протокол IP, дайте рекомендации касательно модернизации ваших систем.

Результаты анализа инфраструктуры должны содержать:

- полную опись серверных систем, рабочих станций и настольных компьютеров;
- необходимые интерфейсы, которые должны иметь эти машины;
- план интеграции их в новую сеть Intranet.

Анализ приложений

Следующий шаг состоит в анализе информационной структуры вашей организации. Соберите сведения о важнейших аспектах информационной системы (включая владельцев, создателей, пользователей и тех, кто поддерживает данные), о правах доступа, контроле за изменениями и улучшениями, о форматах и средствах хранения данных. По завершении такого анализа вам станет понятнее, какие данные надо ввести в формы, готовые для Intranet, у кого и у чего есть необходимость доступа к этим данным. Теперь можно заняться составлением подробного плана интеграции данных в Intranet, а также плана реализации с описанием процесса интеграции.

3.5 Intranet разных масштабов

3.5.1 Intranet небольшой корпоративной сети

Компоненты Intranet различаются почти столь же существенно, как и организации, их использующие. Во многих случаях сеть Intranet оказывается побочным детищем других проектов, причем она развивается снизу вверх, а не сверху вниз. Зачастую отдельный сотрудник или подразделение осознают необходимость в простом распространении информации в пределах организации и для достижения этой цели разрабатывает свою собственную систему. Обычно средств на этот проект не выделяется, более того, он даже не

признается официально. Такого рода системы создаются на базе уже имеющегося оборудования и недорогого программного обеспечения.

Что касается аппаратного обеспечения, то в любой компании вы наверняка найдете работающий с неполной нагрузкой или вовсе не используемый компьютер, пусть и с недостаточно мощным процессором. Это может быть компьютер общего пользования, который занят всего пару часов в день. Подобного компьютера, даже если он не является выделенным, вполне достаточно, особенно на первых этапах становления Intranet.

В некоторых случаях это может оказаться единственно возможным решением. К счастью, серверам Web не требуется мощных вычислительных ресурсов, так что такой вариант может оказаться вполне работоспособным, по крайней мере, до того момента, когда Intranet значительно вырастет в размерах или трафик станет чересчур интенсивным. Тем не менее, чем меньше других задач будет выполнять компьютер, где установлен сервер Web, тем стабильнее окажется Intranet.

Приобретать дорогое коммерческое программное обеспечение сервера Web нет необходимости, особенно когда сеть только начинает создаваться. В Internet вы можете без труда найти вполне приемлемые бесплатные и условно-бесплатные серверы Web. Это программное обеспечение имеется для большинства аппаратных платформ и сетевых операционных систем, в том числе для Windows 95, Windows NT, Macintosh и UNIX.

Небольшие сети часто служат только для доступа с пользовательских ПК к единственному небольшому серверу файлов и печати или главному компьютеру. Если сеть может работать по протоколам TCP/IP, то никаких дополнительных затрат на прокладку кабеля, сетевые платы или другое оборудование, которое используется в сети, не потребуется. Даже относительно медленные сети, такие, как Arcnet и AppleTalk, способны поддерживать Intranet, но, естественно, сеть Ethernet на 10 Мбит/с или Token Ring более привлекательная альтернатива.

Ставшая в последнее время широко доступной вследствие роста популярности Intranet поддержка TCP/IP решает еще одну проблему построения Intranet. Все, что потребуется для предоставления доступа к Web-серверу Intranet, назначить внутренние IP-адреса и ввести в операционную систему необходимую информацию о различных устройствах, таких, как серверы имен, маршрутизаторы и почтовые серверы.

Хотя электронная почта может в известном смысле заменить собой Intranet на основе Web, тем не менее, она остается важным компонентом этой структуры. Многие организации имеют такие внутренние системы обмена электронной почтой, как Lotus cc:Mail, QuickMail компании CE Software или Microsoft Exchange. Все эти инструментальные средства сами по себе достаточно полезны, но их трудно интегрировать с Intranet. Если в вашей организации пока нет электронной почты, то следует в первую очередь обратить внимание на бесплатные или условно-бесплатные программные пакеты почтового сервера SMTP. Среди таких пакетов sendmail, имеющаяся во всех системах на базе UNIX, MailShare для Macintosh и Pegasus Mail для платформы Windows.

3.5.2 Intranet среднего уровня

На создание более сложной сети Intranet требуется чуть больше средств, чем для вышеописанного варианта. Конфигурация такого типа служит лучшим подтверждением жизненности концепции более крупной, более надежной и более дорогой Intranet. Одно из отличий конфигурации среднего размера от сети Intranet младшего класса это использование выделенного сервера Web.

Благодаря применению выделенного сервера Intranet становится значительно более доступной, и при этом она избавляется от проблем, характерных для Intranet на базе настольного ПК. Выделенный сервер быстрее, и он не «исчезнет», если невыделенный компьютер придется перезагрузить.

Выделенный сервер может также функционировать одновременно как сервер Web и как сервер электронной почты. Общепринятой практикой является объединение различных функций Internet/Intranet в одной системе, если компьютер имеет достаточно ресурсов для их поддержки. Кроме того, сервер Web можно установить на компьютере, уже выполняющем другие функции, например на таком, как файловый сервер NetWare или Windows NT Advanced Server. При наличии достаточной вычислительной мощности файловый сервер способен справиться с выполнением и других серверных функций.

Системы такого типа обеспечивают дополнительные преимущества за счет стабильности электрического питания, регулярного создания резервных копий и мониторинга системы. Компьютер необязательно должен быть файловым сервером. Если система имеет избыточную вычислительную мощь, то она может использоваться еще и в качестве сервера Web по крайней мере до тех

пор, пока вы не окажетесь в состоянии поставить для этого отдельный компьютер.

Если позволяет бюджет, коммерческое программное обеспечение сервера Web не будет лишним. И Netscape, и Microsoft выпускают подобные продукты, а также другое программное обеспечение для Internet/Intranet. С момента своего появления Notes компании Lotus предлагается как решение для корпоративной сети в крупной компании. Хотя эта система и не базируется на инструментарии Internet, новый интерфейс Domino интегрирует Notes с браузерами Web. С другой стороны, GroupWise компании Novell, для которого инструментарий Internet также не является базовым, представляет собой прежде всего приложение коллективной работы, хотя и может выполнять некоторые функции Intranet. Эти коммерческие предложения имеют мощные средства обновления, регулярные модернизации и техническую поддержку, отсутствующую в условно-бесплатных и бесплатных пакетах.

Данная модель организации Intranet может быть дополнена за счет включения почтового сервера SMTP. Почтовые серверы SMTP легко интегрируются в Intranet на основе Web, позволяют передавать данные во внешние по отношению к компании системы и открывают удаленным пользователям доступ в Intranet.

3.5.3 Intranet масштаба крупных фирм

Хотя реализация сети Intranet старшего класса возможна, по всей видимости, лишь при условии серьезного финансирования, эту модель можно назвать идеальной для крупных организаций. В конфигурации такого типа выделенный сервер Web, работающий на максимально возможной скорости, способен поддерживать Intranet доступной круглосуточно. Этот сервер должен быть аналогичен другим, уже действующим в сети компании. Обычно выделенный сервер Web старшего класса представляет собой систему с процессором Pentium с тактовой частотой от 100 до 166 МГц. Системы такого типа могут одновременно обслуживать больше пользователей, чем более медленные системы, и они эффективнее при работе со сложными типами данных, такими, как апплеты Java, видеоклипы QuickTime компании Apple и поисковые механизмы для баз данных.

Сеть Intranet старшего класса обычно имеет канал доступа в Internet и, зачастую, коммерческое программное обеспечение сервера Web. Она, как правило, содержит выделенный почтовый сервер на базе SMTP и обеспечивает встроенную клиентскую поддержку

протоколов TCP/IP. Соединения с Internet могут быть самыми разными, от каналов ISDN на 128 Кбит/с до frame relay и каналов T-1 на 1,5 Мбит/с.

При использовании небольших баз данных их ядро может работать как непосредственно на сервере Web, так и на выделенном компьютере. Где лучше разместить ядро базы данных, будет зависеть от типа ядра и частоты обращений к нему. База данных может стать основой любых служб Intranet, где нужны поиск и генерация отчетов.

Еще одна возможность это удаленный доступ. Он может быть организован по телефонным линиям через брандмауэр в такой конфигурации, чтобы наделенные соответствующими полномочиями пользователи могли из Internet получить защищенный доступ в Intranet. Конкретная стратегия удаленного доступа определяется не только применяемыми технологиями, но и корпоративной культурой вашей компании.

Самое замечательное в Intranet возможность сначала создать небольшую сеть, а затем наращивать ее по мере необходимости. Intranet, реализованная с помощью настольного ПК, который обслуживает от 10 до 20 пользователей, может быть преобразована в работающую круглосуточно специализированную систему, которая в состоянии обслуживать тысячи пользователей. Кроме того, Intranet - одна из немногих корпоративных компьютерных систем, которую не нужно покупать сразу полностью.

3.6 Архитектура приложений Intranet

3.6.1 Трехсторонняя модель

Много споров о том, к какой архитектуре относится Intranet. Пытаются даже противопоставить Intranet архитектуре клиент-сервер. Нужно четко понять, что все решения Intranet-приложений для взаимодействия с БД основаны на архитектуре клиент-сервер.

Наличие диалоговых свойств в HTML и интерфейса CGI позволяет строить Intranet-приложения с доступом к БД. Наиболее распространена схема динамической публикации отчетов. При этом в качестве CGI-процедуры используется параметризуемый генератор отчетов. Однако это не единственная схема, возможно применять программы ввода и обновления информации в БД.

Если используются традиционные статичные страницы гипертекста, то в ответ на запрос клиента Web-сервер передает страницу в формате HTML. При работе с базой данных клиент указывает в форме программу или сценарий для запуска на сервере. Серверная процедура получает введенные пользователем данные,

формирует и передает SQL-запрос (определяющий логику управления данными DL) и, возможно, данные к СУБД. Сервер БД по запросу выполняет обновление, вставку, удаление или выборку записей из БД. CGI-процедура полученные результаты преобразует в формат HTML или в формат диалоговых переменных. Затем Web-сервер посылает полученную HTML-страницу или значения диалоговых переменных браузеру для отображения.

Использование CGI-процедур имеет ряд недостатков:

- статичное представление информации, преобразование результата-отчета в HTML-файл, отсутствие динамического просмотра изменения информации в базе данных, процедура "не помнит состояний запросов";
- каждое обращение к БД требует повторного установления соединения;
- такой принцип работы перегружает коммуникационную среду и имеет системные издержки при запуске серверных процессов.

Рассмотренная схема по существу является трехзвенной архитектурой клиент-сервер, где Web-сервер выступает в качестве сервера приложений. Для устранения недостатков CGI используют возможности специальных API для Web-серверов и включают дополнительное "релейное" звено в архитектуру. Все это только подталкивает к дальнейшему совершенствования архитектуры клиент-сервер.

3.6.2 Двусторонняя модель

Предложенная фирмой Sun технология Java ориентирует взаимодействие между клиентом и сервером на поток команд, а не данных. В ходе сеанса обеспечивается фоновая подкачка через сеть на компьютер клиента программных агентов апплетов, которые берут на себя функции обеспечения гибкого взаимодействия. Все, что нужно для этого встроить в Web-браузер исполняющую систему для апплетов.

При построении информационных приложений с использованием Java-технологии получается классическая двух- или трехзвенная архитектура клиент-сервер, а гипертекст уходит на задний план и выполняет лишь роль инициатора апплетов.

Существенным достоинством такой технологии является независимость приложения от аппаратной платформы. Но есть и немало недостатков:

- невысокое быстродействие вследствии интерпретации байт-кодов;

- возврат к оконной метафоре "рабочего стола";
- остаются те же проблемы организации связи с БД.

3.7 Вопросы защищенности

Общая система защиты вашей WEB-системы может состоять из следующих подсистем:

- Подсистема защиты информации от несанкционированного доступа;
- Подсистема защиты внутренней сети от несанкционированного доступа;
- Подсистема защиты информации на стадии ее передачи от источника к пользователю и в обратную сторону.

В зависимости от предполагаемой мощности всей системы защиты в целом вы можете использовать как всю совокупность подсистем, так и некоторые подсистемы в отдельности.

3.7.1 Подсистема защиты информации от несанкционированного доступа

К данной подсистеме относятся задачи общей идентификации и аутентификации пользователя, а также задачи разграничение доступа к различным участкам информации в зависимости от прав (или потребностей) пользователя.

- Общая задача идентификации пользователя сводится к выяснению, имеет ли пользователь право доступа к вашей информации (или вашей сети) в целом. Как правило, для решения данной задачи используются средства операционной системы, которая функционирует на вашем предприятии. Пользователь имеет имя, пароль или другие признаки, определяющие, имеет ли он доступ к какому-либо разделу предоставляемой Вами информации. Эти признаки проверяются средствами операционной системы непосредственно при первой попытке подключения пользователя к вашей сети. Например, при использовании Windows NT Вы можете предоставлять пользователю имя и пароль, контролируемые операционной системой.
- Под аутентификацией пользователя понимают идентификацию пользователя по дополнительным (косвенным) признакам, например по IP адресу подсети пользователя или по электронной подписи. Данные признаки, как правило, отслеживаются специальными средствами, такими как брэндмауэры или специальные компоненты WEB-серверов.

- Разграничение доступа к различным участкам информации, как правило, обеспечивается непосредственно WEB-серверами, которые имеют независимые от ОС или интегрированные с ОС системы идентификации пользователей и внутренние системы каталогизации информации, напоминающие сруктуры размещения информации самих ОС или незначительно отличающиеся от них.

Надо заметить, что если Вы предполагаете использовать WEB-сервер для предоставления статической информации (заранее подготовленных и хранящихся в файлах документов), то решение всех задач по обеспечению разграничения доступа и идентификации пользователей ложится на средства операционной системы и WEB-сервера. Если же основной объем предоставляемой информации основывается на технологии динамической генерации HTML-страниц и использовании WEB-приложений, то проблема разграничения доступа к информации ложится непосредственно на WEB-приложения. В последнем случае умелое комбинирование средств операционной системы, WEB-серверов и WEB-приложений приводит к минимальным затратам на обеспечение описываемой в данном разделе подсистемы защиты и открывает широкое поле деятельности для самостоятельного совершенствования и доработки (в случае специфичных особенностей вашей информации) данной подсистемы.

3.7.2 Подсистема защиты внутренней сети от несанкционированного доступа

К данным подсистемам относятся так называемые «брэндмауэры» или системы FireWall. Они являются надстройкой над TCP/IP и обеспечивают разрешение или запрещение прохождения IP-пакетов в сети. Пропуская все IP-пакеты, проходящие в сети, через себя, брэндмауэры определяют адресата и владельца пакета, точку обращения, исходный порт, конечный порт, а также тип пакета, проверяют по внутренним журналам или базам пользователей права обоих участников данной транзакции и выносят решение о прохождении пакета от отправителя к адресату или о запрещении такового.

Брендмауэры могут представлять собой как чисто программные, так и программно-аппаратные комплексы. В последнем случае снижается риск ошибок системы и повышается защищенность, но, с другой стороны, происходит удорожание данной подсистемы защиты и уменьшается ее гибкость. Системы типа FireWall обычно реализованы в виде отдельных задач, установленных

на выделенные машины. Внешний интерфейс этих задач позволяет быстро настраивать их, задавая наборы правил, поддерживать защищенные формы доступа к администрированию, просматривать журналы событий и т.д.

3.7.3 Подсистема защиты информации на стадии ее передачи от источника к пользователю и в обратную сторону

К данной подсистеме относятся задачи обеспечивающие кодирование информации в источнике и раскодирование ее в приемнике, а также некоторые дополнительные функции по проверке прав на посылку информации из источника и получение ее адресатом.

Существует ряд стандартизированных протоколов обмена данными, таких как **SSL** (Secure Socket Layer) или **SHTTP** (Secure HTTP), обеспечивающих различные способы шифрования сообщений. В случае использования того или иного программного обеспечения WEB могут быть использованы различные протоколы обмена. Реализация защищенных протоколов зависит исключительно от фирмы-производителя ПО для WEB. Однако большинство современных WEB-средств поддерживают тот или иной защищенный протокол, а некоторые фирмы выпускают целые линии своих продуктов, поддерживающих различные уровни безопасности передачи данных.