Понятие информационной системы

Основные задачи администрирования ИС

Информационная система (ИС) – совокупность внутренних и внешних информационных потоков объекта управления, методов, средств и специалистов, участвующих в процессе обработки информации и выработке управленческих решений.

ИС связывает объект и систему управления между собой и с внешней средой через информационные потоки.

Структура информационной системы

При рассмотрении информационных систем можно выделить несколько основных компонентов:

- информация, описывающая состояние системы или процесса;
- информационные технологии хранения, обработки, представления и передачи информации;
- организационная структура и связи между единицами управления, а также методы управления;
- функциональные компоненты информационной системы (отдельные подсистемы, решающие тот или иной набор задач реализующих обработку данных и модели принятия решений).

Составные части ИС:

- *информационное обеспечение* — совокупность методов и средств по размещению и организации информации;
- *программное обеспечение* — совокупность программных средств необходимых для разработки и эксплуатации ИС средствами вычислительной техники;
- *техническое обеспечение* – комплекс технических средств, применяемых для функционирования ИС;
- *правовое обеспечение* – совокупность правовых норм, регламентирующих создание и функционирование информационной системы;
- *лингвистическое обеспечение* – совокупность языковых средств, используемых на различных стадиях создания и эксплуатации ИС;
- *организационное обеспечение* — совокупность методов и средств, позволяющих усовершенствовать организационную структуру объектов и управленческие функции.

Вычислительные сети

Современные информационные системы работают на основе применения вычислительных сетей.

Вычислительная сеть – совокупность компьютеров, связанных коммуникационной системой и снабженных необходимым программным обеспечением, позволяющим пользователям и приложениям получать доступ к ресурсам удаленных компьютеров и обеспечивающим обмен данными.

Распределенные информационные системы

Распределенная ИС обеспечивает высокую степень прозрачности сетевых ресурсов, т.е. распределенная ИС предоставляет пользователю и приложениям сетевые ресурсы в виде единой централизованной виртуальной машины.

Распределенная ИС позволяет распределить процессы по различным компьютерам для их хранения, обработки и представления.

Операционные системы

Операционная система – основа для функционирования прикладных программных продуктов, в том числе, программных компонентов любой информационной системы.

Сетевая операционная система обеспечивает функционирование распределенной информационной системы.

Функциональные компоненты сетевой ОС

Основные компоненты сетевой ОС:

▫ *Средства управления локальными ресурсами* компьютера реализует все функции ОС автономного компьютера (управление процессами, оперативной памятью, управление внешней памятью, пользователями и т.п.)

▫ *Сетевые средства,* разделяемые на три компонента:

Серверная часть ОС – средства предоставления локальных ресурсов и сервисов в общее пользование

Клиентская часть ОС – средства запроса на доступ к удаленным ресурсам и сервисам

Транспортные средства ОС, совместно с коммуникационной системой обеспечивающие передачу сообщений между компьютерами

Функции, процедуры и службы администрирования

Функции администрирования

Процедуры администрирования

Исследование активности

Очистка аудиторских записей из аудиторского журнала

Защита журнала проверки

Службы администрирования

Служба соблюдения правил эксплуатации

Служба проектирования и приемки информационных систем

Службы защиты от вредноностного программного обеспечения

Службы обслуживания сети

Сетевая служба

Службы обмена данными

Категории администраторов

Администратор

Администратор кластера

Администратор компьютера

Администратор сети

Администратор базы данных

Классификация администраторов баз данных

Административные оповещения.

Поскольку информационные системы могут иметь много пользователей, должно существовать лицо или группа лиц, управляющих этой системой. Такое лицо называется администратором информационных систем. В любой организации должен быть хотя бы один человек, выполняющий административные обязанности; если информационная система большая, эти обязанности могут быть распределены между несколькими администраторами.

Функции администрирования

К функциям администрирования относятся:

- инсталляция и обновление версий сервера и прикладных инструментов;

- распределение дисковой памяти и планирование будущих требований системы к памяти;

- создание первичных структур памяти;

- создание первичных объектов по мере проектирования приложений разработчиками;

- модификация структуры данных в соответствии с потребностями;

- зачисление пользователей и поддержание защиты системы;

- соблюдение лицензионного соглашения;

- управление и отслеживание доступа пользователей к информационным системам;

- отслеживание и оптимизация производительности программ;

- планирование резервного копирования и восстановления;

- поддержание архивных данных на устройствах хранения информации;

- осуществление резервного копирования и восстановления;

- обращение в корпорации разработчиков или дилеров за техническим сопровождением.

Процедуры администрирования

Исследование активности системы с целью генерирования следующей общей информации:

- имя пользователя, выполнявшего отслеживаемое предложение;

- код действия, указывающий выполненное предложение;

- объекты, адресуемые в отслеживаемом предложении;

- дату и время выполнения отслеживаемого предложения.

Администратор обязан контролировать рост журнала и его размер. Когда генерируются записи использования системы, журнал системного администратора растет за счет двух факторов:

- числа включенных опций проверки;

- частоты выполнения отслеживаемых операций.

Для контроля за ростом журнала проверки надо использовать следующие методы:

Включать и выключать проверку информационной системы. Когда проверка включена, записи генерируются и поступают в журнал; когда проверка выключена, записи не генерируются.

Жестко контролировать возможности осуществлять проверку объектов. Это можно делать двумя различными способами:

Всеми объектами владеет администратор,

Все объекты содержатся в схемах, которые не соответствуют реальным пользователям информационной системы.

Очистка аудиторских записей из аудиторского журнала

После того, как проверка включена в течение некоторого времени, администратор может удалить записи из журнала, - как для того, чтобы освободить память, так и для облегчения управления этим журналом. Если информация журнала должна архивироваться для целей накопления истории, администратор может скопировать соответствующие записи.

Защита журнала проверки

Осуществляя отслеживание подозрительной деятельности в информационной системе, следует защищать целостность записей журнала проверки, чтобы гарантировать точность и полноту информации.

Службы администрирования:

Служба соблюдения правил эксплуатации

Обязанности администратора: обеспечить правильную и надежную работу информационной системы.

Администратор должен определить обязанности и процедуры по администрированию и обеспечению функционирования компьютеров и сетей. Они должны быть зафиксированы в инструкциях и процедурах реагирования на инциденты. Для уменьшения риска некорректных или несанкционированных действий администратору следует применять принцип разделения обязанностей.

Службы проектирования и приемки информационных систем

Обязанности администратора: свести риск отказов информационных систем к минимуму.

Администратор обязан учитывать, что для обеспечения доступности ресурсов и необходимой производительности информационных систем требуется предварительное планирование и подготовка. Для уменьшения риска перегрузки систем необходимо учитывать будущие потребности и необходимую производительность. Эксплуатационные требования к новым системам следует определять, документировать и проверять до их приемки. Должны быть выработаны требования к переходу на аварийный режим для сервисов, поддерживающих несколько приложений.

Служба защиты от вредоносного программного обеспечения

Обязанности администратора: обеспечить целостность данных и программ.

Для предотвращения и выявления случаев внедрения вредоносного программного обеспечения администратору требуется принятие соответствующих мер предосторожности. В настоящее время существует целый ряд вредоносных программ («компьютерные вирусы», «сетевые черви», «троянские кони» и «логические бомбы»), которые используют уязвимость программного обеспечения по отношению к несанкционированной модификации. Администраторы информационных систем должны быть всегда готовы к проникновению вредоносного программного обеспечения в информационные системы и принимать специальные меры по предотвращению или обнаружению его внедрения. В частности, важно принять меры предосторожности для предотвращения и обнаружения компьютерных вирусов на персональных компьютерах.

Служба обслуживания систем

Обязанности администратора: обеспечить целостность и доступность информационных сервисов.

Для поддержания целостности и доступности сервисов администратору требуется выполнение некоторых служебных процедур: должны быть сформированы стандартные процедуры резервного копирования, регистрации событий и сбоев, а также контроля условий функционирования оборудования.

Сетевая служба

Обязанности администратора: обеспечить защиту информации в сетях.

Управление безопасностью сетей, отдельные сегменты которых находятся за пределами организации, требует особого внимания. Для защиты конфиденциальных данных, передаваемых по открытым сетям, могут потребоваться специальные меры.

Служба защиты носителей информации

Обязанности администратора: предотвратить повреждение информационных ресурсов и перебои в работе организации.

Необходимо контролировать носители информации и обеспечивать их физическую защиту. Следует определять процедуры для защиты носителей информации (магнитные ленты, диски, кассеты), входных/выходных данных и системной документации от повреждения, хищения и несанкционированного доступа.

Служба обмена данными и программным обеспечением

Обязанности администратора: предотвратить потери, модификацию и несанкционированное использование данных.

Администратору следует контролировать, чтобы обмены данными и программами между организациями осуществлялись на основе формальных соглашений. Должны быть установлены процедуры и стандарты для защиты носителей информации во время их транспортировки. Необходимо уделять внимание обеспечению безопасности при использовании электронного обмена данными и сообщениями электронной почты.

Категории администраторов

Администратор

Администратор в Windows – это пользователь, ответственный за настройку и управление контроллерами домена и локальными компьютерами, ведение учетных записей пользователей и групп, присвоение паролей и разрешений, а также помогающий пользователям работать в сети. Администраторы являются членами одноименной группы и обладают полным доступом к домену или компьютеру. Пользователь, который имеет право вносить на компьютере изменения, на уровне системы, устанавливать программное обеспечение и имеет доступ ко всем файлам на компьютере. Пользователь с учетной записью администратора компьютера имеет полный доступ к другим учетным записям пользователей на компьютере.

Администратор кластера

Группа независимых компьютерных систем, называемых узлами, работающих вместе в виде единой системы таким образом, чтобы важные для работы приложения и ресурсы оставались доступными для клиентов, называется кластерами. ***Кластер серверов*** – производит реализацию данной службы. Приложение, используемое для настройки кластера и его узлов, групп и ресурсов, определяется как Администратор кластера. Администрирование кластера может выполняться на любом компьютере доверенного домена, независимо от принадлежности участника к категории узлов кластера.

Cluster.exe – программа, которой можно пользоваться вместо администратора кластера для управления кластерами из командной строки. Программа Cluster.exe также может использоваться для автоматизации задач администрирования при помощи командных сценариев.

Администратор компьютера

Пользователь, управляющий компьютером. Администратор компьютера вносит изменения в систему, включая установку программ и доступ ко всем файлам компьютера, а также может создавать, изменять и удалять учетные записи других пользователей.

Администратор сети

Пользователь, ответственный за планирование, настройку и управление ежедневной работой сети. Администратор сети называется также системным администратором.

Администратор базы данных (АБД)

Администратор базы данных – лицо, отвечающее за выработку требований к базе данных, её проектирование, реализацию, эффективное использование и сопровождение, включая управление учётными записями пользователей БД и защиту от несанкционированного доступа. Не менее важной функцией администратора БД является поддержка целостности базы данных.

Администратор БД отвечает за целостность информационных ресурсов компании. На нем лежит ответственность по созданию, обновлению и сохранности связанных между собой резервных копий файлов, исходя из задач предприятия. Этот человек должен в мельчайших подробностях знать существующие механизмы восстановления программного обеспечения БД.

Возможны ситуации, при которых администратору БД потребуется на основе логических прикладных моделей создавать элементы физической схемы, а также поддерживать связь пользователей с системой и обеспечивать соответствующий уровень информационной безопасности, следя за тем, чтобы доступ к данным имели только те люди, которые в нем нуждаются.

Администратор БД должен уметь определять узкие места системы, ограничивающие ее производительность, настраивать SQL и программное обеспечение СУРБД и обладать знаниями, необходимыми для решения вопросов оптимизации быстродействия БД.

Основные задачи администратора базы данных:

- проектирование базы данных;
- оптимизация производительности базы данных;
- обеспечение и контроль доступа к базе данных;
- обеспечение безопасности в базе данных;
- резервирование и восстановление базы данных;
- обеспечение целостности баз данных;
- обеспечение перехода на новую версию СУБД.

Обязанности администратора

Среди наиболее важных обязанностей администратора – резервное копирование и восстановление информации. Механизм резервирования и восстановления данных

обязан учитывать зависимость бизнеса от информации. Другими словами, если в Вашей прикладной системе приема заказов через Internet любая потеря информации является абсолютно недопустимой, то использование схемы "холодного" резервирования, т.е. подразумевающую полную остановку и отключение БД, в данном случае, совершенно неприемлемо. Для того, чтобы найти наилучшее решение, соответствующее запросам предприятия, администратор должен хорошо разбираться в многообразии методов резервирования и восстановления, знать плюсы и минусы каждого из них.

Кроме того, администратор должен контролировать рост БД. От него требуется держать руководство в курсе относительно предполагаемого роста БД, с тем чтобы иметь возможность своевременно заказать любое необходимое оборудование.

Настройка также является одной из основных зон ответственности администратора БД. И пользователи, и разработчики за советом будут обращаться именно к нему.

Администратор также занимается созданием тестовых конфигураций БД, управлением схемами приложений, внесением изменений в эти схемы, желательно безошибочных, поддержкой пользователей, выражающейся, к примеру, в добавлении в систему новых пользователей, обеспечением информационной безопасности в виде открытия доступа только к запрашиваемым объектам.

Профилактический монитор:

- избавляет администратора от экстренных мер
- разгружает администратора по вечерам и выходным
- ускоряет приобретение опыта.

Средства диагностики:

- превращают младшего АБД в старшего, позволяя последнему сконцентрироваться на других задачах.

Средства анализа:

- помогают при планировании роста БД и будущих затрат.

Средства технического обслуживания:

- помогают при резервном копировании и восстановлении данных, сокращая время операции и уменьшая число ошибок

- помогают при реорганизациях, экономя время, уменьшая количество ошибок и длительность профилактических окон (maintenance window)

- способствуют высокой доступности данных, создавая «незаметные» с точки зрения системы профилактические окна и помогая при резервировании / восстановлении системы.

Классификация администраторов баз данных (АБД)

Основные типы администраторов БД: системный администратор; архитектор БД; аналитик БД, разработчик моделей данных; администратор приложений; проблемно-ориентированный администратор БД; аналитик производительности; администратор хранилища данных.

Существует несколько видов администраторов БД, а их обязанности вполне могут отличаться от компании к компании.

Оперативные (operational) АБД:

- манипулируют дисковым пространством;
- наблюдают за текущей производительностью системы;
- реагируют на возникающие неисправности БД;
- обновляют системное ПО и ПО базы данных;
- контролируют структурные изменения БД;
- запускают процедуры резервного копирования данных;
- выполняют восстановление данных;
- создают и управляют тестовыми конфигурациями БД.

Тактические (tactical) АБД:

- реализуют схемы размещения информации;
- утверждают процедуры резервного копирования и восстановления данных;
- разрабатывают и внедряют структурные элементы БД: таблицы, столбцы, размеры объектов, индексацию и т.п.; сценарии (scripts) изменения схемы БД; конфигурационные параметры БД;
- утверждают план действий в случае аварийной ситуации.

Стратегические (strategic) АБД:

- выбирают поставщика БД;
- устанавливают корпоративные стандарты данных;

- внедряют методы обмена данными в рамках предприятия;

- определяют корпоративную стратегию резервирования и восстановления данных;

- устанавливают корпоративный подход к ликвидации последствий аварии и обеспечению доступности данных.

Старшие (senior) АБД:

- досконально знают свой персонал;

- пользуются высоким спросом;

- могут написать скрипт, который освободит их из запертого сундука, брошенного в океан, и чрезвычайно гордятся своими произведениями;

- тратят уйму времени на подготовку младших АБД;

- очень ценятся руководством и получают бешеные деньги

Младшие (junior) АБД:

- мечтают стать старшим АБД;

- не слишком сильны в написании скриптов;

- имеют большую склонность к использованию средств управления БД;

- тоже неплохо получают.

Прикладные (application) АБД:

- в курсе информационных нужд компании;

- помогают в разработке прикладных задач;

- отвечают за разработку схемы и ее изменения;

- вместе с системным АБД обеспечивают должный уровень резервирования / восстановления данных;

- занимаются построением тестовых БД.

Системные (system) АБД:

- отвечают за все необходимое для резервирования и восстановления данных;

- контролируют производительность системы в целом;

- осуществляют поиск и устранение неисправностей;

- в курсе нынешних и будущих потребностей БД в плане емкости;

- в курсе текущего состояния и нужд БД.

Наемные (contract) АБД:

- приглашаются под конкретную задачу или в качестве консультантов;

- передают персоналу необходимые знания;
- фиксируют свои действия;
- должны прекрасно разбираться в соответствующей области;
- хороши в качестве временного персонала, для оценки проекта или системы.

Администраторы-руководители:

- проводят еженедельные совещания;
- определяют перечень первоочередных задач;
- устанавливают и оглашают официальный курс и стратегию;
- утверждают и корректируют должностные инструкции и список обязанностей;
- следят за наличием соответствующей документации.

Административные оповещения

Оповещения, относящиеся к серверу или к использованию ресурсов. Они уведомляют пользователей о событиях, происходящих в системе безопасности и управления доступом, в сеансах пользователей, в системе управления питанием (при наличии источника бесперебойного питания), при репликации каталога и при печати. Если компьютер инициирует оповещение, сообщение направляется по заранее определенному списку пользователей и компьютеров.

Вопросы для самоконтроля

- Обозначьте основные функции администрирования
- Приведите основные процедуры администрирования
- Расскажите об исследовании активности
- Очистка аудиторских записей из аудиторского журнала
- Защита журнала проверки
- Перечислите основные службы администрирования
- Перечислите категории администраторов
- Приведите классификацию администраторов баз данных
- Приведите основные административные оповещения.

Объекты администрирования

На большинстве современных предприятий, где ведется активная работа с различными информационными системами, рано или поздно встает проблема ввода,

систематизации, обработки и безопасного хранения значительных объемов информации. Версии прикладных инструментов, различные структуры памяти, системы защиты данных и разные виды электронной документации беспорядочно накапливаются в файловых системах компьютеров, затрудняя поиск информации, коллективную работу над документами, их согласование и соблюдение конфиденциальности. Таким образом, требуется средство управления, которое могло бы обеспечить высокую эффективность работы с информационными системами в масштабах всей организации. Для решения этой задачи используется администратор информационных систем.

Объекты администрирования

Объект №1: Непосредственно объекты информационных систем. Контроль за его бесперебойным функционированием, а в случае возникновения неисправностей своевременное сохранение важной информации и резервное копирование.

Объект №2: Программное обеспечение информационных систем, необходимое для предотвращения и выявления случаев внедрения вредоносных программ. Разработка и внедрение соответствующих мер предосторожности. Отслеживание новейших программ и средств для борьбы с возможным проникновением вирусов в систему.

Объект №3: Планирование и проектирование информационных систем. Подготовка и расчет будущей производительности, подробное изучение и корректировка, а возможно, и разработка проектной документации. Доработка критериев приемки информационных систем под данное конкретное производство.

Объект №4: Функционирование компьютеров и сетей. Обеспечение правильной и надежной работы информационных систем. Регулирование и проверка соблюдения правил эксплуатации оборудования пользователями.

Объект №5: Программное обеспечение, необходимое для защиты информации в сетях. Снабжение системы, имеющей конфиденциальные данные, передаваемые по открытым сетям специальными мерами и средствами, определяющими их правовую и информационную охрану.

Объект №6: Электронный обмен данными. Стандарты для защиты носителей информации во время их транспортировки. Отслеживание сроков действия лицензий.

Объект №7: Физическая защита носителей информации. Программное обеспечение, необходимое для предотвращения повреждений информационных ресурсов и возникновения перебоев в работе организации. Разработка средств защиты от хищения и несанкционированного доступа к секретным и конфиденциальным данным организации.

Компоненты в ведении администратора информационных систем

Пользователь. Создание и удаление учетных записей, их блокировка и разблокирование, настройка сценариев входа, консультирование пользователей по различным аспектам работы с системой и нахождению тех или иных ресурсов. Обозначить группу технической поддержки. И возложить на нее обязанности по установке и настройке сетевого клиентского программного обеспечения на компьютерах пользователей.

Управление данными. Обозначение и установление грани доступа разных пользователей к конкретным ресурсам, профилактическое обслуживание баз данных (индексация, оптимизация, упаковка), организация резервного копирования.

Производительность и оптимизация системы. Отбор и конкретное изучение эмпирических правил, помогающих администратору вносить изменения в настройки с минимальным риском ухудшить другие показатели или сделать систему неработоспособной. Снижение риска возможного нарушения работы системы при отключении одного из компонентов.

Учет системных ресурсов. Повышение производительности системы при проведении соответствующей модернизации. Обеспечение возможности платного использования ресурсов. Контроль использования дискового пространства, печати, учет трафика

Техническое обслуживание и модернизация. Очистка от пыли, смазка вентиляторов, подтяжка креплений, контроль состояния аккумуляторов, изменение физической топологии сети. Разработка инструкций для службы технической поддержки. Грамотное формулирование заявок на изменение аппаратной конфигурации. Закупка дополнительных лицензий или обновленной версии программного обеспечения.

Управления активным сетевым оборудованием и сетью в целом.

Информационная безопасность. Составление плана доступа пользователей к ресурсам и контроль его исполнения. Отслеживание появления различных уязвимостей в используемых операционных системах.

Разработчики приложений и служба безопасности

В некоторых случаях база данных должна также иметь одного или нескольких сотрудников службы безопасности. Которые главным образом отвечают за регистрацию новых пользователей, управление и отслеживание доступа пользователей к базе данных, и защиту базы данных.

В обязанности разработчика приложений входит:

- проектирование и разработка приложений данных;
- проектирование структуры данных в соответствии с требованиями приложений;
- оценка требований памяти для приложения;
- формулирование модификаций структуры данных для приложения;
- передача вышеупомянутой информации администратору данных;
- настройка приложения в процессе его разработки;
- установка мер по защите приложения в процессе его разработки.

Реализация служб каталогов

Служба каталогов – это физически распределенное, но логически централизованное хранилище данных, используемое для администрирования всей вычислительной среды и позволяющее собрать всю информацию подобного рода в одной программе. Она обеспечивает универсальный доступ ко всем вычислительным ресурсам, причем для каждого пользователя ведется одна учетная запись, независимо от количества серверов и сервисов, которые этот пользователь получает в распоряжение. По существу, службы каталогов представляют собой системы указателей, размещаемых в базах данных. Служба каталогов должна обеспечивать единую согласованную информацию о сети, а так же средства идентификации, управления доступом, навигации и другие услуги. Одной из важнейших функций таких служб является установление соответствия между сетевыми именами, доступом пользователей или ресурсов и сетевыми адресами. Эта функция, называемая службой имен, позволяет работать с простыми псевдонимами и

переводить их в машинные адреса (или отображать в такой форме).

Служба каталогов обязана обладать следующим набором свойств:

Пользователь должен получать доступ ко всем разрешенным для него службам, ресурсам и приложениям после единственного подключения к сети. Для этого потребуется определенная степень открытости решений служб каталогов. Для успешного функционирования системы разработчикам приложений следует предусмотреть поддержку службы каталогов в своих приложениях.

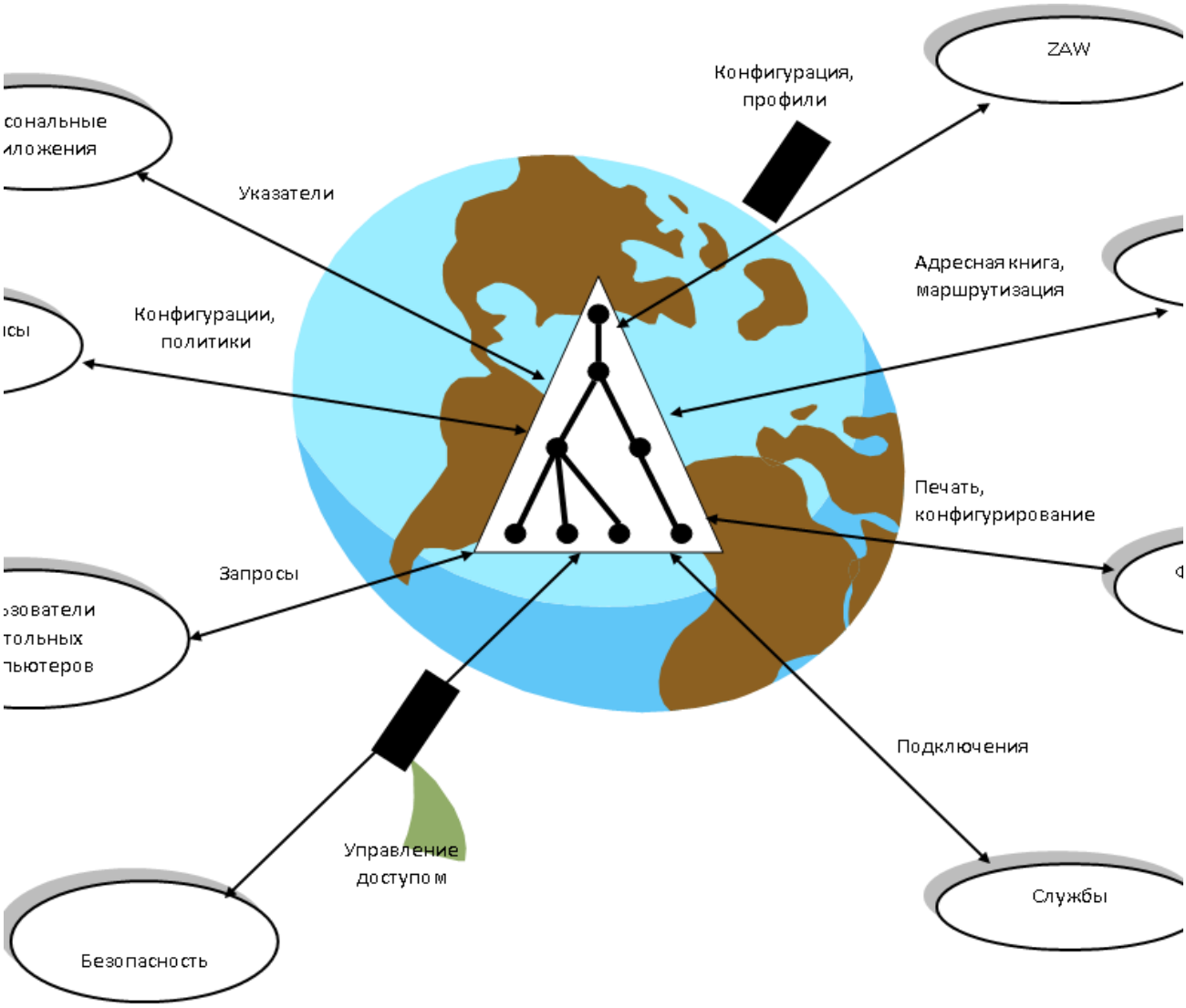
Вся информация о вычислительной среде должна хранится в распределенной форме. Данные следует реплицировать на несколько серверов. В этом случае пользователь или служба, которым потребовался доступ к информации, могут получать ее с относительно близкого и удобного для них сервера.

Для определения целостности информации, поступающей в распоряжение нескольких пользователей, нужна поддержка реплицирования данных. Изменения, внесенные в один из участков каталога, необходимо передавать всем абонентам сети для гарантии тождественности информации вне зависимости от места ее получения.

Система должна поддерживать запросы, составленные как на основании конкретных параметров (имя, номер телефона и т.п.), так и при расширенном поиске (например, все цветные принтеры на первом этаже). Служба каталогов действует по принципу справочного издания «Желтые страницы». С ее помощью можно определять местоположение нужной службы по имени или производить поиск по определенным категориям.

Возможность администрирования не должна зависеть от физического расположения системы. Это означает отказ от необходимости четко определять местонахождения данных средств. К примеру, появляется возможность полного или частичного назначения прав администрирования отдельных участков каталога.

Задачи администрирования представлены на рисунке

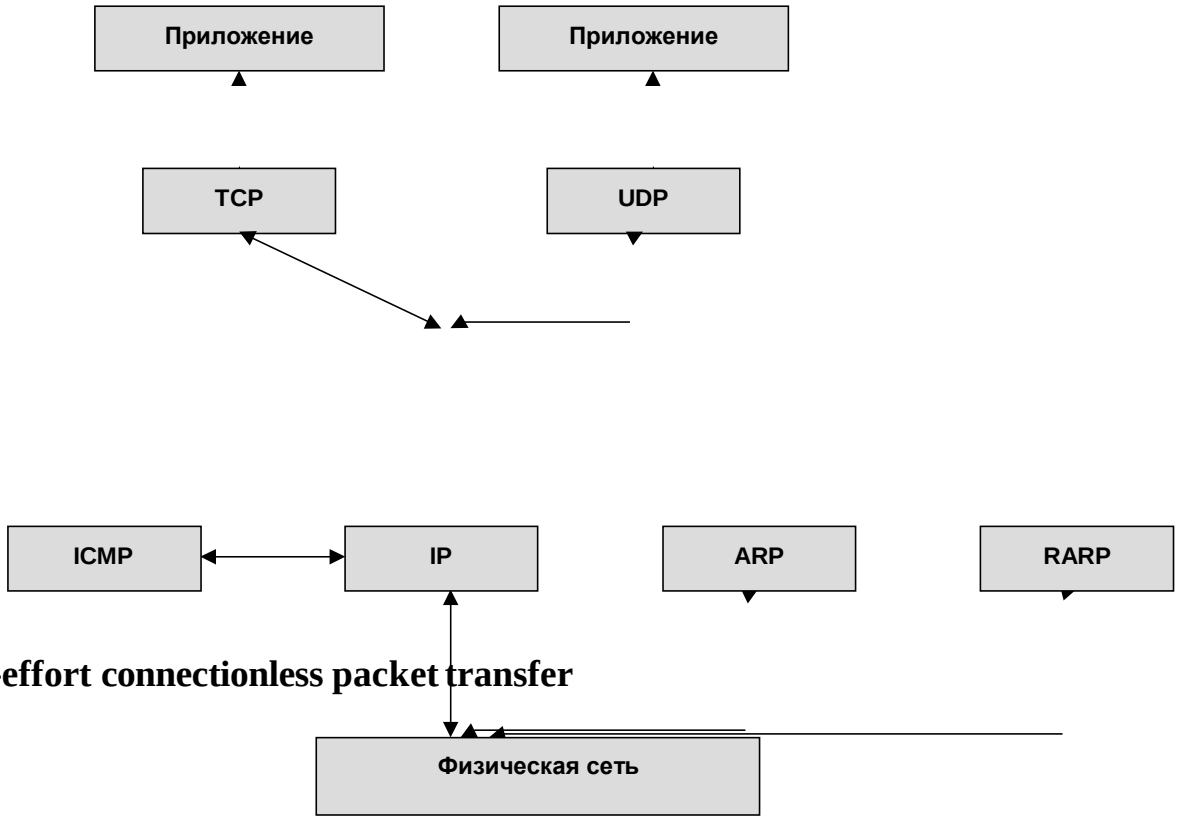


Вопросы для самоконтроля:

- Назовите наиболее значимые объекты администрирования
- Обозначьте компоненты в ведении администратора информационных систем
- Приведите примеры разработчиков приложений и служб безопасности
- Расскажие реализацию служб каталогов
- Приведите основные задачи администрирования

Протокол, стек протоколов

Архитектура сетей TCP/IP



IP - best-effort connectionless packet transfer

Состав стека протоколов TCP/IP

В состав стека протоколов TCP/IP, кроме давших название этим сетям протоколов Transmission Control Protocol и Internet Protocol, входят: User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) и ряд протоколов прикладного уровня, в частности TELNET, FTP, SMTP, SNMP и HTTP.

В отличие от 7-ми уровневой модели OSI протокольный стек TCP/IP разбит на 4 уровня. Сетевой уровень (IP) обеспечивает передачу информации через произвольную комбинацию сетей, использующих этот же набор протоколов. **IP-протокол предоставляет лишь один вид сервиса – передачу пакетов без предварительного установления соединения и настолько хорошо, насколько получиться** (best-effort connectionless packet transfer). Пакеты пересылаются между узлами коммутации без предварительного установления соединения; они маршрутизируются независимо, и пакеты одного приложения могут доставляться по

разным маршрутам. Узлы коммутации, соединяющие смежные сети, могут испытывать перегрузки и уничтожать пакеты. Ответственность за восстановление утерянных пакетов и надлежащий порядок их передачи приложению лежит на транспортном уровне, который представлен протоколами TCP и UDP.

Разнообразие требований сетевых приложений обусловило необходимость двух протоколов транспортного уровня. Так, например, приложения передачи файлов и web (FTP, HTTP) для пересылки своих сообщений используют TCP, в то время как приложения управления сетевыми устройствами, служба имен (SNMP, DNS), потоковые приложения реального времени используют в качестве транспортного протокола UDP. Далее будем называть протокольные блоки TCP сегментами, а блоки UDP – дейтограммами.

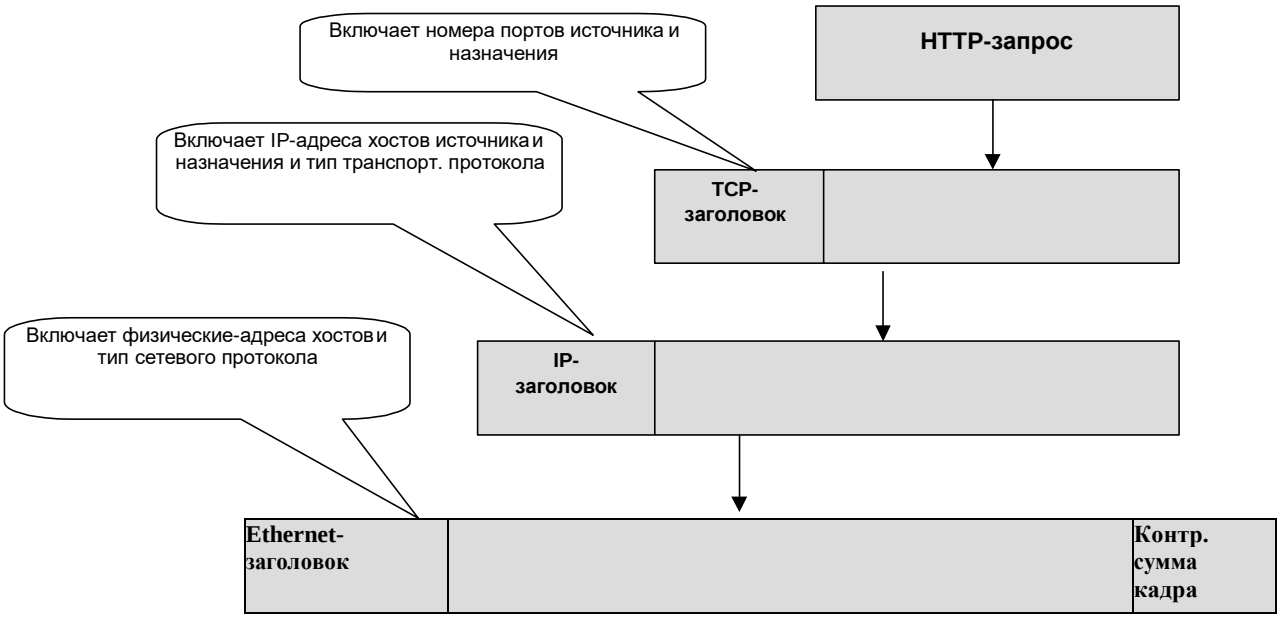
Сетевой уровень (протокол IP) мультиплексирует протокольные блоки транспортного уровня в IP- потоки; при этом сегменты транспортного уровня могут фрагментироваться (если они превышают максимально допустимый размер, определяемый канальным протоколом). Протокольные блоки IP обычно называют пакетами.

После вычисления маршрута передачи пакета, посредством протокола ARP определяется физический адрес следующего на маршруте хоста и пакет направляется на физический уровень сети. Иногда бывает необходимо решить обратную задачу, то есть по заданному физическому адресу определить логический сетевой адрес устройства. В частности, эта проблема актуальна для процедуры загрузки бездисковых станций, когда такая станция рассылает в широковещательном режиме запрос, содержащий ее физический адрес и «просьбу» сообщить ей логический сетевой адрес. Этот запрос обрабатывается сервером RARP, который и передает пославшей его станции требуемую информацию.

Физический уровень TCP/IP сети может использовать любую технологию канального уровня – Ethernet, Token Ring, ATM, PPP и т.д. Но для обеспечения прозрачности физического уровня необходимо, чтобы на сетевом уровне были предусмотрены процедуры дефрагментации пакетов до размера, разрешенного соответствующим протоколом канального уровня. Обратная процедура, т.е. объединение пакетов малых размеров до величины, приемлемой на канальном

уровне, не предусматривается.

Архитектура сетей TCP/IP



Инкапсуляция протокольных блоков в TCP/IP стеке

Протокольные блоки вышележащих уровней инкапсулируются в протокольные блоки нижележащих уровней так, как это показано на слайде. При этом, блок каждого уровня содержит специфическую информацию, позволяющую точно адресовать его. Так, сегмент TCP (UDP-

дейтограмма) содержит в своем заголовке номер **порта**, однозначно определяющий приложение, которому он принадлежит. IP-пакет адресуется **логическим адресом** хоста, также однозначно определяющим его в распределенной сети. Кадр канального уровня включает в себя **физический адрес** ближайшего на маршруте доставки хоста, которому необходимо передать пакет.

IP-протокол.

Основной протокол стека TCP/IP, - Internet Protocol (IP), - по своим функциям соответствует сетевому уровню модели взаимодействия открытых систем (OSI). Механизмы протокола, описанные в документе RFC 791, обеспечивают ненадежную доставку пакетов данных между сетевыми устройствами (устройствами, имеющими сетевой адрес) в режиме без предварительного установления соединения (дейтограммный сервис). Этот тип сервиса часто называют сервисом «настолько хорошо, как получиться» (best effort service), что отражает отсутствие в протоколе процедур контроля доставки пакетов. Решение задачи надежности доставки возлагается на протоколы верхних уровней, главным образом на TCP. Основными функциями протокола IP являются:
формирование пакетов из сегментов транспортного уровня, с предварительной фрагментацией (если необходимо) последних;
обеспечение логической адресации сетевых устройств
поддержка процесса маршрутизации
продвижение пакетов от одного узла коммутации до другого.

Структура IP – пакета

0 4 8 16 31

Версия (Version	**Длина (IHL)**	**Тип сервиса (ToS)**	**Общая длина пакета (Total Lenght)**

Идентификатор		**Флаги**	**Смещение фрагмента**
Время жизни (TTL)	**Протокол (см. след. слайд)**	**Контрольная сумма**	
Адрес отправителя (Source IP address)			
Адрес получателя (Destination IP address)			
Опции (поле переменной длины)			**Выравнивание до 32 бит (padding)**

Формат заголовка IP-пакета

- **Структура IP-пакета.**

- Функции IP-протокола реализуются посредством специальной структуры заголовка пакета, формат которого приведен на слайде.

- Заголовок содержит поля фиксированной длины (первые 20 байт) и поле переменной длины (поле опций), размер которого может достигать 40 байт. Для выравнивания этого поля по 32 битной границе предусмотрено поле «Выравнивание» (Padding) которое заполняется нулями. Рассмотрим назначение полей заголовка.

- **Версия (Version) –** поле определяет номер версии протокола. В настоящее время используется версия 4 и ведется активная подготовка к переходу на версию 6. Версия 5 описывает протокол ST2, разработанный для передачи данных потоковых приложений реального времени. Поле проверяется перед обработкой пакета и пакеты несогласующейся с протокольным стеком приемника версией, отбрасываются. Одновременно, включение версии в каждую дейтограмму позволяет использовать разные, но согласующиеся, версии на разных хостах.
- **Длина заголовка (Internet Header Length, IHL) -** Поле определяет длину заголовка, измеренную в 32-битных словах. Корректный заголовок имеет длину не менее 5 слов. Длина поля опций (в 32- разрядных словах) может быть определена как значение этого поля минус 5.
- **Тип сервиса (Type of service, ToS) –** определяет тип требуемого обслуживания пакета. Первые три бита задают уровень приоритета обслуживания (0-7), 3-5 биты определяют требования к задержке (какая получится, низкая), уровень пропускной способности (обычный, высокий) и надежность доставки (какая получится, высокая). Практически, большая часть маршрутизаторов игнорирует данные этого поля. Однако в настоящее время в связи с разработкой механизмов обеспечения в IP-сетях служб с гаранированным качеством обслуживания делаются попытки использования значений этого поля.
- **Общая длина (Total length)** - поле содержит общую длину пакета, размер которого не может превышать 65535 байт. Практически пакеты такой длины никогда не используются, поскольку технологии канального уровня накладывают свои ограничения. Так, Ethernet не допускает кадров с длиной более 1500 байт, FDDI – 4096

байт и т.д. В этой связи, протокол IP выполняет фрагментацию сегментов данных, поступающих к нему от TCP и UDP протоколов. Следует отметить, что маршрутизатор не выполняет сборку пакетов, даже если следующая сеть имеет параметр MTU (Maximum Transmission Unit), допускающий более крупные пакеты. Сборка пакетов в исходный сегмент производится на месте назначения.

- Поля «**Идентификатор**», **«Флаги**» и «**Смещение фрагмента**» управляют процессом сборки сегмента.
- **Время жизни (Time to live, TTL) -** поле, определяющее максимальное время, которое пакет может существовать в сети. Значение этого поля (в секундах) устанавливается при отправке пакета и уменьшается на единицу по мере прохождения им маршрутизаторов. При достижении нулевого значения этого поля пакет уничтожается. Максимальное значение поля – 255 секунд. Этот механизм помогает избежать перегрузок сети при возникновении ошибок в таблицах маршруизации, приводящих к образованию петель.

- Структура IP – пакета

Значение	Ключевое	Протокол
0	Reserved	Зарезервировано
1	ICMP	Internet Control Message
2	IGMP	Internet Group Management
4	IP	Internet Protocol
6	TCP	Transmission Control Protocol
17	UDP	User Datagram Protocol
89	OSPF	Open Shortest Path First

- Поле «Протокол» заголовка IP-пакета

- **5**

- **Протокол (Protocol) –** поле указывает модулю какого протокола (TCP, UDP, ICMP) передать полученный IP-пакет. На слайде 5. приведены значения этого поля для некоторых из протоколов. В дальнейшем нас будут интересовать TCP, UDP, ICMP.

- Структура IP – пакета

- **0 4 8 16 31**

Вер	**Дли**	**Тип сервиса**	**Общая длина пакета (Total Lenght)**
Идентификатор		**Фл аг**	**Смещение фрагмента**
Время жизни	**Протокол (см. след**	**Контрольная сумма**	
Адрес отправителя (Source IP address)			
Адрес получателя (Destination IP address)			
Опции (поле переменной длины)			**Выравнивание до 32 бит (padding)**

- Формат заголовка IP-пакета

- **4**

- **Контрольная сумма (Header checksum) –** поле содержит значение контрольной суммы**,** рассчитанной только по заголовку. Поскольку значения некоторых полей заголовка изменяются по мере прохождения пакета по маршруту (поле TTL, например), то значения рассматриваемого поля проверяются и пересчитываются на каждом маршрутизаторе. Этот механизм является единственным средством обеспечения достоверности передачи, содержащимся в протоколе IP.
- **Адрес отправителя (Source IP address)** и **Адрес получателя (Destination IP address)** – поля одинаковой длины (32 бита), содержащие соответствующие адреса. Правила адресации в IP-сетях будут рассмотрены далее.
- **Опции (Options)** – необязательное поле, используемое при отладке сетей и для

запроса определенных специфических процедур обработки. В настоящее время используется крайне редко. В связи с разработкой новых протоколов, обеспечивающих большую гибкость в обработке IP-трафика, возможность использования этих полей вновь стала предметом обсуждения комитетов по стандартизации.

- При получении пакета маршрутизатор вычисляет контрольную сумму заголовка пакета и, если она не совпадает со значением поля «Контрольная сумма», то пакет отбрасывается. При положительном результате проверки, производится изменение некоторых полей и рассчитывается новое значение поля
- «Контрольная сумма». Затем по таблице маршрутизации определяется адрес следующего маршрутизатора, на который должен быть направлен этот пакет, и он передается на соответствующий интерфейс.

- Адресация в сетях IP
- **0 8 16 31**

Класс A

Класс B

- **Класс C Класс D**

• К л ас	• Значение первого	• Количество сетей	• Количество хостов	• Удельный вес класса в адресном
• A	• 001 – 126	• 126	• 16	• 50
• B	• 128 – 191	• 16	• 65	• 25
• C	• 192 - 223	• 2 097	• 254	• 12,5

- **6**

- **Адресация в сетях IP.**

- Для идентификации каждого компьютера в IP-сети необходима система их адресации. При этом учитывается, что сетевые устройства (компьютер, маршрутизатор и т.д.) могут иметь несколько сетевых интерфейсов, и каждый из них должен иметь уникальный адрес. Если обратиться к аналогии обычной адресной системы (улица, дом, квартира), то становиться ясной целесообразность построения системы сетевой адресации по иерархии «сеть-интерфейс». Принятая в сетях IP система адресации описана в документах RFC 990 и RFC 997. Каждое сетевое устройство имеет адреса трех типов:
- Физический адрес узла, определяемый используемой технологией канального

уровня. Для Ethernet – это MAC-адрес его сетевой карты, назначаемый фирмой-производителем. Он представляет собой шести-байтовое число, первые три байта которого однозначно определяют фирму-производителя, а последние три байта – уникальны для каждой карточки, произведенной в рамках данной фирмы.

- IP-адрес, состоящий из 4-х байтов, и также являющийся совершенно уникальным.
- Символьный идентификатор – имя, назначаемое по определенным правилам и являющееся полным эквивалентом IP-адреса.

- IP-адрес строится по двухуровневой иерархии, т.е. он объединяет в себе адрес сети и адрес хоста. Разделение сетевого адреса на 2 части имеет большой практический смысл, ибо позволяет магистральным маршрутизаторам существенно сократить размер своих таблиц коммутации, формируя их на основании только сетевой части адреса назначения. Для удовлетворения потребностей адресации сетей различного масштаба были введены несколько классов сетей, отличающиеся размером полей, отводимых для указания номера сети и номера хоста. При этом, размер поля полного адреса всегда равен 32 битам. Структура адресов сетей разных классов приведена на слайде.

- IP-адрес обычно записывается в форме 4-х трехразрядных десятичных чисел, разделенных точкой. Каждое из этих десятичных чисел соответствует одному байту двоичного представления адреса. Так, например, адрес 10000000 10000111 01000100 00000101 в десятичном представлении имеет вид 128.135.68.5. В этом случае, т.к. первые два бита адреса – 10, то это адрес хоста, принадлежащего сети класса **B** и, следовательно, левые 16 бит являются адресом сети, а правые16 бит – адресом хоста.

- Некоторые адреса являются зарезервированными и не могут присваиваться хостам. Так, адрес 127.x.x.x (x – означает любое число, обычно 0) зарезервирован для обратной связи, используемой при тестировании взаимодействия процессов на одной сетевой станции. Когда приложение использует этот адрес в качестве адреса назначения, стек TCP/IP данного хоста возвращает данные приложению, ничего не передавая на физический интерфейс. Поэтому адреса, начинающиеся на 127, запрещается присваивать сетевым устройствам. Другим зарезервированным адресом является, так называемый, широковещательный адрес, содержащий 1, или 0, во всех своих битах. Пакет с адресом назначения 255.255.255.255 (1.1.1.1) будет доставлен всем устройствам сети, к которой принадлежит узел- отправитель, но маршрутизаторы такие пакеты не обрабатывают. Существует и направленное широковещание – способ адресации, при котором один пакет, отосланный в определенную сеть, будет доставлен всем ее хостам. Такой пакет должен содержать корректный адрес сети и иметь все биты адреса хоста равными 1. Так, например, пакет с адресом 184.90.255.255 будет доставлен всем станциям сети класса **B**, имеющей адрес 184.90.

- Из рисунка вверху хорошо видно, что значения первых четырех битов адреса однозначно определяют обе границы его сетевой части. Нетрудно сосчитать, что максимальное число сетей класса **A** равно $2^6+2^5+ \ldots.+2^0 -1 =126$ (сетевой префикс, состоящий из одних нулей недопустим). Каждая сеть класса **A** может содержать $2^{24}-2 = 16\ 777\ 214$ устройств. В целом, адресный блок сетей класса **A** занимает около 50% общего адресного пространства. В таблице внизу слайда содержатся аналогичные

показатели для сетей класса **B** и **C**.

- **Разбиение IP-сети на подсети.**

- Рассмотренная выше двухуровневая схема адресации оказалась недостаточно гибкой и в 1985 году была определена трехуровневая схема адресации (RFC 950). Необходимость перехода к такой системе адресации можно проиллюстрировать следующим примером. Организация получила сеть класса **B**, позволяющую адресовать 65000 хостов. Пока в сети работали относительно немного станций
- она функционировала благополучно. Но с ростом числа активных хостов неизбежно рос и широковещательный трафик, поскольку этот тип пакетов активно используется в служебных целях многими протоколами. Это обстоятельство неизбежно вело к снижению эффективной производительности сети. Кроме того, управление несколькими десятками тысяч подключений из единого административного центра представляет собой очень трудную задачу. К этим проблем следует добавить и то, что любая организация развивается в направлении роста самостоятельности своих подразделений, что также неизбежно должно отражаться и в структуре сети. Возможность же структурирования сети организации за счет получения дополнительных номеров сетей была быстро исчерпана и резкая нехватка адресного пространства стала реальностью еще во второй половине 80-х годов. Кроме того, рост числа используемых сетей вел к росту таблиц маршрутизации магистральных (межсетевых) маршрутизаторов и, следовательно, к снижению их производительности.

- Перечисленные проблемы в значительной степени связаны с проблемой масштабируемости сети, и они, в значительной степени, были разрешены посредством введения в иерархию адресации третьего уровня. Этот уровень, получивший название «уровень подсети», был выделен в пространстве адресов хоста

- Разбиение IP-сети на подсети

- 2-х

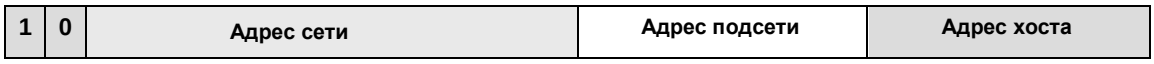
1	0	Адрес сети	Адрес хоста

уровнев

ая

схема

- 3-х уровнев ая схема



- **Схема адресации с введением подсетей**

•	• • Подс	• • Маска	• Эквивал ентный	• Число хостов в
• Исход	• 193.1	• 255.255.	• 193.10.1.	• 254
• Подсе	• 193.1	• 255.255.	• 193.10.1.	• 126
• Подсе	• 193.1	• 255.255.	• 193.10.1.	• 62
• Подсе	• 193.1	• 255.255.	• 193.10.1.	• 30
• Подсе	• 193.1	• 255.255.	• 193.10.1.	• 30

- **Разбиение сети класса «С» на подсети**

• **7**

- При этом поля адреса сети и адреса подсети в совокупности называют расширенным сетевым префиксом. В рассмотренном выше примере, выделение в пространстве адреса хоста 6 разрядов для адреса подсети позволяет организовать 62 подсети, содержащих до 1022 хостов каждая. Такое разбиение на подсети не требует согласования со специальным служебным органом Интернет, регулирующим распределение адресного пространства, Network Information Center.
- Отрицательным следствием введения подсетей стало усложнение процедуры определения адреса хоста. Действительно, сетевые устройства используют старшие биты сетевого адреса для определения класса сети, после чего, в случае двухуровневой иерархии, легко находится граница между битами сетевого адреса и адреса хоста. В трехуровневой системе адресации этот прием работать не сможет. Для определения адреса подсети и адреса хоста потребовалось ввести **сетевую маску –** 32-битный адрес, в котором все биты, соответствующие битам расширенного сетевого префикса, установлены в 1, а соответствующие битам адреса хоста – в 0. Так, например, пусть необходимо в сети класса **B** 132.10 выделить подсеть, содержащую не более 100 хостов. Для адресации такого числа сетевых устройств достаточно располагать 7 битами (2^7 =128), которые и отводятся для адреса хоста; оставшиеся 9 бит отводятся для номера подсети (их можно организовать 2^9 -2=510) а старшие 16 бит – это адрес сети.

- Таким образом, маска подсети, в которой находятся хосты с адресами:
- 132.10.12.129, 132.10.12.130,….,132.10.12.254
- будет иметь вид
- 11111111 11111111 11111111 10000000 (255.255.255.128).
- Если маршрутизатор получит пакет с адресом
  назначения 10000100 00001010 00001100
  10110000 (132.10.12.176)
- и выполнит по отношению к нему и сетевой маске операцию логического И, то результат будет содержать номер подсети. В данном случае получаем:
- 10000100 00001010 00001100 10000000,

- что соответствует адресу подсети 132.10.12.128. Далее, по таблице маршрутизации будет найден следующий узел на пути к этой подсети, и пакет отправится на соответствующий интерфейс.

- Необходимо заметить, что информация о маске подсети IP-пакетом не переносится (хост-источник о структуре сети, в которой находится получатель, ничего не знает). Передача этой информации является задачей протоколов маршрутизации, или она задается статически при конфигурировании маршрутизатора.

- В стандартах, описывающих современные протоколы маршрутизации, часто делается ссылка на длину расширенного префикса сети, а не на маску подсети. В такой записи адрес устройства в рассмотренном выше примере имеет вид 132.10.12.176/25. В качестве примера нумерации подсетей в таблице приведено разбиение сети класса **C** на подсети. Указанное в таблице число хостов в каждой из подсетей на два меньше возможного числа адресов, поскольку адреса, в которых все биты поля адреса хоста установлены в единицу и в ноль, являются зарезервированными и используются как широковещательные для данной подсети. Так при подсетях, приведенных в таблице., адрес 193.10.1.0 является широковещательным лишь для подсети 193.10.1.0/24, а не для всех подсетей. Аналогично, адрес 193.10.1.255 является широковещательным только для подсети 193.10.1.224/27.

- Введение подсетей, решив проблемы масштабирования адресного пространства, потребовало определенного усложнения протоколов маршрутизации, которые должны обрабатывать (и переносить) не только адрес сетевого устройства, но и его маску. В настоящее время все широко используемые протоколы маршрутизации (RIP-2, IS-IS, OSPF) переносят эту информацию.

- **IP маршрутизация.**

- Каждый хост (станция, маршрутизатор) ведет свои маршрутные таблицы, которые и определяют порядок обработки IP-пакетов. Передача пакетов между конечными

станциями, требует взаимодействия

- IP-модулей программного обеспечения этих станций и маршрутизаторов, связывающих сети, в которых они (станции) находятся. Рассмотрим, как обрабатывается пакет на этих сетевых устройствах.

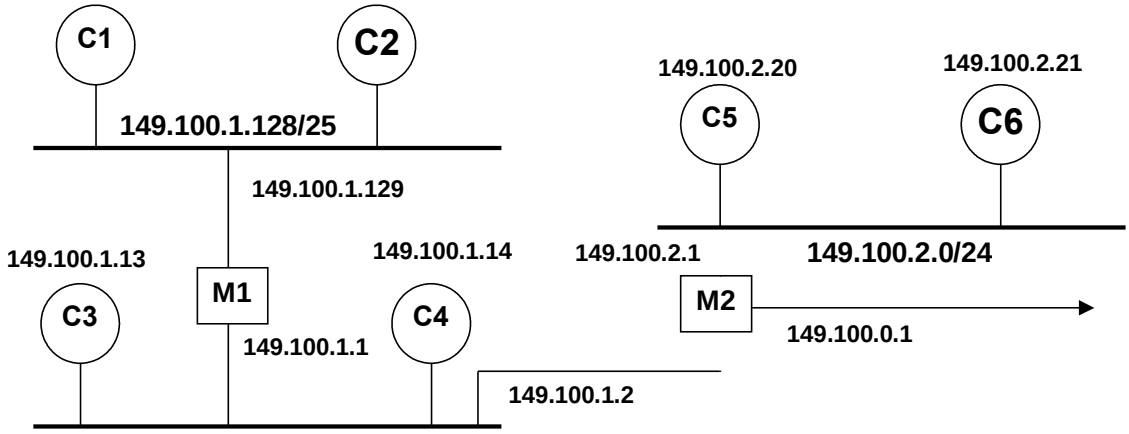
- Если в таблице маршрутизации станции-отправителя указано, что станция назначения является непосредственно присоединенной к той же ЛВС, то из таблицы физических адресов, которая ведется на каждой сетевой станции, извлекается физический адрес узла назначения, пакет инкансулируется в кадр канального протокола и передается к станции назначения. Если таблица маршрутизации станции- отправителя не содержит искомый сетевой адрес, то пакет отправляется по адресу маршрутизатора, который был указан при конфигурировании станции в качестве шлюза по умолчанию (default router, default gateway). Этот шлюз обязательно имеет физический интерфейс в той же ЛВС, что и станция- отправитель. При получении пакета маршрутизатор проверяет, не совпадает ли адрес назначения этого пакета с его собственным IP-адресом. Если это так, то пакет передается модулю протокола, указанного в поле «Протокол» заголовка пакета. В противном случае, маршрутизатор посредством своей таблицы определяет адрес следующего хоста, которому он должен передать этот пакет, и свой интерфейс, на который следует его направить.

- Каждая строка в таблице маршрутизации содержит следующую информацию: IP-адрес сети (узла) назначения, IP-адрес следующего маршрутизатора, способного обеспечить передачу пакета в эту сеть (этому узлу), имя выходного интерфейса и некоторые флаги. Флаги содержат уточняющую информацию о каждой записи в таблице. Так например, флаг **H** определяет, является ли данная строка таблицы маршрутом к хосту (**H**=1), или к сети (**H**=0); флаг **G** уточняет, является ли она маршрутом к другому маршрутизатору (**G**=1), или определяет путь к непосредственно подключенной станции (**G**=0).

- Поиск в таблице маршрутизации ведется следующим образом. Прежде всего, сканируется ее первый столбец с целью нахождения записи, точно соответствующей адресу назначения пакета. Если такая обнаруживается, то пакет отправляется по

адресу, указанному в столбце «Следующий маршрутизатор». В противном случае, ведется поиск строки, содержащей адрес сети назначения. Если такой записи нет, то ищется строка, определяющая маршрут по умолчанию, т.е. маршрут к узлу с более полной информацией о траектории передачи этого пакета. Если не один из перечисленных вариантов не реализуем, то пакет уничтожается, а узлу-отправителю отправляется сообщение «Хост недостижим». Рассмотрим таблицы маршрутизации в сети, изображенной на след. слайде.

- IP – маршрутизация
- **149.100.1.158** **149.100.1.159**



- **149.100.1.0/25**
- **Пример сети, объединенной маршрутизаторами**

- Таблица маршрутизации **C6** :

Адрес назначения	Маска сети	Следующий узел	Флаг	Интерфейс
127.0.0.0	255.0.0.0	127.0.0.1	H	lo0
Default	0.0.0.0	149.100.2.1	G	Eth0
149.100.2.0	255.255.255.0	149.100.2.21		Eth0

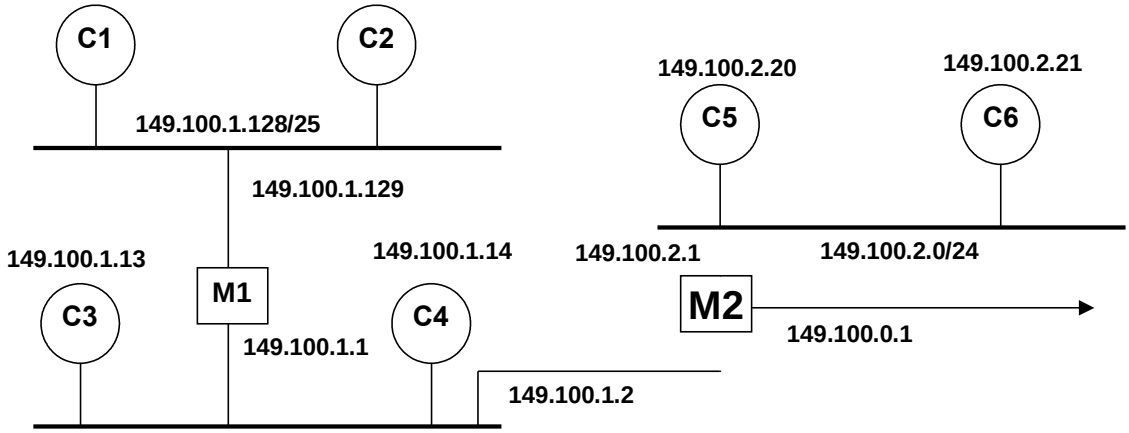
- **8**

- Эта сеть содержит три подсети: 149.100.1.0/25 149.100.1.128/25, 149.100.2.0/24, которые объединены двумя маршрутизаторами M1 и M2. При этом маршрутизатор M2 является шлюзом в Интернет. Адреса интерфейсов маршрутизаторов показаны на рисунке. Предположим, что станция C6 имеет пакет с адресом назначения 149.100.1.159. Таблица маршрутизации C6 выглядит следующим образом (таблица внизу слайда):

- Первая строка таблицы определяет закольцовывающий интерфейс. Вторая строка описывает маршрут по умолчанию и флаг G уточняет, что узел 149.100.2.1 является маршрутизатором. Третья запись таблицы не имеет флага H,

следовательно, она определяет сеть; нет в ней и флага G и это говорит о том, что определяется маршрут к непосредственно подключенной сети и интерфейсом к ней является внешний интерфейс станции С6, имеющий адрес 149.100.2.21. Прежде всего С6 производит поиск адреса станции (или сети) назначения в своей таблице. Поскольку ни тот, ни другой в ней не присутствуют, то пакет будет отправлен в соответствии с маршрутом по умолчанию на маршрутизатор М2 с адресом 149.100.2.1 через интерфейс Eth0.

- IP – маршрутизация
- **149.100.1.158** **149.100.1.159**



- **149.100.1.0/25**

- **Пример сети, объединенной маршрутизаторами**

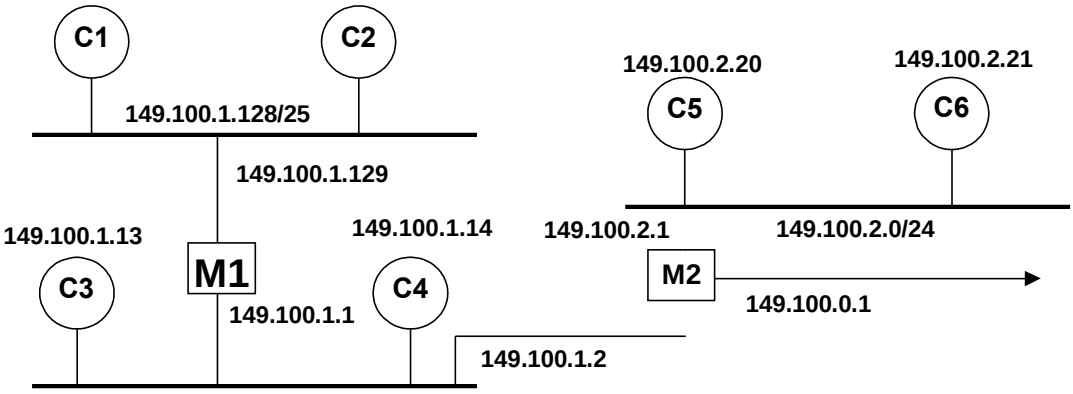
- Таблица маршрутизации **M2** :

Адрес назначения	Маска	Следующий узел	Флаг	Интерфейс
127.0.0.0	255.0.0.0	127.0.0.1	H	lo0
default		149.100.0.1	G	Serial 01
149.100.2.0	255.255.255.0	149.100.2.1		Eth0
149.100.1.0	255.255.255.192	149.100.1.2		Eth1
149.100.1.128	255.255.255.192	149.100.1.1	G	Eth1

- **9**

- Таблица маршрутизации M2 может иметь следующий вид (внизу слайда).
- Выполнив поиск в этой таблице маршрутизатор M2 найдет, что наиболее полно согласуется с адресом назначения маршрут, определенный в строке 5 и отправит пакет к маршрутизатору M1 через интерфейс Eth1.

- IP – маршрутизация
- **149.100.1.158** **149.100.1.159**



- **149.100.1.0/25**
- **Пример сети, объединенной маршрутизаторами**

- Таблица маршрутизации **M1** :

Адрес назначения	Маска	Следующий узел	Флаг	Интерфейс
127.0.0.0	255.0.0.0	127.0.0.1	H	lo0
default		149.100.1.2	G	Eth1
149.100.2.0	255.255.255.0	149.100.1.2	G	Eth1
149.100.1.0	255.255.255.192	149.100.1.1		Eth1
149.100.1.159	255.255.255.255	149.100.1.159		Eth0
149.100.1.128	255.255.255.192	149.100.1.129		Eth0

- **10**

- Таблица маршрутизации M1 представлена внизу в таблице.
- В ней представлен маршрут с адресом назначения точно соответствующим адресу назначения пакета. Поэтому последний передается на интерфейс Eth0 и доставляется станции C2 с IP-адресом 149.100.1.159.

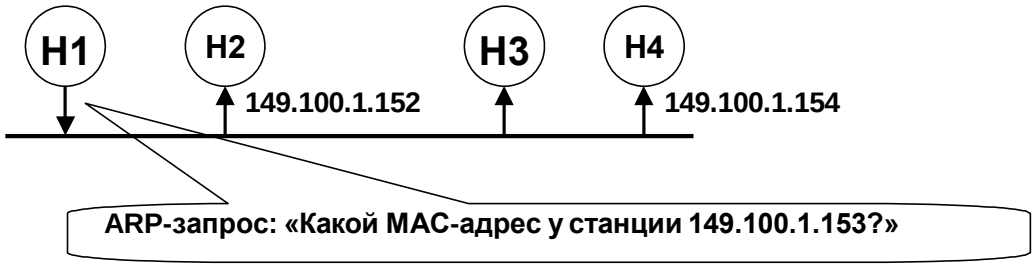
- **Разрешение IP-адресов в физические адреса сетевых устройств. Протокол ARP.**

- Для доставки IP-пакета к станции назначения, или от одного маршрутизатора к другому, необходимо передать его протоколу канального уровня, например

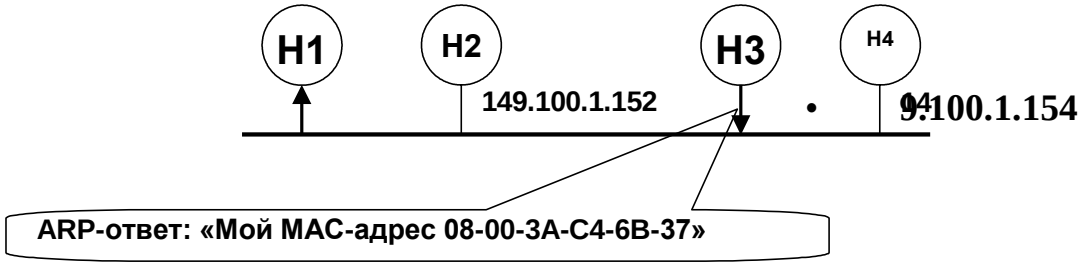
Ethernet. Последний же «умеет» передавать кадры только по физическим адресам устройств, подключенных к среде передачи. В IP- сетях задачу преобразования сетевых адресов в физические решает протокол ARP (Address Resolution Protocol). Идея его функционирования иллюстрируется следующий слайд.

- ARP (Address Resolution Protocol)

- **149.100.1.151** **149.100.1.153**



- **149.100.1.151** **149.100.1.153**



- **Разрешение IP-адреса в локальной сети**

- **11**

- Пусть хост H1 хочет отослать пакет хосту H3, MAC-адрес которого не известен. Хост H1 генерирует так называемый ARP-запрос – специальный пакет, имеющий широковещательный адрес назначения. В теле этого запроса находится IP-адрес хоста, MAC-адрес которого необходимо узнать. Каждый хост сети получив такой пакет, сравнивает находящийся в нем IP-адрес со своим. Если совпадение обнаружено, то этот хост посылает запрашивающей станции ответный пакет

(ARP-ответ), содержащий его физический адрес. На всех остальных станциях сети пакеты ARP-запросов уничтожаются. Для того, чтобы уменьшить количество ARP-запросов, каждое сетевое устройство имеет специальную буферную память, в которой хранится ARP-таблица. Последняя пополняется каждый раз, когда хост получает ARP-ответ.

- В ARP-таблице могут быть как статические, так и динамические записи. Статические записи добавляются администратором и сохраняются в таблице до перезагрузки устройства. Кроме того, в таблице всегда содержится широковещательный адрес (%FFFFFFFFFFFF), который позволяет принимать широковещательные запросы. Динамические записи добавляются и удаляются автоматически. Каждая такая запись имеет потенциальное время жизни. После добавления записи в таблицу включается специальный таймер и, если в течении первых двух минут запись не используется, то она удаляется; в противном случае, время жизни такой записи составляет некое предустановленную величину (обычно 10 минут). Далее приведен фрагмент ARP-таблицы маршрутизатора.

- ARP (Address Resolution Protocol)

IP-	Port	Type	Media Address	Address
20.0.0.	2	Broadcast	%FFFFFFFFFFF	Static
10.0.0.	1	Broadcast	%FFFFFFFFFFF	Static
10.0.0.	1	Local	%080002145DE6	Static
20.0.0.	2	Local	%080002145DE5	Static
10.0.0.	1	External	%080002A56BC0	ARP
20.0.0.	2	External	%080002A719DD	ARP

- **Фрагмент ARP-таблицы маршрутизатора**

0 4 8 16 31

Тип сети		Тип протокола
Длина апп.	Длина сет.	Тип операции
Аппаратный адрес отправителя		
Аппаратный адрес		Сетевой адрес
Сетевой адрес отправителя		Аппаратный адрес
Аппаратный адрес получателя		
Сетевой адрес получателя		

- **Формат ARP-пакета**

12

- Протокол ARP достаточно универсален, и его можно применять в сетях, использующих любые технологии на сетевом и канальном уровнях. Заголовок ARP-пакета имеет формат, отличный от IP- заголовка и поэтому не передается маршрутизаторами. На рисунке внизу представлен формат сообщения ARP.
- В поле «Тип сети» для Ethernet указывается значение 1. Для других типов сетей его значения определяются соответствующим стандартом. Поля «Тип протокола», «Длина аппаратного адреса» и
- «Длина сетевого адреса» обеспечивают отмеченную выше универсальность формата ARP-пакета. В поле «Тип операции» для ARP-запроса указывается 1, для ARP-ответа – 2.

- Устройство, отправляющее ARP-запрос, заполняет в этом пакете все поля, кроме искомого аппаратного адреса. Значение этого поля заполняется станцией, опознавшей свой IP-адрес, указанный в этом пакете в поле «IP-адрес получателя».

- Определение виртуальных частных сетей
- Итак, мы намереваемся передавать через интернет секретные данные организации без использования арендуемых каналов связи, по-прежнему принимая все меры для обеспечения конфиденциальности трафика. Каким же образом нам удастся отделить свой трафик от трафика остальных пользователей глобальной сети? Ответом на этот вопрос является шифрование.
- В интернете можно встретить трафик любого типа. Значительная часть этого трафика передается в открытом виде, и любой пользователь, наблюдающий за этим трафиком, сможет его распознать. Это относится к большей части почтового и веб-трафика, а также сеансам связи через протоколы telnet и FTP. Трафик Secure Shell (SSH) и Hypertext Transfer Protocol Secure (HTTPS) является шифруемым трафиком, и его не сможет просмотреть пользователь, отслеживающий пакеты. Тем не менее, трафик типа SSH и HTTPS не образует виртуальную частную сеть VPN.
- Виртуальные частные сети обладают несколькими характеристиками.

- Трафик шифруется для обеспечения защиты от прослушивания.
- Осуществляется аутентификация удаленного сайта.
- Виртуальные частные сети обеспечивают поддержку множества протоколов.
- Соединение обеспечивает связь только между двумя конкретными абонентами.
- Так как SSH и HTTPS не способны поддерживать несколько протоколов, то же самое относится и к реальным виртуальным частным сетям. VPN-пакеты смешиваются с потоком обычного трафика в интернете и существуют отдельно по той причине, что данный трафик может считываться только конечными точками соединения.
- **Примечание**
- Возможно реализовать передачу трафика через сеанс SSH с использованием туннелей. Тем не менее, в рамках данной лекции мы не будем рассматривать SSH как VPN.
- Рассмотрим более детально каждую из характеристик VPN. Выше уже говорилось о том, что трафик VPN шифруется для защиты от прослушивания. Шифрование должно быть достаточно мощным, чтобы можно было гарантировать конфиденциальность передаваемой информации на тот период, пока она будет актуальна. Пароли имеют срок действия, равный 30 дням (подразумевается политика изменения пароля через каждые 30 дней); однако секретная информация может не утрачивать своей ценности на протяжении долгих лет. Следовательно, алгоритм шифрования и применение VPN должны предотвратить нелегальное дешифрование трафика на несколько лет.
- Вторая характеристика заключается в том, что осуществляется аутентификация удаленного сайта. Эта характеристика может требовать аутентификацию некоторых пользователей на центральном сервере либо взаимную аутентификацию обоих узлов, которые соединяет VPN. Используемый механизм аутентификации контролируется политикой. Политика может предусмотреть аутентификацию пользователей по двум

параметрам или с использованием динамических паролей. При взаимной аутентификации может потребоваться, чтобы оба сайта демонстрировали знание определенного общего секрета (под секретом подразумевается некоторая информация, заранее известная обоим сайтам), либо могут потребоваться цифровые сертификаты.

- Виртуальные частные сети обеспечивают поддержку различных протоколов, в особенности на прикладном уровне. Например, удаленный пользователь может использовать протокол SMTP для связи с почтовым сервером, одновременно используя NetBIOS для соединения с файловым сервером. Оба указанных протокола могут работать через один и тот же цикл связи или канал VPN (см. рис. 11.1).

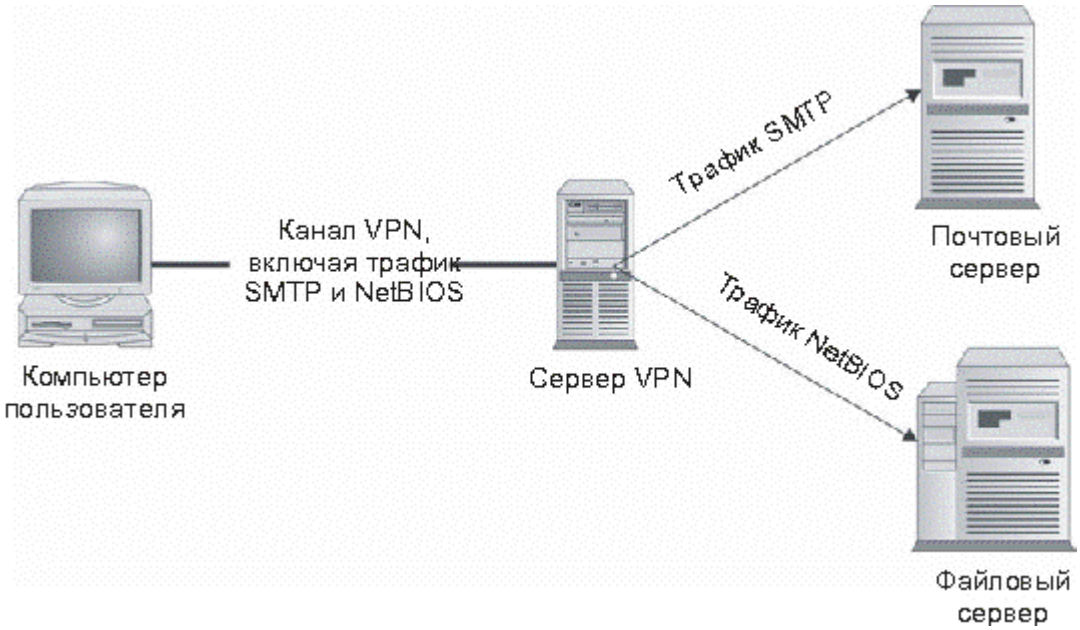


Рис. 11.1. Виртуальные частные сети поддерживают множество протоколов

- VPN соединяет два конкретных объекта, образуя таким образом уникальный канал связи между двумя абонентами. Каждая из конечных точек VPN может единовременно поддерживать несколько соединений VPN с другими конечными точками, однако каждая из точек является отдельной от других, и трафик разделяется посредством шифрования.
- Виртуальные частные сети, как правило, подразделяются на два типа: пользовательские VPN и узловые VPN. Различие между ними заключается в

методе использования, а не в способе отделения трафика каждым из двух типов сетей. В оставшейся части данной лекции будет детально рассказываться о каждом из типов VPN.

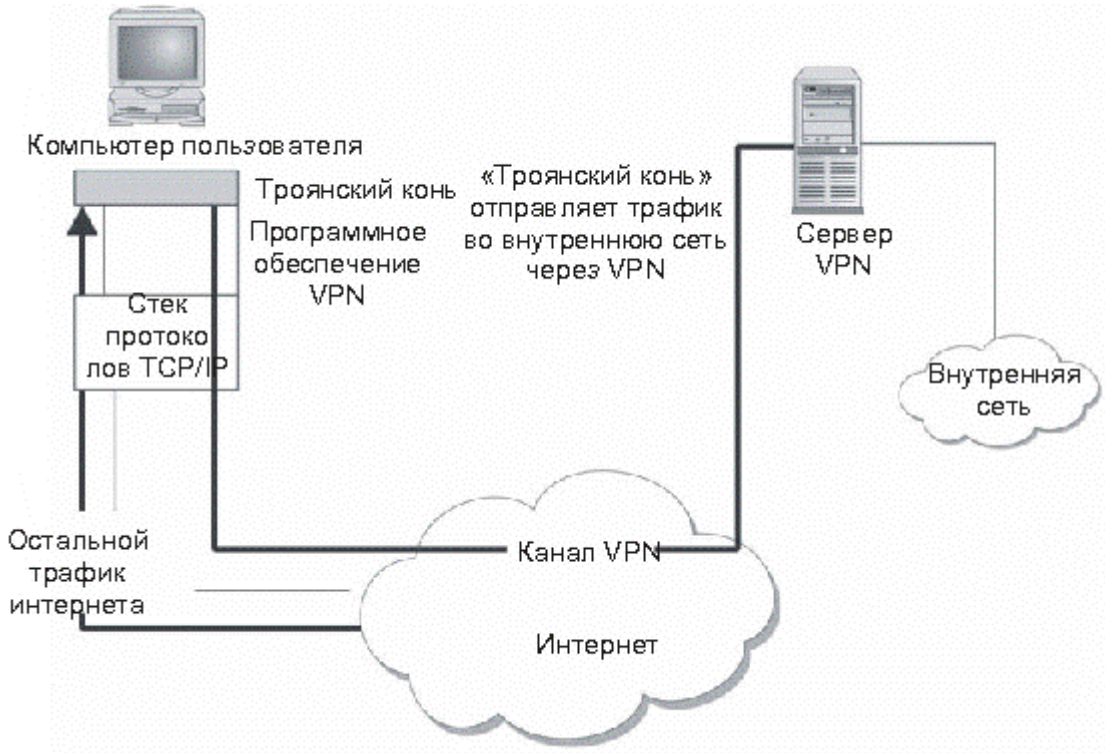
- Развертывание пользовательских виртуальных частных сетей
- Пользовательские VPN представляют собой виртуальные частные сети, построенные между отдельной пользовательской системой и узлом или сетью организации. Часто пользовательские VPN используются сотрудниками, находящимися в командировке или работающими из дома. Сервер VPN может являться межсетевым экраном организации либо быть отдельным VPN-сервером. Пользователь подключается к интернету через телефонное подключение к локальному поставщику услуг, через канал DSL или кабельный модем и инициирует VPN-соединение с узлом организации через интернет.
- Узел организации запрашивает у пользователя аутентификационные данные и, в случае успешной аутентификации, позволяет пользователю осуществить доступ ко внутренней сети организации, как если бы пользователь находился внутри узла и физически располагался внутри сети. Очевиден тот факт, что скорость сетевого соединения будет ограничиваться скоростью подключения пользователя к интернету.
- Пользовательские VPN позволяют организациям ограничивать доступ удаленных пользователей к системам или файлам. Это ограничение должно базироваться на политике организации и зависит от возможностей продукта VPN.
- В то время как пользователь имеет VPN-соединение с внутренней сетью организации, он также может соединяться и работать с интернетом или выполнять другие действия как обычный пользователь интернета. Сеть VPN поддерживается отдельным приложением на компьютере пользователя (см. рис. 11.2).

- 

- **Рис. 11.2.** Конфигурация пользовательской VPN
- **Внимание**!
- В некоторых случаях компьютер пользователя может выступать в роли маршрутизатора между интернетом и сетью VPN (и, следовательно, внутренней сетью организации). Этот тип сетевого атакующего воздействия необходимо тщательно изучить перед применением пользовательской виртуальной частной сети. Некоторые клиенты VPN содержат политику, снижающую риск проявления данной угрозы.
- **Преимущества пользовательских VPN**
- Пользовательские VPN обладают двумя основными преимуществами:
- Сотрудники, находящиеся в командировке, могут осуществлять доступ к электронной почте, файлам и внутренним системам в любое время без необходимости в осуществлении дорогостоящих междугородних и международных телефонных вызовов для соединения с серверами.
- Сотрудники, работающие из дома, могут осуществлять доступ к службам сети, как и сотрудники, работающие в организации, без аренды дорогостоящих выделенных каналов.
- Оба эти преимущества можно приписать к экономии денежных средств. Экономия может заключаться в отказе от использования дорогостоящих

междугородних и международных соединений, арендуемых каналов связи или в выполнении сотрудниками задач по администрированию серверов, принимающих входящие телефонные соединения. Домашние пользователи с DSL или кабельными модемами могут добиться увеличения скорости при использовании линий телефонной связи со скоростями 56 Кбит/с. Все больше гостиничных номеров оборудуются соединениями для доступа в сеть, поэтому для пользователей, находящихся в поездке, создаются все условия для высокоскоростного доступа в сеть.

- **Примечание**
- Увеличение скорости через канал 56 Кбит/с не гарантируется. Средняя скорость соединения зависит от множества факторов, включая скоростные возможности интернет-соединения пользователя, интернет-соединения организации, уровень нагрузки интернета, а также число единовременных соединений с VPN-сервером.
- **Проблемы, связанные с пользовательскими VPN**
- Правильное использование пользовательских VPN может снизить затраты организации, но пользовательские VPN не являются решением всех возможных проблем. При их использовании имеют место значительные риски, связанные с безопасностью, и проблемы реализации, с которыми приходится считаться.
- Возможно, самой большой проблемой безопасности при использовании VPN сотрудником является одновременное соединение с другими сайтами интернета. Как правило, программное обеспечение VPN на компьютере пользователя определяет, должен ли трафик передаваться через VPN, либо его необходимо отправить на какой-либо другой сайт в открытом виде. Если на компьютер пользователя была произведена атака с использованием "троянского коня", возможно, что некий внешний нелегальный пользователь использует компьютер сотрудника для подключения к внутренней сети организации (см. рис. 11.3). Атаки данного типа осуществляются довольно сложно, но они совершенно реальны.

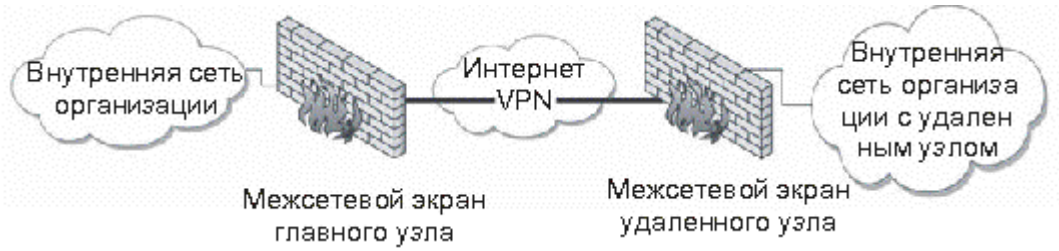
- Пользовательские VPN требуют такого же внимания к вопросам, связанным с управлением пользователями, как и внутренние системы. В некоторых случаях пользователи VPN могут быть привязаны к идентификаторам пользователей в домене Windows NT или Windows 2000 или к другой системе централизованного управления пользователями. Эта возможность упрощает управление пользователями, однако администраторам по-прежнему следует сохранять бдительность и следить за тем, каким пользователям требуется удаленный VPN-доступ, а каким - нет.
- 

- **Рис. 11.3.** Использование "троянского коня" для проникновения во внутреннюю сеть организации
- Если управление VPN-пользователями не связано с центральной системой управления пользователями, этот факт должен учитываться в процедурах управления пользователями, покидающими организацию.
- Пользователи должны проходить аутентификацию перед использованием сетей VPN. Так как VPN позволяет осуществлять удаленный доступ ко внутренней сети организации, эта аутентификация должна быть двухфакторной, то есть запрашивать два аутентификационных параметра.

Одним из параметров может являться сам компьютер пользователя. В этом случае вторым параметром должно быть нечто известное пользователю или непосредственно с ним связанное. В любом случае, второй параметр не должен находиться на компьютере и не должен быть с ним связан.

- В организациях должна приниматься в расчет нагрузка трафиком. Главной точкой нагрузки является VPN-сервер в узле организации. Ключевым параметром нагрузки является ожидаемое число одновременных соединений. При установке каждого соединения VPN-сервер должен иметь возможность расшифровывать дополнительный трафик. Хотя процессор может обеспечивать поддержку больших объемов трафика, он может не обеспечивать шифрование и расшифровку большого числа пакетов без значительных задержек. Следовательно, сервер VPN должен создаваться с учетом ожидаемого числа единовременных соединений.
- Еще один момент может повлиять на использование организацией пользовательской VPN. Он связан с использованием трансляции сетевых адресов (NAT) (для получения дополнительной информации по этой технологии обратитесь к "Архитектура интернета") на противоположном конце соединения. Если ожидается, что сотрудники организации будут пытаться использовать VPN с узлов, защищенных межсетевыми экранами, могут возникнуть проблемы. Например, если организация А является консалтинговой компанией с сотрудниками, работающими в организации Б, в А может возникнуть потребность предоставить своим сотрудникам обратную связь для работы с электронной почтой и получения доступа к файлам. Однако, если эти сотрудники работают с компьютеров, входящих в состав внутренней сети организации Б, в которой используется динамическая NAT для скрытия адресов внутренних систем, это окажется невозможным. Если в вашей организации предпочтение отдается использованию VPN именно таким образом, следует проверить возможности программного обеспечения VPN.
- **Управление пользовательскими VPN**

- Управление пользовательскими VPN, главным образом, заключается в управлении пользователями и их компьютерами. При разделении сотрудников необходимо выполнять соответствующие процедуры по управлению пользователями.
- Разумеется, на компьютерах пользователей должны устанавливаться правильные версии программного обеспечения VPN и реализовываться соответствующие конфигурации. Если компьютеры принадлежат организации, это программное обеспечение является стандартным компонентом для каждого компьютера. Если организация разрешает сотрудникам использовать VPN со своих домашних компьютеров, ей понадобится увеличить общий уровень поддержки этих пользователей, так как различные компьютеры и поставщики услуг интернета могут требовать наличие различных конфигураций.
- Развертывание узловых сетей VPN
- Узловые виртуальные частные сети используются организациями для подключения к удаленным узлам без применения дорогостоящих выделенных каналов или для соединения двух различных организаций, между которыми необходима связь для осуществления информационного обмена, связанного с деятельностью этих организаций. Как правило, VPN соединяет один межсетевой экран или пограничный маршрутизатор с другим аналогичным устройством (см. рис. 11.4).
- Чтобы инициировать соединение, один из узлов осуществляет попытку передать трафик другому узлу. Вследствие этого на обоих противоположных узлах соединения VPN инициируется VPN. Оба конечных узла определяют параметры соединения в зависимости от политик, имеющихся на узлах. Оба сайта будут аутентифицировать друг друга посредством некоторого общего предопределенного секрета либо с помощью сертификата с открытым ключом. Некоторые организации используют узловые VPN в качестве резервных каналов связи для арендуемых каналов.

- **Внимание**!
- При работе с данной конфигурацией необходимо обеспечивать правильную настройку маршрутизации. Кроме того, физический канал связи, используемый для VPN, обязательно должен отличаться от канала, используемого арендуемым соединением. Может оказаться так, что оба соединения осуществляются через один и тот же физический канал связи, вследствие чего не будет обеспечиваться должный уровень избыточности.
- 

- **Рис. 11.4.** Межузловое соединение VPN, проходящее через интернет
- **Преимущества узловых VPN**
- Как и в случае с пользовательскими VPN, основным преимуществом узловой VPN является экономичность. Организация с небольшими, удаленными друг от друга офисами может создать виртуальную частную сеть, соединяющую все удаленные офисы с центральным узлом (или даже друг с другом) со значительно меньшими затратами. Сетевая инфраструктура также может быть применена значительно быстрее, так как в удаленных офисах могут использоваться локальные ISP для каналов ISDN или DSL.
- На базе политики организации могут быть разработаны правила, определяющие, каким образом удаленные сайты будут подключаться к центральному сайту или друг к другу. Если узловая VPN предназначена для соединения двух организаций, то на доступ ко внутренним сетям и компьютерным системам могут налагаться строгие ограничения.
- **Проблемы, связанные с узловыми VPN**
- Узловые VPN расширяют периметр безопасности организации, добавляя новые удаленные узлы или даже удаленные организации. Если уровень

безопасности удаленного узла невелик, VPN может позволить злоумышленнику получить доступ к центральному узлу и другим частям внутренней сети организации. Следовательно, необходимо применять строгие политики и реализовывать функции аудита для обеспечения безопасности организации в целом. В случаях, когда две организации используют узловую VPN для соединения своих сетей, очень важную роль играют политики безопасности, установленные по обе стороны соединения. В данной ситуации обе организации должны определить, какие данные могут передаваться через VPN, а какие - нет, и соответствующим образом настроить политики на своих межсетевых экранах.

- Аутентификация узловых VPN также является важным условием для обеспечения безопасности. При установке соединения могут использоваться произвольные секреты, но один и тот же общий секрет не должен использоваться для более чем одного соединения VPN. Если предполагается использовать сертификаты с открытыми ключами, необходимо создать процедуры для поддержки изменения и отслеживания срока действия сертификатов.
- Как и в случае с пользовательскими VPN, сервер VPN должен поддерживать дешифрование и шифрование VPN-трафика. Если уровень трафика высок, сервер VPN может оказаться перегруженным. В особенности это относится к ситуации, когда межсетевой экран является VPN-сервером, и имеет место интернет-трафик большого объема.
- Наконец, необходимо обдумать вопросы, связанные с адресацией. Если узловая VPN используется внутри одной организации, в ней необходимо наличие одинаковой схемы адресации для всех узлов. В данном случае адресация не представляет какой-либо сложности. Если же VPN используется для соединения двух различных организаций, необходимо предпринять меры для предупреждения любых конфликтов, связанных с адресацией. На рисунке 11.5 отражена возникшая конфликтная ситуация.

Здесь обе организации используют части одного и того же частного адресного пространства (сеть 10.1.1.x).

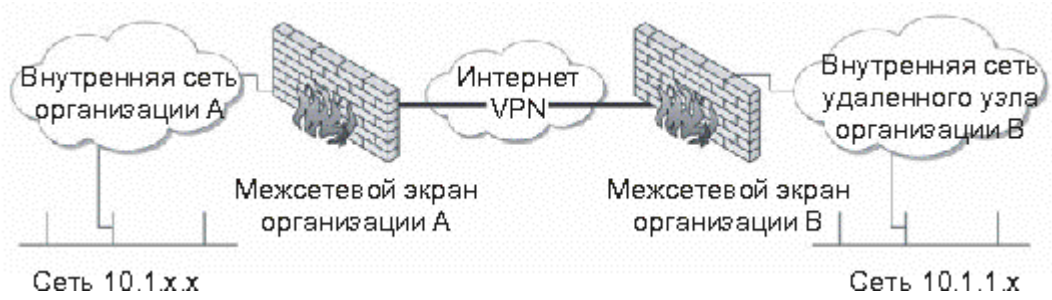
- 

Рис. 11.5. Узловая VPN может вызывать конфликты, связанные с адресацией

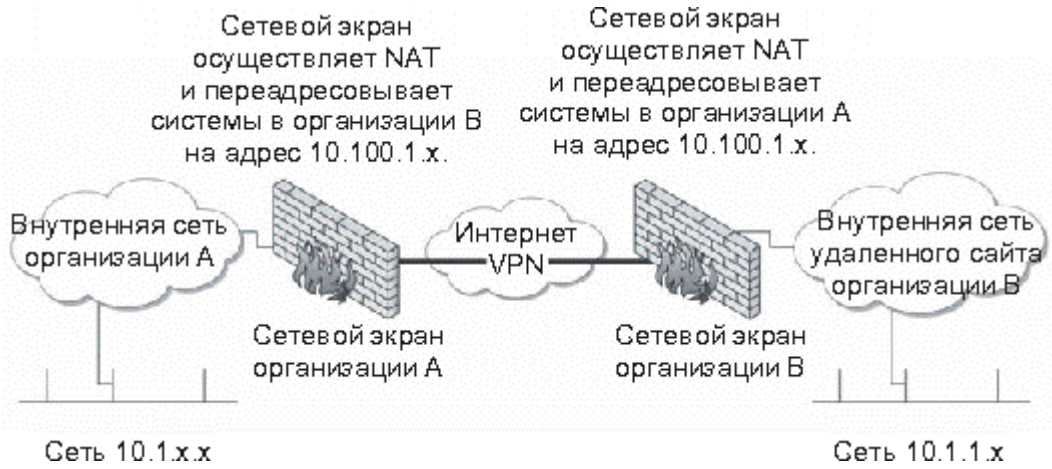
- Очевидно, что схемы адресации будут конфликтовать друг с другом, и маршрутизация трафика не будет функционировать. В данном случае каждая сторона соединения VPN должна выполнять трансляцию сетевых адресов и переадресовывать системы другой организации на их собственную схему адресации (см. рис. 11.6).
- **Управление узловыми VPN**
- 

Рис. 11.6. Узловая VPN использует NAT для предотвращения конфликтов адресации

- При осуществлении контроля над маршрутизацией могут понадобиться дополнительные функции по управлению. На маршрутизаторах внутренних сетей потребуется создать маршруты к удаленным сайтам. Эти маршруты, наряду с управлением схемой адресации, должны четко документироваться

во избежание непреднамеренного удаления маршрутов в процессе управления маршрутизатором.

- **Вопросы для самопроверки**
- Что является основной причиной применения в организациях сетей VPN?
- Информация, передаваемая через VPN, защищается с помощью _____.
- Понятие стандартных технологий функционирования VPN
- Сеть VPN состоит из четырех ключевых компонентов:
- Сервер VPN.
- Алгоритмы шифрования.
- Система аутентификации.
- Протокол VPN.
- Эти компоненты реализуют соответствие требованиям по безопасности, производительности и способности к взаимодействию. То, насколько правильно реализована архитектура VPN, зависит от правильности определения требований. Определение требований должно включать в себя следующие аспекты.
- Количество времени, в течение которого необходимо обеспечивать защиту информации.
- Число одновременных соединений пользователей.
- Ожидаемые типы соединений пользователей (сотрудники, работающие из дома или находящиеся в поездке).
- Число соединений с удаленным сервером.
- Типы сетей VPN, которым понадобится соединение.
- Ожидаемый объем входящего и исходящего трафика на удаленных узлах.
- Политика безопасности, определяющая настройки безопасности.
- При разработке системы также может оказаться полезным указать дополнительные требования, связанные с местоположением сотрудников, находящихся в поездке (имеются в виду узлы в других организациях или в номерах отелей), а также типы служб, которые будут работать через VPN.
- **Сервер VPN**

- Сервер VPN представляет собой компьютер, выступающий в роли конечного узла соединения VPN. Данный сервер должен обладать характеристиками, достаточными для поддержки ожидаемой нагрузки. Большая часть производителей программного обеспечения VPN должна предоставлять рекомендации по поводу производительности процессора и конфигурации памяти, в зависимости от числа единовременных VPN-соединений. Следует обеспечить наличие системы с соответствующими параметрами, а также позаботиться о ее дальнейшей модернизации.
- **Примечание**
- Может потребоваться создание нескольких серверов VPN, чтобы обеспечить поддержку ожидаемой нагрузки. В данном случае ожидаемые VPN-соединения должны как можно скорее распределяться между системами.
- Некоторые производители включают в свои системы методы обхода ошибок и разрешают наличие избыточных серверов VPN. Обход ошибок может не подразумевать распределение нагрузки, поэтому соединения могут по-прежнему требовать распределения между серверами. Это обстоятельство необходимо принимать во внимание при построении систем.
- VPN-сервер должен быть расположен в сети. Сервер может быть межсетевым экраном или пограничным маршрутизатором (см. рис. 11.7), что упрощает размещение VPN-сервера. В качестве альтернативы сервер может являться и отдельной системой. В этом случае сервер должен быть расположен в выделенной демилитаризованной зоне (DMZ) (см. рис. 11.8). В идеальном случае демилитаризованная зона VPN должна содержать только VPN-сервер и быть отдельной от DMZ интернета, содержащей веб-серверы и почтовые серверы организации. Причиной является то, что VPN-сервер разрешает доступ ко внутренним системам авторизованным пользователям и, следовательно, должен рассматриваться как объект с большей степенью доверия, нежели почтовые и веб-серверы, доступ к которым может быть осуществлен лицами, не пользующимися доверием.

Демилитаризованная зона VPN защищается набором правил межсетевого экрана и разрешает передачу только того трафика, который требует VPN.

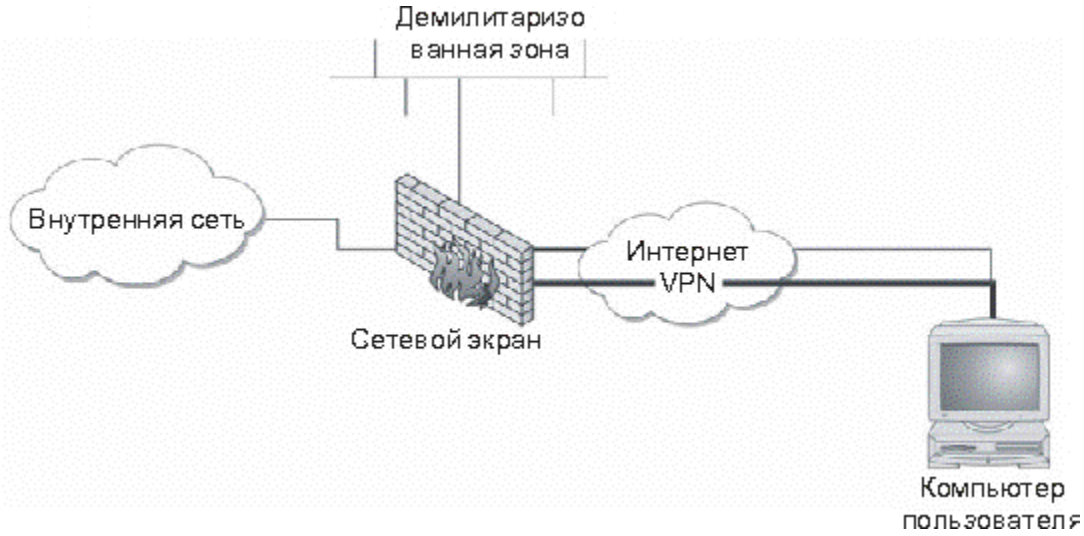
- 

Рис. 11.7. Архитектура сети VPN, в которой межсетевой экран является VPN-сервером

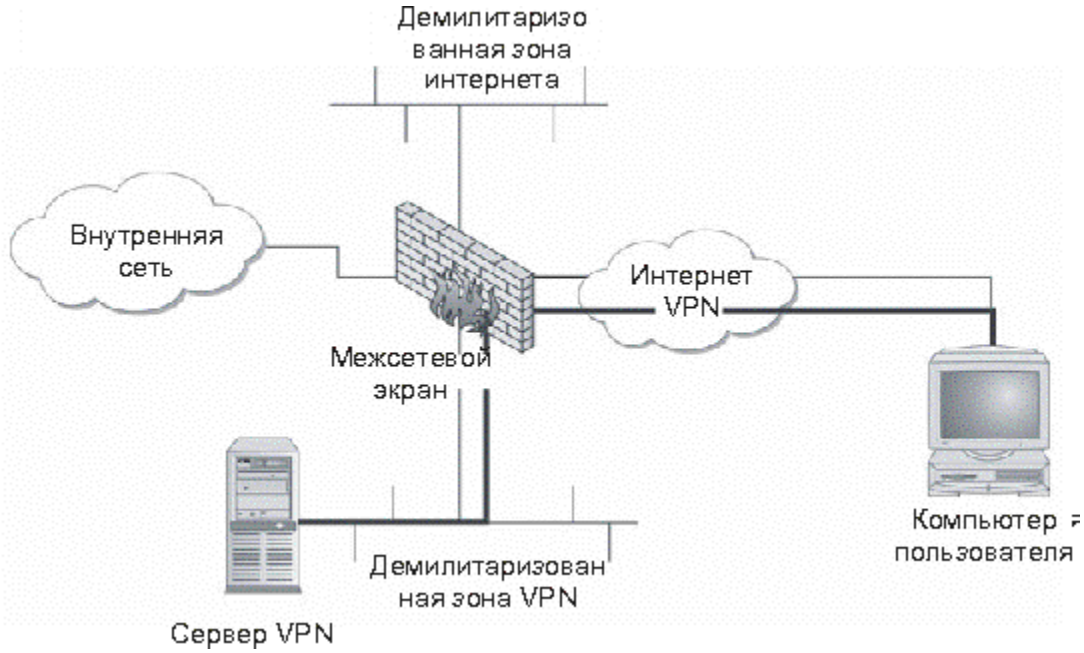
- 

Рис. 11.8. Архитектура сети VPN для отдельного сервера VPN

- Если VPN-сервер расположен в демилитаризованной зоне VPN, межсетевой экран может потребовать усовершенствования для поддержки нагрузки трафика. Даже несмотря на то, что межсетевой экран не будет выполнять функцию шифрования, исходный межсетевой экран может обладать

недостаточными характеристиками для обеспечения вычислительной мощности, необходимой для трафика VPN. Если трафик VPN является важным для организации, на межсетевом экране должна присутствовать некоторая система обхода ошибок. В качестве альтернативы можно использовать отдельную платформу VPN. Такое устройство обеспечит разгрузку межсетевого экрана, взяв на себя функции обработки VPN.

- Правила политики межсетевого экрана для демилитаризованной зоны VPN определены в табл. 11.1. Здесь содержатся правила, необходимые для демилитаризованной зоны интернета и демилитаризованной зоны VPN.
- Правила 1, 2 и 3 относятся к демилитаризованной зоне VPN. Правило 1 позволяет клиентам VPN осуществлять доступ к серверу VPN с использованием любой службы, требуемой программным обеспечением VPN. Правило 2 разрешает VPN-серверу осуществлять маршрутизацию этих соединений во внутреннюю сеть. Правило 3 исключает соединение демилитаризованной зоны интернета с демилитаризованной зоной VPN, изолируя демилитаризованную зону VPN от систем в DMZ интернета, пользующихся меньшим доверием.

Таблица 11.1. Правила политики межсетевого экрана, включающие демилитаризованную зону VPN

Номер правила	**Исходный IP**	**Конечный IP**	**Служба**	**Действие**
1	Любой	VPN-сервер	Служба VPN	Принятие.
2	VPN-сервер	Внутренняя сеть	Любой	Принятие

•	3	•	Любой	•	VPN-сервер	•	Любой	•	Отклонение
•	4	•	Любой	•	Веб-сервер	•	HTTP	•	Принятие
•	5	•	Любой	•	Почтовый сервер	•	SMTP	•	Принятие
•	6	•	Почтовый сервер	•	Любой	•	SMTP	•	Принятие
•	7	•	Внутренняя сеть	•	Любой	•	HTTP, HTTPS, FTP, telnet, SSH	•	Принятие
•	8	•	Внутренняя DNS	•	Любой	•	DNS	•	Принятие
•	9	•	Любой	•	Любой	•	Любой	•	Сброс

- **Алгоритмы шифрования**
- Алгоритм шифрования, используемый в VPN, должен быть стандартным мощным алгоритмом шифрования (в "Шифрование" приведена более подробная информация о системах шифрования). Возникает вопрос: какая же система шифрования самая лучшая? Вообще, все стандартные и мощные алгоритмы могут эффективно использоваться при построении VPN. Различные производители отдают предпочтение различным алгоритмам, в зависимости от ограничений реализации продукта, аспектов, связанных с лицензированием, и предпочтений по программированию. Приобретая программный пакет VPN, следует выслушать комментарии специалистов и

убедиться в том, что производитель использует мощный алгоритм шифрования.

- Читатель может обратить внимание на то, что в предыдущем абзаце уделено особое внимание выбору алгоритма шифрования. Следует заметить, что выбор алгоритма не имеет принципиального значения, если он будет стандартным и в достаточной степени мощным. Гораздо больше влияет на общий уровень безопасности реализация системы. Неправильно реализованная система может сделать бесполезным самый мощный алгоритм шифрования. Приняв во внимание сказанное выше, давайте изучим риски, связанные с использованием VPN. Для того чтобы получить доступ к информации, передаваемой через VPN, злоумышленник должен:
- захватить весь сеанс соединения, т. е. разместить устройство прослушивания между противоположными концами соединения в том месте, через которое должен передаваться весь трафик VPN;
- использовать большие вычислительные мощности и большое количество времени для перехвата ключа с помощью грубой силы и для дешифрования трафика.
- Злоумышленнику гораздо проще использовать имеющуюся уязвимость на компьютере пользователя либо украсть портативный компьютер, например, в аэропорту. Если информация не представляет собой особой важности, в VPN можно использовать любой широко распространенный, мощный алгоритм шифрования.
- **Система аутентификации**
- Третьим компонентом архитектуры VPN является система аутентификации. Как уже говорилось ранее, система аутентификации VPN должна быть двухфакторной. Пользователи могут проходить аутентификацию с использованием того, что они знают, того, что у них есть или с помощью данных о том, кем они являются. При использовании пользовательских VPN отдается предпочтение первым двум вариантам.

- Хорошей комбинацией средств аутентификации являются смарт-карты в паре с персональным идентификационным номером или паролем. Производители программного обеспечения, как правило, предоставляют организациям на выбор несколько систем аутентификации. В данном перечне присутствуют ведущие производители смарт-карт.
- **Примечание**
- Использование смарт-карт повлечет за собой увеличение стоимости использования VPN для каждого пользователя. Несмотря на то, что это обстоятельство повысит стоимость использования соединения, обеспечение более высокого уровня защиты этого стоит.
- Если в организации предпочитают при использовании VPN полагаться только на пароли, они должны быть мощными (как минимум, сочетание из восьми букв, цифр и специальных символов) и регулярно изменяться (каждые 30 дней).
- **Протокол VPN**
- Протокол VPN определяет, каким образом система VPN взаимодействует с другими системами в интернете, а также уровень защищенности трафика. Если рассматриваемая организация использует VPN только для внутреннего информационного обмена, вопрос о взаимодействии можно оставить без внимания. Однако если организация использует VPN для соединения с другими организациями, собственные протоколы использовать, скорее всего, не удастся. В разговоре об алгоритме шифрования было упомянуто, что внешние окружающие факторы могут оказывать большее влияние на безопасность системы, чем алгоритм шифрования. Протокол VPN оказывает влияние на общий уровень безопасности системы. Причиной этому является тот факт, что протокол VPN используется для обмена ключами шифрования между двумя конечными узлами. Если этот обмен не защищен, злоумышленник может перехватить ключи и затем расшифровать трафик, сведя на нет все преимущества VPN.

- При соединении рекомендуется использовать стандартные протоколы. В настоящее время стандартным протоколом для VPN является IPSec. Этот протокол представляет собой дополнение к IP, осуществляющее инкапсуляцию и шифрование заголовка TCP и полезной информации, содержащейся в пакете. IPSec также поддерживает обмен ключами, удаленную аутентификацию сайтов и согласование алгоритмов (как алгоритма шифрования, так и хэш-функции). IPSec использует UDP-порт 500 для начального согласования, после чего используется IP-протокол 50 для всего трафика. Для правильного функционирования VPN эти протоколы должны быть разрешены.
- **Вопрос к эксперту**
- **Вопрос**. Работает ли IPSec через межсетевые экраны?
- **Ответ**. С работой IPSec через межсетевые экраны связаны некоторые особенности. Во-первых, на межсетевом экране должен быть разрешен трафик UDP через порт 500 и последующий IP-трафик с протоколом 50. Возможность установки этих разрешений зависит от межсетевого экрана. Кроме этого, возникает вопрос, связанный с использованием трансляции межсетевых адресов (NAT) (для получения дополнительной информации по этой теме обратитесь к "Архитектура интернета"). Если межсетевой экран осуществляет трансляцию адресов для пакетов при их поступлении из интернета во внутреннюю сеть, то ему нужно соответствующим образом транслировать конечный адрес, чтобы трафик достиг внутреннего клиента. Немногие межсетевые экраны способны выполнять эту функцию при работе с трафиком, не использующим порты UDP или TCP.
- Некоторые поставщики сетевых услуг (в частности, поставщики каналов DSL и кабельных каналов) ограничивают использование этих протоколов в своих сетях. Для того чтобы иметь возможность их использования, клиенту придется приобрести бизнес-пакет услуг вместо обычного стандартного пакета.

- Главной альтернативой протокола IPSec является протокол Secure Socket Layer (SSL), используемый для защиты HTTP (для HTTPS используется порт 443). Однако, принимая во внимание, что технология SSL предназначена для работы на прикладном уровне, она может оказаться не столь эффективной в сравнении с IPSec.
- Типы систем VPN
- Теперь, после обсуждения функционирования сетей VPN, давайте рассмотрим непосредственное применение VPN внутри организации. Помимо вопросов, связанных с политикой и управлением, организации нужно выбрать тип приобретаемой системы VPN. На момент написания данной книги можно выделить три типа VPN-построителей:
- аппаратные системы;
- программные системы;
- веб-системы.
- **Аппаратные системы**
- Аппаратные системы VPN, как правило, базируются на аппаратной платформе, используемой в качестве VPN-сервера. На этой платформе выполняется программное обеспечение производителя, а также, возможно, некоторое специальное программное обеспечение, предназначенное для улучшения возможностей шифрования. В большинстве случаев для построения VPN на системе удаленного пользователя необходимо наличие соответствующего программного обеспечения. Аппаратные платформы также могут использоваться для построения межузловых VPN, хотя это зависит от производителя оборудования.
- Аппаратная система VPN имеет два преимущества.
- Скорость. Оборудование, как правило, оптимизировано для поддержки VPN, посредством чего обеспечивается преимущество в скорости по сравнению с компьютерными системами общего назначения. За счет этого достигается возможность поддержки большего числа одновременных VPN-соединений.

- Безопасность. Если аппаратная платформа специально разработана для приложения VPN, из ее системы удалены все лишние программы и процессы. За счет этого снижается степень подверженности атакам по сравнению с компьютерной системой общего назначения, в которой работают другие процессы. Это не значит, что компьютер общего назначения не может быть должным образом защищен. Как правило, использование компьютера общего назначения требует дополнительных усилий по настройке безопасности.
- **Внимание**!
- Тот факт, что VPN используется на базе аппаратной платформы, не означает, что система никогда не подвергнется атаке. Владелец системы должен регулярно проверять наличие обновлений, выпускаемых производителем системы.
- **Программные системы**
- Программные VPN работают на компьютерных системах общего назначения. Они могут быть установлены на выделенной для VPN системе либо совместно с другим программным обеспечением, таким как межсетевой экран. При загрузке программного обеспечения необходимо обеспечить достаточную мощность аппаратной платформы для поддержки VPN. Так как VPN-продукт устанавливается на компьютеры, имеющиеся в организации, руководство организации должно позаботиться о соответствии компьютеров предъявляемым требованиям.
- Программные VPN-системы могут использоваться таким же образом, как и аппаратные системы. Существует программное обеспечение для поддержки пользовательских и узловых VPN.
- **Примечание**
- При установке программного обеспечения VPN необходимо обеспечить соответствующую конфигурацию системы, а также устранить все уязвимости, установив нужные обновления.
- **Веб-системы**

- Главным недостатком большинства пользовательских систем VPN является потребность в установке программного обеспечения на систему-клиент. Бесспорно, что программное обеспечение, которое устанавливалось на клиентские системы, увеличивало объем работ по управлению пользовательскими VPN. Более того, клиентское программное обеспечение во многих случаях не работало должным образом с некоторыми приложениями, загруженными на компьютер-клиент. Это обстоятельство повышало стоимость поддержки и приводило к тому, что многие организации стали устанавливать на специально выделенные компьютеры только программное обеспечение VPN.
- Указанные проблемы привели к тому, что некоторые производители VPN стали рассматривать веб-браузеры в качестве VPN-клиентов и реализовывать этот подход на практике. Он заключается в том, что пользователь с помощью браузера подключается к VPN через SSL. SSL обеспечивает шифрование трафика, а подтверждение подлинности пользователя выполняется с помощью средств аутентификации, встроенных в систему. Для предоставления пользователю необходимых услуг используется несколько различных механизмов. Среди них можно выделить надстройки браузера и виртуальные машины Java.
- В то время как стоимость поддержки и обслуживания несомненно ниже, на момент написания этой книги ни одна из бесклиентных систем VPN не обеспечивает полную функциональность. Этим сетям VPN присущи ограничения, заключающиеся в наборе используемых приложений и методе подключения пользователей к внутренним системам. Организациям следует рассматривать вариант использования таких систем, так как это снижает затраты на обслуживание, однако необходимо учитывать непосредственные требования пользователей и согласовать их с ограничениями, имеющимися в системах.
- Определение различий между типами VPN

- На предприятии принято решение использовать VPN, в результате чего установлен VPN-построитель. Необходимо составить оценочный отчет о методах шифрования, протоколах туннелирования и аспектах безопасности, связанных с приложениями, которые могут использовать VPN, такими как средства передачи голоса и видеоданных через службы IP (видеоконференции, усовершенствованные и измененные функции PBX) и средства удаленного хранения/резервирования и восстановления. Обязательно ли шифрование данных в каждом из случаев?
- Для каждого из приложений следует выяснить следующее.
- Какой тип VPN лучше использовать для приложения - межузловую или пользовательскую VPN?
- Где расположены конечные узлы VPN? Каким опасностям могут подвергаться эти конечные узлы?
- Налагают ли конечные узлы или пользователи приложения какие-либо дополнительные требования к механизму аутентификации, связанному с VPN?
- Определите соответствующие приложению механизмы аутентификации.
- Отследите информацию во время передачи. Является ли она открытой для перехвата или прослушивания? Если да, определите, обеспечивает ли используемый механизм шифрования должный уровень защиты информации.
- **Выводы**
- То, что хорошо работает с одним приложением, может вовсе не работать с другой программой. Межузловые и пользовательские VPN имеют различные требования к аутентификации и безопасности конечных узлов. Это необходимо принимать в расчет при построении VPN для использования приложением. Выбор механизма шифрования и мощность используемого алгоритма шифрования напрямую влияет на то, какие атаки будут пресекаться. В процессе разработки необходимо принимать во внимание все имеющиеся угрозы безопасности.

- Вопросы для самоконтроля
- Можно ли рассматривать использование SSH как реализацию VPN?
- Почему пользовательские VPN требуют строгой аутентификации?
- Может ли шифрование полностью защитить данные, передаваемые через VPN.
- С чем необходимо комбинировать политику, чтобы обеспечить безопасность VPN?
- Пригодны ли межузловые VPN для использования между организациями?
- Почему адресация является потенциальной проблемой, связанной с межузловыми VPN?
- Какие два критерия должны использоваться для определения того, какое устройство следует использовать - межсетевой экран или VPN-сервер на отдельной системе?
- Если используется отдельный VPN-сервер, должен ли он размещаться в демилитаризованной зоне интернета?
- Почему процесс реализации VPN представляет собой гораздо большее, чем выбор алгоритма шифрования?
- Какие механизмы аутентификации лучше всего использовать для пользовательской VPN?
- **Архитектуры информационных систем**
    - Сетевые операционные системы

- Компьютеры в сети, в зависимости от распределения функций, могут выступать в роли *выделенного сервера* или *клиентского узла*
- *Сеть может быть построена по следующим схемам:*
- ▫ на основе компьютеров, совмещающих функции
- клиента и сервера – *одноранговая сеть*
- ▫ на основе разделения функций клиентов и серверов –
- *сеть с выделенными серверами*

- ▫ сеть, включающая узлы разных типов – *гибридная*
- *сеть*.
- Модели сетевых служб и
- распределенных приложений

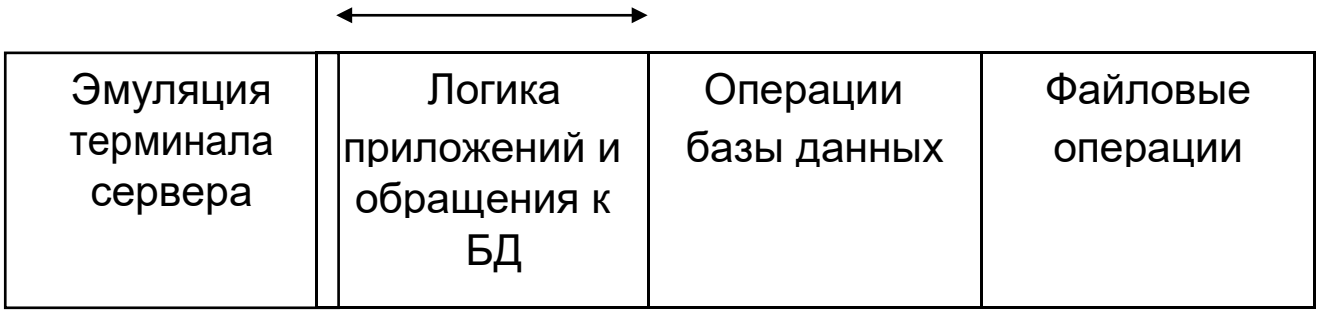
- Выделяют три основных параметра
- организации работы приложений в сети:
- ▫ Способ разделения приложения на части, выполняющиеся на разных компьютерах сети;
- ▫ Выделение специализированных серверов в сети, на которых выполняются некоторые общие для всех приложений функции;
- ▫ Способ взаимодействия между частями приложений, работающих на разных компьютерах.
- Способы разделения приложений на
- части

- Приложения условно можно разделить на
- следующие функциональные части:
- ▫ Средства представления данных на экране;
- ▫ Логика представления данных на экране (описывает правила и сценарии взаимодействия пользователя с приложениями);
- ▫ Прикладная логика (правила для принятия решений,
- вычислительные процедуры и т.п.);
- ▫ Логика данных – операции с данными, хранящимися в некоторой базе;
- ▫ Внутренние операции БД – действия СУБД, вызываемые в ответ на выполнение запросов логики данных;
- ▫ Файловые операции – стандартные операции над файлами и

файловой системой.

- Двухзвенные схемы
- распределенных ИС
- Двухзвенные схемы описывают разделение функций приложения между двумя компьютерами:
- ▫ Централизованная обработка данных;
- ▫ Схема «файл-сервер»
- ▫ Схема «клиент-сервер»
- Централизованная
- обработка данных
- **Компьютер 1**

Компьютер 2



- клиент серве

р

- Достоинства схемы:
- ▫ Ресурсы клиентского компьютера используются в незначительной степени, загружаются только графические средства ввода-вывода;
- ▫ Простота организации программы;
- Недостатки схемы:
- ▫ Недостаточная масштабируемость;

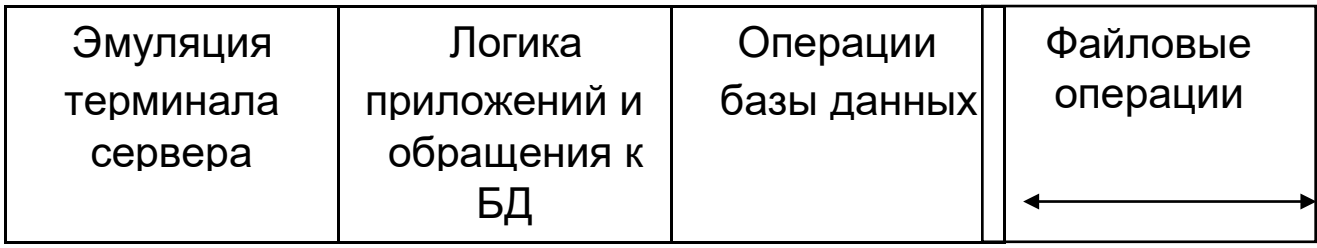
- ▫ Отсутствие отказоустойчивости.

- **Схема файл – сервер**

- **Компьютер**

  1

  Компьютер 2



- клиент

  сервер

- Достоинства схемы:
- ▫ Данная схема обладает хорошей масштабируемостью, поскольку дополнительные пользователи и приложения добавляют лишь незначительную нагрузку на центральный узел – файловый сервер.
- Недостатки схемы:
- ▫ Во многих случаях возрастает нагрузка, что приводит к увеличению времени

- реакции на приложения;
- ▫ Клиентский компьютер должен обладать высокой вычислительной мощностью, чтобы справляться с представлением данных, логикой приложений, логикой данных и поддержкой операции БД
    - **Схема клиент – сервер**

- **Компьютер**

  1 **Ко**

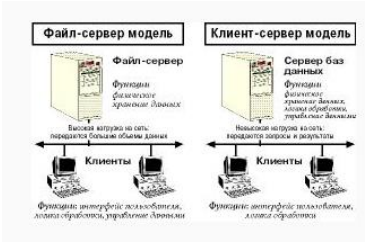
  мпьютер 2

Эмуляция терминала сервера	Логика приложений и обращения к БД	Операции базы данных →	Файловые операции

- клиент

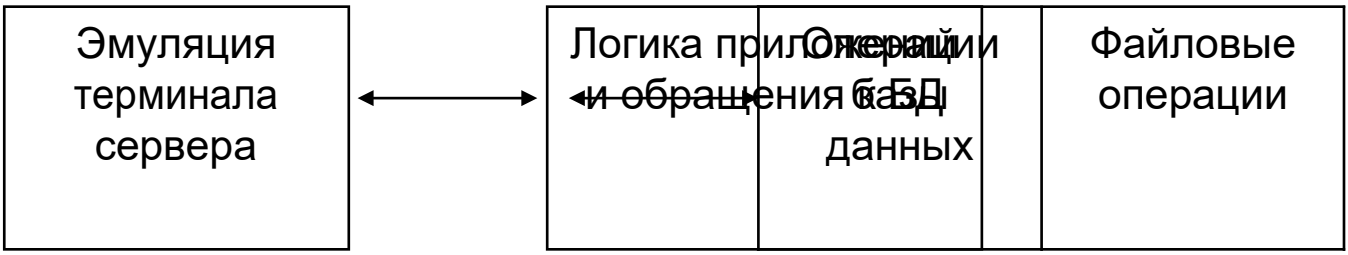
  сервер

- Достоинства схемы:
- ▫ Данная схема более равномерно распределяет функции между клиентской и серверной частями системы;
- Клиентский компьютер выполняет функции, специфические
- для данного приложения;
- Сервер – функции, реализация которых не зависит от специфики приложения, и данные функции могут быть оформлены в виде сетевых служб.



- **Трехзвенные схемы**

- **Компьютер 1** **Компьютер 2** **Компьютер 3**



- клиент Сервер
- приложений

- Централизованная реализация логики приложения решает проблему недостаточной вычислительной мощности клиентских компьютеров для сложных приложений, упрощает администрирование и поддержку системы;

- Упрощается разработка крупных приложений, поскольку четко разделены платформы и инструменты для реализации интерфейса и прикладной логики.

- *Типовая сетевая инфраструктура*
- *современного предприятия*