МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

«САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ»

Информационная безопасность в инфокоммуникационных системах

Учебное пособие

Автор: Гарбар Павел Юрьевич

Санкт-Петербург

2013

Оглавление

Введение

Дисциплина «Информационная безопасность в инфокоммуникационных системах» знакомит студентов с основами, принципами, терминологией и методами обеспечения сетевой безопасности. Также рассматриваются средства для повышения безопасности и защищенности сетевых серверов и сервисов. Студенты, освоившие данную дисциплину, научатся: определять угрозы сетевой безопасности, уязвимости сетей и программ и смогут помогать защищать свои сети и устранять последствия инцидентов безопасности.

Эта дисциплина охватывает общесетевые концепции безопасности, которые будут востребованы на дисциплинах по сетевым (серверным) и настольным операционным системам, так как сейчас вопросы безопасности пронизывают всю сетевую экосистему. Дисциплина развивает навыки принятия решения, показывая жизненные ситуации, с которыми может столкнуться целевая аудитория. Будут представлены задачи по сбору информации и просеиванию деталей, чтобы удовлетворить необходимое требование безопасности.

Аудитория

Настоящая дисциплина рассчитана на 180 академических часов и адресована студентам по компьютерным сетям и администраторам сетевых и настольных операционных систем, которые ежедневно работают с этими системами и хотят повысить их безопасность и обеспечить защищенную и доверенную рабочую среду. В результате слушатели получат базовые знания и навыки, необходимые для освоения методов и инструментов обеспечения безопасности.

Предварительные требования к студентам

Для успешного освоения данной дисциплины необходим следующий уровень квалификации:

- умение использовать настольные операционные системы с графическим интерфейсом;
- опыт управления серверными операционными системами более одного года;
- знания о компонентах компьютерного оборудования, таких как оперативная память, сетевые платы, жесткие диски и центральные процессоры;
- знание принципов организации сетей, в том числе сетевых операционных систем, модели «клиент-сервер», локальных и глобальных сетей.

Цели дисциплины

Освоив дисциплину «Информационная безопасность в инфокоммуникационных системах», студенты познакомятся с основными понятиями сетевой безопасности , обеспечение защиты сетевых операционными системами, а также различными методами обеспечения и повышения безопасности, применяемыми в сетевой среде.

К окончанию изучения дисциплины студенты научатся:

- понимать принципы информационной и сетевой безопасности;
- описывать работу администратора безопасности компьютерной сети;
- понимать основы сетевой безопасности;
- описывать стратегии обеспечения безопасности серверов;
- понимать, как защищать сетевые сервисы;
- понимать, как реализовывать защиту сетей на базе различных сетевых операционных систем.

В материале содержатся теоретические разделы и практические работы, отдельные главы сопровождаются лабораторными работами по соответствующей теме.

1.1. Введение в информационную безопасность
- Управление рисками
- Основополагающие принципы сетевой безопасности

1.2. Организация работы администратора безопасности компьютерной сети.
- Обзор общих принципов проектирования
- Принципы успешного проектирования
- Команда проекта
- Основы управления рисками
- Документирование

2.1. Основы сетевой безопасности.
- Подготовка к защите активов.
- Определение базисной линии безопасной вычислительной среды.
- Защита информации с использованием управления доступом и аутентификацией (установлением подлинности).
- Использование криптографии для защиты информации.
- Использование PKI для защиты информации.
- Применение защиты электронной почты и мгновенного обмена сообщениями.
- Управление безопасностью службы каталога.
- Защита передачи данных.
- Применение и мониторинг безопасности сетевого периметра.
- Управление эксплуатационной безопасностью.
- Обеспечение непрерывности работы.

2.2. Стратегии безопасности сервера:
- Надежность сервера
- Отказоустойчивость
- Резервное копирование
- Масштабируемость
- Доступность
- Защита консоли сервера
- Шифрование

- Гарантированное уничтожение информации (data shredding)
- Подписывание пакетов
- Система отслеживания транзакций (TTS)
- Бесперебойное электропитание (ИБП)
- Защита от вирусов
- Исправления и пакеты поддержки

2.3. Реализация защищенных компьютерных сетей на примере Windows, NetWare.

Приложение I. Справочные материалы.

Условные обозначения

Чтобы отличать разные элементы текста, в материалах дисциплины используются следующие условные обозначения.

Условное обозначение	**Использование**
полужирный	Используется для обозначения команд, их параметров и фрагментов синтаксиса, которые должны набираться в точности как указано. Также выделяет команды меню и кнопки, значки, заголовки и параметры диалоговых окон, названия меню и подписи под значками.
Наименования с Прописной Буквы	Используются для обозначения имен доменов, пользователей, компьютеров, папок, каталогов и файлов, кроме случаев, когда различие между прописными и строчными буквами особо оговаривается. Если не указано иначе, при вводе имени каталога или файла в диалоговом окне или в командной строке можно использовать строчные буквы.
ВСЕ БУКВЫ ПРОПИСНЫЕ	Обозначают названия клавиш и их сочетаний, например ALT+ПРОБЕЛ.
[ ]	В такие скобки заключаются необязательные элементы в описании синтаксиса. Например, [имя_файла] в синтаксисе команды указывает, что в команде можно задать имя файла. Следует вводить только данные, заданные в квадратных скобках, но не сами скобки.
{ }	В такие скобки заключаются обязательные элементы в описании синтаксиса. Следует вводить только данные, заданные в фигурных скобках, но не сами скоб-

	ки.
|	Используется для разделения вариантов альтернативного выбора в описании синтаксиса.
>	Указывает на процедуру с последовательными шагами.
...	Указывает, что предыдущий элемент в описании синтаксиса можно повторять.
. . .	Обозначает опущенную часть примера программного кода.
Рис. 2.1. График	Подпись к рисунку или схеме

I. Введение в информационную безопасность. Организация работы администратора безопасности компьютерной сети.

1.1. Введение в информационную безопасность

Информационная безопасность – это бесперебойное предоставление доступа к информации уполномоченным потребителям.

Это дисциплина покажет, как проектировать безопасную сетевую инфраструктуру. Дисциплина обсуждает темы, такие как подбор команды проекта, моделирование угроз и анализ угроз безопасности, чтобы отвечать деловым требованиям по обеспечению безопасной сетевой вычислительной среды.

Проект безопасности - комплексный план, который направляет процесс внедрения политик и процедур безопасности для организации. Проект безопасности помогает организации организовать свои активы так, чтобы реализовать план безопасности последовательно и в эффективной манере.

Этот глава описывает базовую структуру для проектирования сетевой безопасности и вводит ключевые понятия и концепции, используемые во всей дисциплине.

Основное отличие между проектом и процессом в том, что проект имеет начало и конец, а процесс – действие циклическое и потому – бесконечное. Так что, спроектировав и создав безопасную и защищенную сетевую среду в результате проекта, она передается в повседневную эксплуатацию, которая является процессом. Безопасность нельзя создать один раз и навсегда - любые внешние или внутренние изменения и воздействия приводят к тому, что состояние системы становится не таким безопасным, как раньше и это надо компенсировать новыми средствами и действиями.

Многие организаций недооценивают ценность своей среды информационной технологии (ИТ), часто потому что они исключают существенные косвенные затраты. Если происходит серьезное нападение на серверы в ИТ-среде, это может существенно навредить всей организация. Например, нападение, при котором веб-сайт вашей организации парализован или выведен из строя совсем, может вызвать значительную потерю дохода или потребительского доверия, которое отразится на доходности вашей организации.

Эффективная система безопасности помогает организации защитить свои активы и предотвратить большую часть атак.

Организации инвестируют в сетевую безопасность, чтобы защитить свои активы от угроз.

Активы в компьютерной сети могут включать такие элементы как электронные письма, интеллектуальную собственность, например, как коммерческие тайны или исходный код, базы данных клиентов и средства электронной торговли.

Угроза - опасность или уязвимость для актива. Угрозы активам включают злоумышленников, нападающих и лиц, пытающихся украсть информацию, использую уязвимости приложений, в которых недостает последних обновлений безопасности, и стихийные бедствия, такие как пожары или наводнения, потопы.

У каждой организации есть своя собственная уникальная комбинация клиентов, серверов и пользовательских требований, которые делают планирование всеохватывающей, безопасной рабочей среды основной проблемой. Без последовательного подхода к управлению рисками, некоторые области сети могут извлечь выгоду от чрезвычайно строгой безопасности, в то время как другие будут минимально защищены.

Управление рисками

Дизайн безопасности использует концепцию управления рисками, чтобы подготовит соответствующие ответы на угрозы безопасности. Управление рисками - тщательное исследование критериев, например, вероятности появления угрозы, воздействие угрозы, ценность актива для вашей организации и стоимость решения безопасности [2]. После выполнения анализа рисков, вы можете выбрать соответствующий ответ на угрозу. Данные, собранные во время анализа рисков, также полезно представить высшему управляющему звену и ключевым заинтересованным лицам, чтобы убедить их в важности сетевой безопасности и ее ценности для вашей организации.

Основополагающие принципы сетевой безопасности

Планирование безопасности основано на двух принципах:

- **У пользователей должен быть доступ к ресурсам.** Этот доступ может быть очень простым, например, только локальный вход в настольную систему и доступность списков управления доступа (ACLs) на ресурсах. Это доступ может также включать дополнительные услуги, такие как удаленные сетевые входы в систему, беспроводной сетевой доступ и доступ для внешних пользователей, таких как деловые партнеры или клиенты.
- **Сеть требует безопасной, совместно используемой ИТ- инфраструктуры.** Эта инфраструктура включает всестороннюю физическую безопасность, эффективные границы безопасности, защищенные серверы и услуги, безопасную сеть и эффективный план относительно делегирования полномочий и прав доступа.

Эшелонированная защита

Эшелонированная защита (рис. 1.1) относится к совокупности людей, действий и технологий безопасности. Эшелонированная защита обеспечивает множество уровней защиты сети, защищая от угроз в нескольких пунктах сети. Единственный слой часто неэффективен против многократных и множественных нападений. При использовании эшелонированной защиты, если нападение прорывается через один уровень защиты, то другой уровень обороны продолжает обеспечивать дополнительную защиту активу.

Эшелонированная защита применяет многослойный подход, который:

- Уменьшает шансы атакующего на успех
- Увеличивает риск атакующего быть обнаруженным

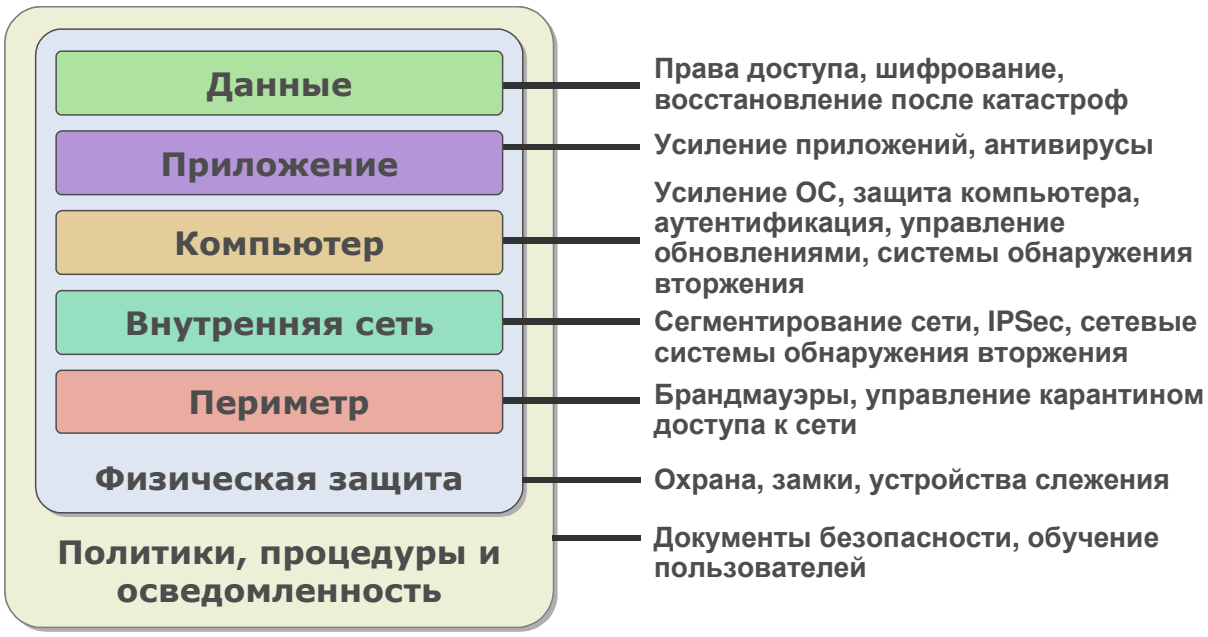

Рисунок 1.1. Эшелонированная защита

Наименьшие необходимые полномочия

Наименьшие необходимые полномочия относится к предоставлению пользователю ресурсов или приложений с наименьшим необходимым для выполнения свой работы полномочий или прав доступа. Такие подходы как использование полномочий по умолчанию или полного доступа к ресурсам или предоставление прав администратора учетной записи обычного пользователя, упрощает администрирование до опасного уровня. Предоставление чрезмерных полномочий может привнести многочисленные уязвимости, которыми легко могут воспользоваться атакующие.

Минимизирование поверхности для атаки

Понятие поверхности атаки относится к точкам входа, которые может использовать атакующий для проникновения в сеть. У сети, в которой минимум доступных областей или точек входа, которые уязвимы для атаки - минимальная поверхность атаки. Сеть, у которой есть несколько у незащищенных соединений с Интернетом - имеет бОльшую поверхность для атаки, чем маленькая, изолированная сеть, у которой есть единственное, защищенное соединение с филиалом.

1.2. Организация работы администратора безопасности компьютерной сети.

Обзор общих принципов проектирования

Проект - это временная деятельность, направленная на достижение определенного результата, создание определенного уникального продукта или услуги. Для выполнения любого проекта требуются ресурсы, в том числе трудовые и финансовые. Цель дисциплины управления проектом заключается в организации данных ресурсов и управлении ими способом, обеспечивающим создание продукта или услуги при соблюдении объема, уровня качества, сроков и стоимости [1].

В нашем случае под проектом будет пониматься построение системы информационной безопасности компьютерной сети организации или предприятия.

Основной заказчик

Основным заказчиком должно являться самое заинтересованное в результате (продукт, услуга, состояние) лицо. Поскольку информационная безопасность важна для всей организации, то основным заказчиком должен стать руководитель компании.

Функциональный руководитель

В отличие от проектной деятельности, являющейся временным и разовым мероприятием, многие операционные задачи повторяются, при этом каждое повторение имеет одно и то же базовое содержание (не путать с итеративной разработкой, при которой задачи повторяются, но различаются содержанием или отдельными деталями). Примером операционной деятельности являются функции управления трудовыми ресурсами и запасами, при решении которых управление сводится к обеспечению адекватного ежедневного и последовательного выполнения текущих задач. Люди, являющиеся исполнителями данной роли, могут занимать различные управленческие должности и решать типовые задачи управления.

Менеджер проекта

В отличие от ролей функциональных руководителей, роль менеджера проекта создана специально для решения уникальных задач. Менеджер проекта, таким образом, должен понимать область своей ответственности, а также выбирать и применять оптимальный процесс управления для создания продукта или услуги в срок и в пределах заданных ограничений. Эти задачи, в сочетании с работами по инициации и завершению проектов, составляют неотъемлемую часть обязанностей менеджера проекта и являются отличительной стороной его роли по сравнению с ролями других менеджеров предприятия.

Исполняющий обязанности менеджера проекта

Часто получается так, что новый проект не имеет выделенного менеджера. Повсеместно встречается ситуация, когда обязанности менеджера проекта частично или в полном объеме принимает на себя опытный член группы. Несмотря на то, что в общем случае наличие временного или частично занятого менеджера проекта лучше, чем его полное отсутствие, существование исполняющего обязанности менеджера в течение длительного времени считается неправильным, поскольку подвергает риску непрерывность и последовательность принятия решений. Более того, временным менеджером проекта зачастую становится член группы, не имеющий достаточного опыта или мотивации для исполнения дополнительных обязанностей, что приводит к несоответствию результата проекта ожиданиям или к полному фиаско.

Технический менеджер проекта

Нередко роль менеджера проекта совмещается с ролью архитектора решения или технического руководителя. Несмотря на то, что такое совмещение часто приносит негативные результаты, оно может оказаться вполне оправданным в случае, если проектная группа невелика (обычно не более 10 участников). Преимуществом наличия в группе технического менеджера проекта является то, что он может осуществлять грамотное планирование проекта за счет глубокого понимания требований и/или принципов проектирования программного обеспечения. Это, в свою очередь, может устранить эффект "испорченного телефона" в группе разработки. Недостаток данного подхода заключается в том, что технический менеджер проекта может не иметь времени, достаточного для планирования проекта, не говоря уже о полном охвате и управлении всеми аспектами проекта.

Менеджер программы

Проекты могут быть настолько сложны и масштабны, что управлять ими становится практически невозможно. Распространенным решением этой проблемы является организация иерархической структуры управления проектом, самый верхний уровень которой называется программой, а последующие уровни представляют собой проекты. Управление программой является особой разновидностью управления проектами, рассматривающей совокупность проектов как единое целое и в то же время не упускающей из виду состояние выполнения каждого проекта в отдельности. К основным обязанностями менеджера программы относятся деление содержания программы на отдельные управляемые фрагменты (проекты), документирование и управление зависимостями проектов, планирование и выполнение эскалации и делегирования.

Менеджер проекта предприятия

Современная организация представляет собой достаточно сложную сущность, в которой на регулярной основе происходит выполнение работ без оформления их в виде проектов. Одним из примеров является реализация архитектуры предприятия и ее различные этапы, такие как разработка концепции, разработка бизнес-сценариев и анализ бизнес-процессов. Некоторые их этих функций могут быть довольно сложными и, следовательно, трудными для управления, если им своевременно не были заданы жесткие границы. Эксперты предметной области, например архитекторы, инженеры процессов и консультанты редко обладают навыками, необходимыми для решения задач, стоящих перед менеджером проекта предприятия. Данное обстоятельство определяет необходимость роли менеджера проекта предприятия, о которой я подробно расскажу ниже.

Основные заботы менеджера проекта

Хотя некоторые менеджеры проекта выглядят более рациональными, информированными, склонными к доверию или опытными, чем другие, каждый из них сталкивается с одними и теми же проблемами. Самые важные из них перечислены ниже.

Оценки

Менеджеры проекта разочаровываются в своих архитекторах, получая от них оценки трудозатрат с запасом в 20, 50 или даже все 100%. Несомненно, многие отрасли достигли уровня развития при котором измерения, оценки и план проекта могут быть получены исключительно на основе стандартной терминологии, высокоуровневого описания содержания работ и отраслевых норм производительности. Зная об этом, менеджер проекта может ожидать того же самого и в индустрии разработки программного обеспечения. Подобные ожидания, однако, зачастую оказываются неоправданными. В ИТ-индустрии, где всё, начиная с инфраструктур и платформ и заканчивая методологиями и инструментами, находится в состоянии постоянного развития, получение результатов адекватной точности требует глубокого понимания требований.

В современной ИТ-индустрии при разработке продуктов или услуг значительный объем работ может быть оценен с приемлемой точностью только в том случае, если оценка основана на детальных, структурированных, разработанных с учетом конкретной методологии требованиях и использует нормы производительности, основанные на результатах ранее успешно завершенных проектов, выполненных одной и той же группой и с использованием одних и тех же технологий. Оценки, сделанные архитекторами, очень часто основываются или на неструктурированных требованиях (что нехорошо), разработанных на основе аналогичных существующих решений (что плохо) или на оценках трудозатрат, полученных от проектных групп (что еще хуже).

Бюджет и затраты

Являясь посредником между организацией-заказчиком и проектной группой, менеджер проекта часто оказывается между молотом потребностей и наковальней действительности. Примером, особенно наглядно демонстрирующим данный разрыв, является несоответствие выделенных ресурсов оценке затрат. В большинстве случаев данная проблема возникает из-за того, что в момент распределения бюджета организации требования были не просто не поняты, а даже еще не собраны. Фактически проектной команде предлагается понять, что может быть разработано в данных обстоятельствах. Менеджеру проекта в такой ситуации остается надеяться на то, что оценки, сделанные архитектором перед началом проекта, окажутся верными.

Методология

Часто успех проекта зависит от правильности выбора и применения методологии. В отличие от строительства и производства, при разработке программного обеспечения существует широкий выбор методологий любого стиля и на любой вкус - от очень формальных до очень гибких. Менеджер проекта редко принимает участие в выборе методологии, но практически всегда отвечает за правильное следование ей. Таким образом, менеджер проекта должен проявить прагматизм и волю к сотрудничеству когда дело дойдет до выбора методологии для использования в проекте.

Принципы успешного проектирования

Успешный проект:

- Отвечает деловым потребностям организации
- Представляет четкий план достижения цели вовремя (рис. 2.1), в рамках бюджета и с заранее оговоренными функциональными возможностями

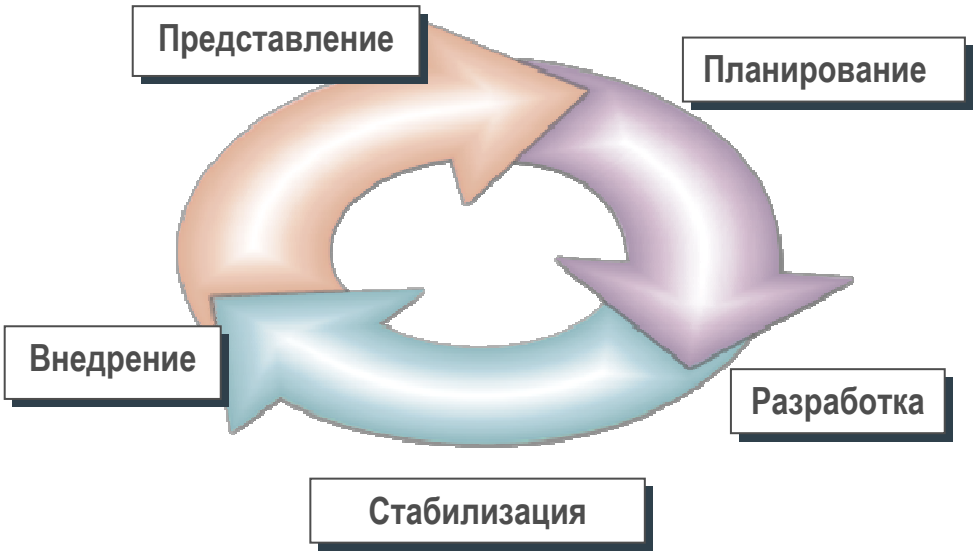

Рис. 2.1. Циклы проекта

Есть несколько проверенных моделей проектирования.

Основные задачи проектирования выполняются в фазах представления и планирования.

Команда проекта

Критерии эффективно работающей команды можно сформулировать в семи пунктах. Пункт первый: управленческая команда легко собирается вместе. Никто не опаздывает. Этот пункт отражает энергетическую согласованность командных действий, своего рода тест. Насколько слаженно собирается команда, настолько согласованно будут решаться другие задачи.

В команду приглашаются участники с должным уровнем профессиональных знаний и навыков. Каждый из членов команды вносит свой вклад на соответствующем этапе проекта. В каждой команде должны быть задействованы специалисты той предметной области, для которой создавался проект.

Для создания системы информационной безопасности могут понадобиться специалисты в таких областях, как:

- Информационная безопасность
- Локальные сети
- Глобальные сети
- Беспроводные сети
- Сетевые операционные системы
- Настольные операционные системы
- Сетевое оборудование
- Служба каталога (directory service)

- Сетевые инфраструктурные сервисы
- Тестирование
- Юриспруденция
- И другие специалисты по мере необходимости.

Критерии эффективно работающей команды

Критерии эффективно работающей команды можно сформулировать в семи пунктах.

1. Управленческая команда легко собирается вместе. Никто не опаздывает. Этот пункт отражает энергетическую согласованность командных действий, своего рода тест. Насколько слаженно собирается команда, настолько согласованно будут решаться другие задачи.

2. Члены команды имеют единое представление об общекомандных целях и задачах, перспективах развития. Должна быть ориентация на общекомандный результат, а не на выполнение отдельных операций участниками команды. Если члены команды думают только о своих функциональных обязанностях, а не ориентируются на общую цель, то вероятность «перетягивания одеяла» возрастает. Акцентируется внимание на сильных и слабых сторонах участников команды, а не команды в целом. Иногда руководителю проекта целесообразно анкетировать членов команды относительно общего видения, тактических и стратегических целей проекта и деятельности команды и проанализировать (можно анонимно или вместе с командой) каждую анкету. Внешние и внутренние кризисы команды зачастую связаны с потерей целевых ориентиров и переориентации сознания членов команды на управленческую борьбу с отдельными людьми или системами. Восстановление целевых ориентиров чаще всего возвращает участников команды на путь конструктивного достижения результата.

3. Каждый член команды имеет личную заинтересованность в достижении командных целей. Эффективность мотивационных процессов отражает эмоциональную и духовную вовлеченность во внутрикомандное взаимодействие, а также ответственность за выполнение своих обязательств. В начале процесса формирования команды можно предложить каждому ее участнику высказаться на тему: «Зачем я участвую в этом проекте, какой вижу свою роль в проекте» (по 1-2 минуты на человека, говорящего нельзя перебивать). Руководитель должен быть готов выслушать любую позицию, без давления, иначе члены команды перестанут искренне говорить о своих мотивах, а начнут «выдавать» то, что хочет слышать руководитель или команда. На более поздних этапах, особенно в кризисные моменты, можно предложить всем членам команды высказаться на темы «Что мне мешает и что помогает в достижении поставленных целей» и «Что мешает и что помогает команде в достижении поставленных целей». Каждый говорит от своего имени и только за себя (1-2 минуты).

4. Информация внутри команды передается без затруднений и искажений (рис. 2.2). Этот критерий отражает доверие членов команды друг к другу. В ситуации управленческой борьбы в команде давать информацию о своей сфере ответственности опасно, так как может произойти «перехват» управления. Целесообразно в такой ситуации предложить каждому члену команды высказаться на тему «Кому из членов команды я доверяю меньше всех, кому больше всех и почему» (1-2 минуты), а затем установить новый порядок обмена необходимой информацией.

Рис. 2.2. Взаимодействие в проектной команде

5. Единая система ценностей и единство правил внутри команды. Каждый человек обладает своей системой ценностей, но в команде должна существовать единая ценностная ориентация, продиктованная видением проекта, стратегическими целями, интегрированными ценностями всех членов команды, фазой развития проекта. Это непременное условие совместного выживания. Глубокие ценностные различия приводят к расколу в команде. В ситуации угрозы раскола команды целесообразно всем участникам команды высказаться на тему «Что нас объединяет и что разделяет» (1-2 минуты) и выработать совместно единую систему ценностей, отделив индивидуальные ценности от общекомандных. В индивидуальной деятельности каждый руководствуется своими ценностями, при командном взаимодействии — общекомандными.

6. Единый лидер, признанный командой. Формальное и неформальное лидерство должно принадлежать только одному лицу в команде, которое управляет активностью остальных членов команды. Лидер должен творчески расти с опе-

режением других членов команды, а не тормозить их развитие. Иногда необходимо дать возможность всем членам команды высказаться на темы «Что вы ожидаете от лидера команды» и «В чем лидер оправдывает или не оправдывает ваши ожидания» (1-2 минуты). Оправдываться нежелательно, лучше всего без критики выслушать все заявления. Это снимает напряженность и дает почву для конструктивного общения.

7. Четко определенная сфера ответственности каждого члена команды, строгое разделение функциональных обязанностей. Эффективность команды определяется сбалансированностью ответственности и индивидуального вклада в процесс управления проектом. При наличии дисбаланса можно создать вместе с командой графическую модель фактического распределения ответственности в команде («как есть») с указанием вариантов «перехвата» управления и ухода от ответственности каждого ее члена. Для этого необходимо выработать систему условных обозначений и понятий, затем графически представить командное взаимодействие с позиций сфер личной ответственности. Здесь нельзя проявлять жалость и выслушивать оправдания, а также оценивать чьи-то действия как позитивные или негативные. Затем следует проанализировать проблемы и построить новую модель («как должно быть»), перераспределив ответственность между членами команды. Эта методика, несмотря на свою жесткость, гуманна по сути, позволяет избавиться от самообмана и устаревших иллюзий.

Основы управления рисками

Как и для основных активов компании самому проекту по созданию системы информационной безопасности могут грозить риски. Для проектной деятельности основными рисками являются:

- Не достижение целей проекта
- Достижение результата, но не с должным уровнем качества
- Превышение сроков
- Превышение бюджета

В остальном управление рисками для проектов согласуется с методиками и для активов (рис. 2.3).

Рис. 2.3. Основы управления рисками

Управление рисками – это исследование относительной ценности активов и соответствующего выделения ресурсов безопасности на основе вероятности проявления риска и значимости актива [3]. Управление рисками помогает приоритезировать усилия и средства, направленные на защиту сети.

Для этого необходимо:

- Знать различные элементы управления рисками;
- Уметь объяснять почему управление рисками важно;
- Идентифицировать совместно используемые активы, для их защиты;
- Категоризировать активы согласно типу;
- Оценивать стоимость актива.

Оценивая риски и создавая план управления рисками вы сможете:

- **Приоритезировать угрозы безопасности.** Можете оценить вероятность возникновения угрозы безопасности относительно других рисков. Это помогает организации определять выделение ресурсов на защиту сети.
- **Определять подходящий уровень безопасности.** Сможете определить момент, при достижении которого, последовательные усовершенствования безопасности становятся неэффективными и дорогостоящими.
- **Обосновать затраты.** Можете использовать количественный анализ рисков, чтобы оправдать расходы на персонал службы безопасности, аппаратные средства и программное обеспечение.
- **Задокументировать все потенциальные вопросы безопасности.** Управление рисками требует полной оценки угроз сети и их потенци-

альное воздействие. Организация, которая принимает спонтанные решение в ответ на угрозы нарушения безопасности, может пропустить критические вопросы безопасности в своей сети.

- **Создавать метрики.** Управление рисками использует метрики, которые помогают судить об успехе плана обеспечения безопасности. Можете также использовать метрики, чтобы подготовить бюджет, который планируют руководители, для службы безопасности.

Документирование

Ведение документации по проекту является одной из важнейших задач участников проекта. Особенно ответственно надо подходить к документированию при разработке системы информационной безопасности, так как каждая неучтенная или пропущенная деталь может обернуться большими проблемами и потерями.

При работе над проектом некоторые документы должны быть созданы сразу и инициировать сам проект, а некоторые будут создаваться в ходе продвижения по жизненному циклу проекта:

- Документ представления и объема
- Документ структуры проекта
- Первоначальный документ оценки рисков
- Документ концепции проекта
- Документ логической структуры сети
- Документ физической структуры сети
- Функциональные спецификации
- План именования сетевых объектов
- Главное расписание проекта

Все эти документы постепенно собираются в «Главный план проекта».

II. Основы сетевой безопасности. Стратегии безопасности сервера. Реализация защищенных компьютерных сетей.

2.1. Основы сетевой безопасности.

Подготовка к защите активов

Эта глава показывает, как происходят распространенные атаки на сети и объясняет связанные с атаками угрозы и уязвимости. Глава также дает обзор того, что персонал сетевой безопасности должен делать, чтобы защитить активы организации.

Актив - что-либо в организации, у которой есть материальное или нематериальные ценности, будь то ресурс или конкурентное преимущество. Организации должны защищать свои активы, чтобы выжить и процветать. Персонал сетевой безопасности играет важную роль в защите активов от случайностей, ошибок, отражает атаки и борется со стихийными бедствия. Следующая таблица показывает примеры активов (табл. 3.1).

Таблица 3.1. Активы

Активы	Примеры
Оборудование	Настольные и переносные компьютеры, серверы сетевое оборудование, резервные копии
Документация	Сетевые диаграммы, политики сетевой безопасности и процедуры, планы помещений
Программы	Операционные системы, прикладные программы, программы собственной разработки
Данные	Промышленные и коммерческие тайны, информация о сотрудниках и клиентах, наработанные данные

Угроза - любое действие, которое представляет возможную опасность для активов. Угрозы имеют тенденцию быть более постоянными, чем уязвимости, потому что основные виды деятельности, которые представляют опасность для активов, не сильно изменяются. Общие угрозы включают:

1) людей, ищущие пути чтобы украсть, изменить или уничтожь данные, системы или оборудование и

2) бедствия, которые могут вызвать разрушение данных, систем или оборудования.

Уязвимость - любая слабость в системе безопасности, которая может быть использована угрозой. Общие причины уязвимостей включают:

1) разрабатываются и регулярно внедряются новые типы аппаратного и программного обеспечения, которые представляют новые уязвимости,

2) загруженные люди, которые делают ошибки, и

3) сетевая безопасность во многих организациях реактивна (т.е. реагирует на произошедшие события), а не превентивна (т.е. не допускает возникновения проблем).

Атака - преднамеренная попытка обойти средства управления безопасностью на компьютере. Всегда создаются новые атаки, чтобы использовать новые уязвимости. Когда сведения об атаке разглашаются, то контрмеры, делающие эту атаку неэффективной, также обычно публикуются.

Термин **атакующий** относится к любому, кто сознательно пытается обойти средства управления безопасностью, чтобы получить доступ чужому компьютеру или сети. Основные суждения об атакующих включают:

Внутренние атакующие могут нанести больше ущерба, чем внешние атакующие. Многие атаки происходят изнутри организации. Атакующие могут быть любопытными людьми или теми, кто сознательно идет на нарушение и пытается вызвать инцидент безопасности. Внутренние атаки более распространены и потенциально более разрушительны, чем внешние атаки, потому что у внутренних атакующих есть законный доступ к физическим и сетевым активам, который упрощает для них возможность повысить полномочия, чтобы получить данные, к которым обычно у них нет доступа.

Новичок, среднеподготовленный и высококвалифицированный атакующие - все представляют существенную угрозу сети. Атакующие варьируются от новичка до опытного программиста. Наименее квалифицированные атакующие, обычно используют существующие программы, а не пишут свои собственные инструменты для атаки. Даже в этом случае новичок и средний программист могут представлять из себя большую угрозу безопасность как и опытные программисты. Они могут разрушить систему, отклоняя доступ пользователей и тратить ценное время организации и ресурсы на восстановление. Кроме того, постоянное присутствие атакующего часто более разрушительно, чем его навык.

Вы никогда не можете знать слишком много о внешних атакующих. Чаще вы вообще о них ничего не знаете. Например, атакующие, которые пишут вирусы и троянских коней никогда не будут известны, если их действия не привлекут явное внимание средств массовой информации. Вирусописатели часто обладают малыми навыками, так как фактически есть программы, которые помогают атакующим создавать вирусы. Часто эти атаки просто раздражающие, но атакующий может использовать распространенность вредоносных программ (malware), чтобы создавать опасные атаки.

Чем обычно мотивируются атакующие:

- Личное продвижение или удовлетворение;
- Денежная выгода;
- Признание среди коллег;
- Публичность, слава;
- Терроризм;
- Чрезмерная бдительность и активность;
- Разрушительный характер;
- Шпионаж.

Сотрудники сетевой безопасности несут ответственность за проектирование, внедрение и применение мер защиты сети. Но они не единственные, кто должен соблюдать меры предосторожности. Ежедневно им должны помогать:

- Сетевые администраторы
- Пользователи
- Разработчики программ
- Руководители всех уровней
- Служба охраны зданий и помещений
- Отдел кадров
- Юристы
- Аудиторы

Чтобы защитить компьютеры и сеть, сотрудники службы информационной безопасности могут:

- Определять и устанавливать базисной линии безопасной вычислительной среды
- Защищать информацию с использованием управления доступом и аутентификацию (установление подлинности)
- Использовать шифрование для защиты информации
- Использовать PKI для защиты информации
- Защищать приложения и компоненты
- Применять защиту электронной почты и мгновенного обмена сообщениями
- Управлять безопасностью службы каталога и DNS
- Защищать передачу данных
- Применять системы безопасности сетевого периметра и мониторить события

Если все же безопасность будет нарушена, то службе информационной безопасности нужно:

- Улучшать и усиливать эксплуатационную безопасность
- Обеспечить непрерывность работы
- Реагировать на инциденты с безопасностью

Определение базисной линии безопасной вычислительной среды

В этом модуле будет показано, как создать безопасную вычислительную среду соответствующую политике безопасности компании. Модуль также предлагает инструкции для защиты физических ресурсов и средств.

Для этого необходимо уметь:

- Описывать доверенную вычислительную базу.
- Описывать инструкции для установления базисной линии безопасности.

- Перечислять общие инструменты, которые можно использовать для контроля базисной линии.
- Объяснять как физически защищать компьютеры.
- Описывать, как можно придерживаться базисной линии.

Доверенная вычислительная база - полная комбинация механизмов защиты в компьютерной системе. Это включает детализированные требования к защите для всех элементов вычислительной среды компании. Вычислительная база считается доверенной, потому что это обеспечивает самую безопасную вычислительную среду, которую организация может предоставит с учетом знаний и возможностей, которыми обладает организация.

Доверенная вычислительная база - реализация политики безопасности компании. Чтобы поставить безопасность под угрозу, атакующий должен скомпрометировать один или более компонентов доверенной вычислительной базы.

Доверенная вычислительная база должна включать механизмы безопасности которые:

- Осуществляют пользовательскую аутентификацию и управление доступом к компьютерам.
- Ограничивают доступ к информации проходящей по сети.
- Обеспечивают конфиденциальность записей и проводят аудиты.
- Убеждаются, что данные не были уничтожены или украдены.

Поддержание доверенной вычислительной базы требует следующих элементов:

- **Подробная конфигурация и процедуры.** Для каждого компонента и конфигурации, определите обязательные настройки. Например, потребуйте длину пароля минимум восемь символов.
- **Исчерпывающая документация.** Задокументируйте каждый шаг конфигурации. Например, задокументируйте компьютеры, у которых включен совместный доступ к файлам и печати.
- **Управление изменениями и конфигурациями.** Определите процедуры для внедрения изменений, например, процедуры для тестирования и применения пакетов обновления.
- **Анализ и пересмотр процедур.** Пересматривайте процедуры регулярно, чтобы обнаружить потенциально слабые места. Например, можете обнаружить, что процедуры для защиты компьютеров, включают не все компоненты операционной системы. По возможности, предоставьте выполнение анализа процедур внешней организации.

Базисная линия безопасности – это подробное описание того, как сконфигурировать и администрировать компьютер. Базисная линия безопасности реализует компоненты базы доверенных вычислений на определенном компьютере. А также описывает все соответствующие параметры конфигурации для безопасных вычислений. Элементы базисной линии безопасности включают:

- **Настройки для служб и приложений.** Например, только указанные пользователи имеют полномочия запускать службу или запускать приложение.
- **Конфигурация компонентов операционной системы.** Например, все файлы примеров, которые идут с веб-сервером, должны быть удалены с компьютера.
- **Назначение прав и полномочий.** Например, только администраторы имеют право на изменение файлов операционной системы.
- **Административные процедуры.** Например, пароль администратора на компьютере должен изменяться каждые 30 дней.

Используйте следующие шаги, чтобы контролировать базисные линии безопасности в организации:

1. **Регулярно сравнивайте конфигурацию каждого компьютера с его базисной линией.** Установите график проверок, чтобы как можно раньше обнаружить проблемы.

2. **Исследуйте причину несоответствий.** Иногда бывают оправданные причины несоответствия. Например, кто-то изменил конфигурацию потому что изменились деловые потребности. Но изменение также могло быть признаком нарушения безопасности. Прежде, чем устранить проблему, исследуйте причины изменения.

3. **Фиксируйте несоответствия.** Сконфигурируйте компьютер, чтобы вернуться к базисной линии и удостоверьтесь, что настройки не будут изменены снова.

4. **Скорректируйте базисную линию по мере необходимости.** Если обнаруживаются новые уязвимости или происходят изменения в деловых потребностях, скорректируйте базисную линию, с учетом этих проблем. После полного тестирования базовых настроек примените новую базисную линию, и затем продолжайте контролировать компьютерную конфигурацию, опираясь на обновленную базисную линию.

Защита информации с использованием управления доступом и аутентификацией (установлением подлинности)

В этом модуле будет рассказано о стратегиях управления тем, как пользователи получают доступ к компьютерным ресурсам; как использовать протоколы единой и многофакторной аутентификации для проверки идентификационных данных пользователей; как применять модель управления доступом для предоставления доступа к компьютерным ресурсам в сети аутентифицированным пользователям.

Управление доступом - процесс авторизации (проверки полномочий) пользователей или групп для получения доступа к объектам, например, таким как сетевые файлы или принтеры. Сетевая безопасность основывается на двух фундаментальных понятиях: аутентификация и авторизация. Управление доступом –

это также определенная модель того, как применять авторизацию. Рассмотрим следующее:

- **Аутентификация.** Процесс проверки идентификационных данных чего-либо или кто-либо. При аутентификации обычно используют имя пользователя и пароль, но можно задействовать любой метод проверки идентификационных данных, таких как смарт-карта, сканирование сетчатки глаза, распознавание речи или отпечаток пальца.
- **Авторизация.** Процесс определения, разрешен ли доступ идентифицированному пользователю или процессу к ресурсу и каков уровень предоставленного доступа для них. Владелец ресурса или кто-то, наделенный полномочиями предоставлять разрешения, определяет, является ли пользователь членом предопределенной группы или имеет свой собственный определенный уровень допуска. Устанавливая разрешения для ресурса, владельца с помощью средств управления доступом определяет, какие сетевые пользователи и группы могут получить доступ к ресурсу.

Принцип **наименьших полномочий** предполагает наделение прав пользователям только в минимально необходимых рамках полномочий для выполнения ими своих служебных обязанностей. Не давая доступа пользователям сверх минимально необходимого для выполнения работы, вы не даете возможность атакующим использовать дополнительные полномочия, чтобы обойти сетевую безопасность.

Есть несколько способов управления доступом к ресурсам. Один из них заключается в том, чтобы определить, обладает ли пользователь необходимым паролем, независимо от идентификационных данных самого пользователя. Другой метод основывается на управлении доступом для отдельных учетных записей пользователей.

Два типа управления доступом:

Парольное управление доступом. Можно применить защиту совместно используемого ресурса на компьютере, требуя пароль для доступа к этому ресурсу. У пользователей запрашивается только этот пароль и, если он его предоставляет (вводит), то получает доступ, например, к файлам. Основанное на пароле управление доступом - слабая форма безопасности, но это удобно в среде, в которой нет необходимости в индивидуальных учетных записях пользователей.

Управление доступом на основе учетных записей пользователей. Этот подход управляет доступом путем наделения пользователя правами и полномочиями. Это дает возможность применить защиту к отдельным ресурсам на основе учетных записей пользователей. Сеть аутентифицирует пользователей при входе в систему. В некоторых сетях после этого пользователи получают уникальный аутентификационный маркер, который они представляют каждый раз, когда они пытаются получить доступ к сетевому ресурсу. Основанное на пользователе управление доступом предлагает централизованный способ предоставления людям определенного доступа к ресурсам, но вы при должны вести учетных записи для каждого пользователя. Управление доступом, основанное на учетных

записей пользователей, может обеспечить основу для единого входа в систему, при котором пользователи аутентифицируются один раз и не должны повторять процесс аутентификации в ходе текущего сеанса при обращении к другим ресурсам.

Существует и **многофакторная аутентификация**, которая требует, чтобы пользователь предоставил по крайней мере две формы идентификации. Как правило, это включает что-то, что пользователь знает, например идентификатор пользователя (имя регистрации) или пароль и что-то, чем пользователь обладает, например, смарт-карта или уникальная биометрическая особенность, такая как отпечаток пальца. Другой пример аутентификаторы SecureID, которые генерируют новый, непредсказуемый код каждые 60 секунд. Пользователь комбинирует это число с секретным PIN для регистрации в системе с защищенными ресурсами. Многофакторная аутентификация усиливает аутентификацию подтверждая, что информация была отправлена или получена определенным человеком и что этот человек присутствовал во время транзакции.

В среде с высокой степенью безопасности системы аутентификации могут интегрироваться с инфраструктура открытых ключей (PKI), смарт-картами и биометрическими свойствами, такими как радужка глаза, голос, отпечаток пальца или рукописная подпись.

Использование криптографии для защиты информации

Криптография (шифрование) - метод сохранения информации в секрете. Чаще всего шифруют информацию при передаче ее из одного места в другое. Можно также шифровать информацию в целях ее безопасного хранения.

В современных организациях криптография обеспечивает конфиденциальность информации, во время передачи ее по сетям или во время хранения на магнитных или других постоянных носителях. Чаще всего организации используют криптографию, чтобы предотвратить от просмотра информацию сторонними лицами.

В криптографии **открытый текст** – это информация до шифрования. **Шифрованный текст (шифротекст)** – уже зашифрованная информация.

Дешифрование зашифрованного текста требует знания или владения секретом, который доступен только владельцу или лицу, уполномоченному расшифровать зашифрованный текст.

Чтобы зашифровать данные, криптография использует **алгоритмы**, которые, в контексте криптографии, являются математическими формулами, которые шифруют или дешифруют данные.

Иногда алгоритмы хранятся в секрете, что делает его более трудным для вскрытия атакующим. Потому что, чтобы дешифровать данные, он должен сначала определить, какой использовался алгоритм шифрования. Однако, сохранение в секрете алгоритма может препятствовать его всестороннему исследованию, которое может показать слабые места в алгоритме, давая, таким образом, ложное чувство безопасности.

Большинство коммерчески используемых алгоритмов общедоступны. Секретные алгоритмы иногда используются правительственными спецслужбами.

Многие алгоритмы шифрования используют ключ как переменную величину, что каждый раз изменяет результат шифрования. Не зная ключ данные трудно дешифровать. Преимущество применения алгоритма с использованием ключей, в том, что многочисленные пользователи могут использовать тот же алгоритм, чтобы зашифровать или дешифровать различные данные. Если знаете алгоритм и один ключ, то вы не можете дешифровать данные, которые были зашифрованы тем же алгоритмом, но с другим ключом. Применение алгоритма с использованием ключа позволяет использовать общедоступный алгоритм и не бояться за раскрытие данных.

Например, использование ключа длиной в 10 битов, может произвести 1,024 вариантов шифрованного текста при использовании одного и того же алгоритма и простого (открытого) текста. Увеличение длины и сложности ключа увеличивает стойкость шифрования (рис. 3.1).

Рисунок 3.1. Стойкость алгоритма и длина ключа

Современная криптография может обеспечить конфиденциальность, целостность данных, аутентификацию, невозможность отказаться и антиповтор, что помогает обеспечивать безопасность данных.

- **Конфиденциальность.** Гарантирует, что только авторизованный персонал может получить доступ информация. Шифрование данных является одним из способов обеспечить конфиденциальность.
- **Целостность данных.** Гарантирует, что возможно обнаружить несанкционированную модификацию данных. Целостность защищает от атаки «человек в середине», в которой атакующий изменяет данные

во время передачи, например, перехват электронного письма и изменение сообщения перед передачей его получателю.

- **Аутентификация.** Проверяет, что данные действительно пришли от пользователя или компьютера, который отправлял эту информацию. Это также защищает от атаки «человек в середине».
- **Невозможность отказаться.** Гарантирует, что человек или процесс не могут отказаться от того, что это именно они выполняли задачи или отправляли данные. Например, невозможность отказа не дает одному из участников договора утверждать, что он не подписывал этот договор, если под ним стоит его подпись.
- **Антиповтор.** Препятствует тому, чтобы атакующий перехватил сообщение и отправил его снова в более позднее время. Например, атакующий мог перехватить последовательность входа в систему и затем воспроизвести сетевые пакеты, чтобы войти в систему в более позднее время. Меры предосторожности от повтора, такие как добавление зашифрованных меток времени к данным, предотвращают такие атаки.

Использование PKI для защиты информации

Инфраструктура PKI обеспечивает распространение цифровых сертификатов среди пользователей и компьютеров, а также управление этими сертификатами безопасным и надежным способом.

PKI — это система компонентов, которая позволяет проводить проверку подлинности и определение удостоверений каждой стороны, вовлеченной в обмен цифровыми данными, посредством шифрования с использованием открытых ключей.

Ниже перечислены компоненты, из которых состоит инфраструктура PKI.

- **Центры сертификации или удостоверяющие центры (ЦС или УЦ).** Центры сертификации представляют людей, процессы и средства, используемые для создания цифровых сертификатов и безопасной привязки удостоверения пользователя к его открытым ключам. Перед выдачей цифрового сертификата пользователю ЦС проверяет удостоверение пользователя и правомочность его попытки получения сертификата.

  ЦС помещает на сертификат свою цифровую подпись, которая удостоверяет происхождение сертификата из доверенного источника, а также действует как защитная печать на самом сертификате, предотвращая любые попытки несанкционированного изменения сертификата.

  Кроме того, ЦС работает иерархическим образом: центры сертификации, выдающие сертификаты, могут использовать другой, более доверенный ЦС в качестве своего родительского центра, чтобы обеспечить уровень доверия, необходимый в среде PKI.

- **Списки отозванных сертификатов.** В спискам отзыва сертификатов содержатся сертификаты, которые были отозваны или удалены из ЦС до истечения срока действия сертификата.
- **Средства управления сертификатами и центрами сертификации.** На сервере Windows Server 2008 R2, настроенном в качестве центра сертификации, доступен особый набор средств, предназначенных для создания сертификатов и управления ими, управления центрами сертификации, а также для обслуживания различных компонентов среды PKI.
- **Сертификаты.** Цифровые сертификаты являются основным элементом работы инфраструктуры PKI. Инфраструктура PKI в первую очередь предназначена для правильного управления этими сертификатами.

Применение защиты электронной почты и мгновенного обмена сообщениями

Одна из главных угроз сегодняшнего дня состоит в заражении корпоративных сетей вредоносным кодом. Вредоносный код может очень серьезно нарушить правильное функционирование корпоративной сети, и разработчики вредоносного кода постоянно изобретают все более хитроумные способы для внедрения этого кода в среду.

Одним из наиболее распространенных и эффективных способов внедрения вредоносного кода в среду является использование электронной почты. Вследствие своего широкого распространения, безусловной необходимости для работы любой организации и естественного доверия механизму доставки, электронная почта, зараженная вредоносным кодом того или иного типа, продолжает оставаться проблемой для ИТ- администраторов.

На этом уроке приводятся основные сведения о различных способах устранения угроз, создаваемых небезопасными действиями электронной почты в целом ряде областей корпоративной среды.

Нежелательная почта

Нежелательная почта, как правило, представляет собой незапрошенные сообщения, которые поступают в папку «Входящие». Такие сообщения обычно распространяются с помощью массовой рассылки нежелательной почты. Получение или сбор адресов электронной почты осуществляется самыми разными способами — главным образом, путем извлечения адресов из интернет-форумов и сообщений. Затем полученные адреса используются для рекламы товаров и услуг, часть которых распространяется в нарушение законодательства. Зачастую лица, рассылающие нежелательную почту, включают в сообщения ложные сведения, чтобы придать таким сообщениям более законный вид, чем это есть на самом деле, а кроме того в нежелательной электронной почте иногда содержатся вирусы.

Фишинг

Одна из форма нежелательной почты называется фишингом. Фишинг — это попытка получения конфиденциальной информации пользователей. Самая распространенная форма фишинга — сбор ключевых сведений о безопасности и банковской информации у пользователей за счет их перенаправления на поддельный веб-сайт. С каждым годом количество фишинговых атак неуклонно растет. Это простой способ получить доступ к информации, которая может пригодиться неоднократно, без постоянной отправки пользователям нежелательной почты с предложениями приобрести товары или услуги. Системы Windows Server 2008 R2, Windows 7 и браузер Windows Internet Explorer 8 включают фильтр фишинга, который сравнивает сайты с известными поддельными вебсайтами, заведомо пытающимися собрать информацию у ничего не подозревающих пользователей.

Спуфинг

Спуфинг — это еще одна распространенная угроза, которая заключается в том, что отправитель пытается выдать себя за другого пользователя, скрывая или маскируя свою подлинную личность. Спуфинг позволяет пользователю А изменить электронную почту, которую он отправляет пользователю Б, таким образом, чтобы она казалась полученной от совершенно другого пользователя, а не от своего реального отправителя.

Фильтрация содержимого

Наиболее распространенным методом идентификации нежелательной электронной почты является фильтрация содержимого. В этом методе для перехвата электронной почты, отправляемой на почтовый сервер (самый распространенный случай) или с почтового сервера, обычно используют программное обеспечение, устанавливаемое на сервере, или специальное устройство. После этого электронная почта проверяется на основе существующей базы данных или каталога известных терминов или шаблонов, имеющих отношение к нежелательной почте. Сообщения электронной почты, которые определены как нежелательные, не достигают своего места назначения, поскольку они удаляются или отправляются в область карантина.

Фильтрация отправителей и получателей

Аналогично фильтрации содержимого, фильтрация отправителей и получателей выборочно фильтрует входящие или исходящие сообщения электронной почты. Однако в этом способе фильтрация осуществляется на основе относительно статической базы данных отправителей и (или) получателей. Предусмотрено два типа фильтрации отправителей и получателей.

- Фильтрация по черному списку определяют адреса электронной почты, о которых известно, что они связаны с нежелательными действиями. Сообщения электронной почты, поступающие с адресов из черного списка, фильтруются и удаляются.
- Фильтрация по белому списку выполняет обратное действие по сравнению с фильтрацией по черному списку. При использовании фильтрации по белому списку адреса электронной почты, содержащиеся в

базе данных белого списка, считаются допустимыми адресами. Фильтрация по белому списку чаще всего применяется в сочетании с фильтрации содержимого, чтобы предотвратить ситуации, когда сообщения электронной почты, поступающие от допустимых отправителей, неверно идентифицируются как нежелательная почта.

Списки запрещенных и разрешенных IP-адресов

Другой способ определения источника сообщений электронной почты состоит в использовании IP-адресов. На почтовых серверах можно настроить проверку на основе базы данных IP-адресов, которые считаются допустимыми адресами или адресами, помеченными как источники рассылки нежелательной почты. Аналогично фильтрации адресов электронной почты, черные и белые списки IP-адресов часто используют в сочетании с более сложной фильтрацией содержимого, чтобы сократить количество ошибочных результатов.

Мгновенные сообщения

Мгновенные сообщения - это очень популярный способ общения с друзьями и коллегами. Однако он привлек внимание злоумышленников. Мгновенные сообщения могут содержать ссылки на небезопасные веб-сайты или использоваться для запуска передачи файлов и сеансов удаленного управления или для осуществления доступа к файлам и содержимому компьютера.

Многие пакеты ПО для обеспечения безопасности защищают от вирусов в файлах, которые могут передаваться через мгновенные сообщения. Однако важно с осторожностью относиться к сведениям, раскрываемым во время беседы с помощью мгновенных сообщений, так как эти сообщения часто передаются в виде простого текста.

Управление безопасностью службы каталога

Обеспечение безопасности серверов под управлением серверной ОС — это непрерывный процесс, подразумевающий регулярную проверку и обслуживание для максимального снижения уязвимостей серверов к возможным атакам. При обеспечении безопасности серверов необходимо принять во внимание несколько областей.

Обеспечение обновлений

Операционные системы, в том числе серверные, постоянно развиваются и изменяются в ответ на возникающий спрос на новые возможности, обнаружение новых угроз безопасности и прочие изменения в мире вычислительных сред. Кроме того, установленные на серверах приложения также испытывают постоянные изменения по многим из перечисленных причин. Вследствие непрерывного изменения, операционные системы и работающие в них приложения постоянно обновляются. Многие процессы обновления, например с помощью Центра обновления Майкрософт или служб Windows Server Update Services (WSUS), в

целом автоматизированы, однако необходимо регулярно проверять исправность работы этих автоматизированных процессов.

Безопасность учетных записей пользователей

В задаче обеспечения целостности серверной среды крайне важную роль играет состояние безопасности учетных записей сервера (и, если применимо, домена). К паролям учетных записей необходимо применять политику сложности паролей, а кроме того, пароли следует регулярно обновлять для предотвращения несанкционированного доступа к учетным записям. Неиспользуемые учетные записи необходимо отключать или удалять из системы. Учетные записи с повышенными привилегиями, такие как учетные записи администратора, должны тщательно контролироваться и использоваться только по их непосредственному назначению. Для большей надежности такие учетные записи можно защитить дополнительными средствами обеспечения безопасности, например смарт-картами или устройствами биометрической проверки подлинности.

Контроль учетных записей

Контроль учетных записей — это компонент системы безопасности, позволяющий пользователям «повышать» уровень своей учетной записи с обычного пользователя до администратора без выхода из системы, смены пользователя или использования команды «Запуск от имени».

Контроль учетных записей — это набор компонентов, а не просто запрос. Эти компоненты, к которым относится переназначение файлов и реестра, обнаружение установщика, запрос функции контроля учетных записей и служба установщика ActiveX, позволяют пользователям Windows использовать учетные записи, не входящие в группу администраторов. Эти учетные записи располагают обычным доступом и, в общем, имеют минимальные полномочия.

Неиспользуемые службы и компоненты

Отключение неиспользуемых служб и компонентов операционной системы не только сокращает потенциальную уязвимость сервера к атакам, но также предоставляет дополнительное преимущество в виде потенциального увеличения производительности.

Защита передачи данных

Одна из наиболее важных вещей, которые необходимо понять, состоит в том, что злоумышленники пытаются получить доступ к сети, используя самые разные средства и методы. Обнаружив способ проникновения, пусть даже небольшой и кажущийся безобидным, они могут развить этот успех и расширить атаку. По этой причине крайне необходимо реализовать целостный подход к безопасности сети, чтобы одна дыра или пробел не приводили к другой.

Для защиты сети от злоумышленных атак можно использовать все перечисленные ниже механизмы защиты.

- Протокол IPsec. Протокол IPsec предоставляет способ проверки подлинности обмена данными по протоколу IP между двумя узлами и, при необходимости, шифрования сетевого трафика.
- Брандмауэры. Брандмауэры позволяют блокировать сетевой трафик на основе его типа.
- Сети периметра. Сеть периметра — это изолированная область сети, в которую и из которой поступает определенный поток сетевого трафика. Если необходимо сделать сетевые службы доступными через Интернет, не рекомендуется подключать размещающие серверы непосредственно к Интернету. Размещая эти серверы в сети периметра, можно сделать их доступными для пользователей Интернета, не предоставляя этим пользователям доступ к корпоративной интрасети.
- Виртуальные частные сети (VPN). Если пользователям необходимо подключиться к корпоративной интрасети из Интернета, очень важно обеспечить максимальную безопасность процесса подключения. Интернет — это общедоступная сеть, и передаваемые через него данные подвержены атакам по перехвату информации или атакам «злоумышленник в середине». Обеспечивая проверку подлинности и шифрование обмена данными между удаленными пользователями и корпоративной интрасетью путем использования сети VPN, можно снизить эти риски.
- Усиление защиты серверов. Выполняя только необходимые службы, можно сделать серверы более безопасными по своей природе. Чтобы определить необходимые службы, следует установить базовый показатель безопасности для серверов. Иногда бывает сложно точно определить, какие службы сетевой ОС требуются для поддержки желаемой функциональности, поэтому для выполнения этой задачи необходимо использовать такие средства, как мастер настройки безопасности.
- Обнаружение вторжений. Безусловно, необходимо реализовать все предыдущие методы обеспечения безопасности сети, однако не менее важно осуществлять мониторинг сети для обнаружения признаков атаки. Для выполнения этой задачи можно внедрить системы обнаружения вторжений. Системы обнаружения вторжений можно реализовать в устройствах периметра сети, таких как маршрутизаторы, подключенные к Интернету.

Применение и мониторинг безопасности сетевого периметра

Чтобы сделать сетевые приложения доступными для пользователей, подключенных к Интернету, необходимо опубликовать эти приложения. Одним из распространенных способов публикации приложений при поддержании надле-

жащего уровня безопасности является использование серверов, размещенных в сети периметра [4].

Брандмауэр помогает защитить компьютер от попыток несанкционированного доступа со стороны компьютеров, размещенных в Интернете. Брандмауэры реализуются с использованием программного обеспечения, оборудования или комбинации этих компонентов. Брандмауэры работают по принципу фильтрации сетевого трафика на основе его характеристик; они разрешают или блокируют трафик в зависимости от настройки.

Брандмауэры бывают четырех типов, Они перечислены ниже.

- Шлюзы уровня приложения. Работают на уровне приложения модели OSI. Шлюзы уровня приложения выполняют проксирование запросов, поступающих в сеть или из сети, и блокируют трафик, для которого не определен прокси. Другими словами, HTTP-прокси не пропускает FTP-трафик. Шлюзы уровня приложения позволяют настроить фильтры NAT Traversal, которые могут поддерживать параметры преобразования IP-адресов и портов с целью поддержки определенных протоколов уровня приложения. Это позволяет приложениям, предназначенным, например, для обмена мгновенными сообщениями или передачи файлов, работать через брандмауэр без необходимости открытия нескольких специальных портов.
- Шлюзы сеансового уровня. Работают на уровне сеанса модели OSI и отслеживают датаграммы между обменивающимися данными узлами для проверки законности запрошенных сеансов. Шлюзы сеансового уровня отслеживают процесс квитирования TCP — используемый для установки TCP-сеансов между узлами — чтобы определить законность сеанса. Кроме того, данные, передаваемые из сети на удаленные узлы, кажутся исходящими из шлюза сеансового уровня. Это бывает полезно для скрытия информации о сети от удаленных узлов.
- Фильтры пакетов. Работают на сетевом уровне модели OSI и часто реализуются в составе маршрутизатора. Каждый пакет фильтруется и сравнивается со списком действий для определения соответствующего действия, которое необходимо выполнить для пакета. Действия заключаются в разрешении или блокировке пакета. Эту функциональность обеспечивает большинство широкополосных маршрутизаторов.
- Многоуровневая проверка с отслеживанием состояния. Эти брандмауэры объединяют аспекты трех других типов маршрутизаторов, обеспечивая наивысший уровень безопасности. Брандмауэры, выполняющие многоуровневую проверку с отслеживанием состояния, проверяют данные на всех семи уровнях модели OSI. В отличие от других брандмауэров, брандмауэры для многоуровневой проверки с отслеживанием состояния проверяют не только заголовок пакета, но и его данные. Каждый пакет рассматривается и сравнивается с образцами пакетов для определения вероятности содержания в пакете злоумышленных данных.

Для настройки сети периметра предусмотрен целый ряд различных способов, часть которых перечислена ниже.

- **Брандмауэр с тремя адаптерами.** Одно устройство или компьютер с несколькими сетевыми картами, одна из которых подключена к Интернету, другая — к сети периметра, а остальные — к интрасети. Для создания разделения между сетями используется программное обеспечение, установленное на узле. Разделение обеспечивается за счет фильтрации в устройстве брандмауэра, чтобы между интерфейсами, обозначенными как общедоступный, частный и периметр, передавался только определенный трафик. Данное решение хорошо работает в небольших сетях; однако из-за того, что устройство брандмауэра подключено непосредственно ко всем трем сетям, оно обеспечивает невысокий уровень безопасности по сравнению с другими решениями.
- **Конфигурация с двумя брандмауэрами.** В данном сценарии два брандмауэра последовательно подключены через три сети: Интернет, сеть периметра и корпоративную интрасеть. Оба брандмауэра непосредственно подключены к сети периметра. Брандмауэры настроены для разрешения передачи между подключенными к ним сетями только соответствующего трафика. Это более сложное и дорогостоящее решение, поскольку для него необходимо настроить дополнительное оборудование и программное обеспечение, однако оно обеспечивает более безопасную среду и рекомендуется для использования в более крупных сетях.

Благодаря сочетанию оборудования и программного обеспечения, а также соответствующей настройки можно создать сеть периметра с оптимальным уровнем сетевой изоляции и одновременно обеспечить необходимый обмен данными между устройствами, расположенными в каждой из трех сетей.

2.2. Стратегии безопасности сервера

Сетевые ОС предоставляют много возможностей и инструментов для защиты вашей сети. Для общего понимания функций безопасности сетевой ОС необходимо изучить раздел «Обзор функций безопасности» соответствующей ОС.

Важные стратегии безопасности включают в себя:

- надежность сервера
- отказоустойчивость
- резервное копирование
- масштабируемость
- доступность
- защита консоли сервера
- шифрование
- гарантированное уничтожение информации (data shredding)
- подписывание пакетов
- система отслеживания транзакций (TTS)
- бесперебойное электропитание (ИБП)
- защита от вирусов
- исправления и пакеты поддержки

Нужно следить за потенциальными рисками и проводить аудит.

А также необходимо обеспечить безопасность рабочих станций.

Надежность сервера

Серверная (сетевая) операционная система – это наиболее надежная, экономически эффективная платформа для предоставления безопасного, беспрерывного доступа к сетевым и информационным ресурсам, созданная инженерами для работы критически важных деловых приложений и сервисов с поддержкой открытых исходных кодов. Серверная ОС дает вам выбор и гибкость, демонстрируя большую интероперабильность приложений, постоянную доступность и инструменты, которые предлагают вам новый уровень продуктивности для таких сервисов:

- Сервисы, повышающие продуктивность
- Сервисы беспрерывной работы
- Сервисы для критически важных программ
- Сервисы с открытыми исходными кодами

Компании-производители серверных ОС рекомендует для своих серверов применять оборудование серверного класса, прошедшее тестирование и получившее сертификацию Novell, Microsoft, SLES, Red Hat и других.

Для прикладных программных продуктов также предусмотрена сертификация.

Надежность – характеризуется большим временем наработки на отказ – система может непрерывно работать продолжительное время, без сбоев и не требуя плановых остановов.

Надежные компоненты позволят вам долго работать без сбоев.

В сетевых ОС есть четкая система обработки исключительных ситуаций – АВОСТов (аварийных остановов, ABEND, BSOD, Kernel Panic). Вызвавший такую ситуацию сервис останавливается.

Современные серверные ОС позволяет запускать непроверенные или ненадежные приложения в отдельных защищенных адресных пространствах, так что сбой в работе приложения не повлияет на операционную систему и другие приложения. Есть возможность автоматического перезапуска такого приложения.

Все это позволяет серверам обеспечивать продолжительное время беспрерывной работы.

Отказоустойчивость

Ваше сетевое решение должно предоставлять надежный и отказоустойчивый доступ к данным для пользователей и приложений. Один из способов повысить надежность доступа – это обеспечить их отказоустойчивость, а это достигается путем избыточности компонентов для устранения единой точки отказа в вашей сети. Сетевые ОС поддерживают избыточность устройств, соединений и серверов.

Отказоустойчивость предоставляет возможность пережить сбой или обеспечить малое время восстановления.

Отказоустойчивость в сетевых ОС обеспечивается несколькими путями.

Сетевая ОС может защищать данные, применяя дублирование таблиц размещения каталогов и файлов (DET - Directory Entry Table, FAT - File Allocation Table) для традиционной файловой системы, дублирование служебной информации об NSS, NTFS и LVM томах и пулах, систему отслеживания транзакций (TTS - Transaction Tracking System) и предоставляя возможность использовать источники бесперебойного питания (ИБП, UPS - Uninterrupted Power Supply).

Сетевые ОС обеспечивает отказоустойчивость дисковой подсистемы с помощью перенаправления сбойных секторов на заранее зарезервированные нормальные секторы жесткого диска, зеркалирования и дуплексирования дисковых разделов (до NetWare 6.0, Windows 2003), а также применения других программных уровней RAID (0, 1, 5, 10 и 15) в NetWare 6.5, Windows 2003R2 и многих современных Linux-дистрибутивах.

Зеркалирование разделов – копирование блоков на раздел другого диска (от 2 до 8).

Дуплексирование разделов – для копирования блоков используются несколько контроллеров, шлейфов и дисков – нет единой точки отказа в дисковой подсистеме.

Для современных систем хранения (SAN – Storage Area Network) может использоваться несколько путей до устройств хранения (multipath).

Управление целостностью данных на серверах

Сетевые ОС имеют несколько свойств томов, которые помогают обеспечивать целостность данных:

- Немедленная запись данных на диск при закрытии файла (Flush Files Immediately)

- Применение системы слежения за транзакциями приложений для отката незавершенных изменений (Transaction Tracking System)
- Применение мгновенных снимков томов для резервного копирования открытых файлов (File-Level Snapshot)

Для сетевых интерфейсов сетевые ОС поддерживает распределение нагрузки, объединение и резервирование (load balancing, teaming/aggregation and failover) каналов связи для сетевых плат.

В некоторых сетевых ОС большинство программ и драйверов могут динамически загружаться и выгружаться в процессе работы и не требуют перезагрузки сервера. Так, например, можно выгрузить старую версию программы, установить новую и запустить уже обновленную версию. То же самое можно сделать и с большинством драйверов устройств – выгрузить старую версию (или некорректно работающую), установить новую, загрузить новую версию драйвера и продолжить работу.

Кроме того, ряд серверных операционных систем на платформе x86 поддерживают добавление или замену устройств в горячем режиме (Hot Plug), это могут быть как внешние устройства хранения, подключаемые по шине USB, жесткие диски с поддержкой горячей замены (hot swap), так и некоторые сетевые и дисковые контроллеры (требуется сервер с поддержкой Hot Plug PCI). В случае отказа такого контроллера, он останавливается, обесточивается, меняется на новый и включается в работу без остановки и выключения всего сервера.

Серверные ОС также поддерживает работу в виртуальной среде (hypervisor aware) или сами могут выступать в роли хостовой ситемы. Это позволяет быстро запустить виртуальный сервер на другом физическом компьютере и с наилучшей производительностью.

Кластеризация

В серверных ОС также применяются схемы повышения отказоустойчивости на уровне всей системы [5].

Для Novell NetWare это были:

NetWare 3 - NetWare SFT-III – два зеркальных сервера

NetWare 4 – Vinca Standby Server – прообраз кластера (один к одному, один ко многим).

NetWare 5 – кластер в виде отдельного продукта (до 32 узлов)

NetWare 6 – 2-узловой кластер входит в состав продукта (остальные узлы – до 32 – оплачиваются дополнительно).

NetWare 6 – кластерное программное обеспечение входит в состав продукта и сразу предоставлена лицензия на 2-узловой кластер.

Novell Cluster Services (NCS) – это ключевой компонент Open Enterprise Server (в него входит Novell NetWare 6.5 и SuSE Linux Enterprise Server 9 или 10), который помогает вам управлять всеми ресурсами в вашей сети хранения данных (Storage Area Network - SAN). Novell Cluster Services интегрирован с Open Enterprise Server и вместе эти продукты позволяют вам:

- Предоставлять непрерывный доступ к данным и ресурсам
- Масштабироваться в соответствии с растущими требованиями в объемах хранения
- Снижать стоимость управления хранения данных

Microsoft для разных версий и редакций Windows Server предлагает два типа кластеров:

- Кластер с балансировкой нагрузки
- Отказоустойчивый кластер

Novell Cluster Services существенно облегчает управление SAN. Например, вы можете управлять ресурсами на iSCSI или Fibre Channel SAN из любого места с помощью вэб-браузера с поддержкой Java. Также поддерживается работа кластера без совместно используемого дискового массива (для ограниченного числа приложений). Еще одной впечатляющей возможностью Novell Cluster Services является поддержка узлов с разными операционными системами – NetWare и Linux!

Применяя это решение, вы сможете следующее:

- Управлять SAN и кластером удаленно
- Объединять до 32 узлов Open Enterprise Server(NetWare или Linux) в кластер
- Поддерживать различную инфраструктуру SAN - iSCSI и Fibre Channel
- Более эффективно использовать дисковое пространство
- Динамически конфигурировать кластер и устройства хранения без перезагрузки (зависит от файловой системы)
- Получать уведомления по SMTP
- Поддерживать передачу управления после сбоя и возвращения его обратно (failover и failback)
- Поддерживать передачу управления после сбоя на несколько узлов кластера (fan-out failover)
- Использовать Business Continuity Clustering для автоматизации управления между кластерами – географически разнесенный кластер кластеров (site-to-site failover)

Геокластеры

После выхода Netware 6.5 вышел Business Continuity Clustering – географически разнесенный кластер, кластер кластеров.

Novell Business Continuity Clustering защищает ваши ключевые бизнес-системы от простоев и катастроф. Созданный на основе Novell Cluster Services (NCS) и Novell Open Enterprise Server, Business Continuity Clustering единственный продукт на рынке, который автоматизирует конфигурирование и управление высокодоступным кластерным решением.

Business Continuity Clustering работает с Open Enterprise Server и Novell Cluster Services, предоставляя передачу управления после сбоя для критических сетевых сервисов на другую площадку. Сетевые сервисы, работающие на кластерах NetWare или SUSE Linux Enterprise Server, могут быть легко переброшены на другой кластер или вообще другой географический регион. Это позволяет избежать простоев, обеспечивает доступность важных сервисов, устраняет риск несоответствия требованиям и минимизирует возможность человеческой ошибки.

Microsoft с выпуском Windows Server 2012 обеспечила работу узлов кластера в разных IP-сетях, что дает возможность тоже строить географически разнесенные кластеры.

Резервное копирование

Резервное копирование – одна из важнейших задач системного администратора. Практически все современные операционные системы имеют встроенные средства резервного копирования и восстановления информации. Конечно, специализированные программы и устройства обладают большими возможностями, но встроенные средства можно использовать в любых ситуациях.

Для полнофункционального резервного копирования необходимы модули (агенты) для файловой системы, eDirectory и Active Directory, других приложений, поддержка ведущих разработчиков оборудования и программ резервного копирования, восстановление удаленных файлов, мгновенных снимков (snapshot), версий фалов (File Versioning and Archiving).

Архивирование – поддержка миграции данных на другие устройства хранения (migrate).

Salvage

Функция спасения (salvage) удаленных файлов на серверах NetWare спасла не одного администратора и пользователя! Вы можете восстановить файлы и папки, которые были удалены с томов NetWare, но еще не были уничтожены (purge). Более того – в большинстве случаев, пользователи могут это сделать самостоятельно, не привлекая сетевого администратора. По умолчанию сервер NetWare такие удаленные файлы до тех пор, пока у него достаточно места на томе для размещения новых файлов. Для немедленного высвобождения этого пространства или для большей безопасности удаленных конфиденциальных данных можно вручную запустить процесс уничтожения удаленных файлов. После такой процедуры файлы и папки можно восстановить только из резервной копии.

Масштабируемость

Масштабируемость показывает способность к увеличению емкости, производительности, мощности, скорости и т.п.

Вертикальная масштабируемость:

- Увеличение возможностей одного сервера
- Достигается добавлением большего или лучшего оборудования в сервер

Горизонтальная масштабируемость:

- Увеличивает емкость приложения
- Достигается добавлением серверов для выполнения вычислений

Масштабируемость сервера – многопроцессорность без переустановки, замена/добавление устройств в горячем режиме, динамическая загрузка/выгрузка программ и драйверов, объединение сетевых карт, настройки по умолчанию, поддержка различных протоколов (IPX/SPX, TCP/IP).

Доступность

Доступность – это уровень сервиса, который предоставляет приложение, служба или система, выражается обычно в процентном соотношении времени, когда услуга предоставляется и не предоставляется с указанным качеством.

В частности, свойство доступность информации (ресурсов автоматизированной системы) — является одним из основных критериев информационной безопасности объекта.

Высокодоступные системы или сервисы доступны 99% времени или выше.

Высокая доступность:

- Требования отличаются в зависимости от того, как измерять доступность
- Обычно не учитывается время плановых простоев при расчете доступности

В сетевых ОС высокая доступность обеспечивается не только надежными компонентами и средствами повышения отказоустойчивости (см. выше), но и разнообразием способов доступа к информации.

Надежность – большое время наработки на отказ – система может непрерывно работать продолжительное время, не требуя плановых остановов.

Отказоустойчивость – способность пережить сбой или быстро восстановиться после сбоя.

Высокая доступность – поддержка различных протоколов (IPX/SPX, TCP/IP, HTTP/HTTPS, NCP, FTP, WebDAV, CIFS, NFS, AFP(AppleShare)), кластер и геокластер, добавление или замена устройств на ходу.

Защита консоли сервера

Защита серверной комнаты

Безопасность серверной должна включать меры безопасности на физическом, процедурном уровне и для персонала. По крайней мере, все серверные должны оснащаться замками на дверях, чтобы ограничить доступ только для уполномоченного персонала. Также могут быть необходимы дополнительные средства физической защиты в зависимости от эксплуатационных потребностей.

Примеры дополнительной физической безопасности включают возможные комбинации из нижеследующего:

- Охрана, наблюдающая за входами и выходами
- Сотрудник службы безопасности сопровождает персонал при работе в серверной
- Служебный пропуск или маркер с аутентификацией и схемой аудита
- Кодовый замок на двери, который требуют ввода кода доступа
- Камеры видеонаблюдения для фиксации действий
- Датчики и аварийные сигналы для обнаружения и предупреждения о несанкционированном доступе

Защита консоли

Первый принцип консольной безопасности сервера - физическая безопасность. Если не обеспечите физическую безопасность, все остальное будет иметь небольшое значение.

Системный блок должен быть зафиксирован в таком месте, где никто не сможет унести его или выключить/перезагрузить. Некоторые администраторы сети убирают и клавиатуру и монитор и управляют сервером удаленно при помощи средств удаленного управления.

Блокировка консоли должна быть активирована и для физической консоли и для утилит удаленного доступа. Блокировка консоли не заменяет безопасность консоли, а только дополняет ее.

Шифрование

В современных серверных операционных системах может применяться шифрование как на уровне отдельных файлов, так и для разделов или логических томов целиком.

Например, для NetWare это Encrypted Volume Support (EVS) for NSS, в Microsoft Windows Server 20xx Encrypting File System и BitLocker, в Linux – LUKS [6].

Encrypted Volume Support (EVS) for NSS

Encrypted Volume Support (EVS) для NSS соответствует юридическому стандарту создания данных, которые будут недоступны программному обеспечению, если будет предпринята попытка обойти нормальное управление доступом, например, если носители будут украдены. EVS доступен только вновь создаваемых томов NSS. EVS хранит пользовательские данные в зашифрованном формате на томе NSS, все дисковые операции прозрачны для большинства приложений, программ NLM и утилит резервного копирования, которые в настоящее время работают с NSS.

Любой том NSS, кроме тома SYS:, в момент создания тома может быть выбран для шифрования. Атрибут шифрованного тома сохраняется в течение всего жизненного цикла тома. Зашифрованный том не может быть в последствии преобразован в незашифрованный, и при этом незашифрованный том не может быть

позже преобразован в зашифрованный. Это решение надо принимать только во время создания нового тома.

Шифрованная файловая система (EFS)

Файловая система EFS предоставляет базовые возможности шифрования на уровне файлов для файлов и папок, сохраняемых на томах NTFS. EFS поддерживает стандартные алгоритмы шифрования, а также шифрование на основе смарт-карт. По умолчанию пользователи создают самозаверяющие ключи шифрования, которые позволяют шифровать и расшифровывать файлы и папки. Прочие пользователи не могут просматривать содержимое файлов, если у них нет ключа.

Файловая система EFS предоставляет быстрый и удобный способ шифрования файлов и папок, содержащих конфиденциальные данные, благодаря которому пользователи могут быть уверены в безопасности своих данных независимо от разрешений, предоставляемых для доступа к файлам и папкам.

EFS позволяет шифровать содержимое файлов, но не метаданные файлов, такие как имя, размер, расширение файлов и назначаемые разрешения.

BitLocker

Шифрование диска BitLocker — это встроенная в ОС Windows Server 2008 R2 система, которая обеспечивает полное шифрование томов операционной системы, а также дополнительных томов данных.

BitLocker-to-Go™ позволяет шифровать съемные диски данных, такие как USB-устройства флэш-памяти и съемные жесткие диски. Также как и в файловой системе EFS, в системе Bitlocker используются ключи шифрования, однако в ней предусмотрено больше возможностей для управления ключами. Пользователи могут сохранять ключи шифрования на съемных USB-накопителях, встраивать ключи доступа или особый аппаратный компонент, называемый доверенным платформенным модулем (TPM), чтобы обеспечить возможность расшифровки зашифрованного тома только при его подключении к определенной системе.

Функции BitLocker просты в реализации; по завершении их настройки они обеспечивают прозрачный доступ к файловой системе.

Шифрование диска Windows BitLocker обеспечивает защиту операционной системы компьютера и данных, хранящихся на томе операционной системы, гарантируя, что данные компьютера остаются зашифрованными, даже если проникновение на компьютер происходит, когда операционная система не работает. BitLocker предоставляет тесно интегрированное с Windows Server 2008 R2 решение, которое предназначено для устранения угроз кражи или раскрытия данных, возникающих в результате потери, кражи или неправильного вывода из эксплуатации компьютеров.

Данные на потерянном или украденном компьютере становятся уязвимыми к несанкционированному доступу, если пользователь запускает одно из средств программных атак для этих данных или переносит жесткий диск компьютера на другой компьютер. BitLocker помогает уменьшить риск несанкционированного доступа к данным путем усиления защиты систем и файлов Windows. BitLocker

также позволяет сделать данные недоступными при выводе из эксплуатации или переработке компьютеров, защищенных с помощью технологии BitLocker.

Гарантированное уничтожение информации (data shredding)

Гарантированное уничтожение данных (data shredding) скрывает удаленные файлы, перезаписывая их случайными образцами шестнадцатеричных символов. Это препятствует тому, чтобы неавторизованные пользователи использовали дисковый редактор, чтобы получить доступ к удаленным файлам.

Если атрибут Data Shredding для тома NSS не установлен, то возможен несанкционированный доступ к данным. Человек может считать блоки удаленного файл и затем извлечь данные.

Гарантированнее уничтожение данных перезаписывает эти блоки от 1 до 7 проходов. Таким образом не остается даже следа от удаленных файлов. Такой процедуре подвергаются только удаленные и очищенные файлы. Если для тома включен атрибут Salvage (спасение), то удаленные файлы сохраняются на томе еще какое-то время, в течение которого они могут быть восстановлены. По прошествии установленного времени файлы переходят в разряд удаленных и очищаемых, что приводит к их полному уничтожению на диске.

Гарантированное уничтожение данных потребляет много дисковой пропускной способности, что может привести к потере производительности, потому что для уничтожения данных используется многократная запись. Чтобы уменьшить эту нагрузку можно снизить количество проходов для перезаписи блоков.

Подписывание пакетов

Вы можете улучшить защиту сети, используя предоставляемую NetWare функцию подписи пакета NCP (NCP Packet Signature).

В последующих подразделах описаны параметры, используемые в конфигурационном файле рабочей станции-клиента (NET.CFG), процедуры их установки, а также команда SET, используемая на каждом NetWare сервере.

Использование подписи пакета NCP для улучшения защиты

Подпись пакета NCP - это усовершенствованная возможность защиты серверов и рабочих станций посредством использования архитектуры NetWare Core Protocol, предотвращающая подлог пакетов.

Использование подписи пакета NCP необязательно, так как это занимает ресурсы процессора и уменьшает производительность в целом, как рабочей станции-клиента, так и сервера NetWare.

Если подпись пакета NCP не установлена, опытные сетевые операторы могут посредством манипуляций с программным обеспечением рабочей станции-клиента посылать подложные запросы NCP серверу NetWare. С помощью подделки настоящих пакетов с запросами NCP нарушитель может получить доступ ко всем сетевым ресурсам.

Как работает подпись пакета NCP

Подпись пакета NCP предотвращает подлог, требуя, чтобы сервер и рабочая станция-клиент "подписывали" каждый пакет NCP, используя шифрование по алгоритму RSA с использованием личного и общего ключей. Подписи различны для каждого пакета.

Пакеты NCP с неправильными подписями отклоняются без разрыва соединения рабочей станции-клиента с сервером. Однако предупреждающее сообщение с записью об источнике неправильного пакета заносится в журнал ошибок, посылается на соответствующую рабочую станцию и на консоль сервера NetWare.

Если подпись пакета NCP установлена на сервере и на всех рабочих станциях-клиентах сети, то практически невозможно подделать пакет NCP так, чтобы это осталось незамеченным.

Когда использовать подпись пакета NCP

Подпись пакета NCP не требуется для каждой инсталляции. Администраторы некоторых сетей могут отказаться от использования подписи пакета NCP, допуская определенный риск в защите.

Допустимый риск при организации защиты

Ниже приведены примеры ситуаций, в которых может не потребоваться использование подписи пакета NCP:

- На сервере содержатся только исполняемые программы.
- Всем пользователям рабочих станций-клиентов в сети можно доверять с точки зрения сетевого администратора.
- Данные на сервере NetWare не имеют особой ценности; доступ к ним, их потеря или изменение не имеют существенного значения.

Серьезный риск при организации защиты

Использовать подпись пакета NCP рекомендуется в следующих случаях:

- В сеть могут проникнуть неправомочные пользователи рабочих станций.
- Имеется простой физический доступ к кабельной системе сети.
- В сети есть неконтролируемые, общедоступные рабочие станции-клиенты.

Опции подписи пакета NCP

Доступны несколько опций подписи в диапазоне от "никогда не подписывать пакеты NCP" до "всегда подписывать пакеты NCP". Серверы NetWare и се-

тевые рабочие станции-клиенты имеют четыре уровня подписи, которые объясняются в приведенной ниже таблице.

Таблица 4.1. Уровни подписи пакета NCP

Уровень	Назначение
0	Не подписывать пакеты.
1	Подписывать пакеты, только если сервер запрашивает подпись (опция NCP сервера NetWare установлена в 2 или больше).
2	Подписывать пакеты, если сервер может подписывать (опция NCP сервера NetWare установлена в 1 или больше).
3	Подписывать пакеты и требовать от сервера подпись пакета (или регистрация в сети будет неудачной).

На сегодняшний день подобный принцип защиты пакетов применяется в IPsec.

IPsec

IPsec — это платформа открытых стандартов для защиты обмена данными по сетям IP посредством криптографических служб безопасности. IPsec поддерживает:

- одноранговую проверку подлинности на уровне сети;
- проверку подлинности источника данных;
- обеспечение целостности данных;
- обеспечение конфиденциальности данных;
- защиту от повторной передачи перехваченных данных.

IPsec обычно используется для обеспечения конфиденциальности, целостности данных и проверки их подлинности при передаче по небезопасным каналам. Первоначально эта платформа предназначалась для защиты трафика в публичных сетях, однако ее реализации часто используются для повышения уровня безопасности частных сетей, поскольку организации не всегда уверены в отсутствии уязвимостей их частных сетей, которыми могут воспользоваться злоумышленники.

IPsec обладает следующими преимуществами.

- Предложение взаимной проверки подлинности перед началом обмена данными и в ходе обмена.
- Принудительная взаимная идентификация сторон в процессе обмена данными.
- Обеспечение конфиденциальности данных посредством шифрования IP-трафика и проверки подлинности цифровых пакетов.

IPsec работает в двух режимах.

- **Транспортный режим.** Это режим IPsec по умолчанию. В транспортном режиме IPsec шифрует только полезные IP-данные, IP-заголовки

не шифруются. Транспортный режим следует выбирать для сквозного обмена данными, например между клиентом и сервером.

- **Туннельный режим.** В туннельном режиме IPsec шифрует как полезные данные, так и заголовки IP-пакетов. Туннельный режим прежде всего предназначен для обмена данными между двумя сетями, когда данные передаются через ненадежную сеть, такую как Интернет.

Система отслеживания транзакций (TTS)

NetWare содержит функцию, следящую за транзакциями, названную системой отслеживания транзакций (TTS). Если отмечаете файл как транзакционный, TTS может предотвратить повреждение записей в файле, отменяя незавершенные транзакций и ведя учет подтвержденных данных.

ПРИМЕЧАНИЕ: файл, отмеченный как транзакционный, не может быть удален или переименован.

TTS может также отменить сокращение или увеличение файла и многократные изменения в той же области данных во время единственной транзакции. TTS может даже отменить прерванные отмены, если сервер NetWare перестал работать в процессе отката транзакций.

По умолчанию NetWare использует TTS, чтобы защитить базу данных NDS/eDirectory от повреждения. Также TTS может защитить от таких типов ошибок приложения любого типа, которые используют работу и блокировкой отдельных записей, включая традиционные базы данных, некоторые приложения электронной почты и некоторых коллективных планировщиков.

Файлы, которые не организованы в виде дискретных записей (такие как файлы обработки текста) не могут быть защищены TTS.

Транзакции в сети могут быть прерваны в любой из следующих ситуаций:

- Электропитание рабочей станции или сервера было нарушено во время транзакции
- Аппаратура сервера или рабочей станции дала сбой (например, ошибка четности)
- Сервер или рабочая станция зависла в ходе транзакции (программный сбой)
- Сетевое оборудование (такое как концентратор, коммутатор или маршрутизатор) дало сбой в процессе транзакции

Бесперебойное электропитание (ИБП)

Источник бесперебойного питания (ИБП - UPS) - модуль резервного питания, который предоставляет бесперебойное питание, если происходит отключение электроэнергии. ИБП - необходимая часть сети. Он не только помогает предотвращать повреждение компьютеров от скачков напряжения и снижений напряжения, но это также предотвращает потерю данных во время отключений электроэнергии.

Существуют онлайновые и оффлайновые системы ИБП:

Онлайновый ИБП. Активно изменяет электропитание, когда оно проходит через модуль. Если происходит отключение электроэнергии, то модуль фактически уже активен и продолжает обеспечивать электропитание.

Онлайновый UPS обычно дороже, чем оффлайновый UPS, но обеспечивает почти постоянный источник энергии во время отключений электроэнергии.

Оффлайновый ИБП. Контролирует линию электропитания. Когда питание пропадает, ИБП активируется.

Недостаток этого метода - небольшая задержка перед тем, как оффлайновый ИБП активируется. Однако, большинство оффлайновых систем ИБП достаточно оперативны, чтобы компенсировать эту задержку.

Поскольку системы ИБП могут быть дорогими, большинство компаний подключает их только к самым критическим устройствам, таким как серверы, маршрутизаторы и дисковые массивы.

Подключение ИБП к серверу позволяет серверу должным образом закрыть файлы и сохранить состояние кэша на диск.

К сожалению, большинство программ работает на рабочей станции, и данные, находящиеся в оперативной памяти, не сохраняются во время отключения электроэнергии. Поэтому рабочие станции тоже стоит оснащать отдельными ИБП или подключать к системе гарантированного электропитания в здании.

Кроме того, рабочие места можно оснащать устройствами защиты от всплесков напряжения.

Защита от вирусов

Вирус — это фрагмент вредоносного кода, который копирует себя и распространяется в определенном виде или форме. Такой код обычно распространяется с помощью нежелательной почты или путем получения доступа к другим компьютерам и попытки их заражения. Слово «вирус» стало универсальным термином для обозначения традиционных вирусов, распространение которых не имело другой цели, кроме использования соответствующего кода. Однако сейчас этим термином называют вредоносные программы, программы для показа рекламы, шпионское ПО и все программы, которые заражают компьютеры. Многие вирусы выполняют вредоносные действия на зараженных компьютерах, такие как кража данных или отключение важных приложений.

Оберегайте сеть от вирусов. Расскажите пользователям о вирусных опасностях и осуществляйте процедуры, которые снижают риск вирусных эпидемий, например такие:

Регулярно производите резервное копирование.

Храните несколько версий архивированных резервных копий, таким образом, вы сможете получить резервную копию еще не зараженного файла.

Сохраните загрузочную дискету, защищенную от записи, или компакт-диск с последним антивирусным сканером и программным обеспечением удаления вирусов для всех серверов и рабочих станций.

Сохраните резервные копии исполняемых файлов и пометьте их «Только для выполняются» (Execute Only).

Узнайте о методах инфицирования последних вирусов.

Расскажите сетевым пользователям о том, как обнаружить вирусы.

Предупредите пользователей относительно опасностей вирусов. Убедите их не использовать дискеты, съемные диски, флэшки и файлы, которые были использованы в компьютерах вне работы.

Научите пользователей выключать свои рабочие станции сазу после обнаружения вирусов.

Избегайте использования администраторской учетной записи, если это возможно. Чем меньше полномочий, которые имеет учетная запись, тем меньше действий может выполнить вирус, тем меньше у него шансов уничтожить данные и продолжать распространяться.

Антивирусную защиту надо устанавливать на серверах, рабочих станциях и пограничных устройствах (шлюзах, где это возможно).

Исправления и пакеты поддержки

Повсеместно вычисления выполняются в постоянно меняющейся среде. Ежедневно появляются новые технологии, в то время как новые способы использовать эти технологии, кажется, появляются ежечасно. По мере развития технологий и появления потребности в обеспечении безопасности необходимо подготовить серверную инфраструктуру к эффективной работе и одновременно защитить ее.

При работе со статическим, не обновляемым сервером под управлением сетевой ОС необходимо ответить на следующие вопросы.

Уязвим ли сервер к злоумышленному коду, использующему потенциально слабые места в операционной конфигурации этого сервера или в конфигурации приложений?

Как при установке нового устройства убедиться в том, что установлена последняя версия драйвера?

Как убедиться в том, что используются последние и наиболее совместимые версии приложений?

Необходимо обновить серверы с сетевой ОС, чтобы гарантированно избежать упомянутых выше проблем, однако даже настройка одного сервера вручную является трудоемкой и времязатратной операцией, не говоря о конфигурации сотен серверов.

Основным источником обновлений для операционных систем является вебсайт обновлений производителя. Там хранится каталог обновлений, доступных для загрузки и установки на компьютер.

Многие сетевые ОС имеют средства локального хранения обновлений, полученных с вэб-сайта производителя, для распространения их в сети своей организации.

Однако обязанностью администратора является убедиться, что доступные средства приспособлены для использования в соответствующей среде, и обеспечить защиту и регулярное обновление инфраструктуры.

Для программных продуктов компании Microsoft таким средством является Windows Server Update Services (WSUS).

Windows Server Update Services (WSUS)

Служба WSUS позволяет сетевым администраторам упростить процедуру применения обновлений на всех компьютерах сетевой среды и усилить контроль над процессом.

Если службы WSUS установлены на сервере, они загружают все последние обновления с серверов Центра обновления Windows в Интернете, а затем все другие компьютеры настраиваются для загрузки своих обновлений непосредственно с сервера WSUS.

В стандартной реализации службы WSUS файлы обновления с серверов Центра обновления Майкрософт загружаются только сервером службы WSUS, а не независимо каждым компьютером. Сервер службы WSUS загружает копию каждого доступного обновления и сохраняет его в локальном хранилище данных, предоставляя доступ к нему всем компьютерам в сети. Поскольку сервер службы WSUS загружает только одну копию каждого обновления, значительно снижается используемая в процессе обновления пропускная способность. Служба WSUS также предоставляет администраторам возможность изучать, оценивать и тестировать обновления до развертывания в сетевых клиентах.

Сервер службы WSUS имеет несколько компонентов и параметров, которые можно настроить в соответствии с потребностями среды.

- **Синхронизация.** Этот параметр контролирует время синхронизации службы WSUS с серверами Центра обновления Майкрософт в Интернете для загрузки новых обновлений.
- **Продукты.** Этот параметр задает продукты, для которых служба WSUS загрузит обновления. Сюда относятся серверные и клиентские операционные системы Windows, а также многие приложения и серверные продукты Microsoft, такие как Microsoft Office, SQL Server, Exchange Server и многие другие.
- **Классификации.** Существует несколько разных классификаций обновлений Майкрософт, определяющих тип и срочность обновления. Этот параметр позволяет выбрать классификации для синхронизации службой WSUS.
- **Языки.** По умолчанию служба WSUS синхронизирует только обновления на языке, заданном при установке Windows Server 2008 R2.
- **Утверждения.** Этот параметр контролирует применение обновлений к клиентам и определяет классификации, задаваемые для автоматического утверждения и последующей установки. По умолчанию служба WSUS автоматически утверждает все обновления безопасности, критические обновления и обновления определений для серверов. Для клиентов служба WSUS утверждает все обновления безопасности, критические обновления и обновления определений, а также пакеты обновлений.

- **Хранение.** Служба WSUS загружает только утвержденные обновления и по умолчанию хранит их в формате Cab в папке C:\WSUS\WsusContent.
- **Серверные обновления.** По умолчанию серверы загружают последние обновления с сервера WSUS и информируют администратора о своей готовности к установке. Администратор должен установить их вручную с использованием приложения панели управления Центра обновления Windows.
- **Клиентские обновления.** Клиенты подключаются к серверу WSUS и загружают последние обновления для соответствующих операционных систем, а затем автоматически устанавливают их в соответствии с заданным расписанием. При необходимости клиент автоматических обновлений перезапускает компьютер по завершении установки обновлений.

Служба WSUS управляется с использованием оснастки MMC, позволяющей настраивать параметры, просматривать статус обновлений и управлять им, а также добавлять новые клиентские компьютеры или группы в сервер WSUS.

SLES Update

У OES 11 администраторов есть три варианта для обновления серверов заплатками (патчами) от Novell.

ZENworks Linux Management - продукт корпоративного уровня, который требует отдельной лицензии. Это предоставляет обновления для продуктов SUSE Linux Enterprise, OES и Red Hat Enterprise Linux (RHEL). В дополнение к локальному хранению обновлений для загрузки ZENworks Linux Management также способен «проталкивать» обновления на указанные устройства с помощью единого веб-интерфейс.

Subscription Management Tool (SMT) для SUSE Linux Enterprise - этот продукт не требует отдельной лицензии. Это позволяет, локально хранить патчи из онлайнового репозитария обновлений Novell на сервере, что обеспечивает больше безопасности и значительно уменьшает веб-трафик, связанный с обновлениями сервера. SMT доступен для скачивания на сайте загрузок Novell.

Novell Online Update Servers - для тех, кому не требуется внутреннего источника обновления, серверы OES 11 могут быть легко сконфигурированы, чтобы непосредственно получать доступ к онлайновому репозитарию патчей.

Red Hat Network

Red Hat Enterprise Linux 6 предоставляет гибкие методы управления подписками.

Подписки Red Hat Network теперь определяются не каналами, а обслуживаемыми продуктами и их числом. Соответственно доработаны инструменты управления подписками.

- Старая версия RHN теперь известна как RHN Classic.

- Оба вида RHN доступны параллельно.
- Окружения, взаимодействующие с Satellite или прокси-сервером, по-прежнему будут использовать RHN Classic.

Теперь в списке опций помощника Firstboot можно выбрать Red Hat Network Classic. По умолчанию будет выбрана платформа управления RHN на основе сертификатов.

Оба типа являются взаимозаменяемыми. Если для системы выбран один тип RHN, то другой тип ее сможет распознать. В то же время оба типа не могут работать параллельно.

2.3. Реализация защищенных компьютерных сетей на примере Windows, NetWare.

В этой главе будут представлены практические работы по организации защиты серверов на базе серверных операционных систем Microsoft Windows Server 2008 R2 и Novell NetWare 6.5.

Лабораторная работа для Microsoft Windows Server 2008 R2.
Шифрование файлов.

Упражнение 1. Шифрование отдельных файлов с помощью EFS

Право доступа к зашифрованным файлам можно предоставлять отдельным пользователям. Для предоставления другим пользователям общего доступа к зашифрованному файлу выполните представленные ниже действия.

1. Щелкните зашифрованный файл правой кнопкой мыши в проводнике и выберите пункт **Свойства**.
2. На вкладке **Общие** нажмите кнопку **Дополнительно**.
3. В диалоговом окне **Дополнительные атрибуты** нажмите кнопку **Сведения** в разделе **Атрибуты сжатия и шифрования**.
4. В диалоговом окне **Сведения о шифровании** нажмите кнопку **Добавить**.
5. Добавьте пользователя с локального компьютера или из доменных служб Active Directory.

Внедрение программ обеспечения безопасности

Упражнение 1. Ограничение на приложения с помощью AppLocker

Задание 1. Создайте объект групповой политики, чтобы применить правила исполняемых файлов AppLocker по умолчанию

1. На виртуальной машине LAB-DC1 нажмите кнопку **Пуск**, щелкните **Администрирование** и выберите оснастку **Управление групповой политикой**.
2. Последовательно разверните узлы **Лес: lab-sec.com** и **Домены**.
3. Разверните узел **lab-sec.com**.
4. Щелкните **Объекты групповой политики**.
5. Щелкните правой кнопкой мыши **Объекты групповой политики** и выберите **Создать**.
6. Назовите новый объект групповой политики **Политика ограниченного использования WordPad** и нажмите кнопку **ОК**.
7. Правой кнопкой мыши щелкните элемент **Политика ограниченного использования WordPad** и выберите команду **Изменить**.
8. Последовательно разверните **Конфигурация компьютера**, **Политики**, **Конфигурация Windows** и **Параметры безопасности**, **Политики управления приложениями** и **AppLocker**.
9. Выберите **Правила исполняемых файлов**, затем щелкните правой кнопкой мыши и выберите команду **Создать новое правило**.
10. Нажмите кнопку **Далее**.
11. На экране **Разрешения** выберите **Запретить** и нажмите кнопку **Далее**.

12. На экране **Условия** выберите **Издатель** и нажмите кнопку **Далее**.
13. Нажмите кнопку **Обзор...**, затем щелкните **Компьютер**.
14. Дважды щелкните значок **Локальный диск (C:)**.
15. Последовательно дважды щелкните **Program Files**, **Windows NT**, **Стандартные**, выберите **wordpad.exe** и нажмите кнопку **Открыть**.
16. Переместите ползунок вверх на **Имя файла:** и нажмите кнопку **Далее**.
17. Еще раз нажмите кнопку **Далее** и щелкните **Создать**.
18. При запросе на создание правил по умолчанию нажмите кнопку **Да**.
19. В редакторе групповых политик последовательно разверните узлы **Конфигурация компьютера**, **Конфигурация Windows** и **Параметры безопасности**.
20. Разверните узел **Политики управления приложениями**.
21. Щелкните **AppLocker**, затем щелкните правой кнопкой мыши и выберите пункт **Свойства**.
22. На вкладке **Применение** в разделе **Правила исполняемых файлов** установите флажок **Настроено** и выберите **Принудительное применение правил**.
23. Нажмите кнопку **ОК**.
24. В редакторе групповых политик последовательно разверните узлы **Конфигурация компьютера**, **Конфигурация Windows** и **Параметры безопасности**.
25. Щелкните **Системные службы**, затем дважды щелкните **Удостоверение приложения**.
26. В диалоговом окне **Свойства: удостоверение приложения** установите флажок **Определить следующий параметр политики**.
27. Выберите значение **автоматически** в поле **Выберите режим запуска службы** и нажмите кнопку **ОК**.
28. Закройте редактор управления групповыми политиками.

Задание 2. Примените объект групповой политики к домену Lab-sec.com
1. В окне управления групповыми политиками разверните
Лес: Lab-sec.com.
2. Разверните узел **Домены**.
3. Разверните **Lab-sec.com**.
4. Разверните **Объекты групповой политики**.
5. Перетащите **Политика ограниченного использования WordPad** к верхней части контейнера домена Lab-sec.com.
6. Нажмите кнопку **ОК**, чтобы связать объект групповой политики с доменом.
7. Закройте Консоль управления групповыми политиками.
8. Нажмите кнопку **Пуск**, в поле **Найти программы и файлы** введите **cmd** и нажмите клавишу ВВОД.
9. В окне командной строки введите **gpupdate /force** и нажмите клавишу ВВОД. Подождите, пока политика обновится.

Задание 3. Проверьте правило AppLocker
1. Войдите в виртуальную машину **LAB-CL1** под учетной записью **Lab-sec\Alan** с паролем **Pa$$w0rd**.

2. Нажмите кнопку **Пуск**, в поле **Найти программы и файлы** введите **cmd** и нажмите клавишу ВВОД.
3. В окне командной строки введите **gpupdate /force** и нажмите клавишу ВВОД. Подождите, пока политика обновится.
4. Нажмите кнопку **Пуск**, щелкните **Все программы**, затем **Стандартные** и **WordPad**.
5. При отображении сообщения нажмите **ОК**.

Упражнение 2. Использование мастера настройки безопасности
Задание 1. Создайте политику безопасности
1. На виртуальной машине LAB-DC1 нажмите кнопку **Пуск**, **Администрирование** и запустите **Мастер настройки безопасности**.
2. На странице **Мастер настройки безопасности** нажмите кнопку **Далее**.
3. На странице **Действие настройки** выберите **Создать новую политику безопасности** и нажмите кнопку **Далее**.
4. На странице **Выбор сервера** примите имя сервера по умолчанию **LAB-DC1** и нажмите кнопку **Далее**.
5. На странице **Обработка базы данных настройки безопасности** можно щелкнуть **Просмотр базы данных** и просмотреть обнаруженную конфигурацию сервера LAB-DC1.
6. Нажмите кнопку **Далее**.
7. На начальной странице раздела **Настройка служб на основе ролей** нажмите кнопку **Далее**.
8. На странице **Выбор ролей сервера** можно просмотреть обнаруженные параметры сервера LAB-DC1, однако изменять их не следует. Нажмите кнопку **Далее**.
9. На странице **Выбор клиентских возможностей** можно просмотреть обнаруженные параметры сервера LAB-DC1, однако изменять их не следует. Нажмите кнопку **Далее**.
10. На странице **Выбор управления и других параметров** можно просмотреть обнаруженные параметры LAB-DC1, однако изменять их не следует. Нажмите кнопку **Далее**.
11. На странице **Выбор дополнительных служб** можно просмотреть обнаруженные параметры сервера LAB-DC1, однако изменять их не следует. Нажмите кнопку **Далее**.
12. На странице **Обработка неопределенных служб** не изменяйте параметр по умолчанию **Не изменять режим запуска этой службы**. Нажмите кнопку **Далее**.
13. На странице **Подтверждение изменений для служб** в списке **Просмотреть** выберите **Все службы**.
14. Просмотрите параметры в столбце **Текущий режим запуска**, отражающем режимы запуска служб на виртуальной машине LAB-DC1, и сравните их с параметрами в столбце **Режим запуска политики**.
15. В списке **Просмотреть** выберите **Измененные службы**.
16. Нажмите кнопку **Далее**.

17. На начальной странице раздела **Сетевая безопасность** нажмите кнопку **Далее**.
18. На странице **Правила сетевой безопасности** можно проверить правила брандмауэра, полученные из конфигурации LAB-DC1. Не меняйте никакие параметры. Нажмите кнопку **Далее**.
19. На начальной странице раздела **Параметры реестра** нажмите кнопку **Далее**.
20. На каждой из страниц раздела **Параметры реестра** проверьте параметры, не изменяя их, и нажмите кнопку **Далее**. Нажимайте кнопку **Далее** на всех страницах, пока не появится страница **Сводка параметров реестра**, просмотрите параметры и нажмите кнопку **Далее**.
21. На начальной странице раздела **Политика аудита** нажмите кнопку **Далее**.
22. На странице **Политика аудита системы** проверьте параметры, но не изменяйте их. Нажмите кнопку **Далее**.
23. На странице **Сводка политики аудита** проверьте параметры в столбцах **Текущее значение** и **Параметр политики**. Нажмите кнопку **Далее**.
24. На начальной странице раздела **Сохранение политики безопасности** нажмите кнопку **Далее**.
25. В поле **Имя файла политики безопасности** щелкните конец пути к файлу и введите **Политика безопасности контроллера домена**.
26. Нажмите кнопку **Просмотр политики безопасности**.
27. Нажмите кнопку **Да**.
28. Завершив изучение политики, закройте окно.
29. В мастере настройки безопасности нажмите кнопку **Далее**.
30. На странице **Применение политики безопасности** примите параметр по умолчанию **Применить позже** и нажмите кнопку **Далее**.
31. Нажмите кнопку **Готово**.

Задание 2. Преобразуйте политику безопасности в объект групповой политики
1. На виртуальной машине LAB-DC1 нажмите кнопку **Пуск**, в поле **Найти программы и файлы** введите **cmd** и нажмите клавишу ВВОД.
2. Введите команду **cd c:\windows\security\msscw\policies** и нажмите клавишу ВВОД.
3. Введите команду **scwcmd transform /p:"Политика безопасности контроллера домена.xml" /g:"DC Security Policy"** и нажмите клавишу ВВОД.
4. Закройте окно командной строки.
5. Нажмите кнопку **Пуск**, щелкните **Администрирование**, затем **Управление групповой политикой**.
6. В дереве консоли последовательно разверните узлы **Лес:Lab-sec.com**, **Домены**, **Lab-sec.com** и **Объекты групповой политики** и щелкните **DC Security Policy**. Это объект групповой политики, созданный командой Scwcmd.exe.
7. Перейдите на вкладку **Параметры**, чтобы просмотреть параметры объекта групповой политики.
8. Закройте Консоль управления групповыми политиками.

Лабораторная работа для Novell NetWare 6.5.
Защита консоли сервера NetWare

Задание 1. Защитите консоль сервера NetWare

1. На виртуальной машине NW65 одновременно нажмите Ctrl+Esc и нажмите клавишу ВВОД.
2. В появившемся списке обратите внимание на то, что экран системной консоли имеет всегда имеет порядковый номер 1.
3. В сроке приглашения введите **1** и нажмите клавишу ВВОД.
4. В сроке приглашения введите **ea** (edit AUTOEXEC.NCF) и нажмите клавишу ВВОД.
5. С помощью клавиш навигации перейдите к концу файла AUTOEXEC.NCF в редакторе и в нижней строке введите **LOAD SCRSAVER** и нажмите клавишу ВВОД.
6. В следующей строке введите SECURE CONSOLE и нажмите клавишу ВВОД.
7. Нажмите клавишу ESC и сохраните файл, выбрав YES.

Теперь при следующей загрузке сервера консоль будет защищена автоматически.

8. В сроке приглашения введите **SCRSAVER** и нажмите клавишу ВВОД.
9. В сроке приглашения введите **SECURE CONSOLE** и нажмите клавишу ВВОД.

Теперь консоль сервера защищена в текущем сеансе.

Защита данных на сервере NetWare

Задание 2. Создайте зашифрованный том на сервере NetWare с гарантированным уничтожением файлов.

1. На виртуальной машине NW65 одновременно нажмите Ctrl+Esc и нажмите клавишу ВВОД.
2. В появившемся списке обратите внимание на то, что экран системной консоли имеет всегда имеет порядковый номер 1.
3. В сроке приглашения введите **1** и нажмите клавишу ВВОД.
4. В сроке приглашения введите **nssmu** и нажмите клавишу ВВОД.
5. В главном меню выберите **Partitions** и нажмите клавишу ВВОД.
6. Посмотрите на список существующих разделов в окне Partitions в левой части экрана.
7. Для создания нового раздела нажмите клавишу INSERT.
8. В списке свободного пространства выберите доступный элемент и нажмите клавишу ВВОД.
9. В появившемся списке типов разделов выберите **NSS** и нажмите клавишу ВВОД.
10. В поле **New partition size**: введите размер нового раздела **1024** (в мегабайтах) и нажмите клавишу ВВОД.
11. В поле **(Optional) Pool Name:** введите название дискового пула **SecPool** и нажмите клавишу ВВОД.

12. Нажмите стрелку вниз и перейдите к пункту **Create** и нажмите клавишу ВВОД.
13. Дважды нажмите клавишу ESC для выхода в главное меню.
14. Перейдите к пункту **Volumes** и нажмите клавишу ВВОД.
15. Для создания нового логического тома нажмите клавишу INSERT.
16. Наберите название нового тома **SECVOL** и нажмите клавишу ВВОД.
17. На вопрос **Encrypt Volume?** (Зашифровать том?) выберите ответ **Yes** (Да) и нажмите клавишу ВВОД.
18. В поле пароля ведите **novell** и нажмите клавишу ВВОД.
19. Подтвердите пароль **novell** и нажмите клавишу ВВОД.
20. Проверьте название тома **SECVOL**, выберите **Ok** и нажмите клавишу ВВОД.
21. В списке пулов выберите SECPOOL и нажмите клавишу ВВОД.
22. В свойствах нового тома выберите **Data Shredding**:, нажмите клавишу **Y** и нажмите клавишу ВВОД.
23. В поле **Times to shred data:** введите 5 (5 проходов) (рис. 5.1) и нажмите клавишу ВВОД.
24. Перейдите к пункту **Create** и нажмите клавишу ВВОД.
25. В списке логических томов вы увидите вновь созданный зашифрованный том с затиранием уничтоженных файлов.
26. Дважды нажмите клавишу ESC для выхода из утилиты **NSS Management Utility**, подтвердите выход и нажмите клавишу ВВОД.
27. В системном приглашении наберите команду **volume** и нажмите клавишу ВВОД.
28. В списке смонтированных томов убедитесь, что присутствует том **SECVOL**.

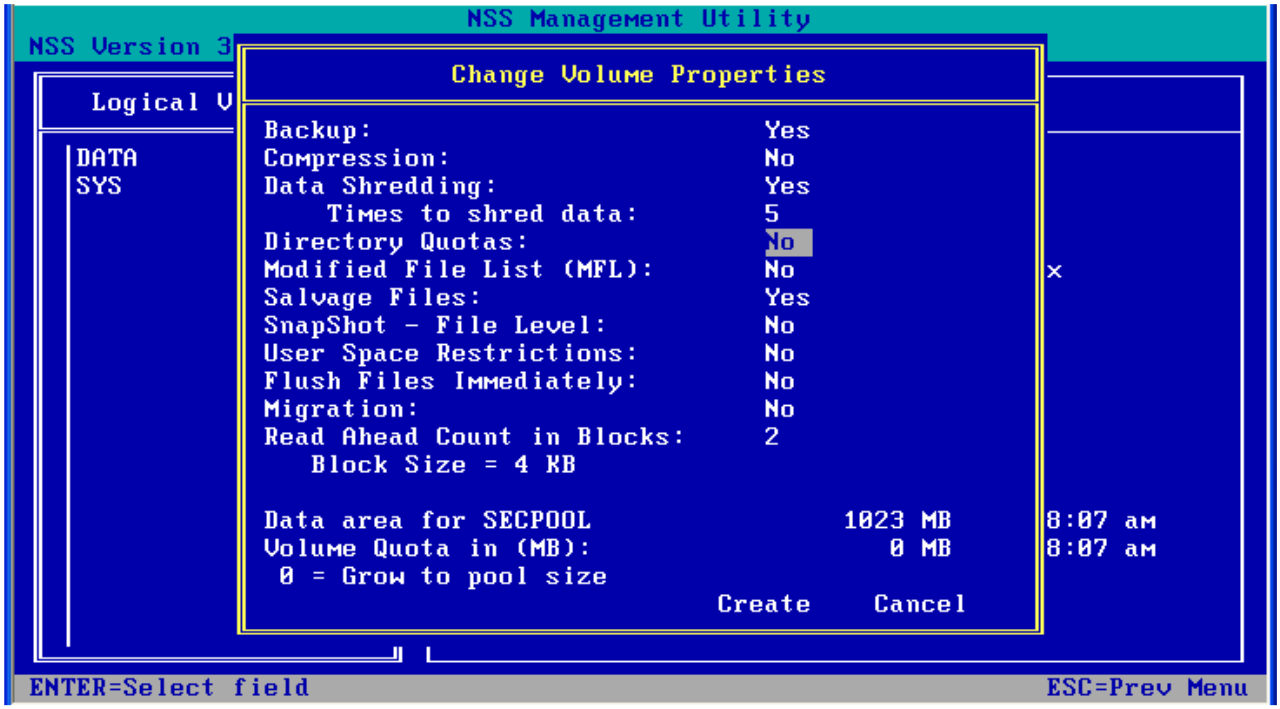

Рис. 5.1. Свойства тома SECVOL

Список литературы

1. Project Management Institute, A Guide to the Project Management Body of Knowledge, Fourth Edition, - Project Management Institute; 4 edition – 459 стр., ASIN: B004MME6HK
2. Risk Management Guide for Information Systems, from the National Institute of Standards and Technology (NIST), at http://csrc.ncsl.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.
3. The Microsoft white paper, Risk Model for Operations
4. Eric Cole, Network Security Bible, 2 edition – Wiley – 936 стр., ISBN-10: 0470502495, ISBN-13: 978-0470502495
5. Гаскин Д., Администрирование Novell NetWare 6.0/6.5 (+CD-ROM), - СПб.: БХВ-Санкт-Петербург - 1056 стр., ISBN 5-94157-233-6
6. Michael Jang, RHCSA/RHCE Red Hat Linux Certification Study Guide (Exams EX200 & EX300), 6th Edition, - McGraw-Hill Osborne Media – 1072 стр., ASIN: B0087OSS3C

Приложение I

Справочные материалы

1. Краткая история компьютерных сетей

Первые электрические вычислительные системы были очень большими – они занимали целые здания, и эксплуатировались, управлялись и обслуживались учеными. Собственно результаты вычислений использовали на месте, никуда не передавая, так как все заинтересованные лица находились тут же.

Потом появилась необходимость обменяться полученными результатами. Вот тут-то и начинается история вычислительных сетей!

Поскольку первые вычислительные комплексы были очень дорогими, то редкие страны могли себе позволить их создание. И даже если в стране было построено уже несколько таких комплексов, то находились они в разных городах, далеко друг от друга, что затрудняло из без того непростую задачу обмена полученными результатами. Поэтому первое соединение вычислительных систем друг с другом было осуществлено, как это ни поразительно, на большом расстоянии, то, что сейчас называют удаленным доступом. Для этого использовали существующую телефонную сеть и вместо голоса передали данные между компьютерами. Случилось это в 1965 году, когда Лоренс Робертс (Lawrence G. Roberts) [1], исследователь из Массачусетсского технологического института (MIT), работающий с Томасом Мерриллом (Thomas Merrill) под общим руководством Дж. Ликлайдера[1], соединил компьютер TX-2 в Массачусетссе с компьютером Q-32 в Калифорнии, используя низкоскоростную телефонную линию (других, собственно, тогда не было). Получилось то, что позже стали называть WAN (Wide Area Network – ГВС, глобальная вычислительная сеть) территориально распределённой сетью.

Ларри Робертса еще иногда называют «Отцом ARPANET». Он получил это прозвище когда руководил командой инженеров создавших ARPANET. Также Робертс был основным архитектором ARPANET.

ARPANET

ARPANET – сокращение от Advanced Research Projects Agency Network. Эта сеть была создана в 1969 году по заданию агентства ARPA; разрабатывалась она Калифорнийским Университетом в Лос-Анджелесе (UCLA), Стэнфордским исследовательским центром, Университетом штата Юта и Университетом штата Калифорния в Санта-Барбаре.

При создании ARPANET перед сетью ставились задачи, сформулированные Минобороны: необходимо было создать такую систему коммуникации, которая продолжала бы работу после повреждения её части – даже центральной, и которая бы функционировала после ядерной атаки.

Сеть развивалась очень быстро, стала международной и, хотя в 1990 году прекратила своё существование, она заложила технологические основы Интернета, то есть, фактически была его прародителем.

Джозеф Карл Робнетт Ликлайдер (Joseph Carl Robnett Licklider) стал первым директором Information Processing Techniques Office (IPTO) в Advanced Research Projects Agency (ARPA) в 1962 году. Он предвидел необходимость объединения компьютеров в сеть, необходимость простых пользовательских интерфейсов. Его идеи предвосхитили компьютерную графику, интерфейсы, работающие по принципу указания и выбора (point-and-click), цифровые библиотеки, электронную коммерцию (e-commerce), дистанционное банковское обслуживание (online banking), а также размещаемое в сети ПО.

Работая в Массачусетсском Технологическом Институте (MIT), Леонард Клейнрок изобрёл новый способ передачи информации с помощью разбиения ее на части – пакеты. Технология существенно повысила надежность и скорость передачи данных. В 1961 году вышла первая статья Клейнрока о пакетной коммутации. Первая книга Клейнрока, посвященная теории пакетной коммутации, была выпущена в 1964 году. Три человека считаются изобретателями пакетной коммутации: Леонард Клейнрок (Leonard Kleinrock), Дональд Дэвис (Donald Davies) и Пол Бэрэн (Paul Baran).

А в сентябре 1969 года, вместе с группой выпускников Калифорнийского Университета в Лос-Анджелесе (UCLA), 29 октября Клейнрок соединил компьютеры SDS (Scientific Data Systems) Sigma 7 с помощью Interface Message Processor (первый коммутатор пакетов) так что они стали первыми узлами в сети ARPANET.

29 октября 1969 г. принято считать днем рождения Сети. В этот день в 22:30 была предпринята самая первая, правда, не вполне удавшаяся, попытка дистанционного подключения к компьютеру, находившемуся в исследовательском центре Стэндфордского Университета (SRI), с другого компьютера, который стоял в Калифорнийском Университете в Лос-Анджелесе (UCLA). С удалённых друг от друга на расстояние 500 км компьютеров в SRI и UCLA попытались зарегистрироваться, введя слово “login”, и успешно передали символ “l”, потом “o”, а на передаче “g” система дала сбой, так что первое послание по будущему Интернету было “lo”! Спустя примерно час им все же удалось установить соединение.

Затем к ним подключили ещё два узла: Калифорнийский Университет Санта-Барбары (UCSB) и Университет штата Юта (UTAH).

Именно эти 4 организации распределили между собой основные функции по созданию компонентов глобальной сети:

- UCLA – проведение измерительных испытаний;
- SRI – создание информационного центра;
- UCSB – разработка математического аппарата;
- UTAH – первые работы по трёхмерной графике.

Проведение испытаний стало возможно благодаря тому, что к 1 Сентября 1969 года компания BBN изготовила 1-вые экземпляры устройства IMP (Interface Message Processor), обеспечивающего связь между компьютерами по телефонным каналам.

В 1972 году в Вашингтоне прошла первая Международная конференция по компьютерным коммуникациям. На конференции присутствовали ученые из 10 стран. Участникам конференции была представлена сеть ARPANet.

В 1972 году была создана общественная организация INWG – рабочая группа по международным сетям, под руководством Винсента Сёрфа [1]. Она координировала работу по созданию возможности межсетевого обмена. Для объединения сетей, работающих по протоколу IP и сетей, работающих по другим протоколам, необходимо было создать специальный межсетевой протокол. Этот протокол был создан Винсентом Сёрфом [1] и Робертом Канном [1] в 1974 году и назван TCP.

После объединения в 1982 году двух протоколов TCP и IP в один, протокол TCP/IP стал стандартным протоколом объединенной сети – Интернет. В этом же году Сёрф и его коллеги ввели термин «Интернет». Сегодня их называют «Отцами Интернета».

Россия впервые получила доступ к Интернету в начале 80-х годов. Доступ был осуществлен Институтом атомной энергии им. И. В. Курчатова. В 1990 году создается РЕЛКОМ – сеть пользователей UNIX.

20 марта 1998 впервые проводится Всемирный День Интернет.

Концепция публикации общедоступных документов с гиперссылками и обмена ими помощью протокола передачи гипертекста по компьютерным сетям, которая легла в основу Интернета в современном представлении, была разработана в 1989 году в Европейской лаборатории физики элементарных частиц (CERN) в Женеве, англичанин Тим Бернерс-Ли (Tim Berners-Lee) [1] придумал название World Wide Web (WWW) в 1990 году.

2. Основы сетевого взаимодействия

В этой главе будут рассмотрены предпосылки, приведшие к созданию сетей и основные элементы сетей.

Причины создания компьютерных сетей

Большие вычислительные машины были очень дорогими устройствами и обслуживались учеными и высококлассными специалистами. Периферийные устройства, необходимые для ввода данных и команд, для вывода и хранения результатов стоили значительно меньше самого вычислителя, а полученные данные использовались как исходный или промежуточный материал для дальнейшей работы самих ученых, которые группировались около таких вычислительных центров.

Потом появилась необходимость обмениваться результатами вычислений с другими учеными, находящихся в других городах, потому что вычислительные центры находились при университетах и специальных лабораториях распределенных по всей стране.

Поначалу данные передавались доступными на тот момент способами – надиктовывались по телефону, пересылались с курьерами на появившихся пер-

фолентах и перфокартах, а распечатанные результаты можно было передать по фототелеграфу (предвестник факса).

С переходом на новую элементную базу – с ламп на транзисторы – уменьшились размеры вычислительных машин, они стали дешевле и получили широкое распространение. В одном здании уже могло располагаться несколько вычислительных машин. К ним стали разрабатывать и производить новые периферийные устройства, в том числе и сменные носители: магнитные барабаны, ленты и диски. Когда-то магнитные диски были большими и располагались в виде стопки дисков в круглой коробке, которая вкладывалась в стойку с двигателем и магнитными головками. Первые дискеты (floppy disc – гибкий диск) тоже были немаленькими (8 дюймов), хотя значительно меньше и легче, чем барабаны и жесткие диски. Но все равно эти большие и средние компьютеры были все еще отдельными информационными островками.

Передача данных уже могла осуществляться в пределах шаговой доступности и переноска лент и дисков получила название «snake net» (змеиная сеть), так как люди переносили их «змейкой» по коридорам, а для гибких дисков было еще одно шутливое название – «floppy net» (гибкая сеть или дискетная сеть).

С появлением и глобальным распространением персональных компьютеров необходимость передачи информации между ними стала крайне важна. Кроме потребности в передаче результатов работ на каждом отдельном компьютере, появилась необходимость эффективно использовать дорогостоящее периферийное оборудование, например, принтеры и устройства хранения. Оснащать каждое рабочее место полным комплектом такого оборудования было накладно, так как использовалось оно не все рабочее время.

Кроме удовлетворения насущных потребностей пользователей компьютеров создание компьютерных сетей сулило и новые возможности: совместная работа, дающая синергетический эффект, быстрый обмен результатами, сокращение расходов на дорогую периферию, ускорение работ.

Таким образом, явные потребности и потенциальные возможности привели к созданию компьютерных сетей.

Основные принципы общения

Для обеспечения взаимодействия между вычислительными системами должны быть соблюдения некоторые технические и организационные требования.

На примере общения между двумя людьми покажем основные принципы и компоненты такого взаимодействия (рис.2.1).

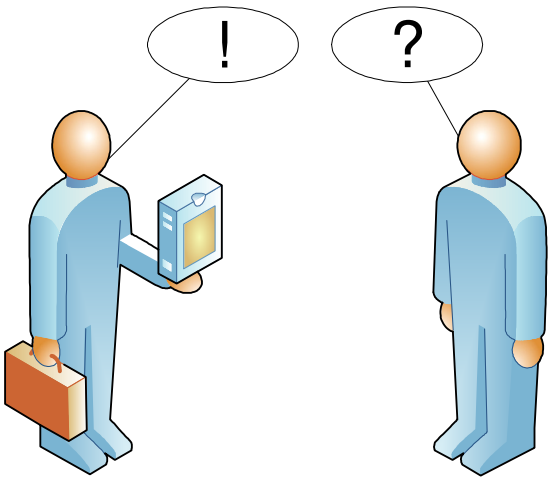

Рис. 2.1. Общение

1. Для начала нужны потенциальные участники общения. Если никого нет, то и общаться некому и не с кем.
2. Желание или необходимость общения.
3. Физическая возможность общения.
4. Люди приветствуют друг друга.
5. Пытаются найти общий язык для общения.
6. Если они понимают друг друга, то происходит обмен информацией.
7. По завершении разговора люди прощаются.

Теперь то же самое, но чуть подробнее и с уклоном в сетевые технологии.

1. Для общения нужно минимум два собеседника, а для обмена данными нужны как минимум два компьютера. Участников общения может быть и больше, а вот если никого рядом нет, то и общаться не с кем.
2. Также необходимо желание как минимум одного участника поделиться информацией, ну или он просто должен это сделать, например, докладывать об обстановке на объекте каждый час.
3. Люди должны иметь физическую возможность передать информацию, например с помощью голоса по воздуху на короткое расстояние, подавая видимые знаки в светлое время на большие расстояния, или тактильными сигналами скрытно или в темноте, а также если они не видят и не слышат. У компьютеров тоже должна быть физическая среда для передачи данных (media). Это может быть металлический кабель и электрические сигналы, оптическое волокно и световые сигналы, радиоволны для беспроводной передачи.
4. По правилам хорошего тона прежде чем начать разговор люди должны поздороваться и представиться друг другу. Для компьютеров такой процесс называется установлением соединения и даже «рукопожатием» (handshaking).
5. Общий язык для общения важен, так как без него люди не будут понимать друг друга. Люди из одной страны обычно сразу понимают собеседника еще во время приветствия. Людям из разных стран, говорящих на разных языках приходится как-то приходить к соглашению, каким общим языком

они владеют для продолжения разговора. Часто этот процесс начинается «на пальцах» (не путать с распальцовкой!) и пробных предложений на разных языках и, в лучшем случае, люди после 1-3 попыток находят общий язык, а в худшем случае им приходится завершать общение. У компьютеров такой процесс называется «согласованием» (negotiation). Еще один хороший вариант перевода слова negotiation, подходящий к этому случаю,- это преодоление затруднений.

6. Если люди поняли друг друга, то собственно после этого и начинается конструктивное общение и обмен сведениями. У компьютеров происходит передача данных.
7. По завершении разговора люди дают знать об этом собеседнику и прощаются с ним. У компьютеров завершается (разрывается) соединение.

Процедура установления и завершения соединения, способ обмена информацией, проверка соединения называется протоколом.

Итак, мы выяснили, что для обмена информацией между компьютерами нужно желание, возможность и правила общения.

Базовые сетевые элементы

Компьютеры выполняют команды, заложенные в них программистами, так что за желание общаться отвечают люди, которые эти компьютеры используют.

Возможность обмена обеспечивается такими сетевыми компонентами как: кабели, разъемы, сетевые платы, коммутаторы, маршрутизаторы, компьютеры, принтеры и пр.

А собственно обмен данными происходит между сетевыми сервисами (службами) и их потребителями, а регулируется он с помощью протоколов.

Базовые сетевые элементы можно разбить на такие категории:

- Сетевые узлы
- Сетевые протоколы
- Сетевые сервисы

Сетевые узлы

Сетевые узлы – это сетевые устройства или вычислительные машины, подключенные к сети. Узлами могут быть компьютеры или другие устройства, например, принтеры, сканеры, дисковые хранилища.

Каждый узел в сети обладает уникальным адресом, так что каждый узел сети отличается от любого другого узла.

Сейчас применяется трехуровневая адресация для идентификации устройств в сети. Эти уровни представлены ниже:

Физический или аппаратный адрес. Этот адрес используется для идентификации получателя сетевых кадров. Такой адрес задается производителем при создании сетевой платы.

Также этот адрес известен как адрес узла или MAC-адрес (от Media Access Control – управление доступом к среде). MAC-адрес является идентификатором, который служит физическим адресом для сетевой платы.

MAC-адрес состоит из 48 бит и обычно представляется в 12 символьном шестнадцатеричном виде, где байты разделены двоеточием или дефисом.

Вот пример такого адреса:

AE:00:5E:16:DF:34

Первые три байта обозначают производителя сетевой платы, а последние три – серийный номер самой платы, например:

00:0D:61:xx:xx:xx – Marvel;

00:02:B3:xx:xx:xx, 00:03:47:xx:xx:xx – Intel.

Полный ежедневно обновляемый список идентификаторов доступен на сайте IEEE (Institute of Electrical and Electronics Engineers) по адресу:

http://standards.ieee.org/develop/regauth/oui/oui.txt[2]

Кроме того сейчас еще применяется 64-bit Extended Unique Identifier (EUI-64 – 64-битный расширенный уникальный идентификатор), который тоже представляется как шестнадцатеричные октеты, разделенные двоеточиями или дефисами, например:

AC:DE:48:FF:FE:23:45:67

Адрес сети (сетевой адрес). Этот адрес служит для идентификации сегмента сети, в котором находятся устройства.

Этот адрес используется для определения сетевого адреса устройств отправляющего и принимающего кадр. Такой адрес служит для направления кадра в тот сегмент сети где находится получающее устройство.

Сетевой адрес анализируется такими устройствами как маршрутизаторы для принятия решения куда направить кадр для устройства-получателя.

Адрес сервиса. Этот адрес служит для идентификации логического порта или сокета, связанного с определенным сетевым сервисом, расположенным на каком-либо сервере.

Логический порт или сокет – это программный компонент, который позволяет удаленной программе, например, вэб-браузеру, связываться с локальной программой, например, вэб-сервером.

Адрес сервиса используется для направления кадров соответствующему поставщику или запросчику того или иного сетевого сервиса на узле. Сетевая операционная система присваивает уникальный адрес каждому сервису.

Среда передачи

Среда передачи – это путь, используемый сетевыми компонентами для передачи данный или доступа к ресурсам.

Среда передачи может быть ограниченной и неограниченной. Технологии с ограничениями применяют кабели (электропроводящие или оптические), а неограниченные технологии используют радиоволны для передачи.

Следующий рисунок 2.2 дает представление о путях прохождения данных в сетях.

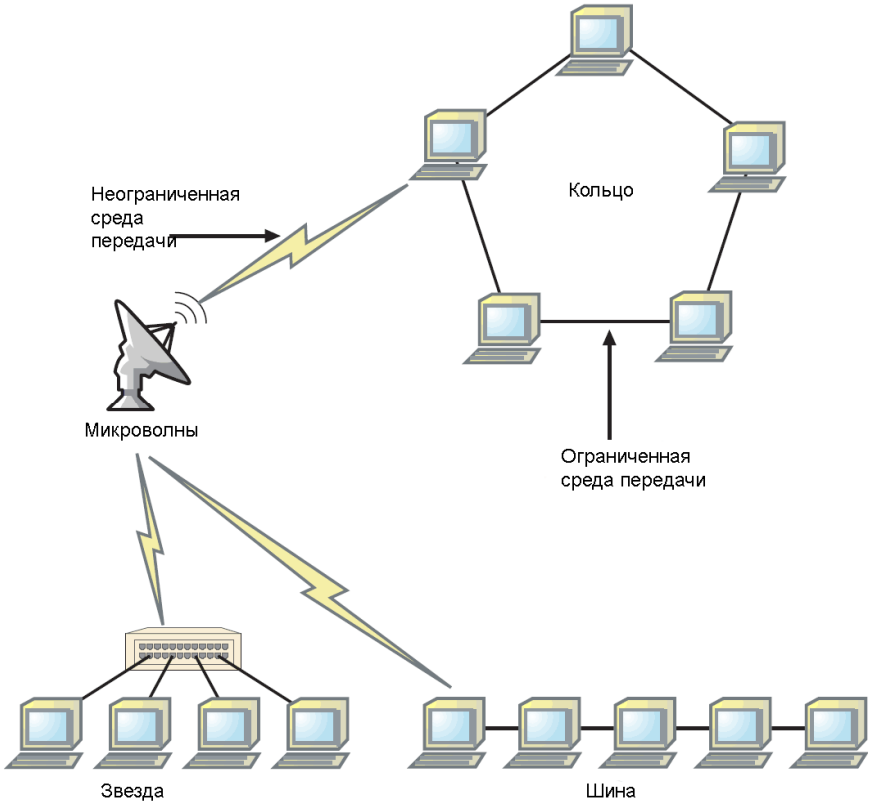

Рис. 2.2. Среда передачи

Наиболее распространенные среды передачи перечислены ниже:

- Кабели из медных проводов (ограниченная)
- Оптоволоконные кабели (ограниченная)
- Радиоволны или микроволны (неограниченная)
- Инфракрасное излучение (неограниченная)

Сетевые протоколы

Сетевые протоколы позволяют сетевым элементам общаться друг с другом.

Сетевой протокол – это набор процедур, правил и соглашений, а также способ передачи сообщений между разными узлами в сети. При использовании одного протокола даже совершенно разные компьютеры или другие сетевые устройства могут общаться друг с другом.

Протоколы имеют разные возможности в зависимости от того, для каких целей их разрабатывали.

Есть два основных типа протоколов:

- **Маршрутизируемые протоколы.** Маршрутизируемые протоколы позволяют сообщениям переходить (или продвигаться) из одной сети в другую и далее, пока не будет достигнута конечная сеть, в которой находится устройство-получатель. В общем, такой пересылкой занимаются сетевые устройства называемые маршрутизаторами.
- **Немаршрутизируемые протоколы.** Немаршрутизируемые протоколы не имеют возможности пересылать сообщения за пределы своего сетевого

сегмента. Они передают сообщения в пределах своей сети от устройства-источника непосредственно устройству-получателю.

В дополнение к классификации протоколов по их способности маршрутизировать пакеты или нет они могут еще подразделяться по методам соединения:

- **С установлением соединения.** Протоколы с установлением соединения сначала устанавливают соединение между узлами, в процессе передачи данных контролируют их успешную доставку до получателя, а потом завершают соединение. Контроль доставки обеспечивается отправкой отправителю подтверждений (квитанций) о получении от него сообщений принимающей стороной. Таким образом отправитель убеждается, что его сообщения были получены. Еще их называют протоколы с квитированием.

  Пояснить суть поможет такой пример. При телефонном разговоре звонящий дожидается пока другой абонент снимет трубку (т.е. его уже могут слушать), потом (на всякий случай) убеждается, что его слушает действительно тот человек, которому он звонил, а не кто-то другой. В процессе разговора абонент периодически повторяет сказанное звонящим – таким образом гарантируется, что сказанное было услышано, а если не расслышал, то переспрашивает. По завершении разговора оба человека прощаются и вешают трубку, тем самым подтверждая, что все данные были переданы и новых данных не будет. Если этого не делать, то один из людей может ждать продолжения разговора до бесконечности.

  Эти протоколы были разработаны для ненадежных соединений с низким качеством сигнала. Современные сети стали лучше, но такие протоколы продолжают широко применяться.

- **Без установления соединения.** Протоколы без установления соединения (без квитирования) пересылают данные по сетям, но не предоставляют подтверждение получения сообщения устройством-получателем. Такие протоколы проще в реализации, у них меньше накладные расходы на передачу и они быстрее, чем с установлением соединения. Такие протоколы могут применяться для рассылки сообщений большому числу получателей одновременно.

  Это объяснит такой пример. Когда человек отправляет SMS-сообщение со своего телефона, он рассчитывает на то, что его короткое сообщение дойдет быстро. Но он не может быть уверен в том, что сообщение получено нужным человеком, что оно получено вовремя или что оно вообще доставлено, например, телефон абонента выключен.

  Такие протоколы предназначены были в первую очередь на доставку не очень критичных сведений с минимальными затратами на транспортировку, а так же на сети с улучшившимся качеством связи, где дополнительный контроль доставки казался излишним.

Сетевые сервисы

Сетевые сервисы – это программы, которые дают возможность пользователям совместно использовать сетевые ресурсы. Сетевые сервисы требуют ресурсов и вычислительных возможностей для выполнения своих задач, например, обрабатывать данные, хранить файлы и т.д.

Некоторые типы сетевых сервисов

Следующие сетевые сервисы часто используются компьютерными программами для выполнения своих задач:

- Сетевая служба каталога (network directory service)
- Сетевые файловые сервисы
- Сервисы сетевой печати
- Сервисы передачи сообщений
- Сервисы сетевых приложений
- Сервисы сетевых баз данных

Сетевая служба каталога (network directory service)

Сетевая служба каталога [3] предоставляет информацию о расположении сетевых ресурсов, таких как файловые серверы, принтеры, приложения и другие сетевые сервисы. Это позволяет пользователям легко находить нужные им сетевые услуги и подключаться к ним, а администраторам – управлять и обеспечивать безопасность доступа к сетевым ресурсам и объектам. **Служба каталога** – это комбинация сервисов, которые обеспечивают обнаружение, безопасность, хранение и управление взаимоотношениями для различных ресурсов и объектов.

Сетевая служба каталога должна выполнять следующие функции:

- Предоставлять доступ к ресурсам по всей сети, а не только на одном сервере;
- Обеспечивать безопасный и защищенный доступ к сетевым ресурсам;
- Предоставлять масштабируемую, индексируемую и кэшируемую базу данных специального назначения для высокой производительности;
- Управлять взаимоотношениями между сущностями в службе каталога, такими как, например, пользователями и необходимыми им ресурсами.

Обычно службы каталога используются для:

- Организации данных;
- Упрощения доступа к сетевой информации;
- Обеспечения безопасности;
- Предоставления услуг потребителям.

Сетевые файловые сервисы

Сетевые файловые сервисы состоят из программ, используемых для хранения, получения или перемещения файлов, содержащих данные или код. Эти сервисы также позволяют проводить резервное копирование важных данных и эффективно использовать устройства хранения.

Сетевые файловые сервисы включают следующее:

- Сохранение, извлечение, перемещение и передача файлов по сети;
- Резервное копирование и восстановление файлов;
- Синхронизация обновлений.

Сервисы сетевой печати

Сервисы сетевой печати используются для управления и контроля доступа к принтерам, факсам, копировальным аппаратам и многофункциональным устройствам.

Сервисы сетевой печати принимают задания на печать от сетевых компьютеров, сохраняют их, переводят в формат определенного типа устройства печати и обеспечивают взаимодействие с принтером по сети.

Функции сервисов сетевой печати включают:

- Обеспечение множественного подключения к ограниченным ресурсам;
- Одновременная обработка нескольких заданий печати;
- Совместное использование специализированных ресурсов печати.

Сервисы передачи сообщений

Сервисы передачи сообщений дают возможность пользователям обмениваться текстами, рисунками, цифровым видео и звуком. Так же они помогают пользователям организовывать и содержат в порядке пользовательскую и служебную информацию.

Сервисы передачи сообщений включают следующие приложения:

- Электронная почта;
- Сетевые предупреждения (network alerts);
- Голосовая почта;
- Приложения для совместной работы.

Сервисы сетевых приложений

Сервисы сетевых приложений позволяют компьютерам предоставлять свои вычислительные возможности в совместное пользование. Вот только пара примеров сервисов сетевых приложений:

- Функции специализированных серверов, например, безопасности или обсчета экспериментальных моделей;
- Расширенные серверные возможности.

Сервисы сетевых баз данных

Сервисы сетевых баз данных позволяют вам сохранять и извлекать данные, хранящиеся в базе данных на сервере. Данные из баз данных могут быть востребованы многими приложениями. Сервисы сетевых баз данных обеспечивают возможность управления и манипулирования данными другими компьютерами по сети. Также они обеспечивают разграничение доступа к данным и безопасность данных.

Такие сервисы делают возможным работу приложений в режиме «клиент-сервер». Эти приложения запрашивают данные с сервера и локально обрабатывают их на клиентском компьютере.

Вот лишь некоторые функции сервисов сетевых баз данных:

- Хранение данных;
- Распределение данных;
- Репликация данных.

Типы сетей

По территориальной протяженности сети могут быть отнесены к следующим типам:

- Near field (NFC) – сеть ближнего поля действия
- Body Area Network (BAN) – носимая или нательная сеть
- Personal Area Network (PAN) – персональная сеть
- Near-me Area Network (NAN) – сеть «около меня»
- Local Area Network (LAN) – локальная вычислительная сеть (ЛВС):
    - Home Area Network (HAN) – домашняя сеть
    - Storage Area Network (SAN) – сеть устройств хранения
- Campus Area Network (CAN) – кампусная сеть
- Backbone – магистральная сеть
- Metropolitan Area Network (MAN) – городская вычислительная сеть
- Wide Area Network (WAN) – глобальная вычислительная сеть (ГВС)
- Internet – Интернет
- Interplanetary Internet – межпланетный Интернет

Рассмотрим некоторые из них.

Local Area Network (LAN)

Local Area Network (LAN) – локальная вычислительная сеть (ЛВС), представленная на рисунке 2.3, наверное, самый распространенный тип сети, который характеризуется небольшой протяженностью (от нескольких метров до нескольких сотен метров), охватывающей компьютеры в одном здании или помещении и связанные с помощью кабелей или беспроводной связью [4].

Общие характеристики локальных сетей:

- Небольшая протяженность
- Высокая скорость передачи данных
- Низкие задержки
- Высокая надежность

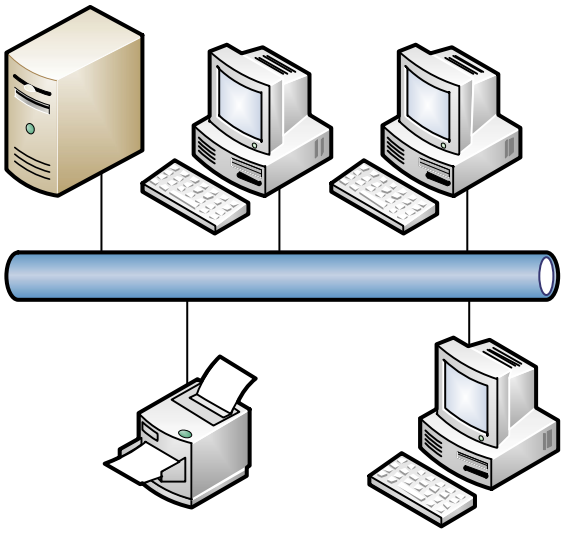

Рис. 2.3. Локальная вычислительная сеть (ЛВС – LAN)

Wide Area Network (WAN)

Wide Area Network (WAN) – глобальная вычислительная сеть (ГВС), представленная на рисунке 2.4, связывает сети на большом расстоянии – до тысяч километров.

Основные характеристики глобальных вычислительных сетей:

- Большая протяженность
- Низкая скорость передачи данных (по сравнению с ЛВС)
- Высокие задержки
- Низкая надежность соединения

В последние годы границы между локальными и глобальными сетями стали размытыми, так как новые среды передачи данных (одномодовое оптоволокно) могут растягивать локальную сеть до ста километров, а в глобальных сетях выросли скорости и надежность соединения. Технологии, которые раньше применялись в глобальных сетях, сейчас повсеместно встречаются и в локальных сетях.

Глобальные сети могут принадлежать одной компании, тогда они называются *корпоративными*, или же иметь общедоступное подключение и объединять сети разных компаний друг с другом, такой вариант получил собственное название – *Интернет*.

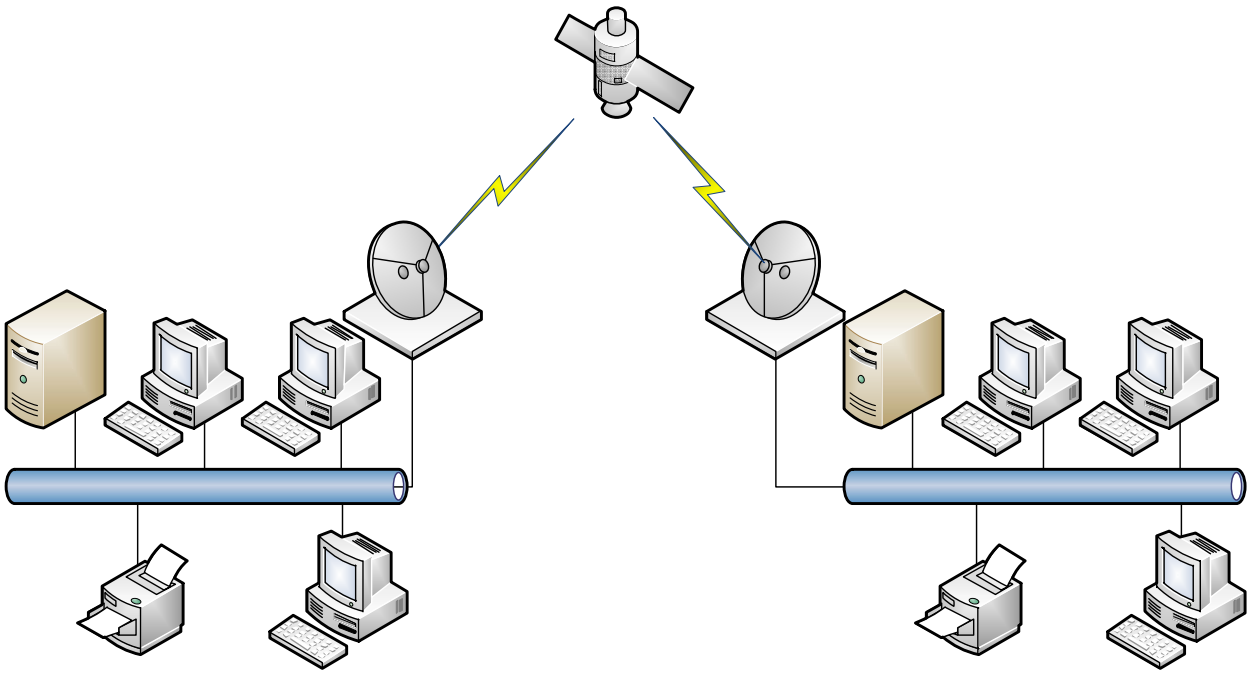

Рис. 2.4. Глобальная вычислительная сеть (ГВС – WAN)

Типы вычислительных моделей

По месту проведения вычислений можно выделить несколько типов:

- Централизованные вычисления
- Распределенные вычисления:
    - Одноранговые сети
    - Сети с выделенным сервером
- Совместные вычисления

Централизованные вычисления

Централизованные вычисления (рис. 2.5) – это самая старая модель компьютерных вычислений, так как большие вычислительные машины, еще не будучи связанными сетями, обслуживали большое количество соединений от простых терминалов (сначала электрическая пишущая машинка, а потом экран и клавиатура), тогда как хранение, организация и обработка данных проводилась на самом большом компьютере.

Терминалы практически не имели вычислительных возможностей за что их называли «тупыми» (dumb) терминалами. Терминалы подключались к большой вычислительной машине с помощью кабелей.

В современном мире такой подход опять нашел применения в терминальных сессиях, когда персональные компьютеры подключаются к одному из более мощных серверов, на котором работают программы, и используются только как устройства ввода/вывода, а вычисления проводятся на сервере.

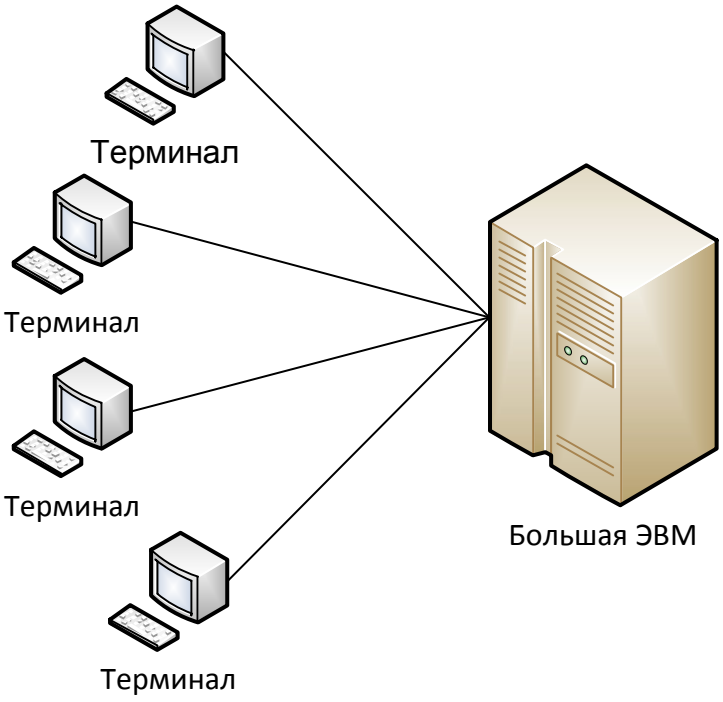

Рис. 2.5. Централизованные вычисления

Распределенные вычисления

При распределенных вычислениях в сети присутствуют компьютеры с разными вычислительными способностями.

В этой модели приложение разбивается на задачи, а каждая задача запускается на выполнение на наиболее подходящем для этого компьютере. После того как задачи выполнены их результаты отсылаются на компьютер, который запрашивал данные.

Примером таких вычислений сейчас могут служить многоуровневые вэб-приложения с вэб-сервером, уровнем бизнес-логики и, например, базой данных, а результаты будут отображаться в браузере на рабочей станции.

Клиенты и серверы

При распределенных вычислениях компьютеры могут выступать в разных ролях – как потребители вычислительных услуг и как их поставщики. Если компьютер запрашивает услуги в сети, то он является *клиентом*. Если же наоборот, поставляет услуги или данные в сеть, то *сервером*. Сетевые серверы могут выполнять множество разнообразных задач разного уровня сложности.

Одноранговые сети

Когда сеть небольшая и все компьютеры периодически выступают и как клиенты и как серверы для других компьютеров, то такая сеть является одноранговой, то есть с равноправными участниками сетевого взаимодействия. Администратор, отвечающий за сопровождение сети, обычно не требуется. Безопасность обеспечивается с использованием локальной базы данных каталога, имеющейся на каждом компьютере. Пользователь каждого компьютера сам определяет, какие данные с этого компьютера могут быть предоставлены для совместного использования в сети.

Одноранговые сети (рис. 2.6) также называются рабочими группами. Под термином «рабочая группа» понимается небольшое объединение сотрудников (обычно не более десяти), работающих вместе. Одноранговые сети удобно развертывать при следующих условиях:

- число пользователей не превышает десяти;
- пользователи имеют общий доступ к ресурсам и принтерам, но специализированных серверов не существует;
- проблема безопасности отсутствует;
- организацию и сеть не предполагается существенно расширять в обозримом будущем.

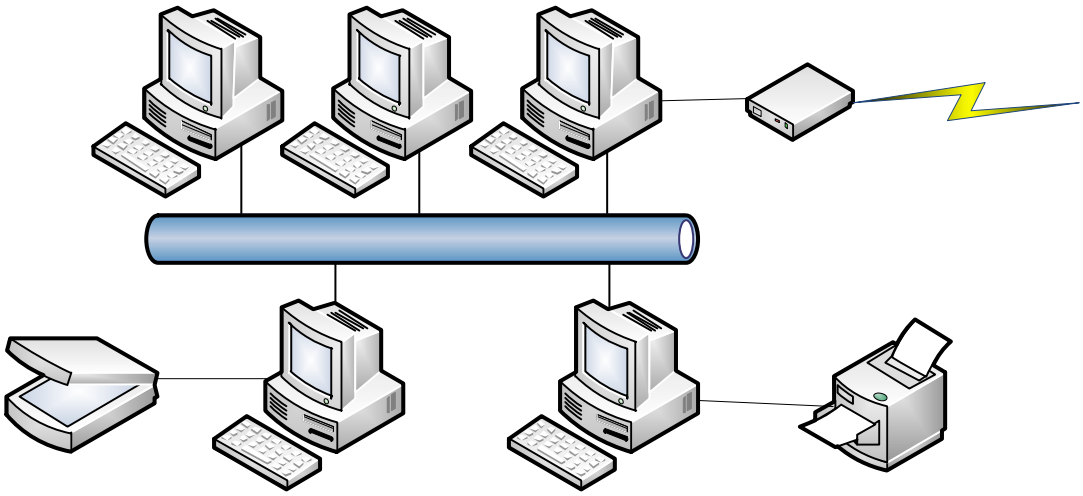

Рис. 2.6. Одноранговая сеть

Сети с выделенным сервером

При повышенных потребностях в совместных ресурсах в сети создаются выделенные серверы. Выделенный сервер функционирует как сервер, предоставляя свои услуги в сеть. Конфигурация таких серверов оптимизируется для обработки запросов от клиентов сети.

Сети типа «клиент-сервер» (рис. 2.7) стали стандартной моделью, применяемой при организации сетей. По мере того, как сеть расширяется вследствие

увеличения числа подключенных компьютеров, расстояний между ними и объемов передаваемого трафика, возникает необходимость в дополнительных серверах. Распределение задач сетевой обработки среди нескольких серверов гарантирует максимально эффективное выполнение каждой задачи. Кроме того, если задачи сетевой обработки передаются серверам, снижается нагрузка на рабочие станции. В крупных сетях распространены специализированные серверы, что позволяет качественнее удовлетворять растущие потребности пользователей.

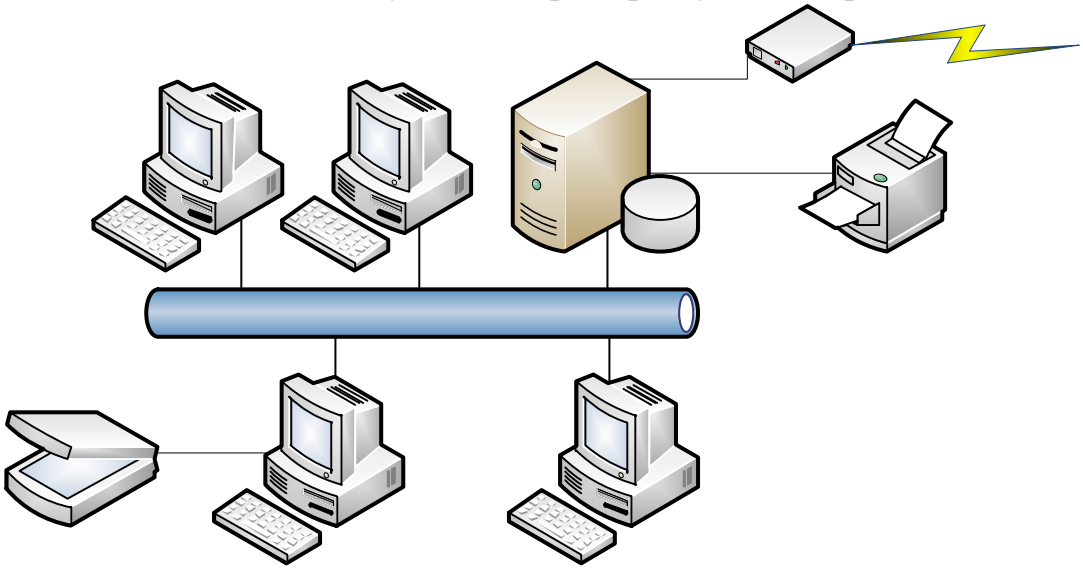

Рис. 2.7. Сеть с выделенным сервером

Совместные вычисления

Совместные вычисления (рис. 2.8) схожи с распределенными вычислениями. В обеих моделях приложение разбивается на отдельные задачи, которые выполняются различными компьютерами.

В модели совместных вычислений эти задачи имеют большую дискретность и более универсальные, т.е. для их выполнения подходит большинство компьютеров в сети. Если один из компьютеров закончил выполнять свои задачи он может взять на обработку часть оставшихся задач у другого компьютера в сети. Таким образом общая работа будет выполнена быстрее, а все не будут ожидать пока свою задачу завершит самое медленное устройство.

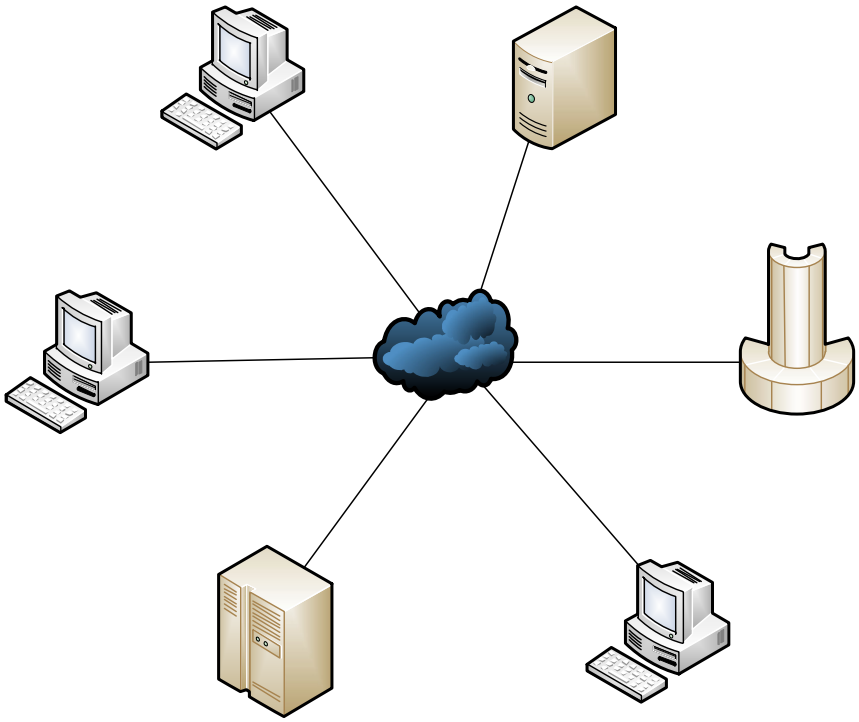

Рис. 2.8. Совместные вычисления

Контрольные вопросы ко 2-й главе.

1. Что является определением сетевого сервиса:
    a. Программа, которая позволяет совместно использовать сетевые ресурсы.
    b. Путь, по которому сетевые устройства могут обмениваться данными.
    c. Правила, по которым общаются различные сетевые устройства.
2. Что является определением средой передачи данных:
    a. Программа, которая позволяет совместно использовать сетевые ресурсы.
    b. Путь, по которому сетевые устройства могут обмениваться данными.
    c. Правила, по которым общаются различные сетевые устройства.
3. Что является определением протокола:
    a. Программа, которая позволяет совместно использовать сетевые ресурсы.
    b. Путь, по которому сетевые устройства могут обмениваться данными.
    c. Правила, по которым общаются различные сетевые устройства.
4. Какие типы сетей определяются по территориальному признаку:
    a. LAN
    b. NAL
    c. WAN
    d. ICANN

3. Сетевые стандарты

Для обмена данными между узлами необходима согласованная модель взаимодействия. Эта модель должна учитывать аппаратное и программное обеспечение и способы передачи данных. В этой главе рассматривается значение этой модели, дается ее описание и представляются некоторые из стандартов, на которые опираются современные сетевые технологии.

Основные темы этой главы:

- Описание эталонной модели Международной организации по стандартизации взаимодействия открытых систем (МОС/ВОС – ISO/OSI)
- Стандарты Института инженеров электротехники и электроники серии 802.x (IEEE 802.x)
- Выбор подходящего стандарта для проектирования сети

Введение

Сетевые стандарты – это набор правил, которые необходимо соблюдать для успешного взаимодействия между устройствами в сети.

На начальных этапах становления сетей многие производители создавали свои собственные устройства и программы, которые могли работать друг с другом, но не с сетевыми устройствами других поставщиков. Потребители страдали от такой несовместимости и это послужило поводом для разработки и создания стандартов, при соблюдении которых, устройства и программы разных поставщиков могли бы работать вместе.

Наиболее распространенные стандарты зиждутся на эталонной модели Международной организации по стандартизации взаимодействия открытых систем (МОС/ВОС – International Standard Organization / Open Systems Interconnection (ISO/OSI)). Стандарты Института инженеров электротехники и электроники (Institute of Electrical and Electronics Engineers – IEEE) основываются на модели МОС/ВОС.

Понимание этой модели и знание стандартов поможет в понимании процессов коммуникаций в сетях.

Описание эталонной модели Международной организации по стандартизации взаимодействия открытых систем

Эталонной модель Международной организации по стандартизации взаимодействия открытых систем (International Standard Organization / Open Systems Interconnection) коротко МОС/ВОС или ISO/OSI служит костяком для разработки и применения стандартов сетевого взаимодействия [3].

Эта модель состоит из семи уровней, каждый их которых определяет, как сетевые задачи разбиваются на логические группы.

Таблица 3.1. Семь уровней модели МОС/ВОС

Уровень (layer)	**Название**	**Функции**	**Порция данных**
7	Прикладной Application	Доступ к сетевым службам	Данные
6	Представительский Presentation	Преобразование и шифрование данных	Данные
5	Сеансовый Session	Управление сеансом связи	Данные
4	Транспортный Transport	Прямая связь между двумя конечными устройствами и обеспечение надежной передачи	Сегмент

3	Сетевой Network	Определение маршрута и логическая адресация	Пакет
2	Канальный Data link	Физическая адресация, проверка надежности физического соединения	Кадр
1	Физический Physical	Работа со средой передачи, сигналами и двоичными данными	Бит

В литературе наиболее часто принято начинать описание уровней модели OSI с 7-го уровня, называемого прикладным, на котором пользовательские приложения обращаются к сети. Модель OSI заканчивается 1-м уровнем — физическим, на котором определены стандарты, предъявляемые независимыми производителями к средам передачи данных:

- тип передающей среды (медный кабель, оптоволокно, радиоэфир и др.),
- тип модуляции сигнала,
- сигнальные уровни логических дискретных состояний (нуля и единицы).

Любой протокол модели OSI должен взаимодействовать либо с протоколами своего уровня, либо с протоколами на единицу выше и/или ниже своего уровня. Взаимодействия с протоколами своего уровня называются горизонтальными, а с уровнями на единицу выше или ниже — вертикальными. Любой протокол модели OSI может выполнять только функции своего уровня и не может выполнять функций другого уровня, что не выполняется в протоколах альтернативных моделей.

Каждому уровню с некоторой долей условности соответствует свой операнд — логически неделимый элемент данных, которым на отдельном уровне можно оперировать в рамках модели и используемых протоколов: на физическом уровне мельчайшая единица — бит, на канальном уровне информация объединена в кадры, на сетевом — в пакеты (датаграммы), на транспортном — в сегменты. Любой фрагмент данных, логически объединённых для передачи — кадр, пакет, датаграмма — считается сообщением. Именно сообщения в общем виде являются операндами сеансового, представительского и прикладного уровней.

К базовым сетевым технологиям относятся физический и канальный уровни.

Для запоминания названий 7-и уровней модели OSI на английском языке рекомендуют использовать фразу "All people seem to need data processing", в которой первые буквы слов соответствуют первым буквам названий уровней. Для запоминания уровней на русском языке существует фраза: "Просто представь себе тачку, стремящуюся к финишу", первые буквы слов в которой так же соответствуют первым буквам названий уровней.

Прикладной уровень

Прикладной уровень (уровень приложений; англ. application layer) — верхний уровень модели, обеспечивающий взаимодействие пользовательских приложений с сетью:

- позволяет приложениям использовать сетевые службы:

  - удалённый доступ к файлам и базам данных,
  - пересылка электронной почты;
- отвечает за передачу служебной информации;
- предоставляет приложениям информацию об ошибках;
- формирует запросы к уровню представления.

Протоколы прикладного уровня: RDP, HTTP, SMTP, SNMP, POP3, FTP, XMPP, OSCAR, Modbus, SIP, TELNET, AFP — Apple Filing Protocol, NCP — NetWare Core Protocol, SMB – Server Message Block.

Представительский уровень

Представительный уровень (уровень представления; англ. presentation layer) обеспечивает преобразование протоколов и кодирование/декодирование данных. Запросы приложений, полученные с прикладного уровня, на уровне представления преобразуются в формат для передачи по сети, а полученные из сети данные преобразуются в формат приложений. На этом уровне может осуществляться сжатие/распаковка или кодирование/декодирование данных, а также перенаправление запросов другому сетевому ресурсу, если они не могут быть обработаны локально.

Уровень представлений обычно представляет собой промежуточный протокол для преобразования информации из соседних уровней. Это позволяет осуществлять обмен между приложениями на разнородных компьютерных системах прозрачным для приложений образом. Уровень представлений обеспечивает форматирование и преобразование кода. Форматирование кода используется для того, чтобы гарантировать приложению поступление информации для обработки, которая имела бы для него смысл. При необходимости этот уровень может выполнять перевод из одного формата данных в другой.

Уровень представлений имеет дело не только с форматами и представлением данных, он также занимается структурами данных, которые используются программами. Таким образом, уровень 6 обеспечивает организацию данных при их пересылке.

Чтобы понять, как это работает, представим, что имеются две системы. Одна использует для представления данных расширенный двоичный код обмена информацией EBCDIC, например, это может быть мейнфрейм компании IBM, а другая — американский стандартный код обмена информацией ASCII (его используют большинство других производителей компьютеров). Если этим двум системам необходимо обменяться информацией, то нужен уровень представлений, который выполнит преобразование и осуществит перевод между двумя различными форматами.

Другой функцией, выполняемой на уровне представлений, является шифрование данных, которое применяется в тех случаях, когда необходимо защитить передаваемую информацию от приема несанкционированными получателями. Чтобы решить эту задачу, процессы и коды, находящиеся на уровне представлений, должны выполнить преобразование данных. На этом уровне существуют и другие подпрограммы, которые сжимают тексты и преобразовывают графические изображения в битовые потоки, так что они могут передаваться по сети.

Протоколы уровня представления: ICA — Independent Computing Architecture, LPP — Lightweight Presentation Protocol, NDR — Network Data Representation, XDR — eXternal Data Representation, X.25 PAD — Packet Assembler/Disassembler Protocol.

Сеансовый уровень

Сеансовый уровень (англ. session layer) модели обеспечивает поддержание сеанса связи, позволяя приложениям взаимодействовать между собой длительное время. Уровень управляет созданием/завершением сеанса, обменом информацией, синхронизацией задач, определением права на передачу данных и поддержанием сеанса в периоды неактивности приложений.

Протоколы сеансового уровня: ADSP (AppleTalk Data Stream Protocol), ASP (AppleTalk Session Protocol), H.245 (Call Control Protocol for Multimedia Communication), ISO-SP (OSI Session Layer Protocol (X.225, ISO 8327)), iSNS (Internet Storage Name Service), L2F (Layer 2 Forwarding Protocol), L2TP (Layer 2 Tunneling Protocol), NetBIOS (Network Basic Input Output System), PAP (Password Authentication Protocol), PPTP (Point-to-Point Tunneling Protocol), RPC (Remote Procedure Call Protocol), RTCP (Real-time Transport Control Protocol), SMPP (Short Message Peer-to-Peer), SCP (Secure Copy Protocol), ZIP (Zone Information Protocol), SDP (Sockets Direct Protocol)..

Транспортный уровень

Транспортный уровень (англ. transport layer) модели предназначен для обеспечения надёжной передачи данных от отправителя к получателю. При этом уровень надёжности может варьироваться в широких пределах. Существует множество классов протоколов транспортного уровня, начиная от протоколов, предоставляющих только основные транспортные функции (например, функции передачи данных без подтверждения приема), и заканчивая протоколами, которые гарантируют доставку в пункт назначения нескольких пакетов данных в надлежащей последовательности, мультиплексируют несколько потоков данных, обеспечивают механизм управления потоками данных и гарантируют достоверность принятых данных. Например, UDP ограничивается контролем целостности данных в рамках одной датаграммы, и не исключает возможности потери пакета целиком, или дублирования пакетов, нарушение порядка получения пакетов данных; TCP обеспечивает надёжную непрерывную передачу данных, исключающую потерю данных или нарушение порядка их поступления или дублирования, может перераспределять данные, разбивая большие порции данных на фрагменты и наоборот склеивая фрагменты в один пакет.

Протоколы транспортного уровня: ATP (AppleTalk Transaction Protocol), CUDP (Cyclic UDP), DCCP (Datagram Congestion Control Protocol), FCP (Fiber Channel Protocol), IL (IL Protocol), NBF (NetBIOS Frames protocol), NCP (NetWare Core Protocol), SCTP (Stream Control Transmission Protocol), SPX (Sequenced Packet Exchange), SST (Structured Stream Transport), TCP (Transmission Control Protocol), UDP (User Datagram Protocol).

Сетевой уровень

Сетевой уровень (англ. network layer) модели предназначен для определения пути передачи данных. Отвечает за трансляцию логических адресов и имён в физические, определение кратчайших маршрутов, коммутацию и маршрутизацию, отслеживание неполадок и «заторов» в сети.

Протоколы сетевого уровня маршрутизируют данные от источника к получателю. Работающие на этом уровне устройства (маршрутизаторы) условно называют устройствами третьего уровня (по номеру уровня в модели OSI).

Протоколы сетевого уровня: IP/IPv4/IPv6 (Internet Protocol), IPX (Internetwork Packet Exchange, протокол межсетевого обмена), X.25 (частично этот протокол реализован на уровне 2), CLNP (сетевой протокол без организации соединений), IPsec (Internet Protocol Security), ICMP (Internet Control Message Protocol), IGMP (Internet Group Management Protocol), RIP (Routing Information Protocol), OSPF (Open Shortest Path First).

Канальный уровень

Канальный уровень (англ. data link layer) предназначен для обеспечения взаимодействия сетей на физическом уровне и контроля за ошибками, которые могут возникнуть. Полученные с физического уровня данные он упаковывает в кадры, проверяет на целостность, если нужно, исправляет ошибки (формирует повторный запрос поврежденного кадра) и отправляет на сетевой уровень. Канальный уровень может взаимодействовать с одним или несколькими физическими уровнями, контролируя и управляя этим взаимодействием.

Спецификация IEEE 802 разделяет этот уровень на два подуровня: MAC (англ. media access control) регулирует доступ к разделяемой физической среде, LLC (англ. logical link control) обеспечивает обслуживание сетевого уровня.

На этом уровне работают коммутаторы, мосты и другие устройства. Говорят, что эти устройства используют адресацию второго уровня (по номеру уровня в модели OSI).

Протоколы канального уровня: ARCnet, ATM, Cisco Discovery Protocol (CDP), Controller Area Network (CAN), Econet, Ethernet, Ethernet Automatic Protection Switching (EAPS), Fiber Distributed Data Interface (FDDI), Frame Relay, High-Level Data Link Control (HDLC), IEEE 802.2 (provides LLC functions to IEEE 802 MAC layers), Link Access Procedures, D channel (LAPD), IEEE 802.11 wireless LAN, LocalTalk, Multiprotocol Label Switching (MPLS), Point-to-Point Protocol (PPP), Point-to-Point Protocol over Ethernet (PPPoE), Serial Line Internet Protocol (SLIP, obsolete), StarLan, Spanning tree protocol, Token ring, Unidirectional Link Detection (UDLD), x.25.

В программировании этот уровень представляет драйвер сетевой платы, в операционных системах имеется программный интерфейс взаимодействия канального и сетевого уровней между собой. Это не новый уровень, а просто реализация модели для конкретной ОС. Примеры таких интерфейсов: ODI, NDIS, UDI.

Физический уровень

Физический уровень (англ. physical layer) — нижний уровень модели, предназначенный непосредственно для передачи потока данных. Осуществляет передачу электрических или оптических сигналов в кабель или в радиоэфир и, соответственно, их приём и преобразование в биты данных в соответствии с методами кодирования цифровых сигналов. Другими словами, осуществляет интерфейс между сетевым носителем и сетевым устройством.

На этом уровне также работают концентраторы, повторители сигнала и медиаконвертеры.

Функции физического уровня реализуются на всех устройствах, подключенных к сети. Со стороны компьютера функции физического уровня выполняются сетевым адаптером или последовательным портом. К физическому уровню относятся физические, электрические и механические интерфейсы между двумя системами. Физический уровень определяет такие виды сред передачи данных как оптоволокно, витая пара, коаксиальный кабель, спутниковый канал передач данных и т. п. Стандартными типами сетевых интерфейсов, относящимися к физическому уровню, являются: V.35, RS-232, RS-485, RJ-11, RJ-45, разъемы AUI и BNC.

Протоколы физического уровня: IEEE 802.15 (Bluetooth), IRDA, EIA RS-232, EIA-422, EIA-423, RS-449, RS-485, DSL, ISDN, SONET/SDH, 802.11 Wi-Fi, Etherloop, GSM Um radio interface, ITU и ITU-T, TransferJet, ARINC 818, G.hn/G.9960.

Коммуникационный процесс в модели МОС/ВОС

Процесс связи между двумя узлами в модели МОС/ВОС начинается с инкапсуляции (вкладывания) данных в своеобразный конверт на каждом уровне (рис. 3.1). *Инкапсуляция* – это процесс добавления служебных сведений каждого уровня для передачи порции данных на нижележащий уровень.

При обработке принятых данных они перемещаются с нижних уровней вверх, при этом служебные сведения нижнего уровня изымаются перед передачей данных вышележащему уровню. Процесс изъятия служебных данных называется *деинкапсуляцией*.

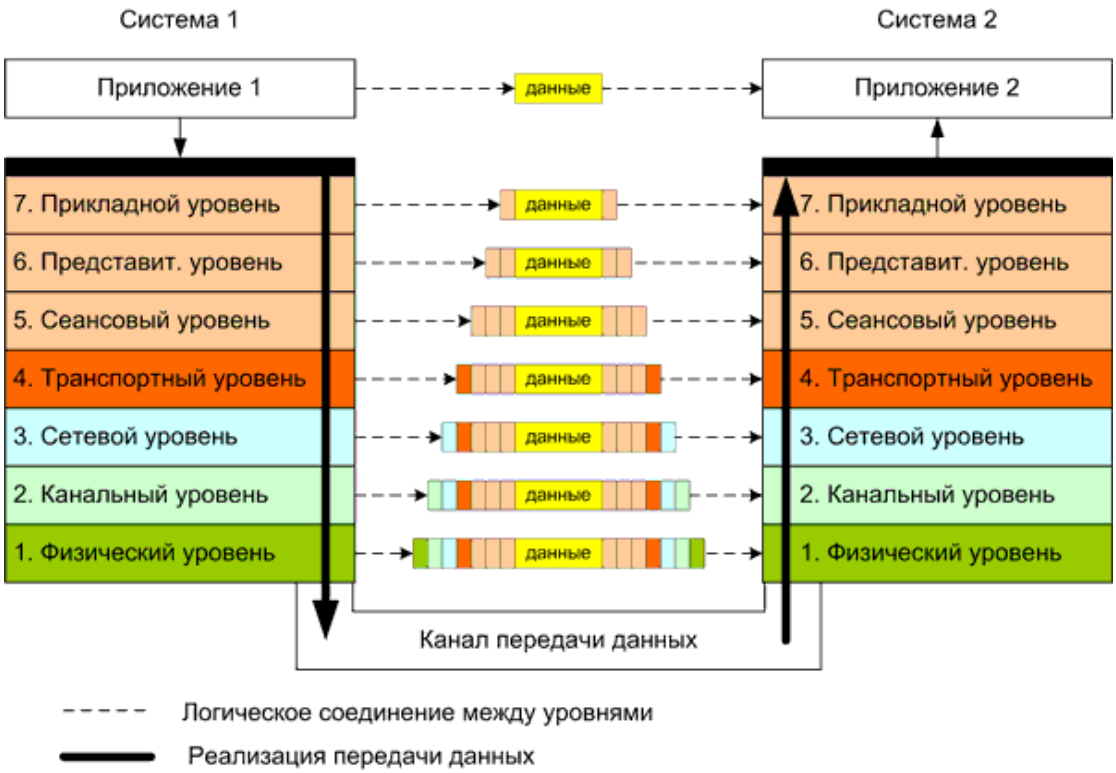

Рис. 3.1. Коммуникационный процесс в модели МОС/ВОС

Взаимодействие между одинаковыми уровнями на разных системах регламентируется *протоколом*, а взаимодействие между разными уровнями в пределах одной системы называется *интерфейсом*.

Стандарты IEEE 802.x

Стандарты Института инженеров электротехники и электроники серии 802.x (IEEE 802.x) [2] были созданы для того, чтобы разные производители сетевого оборудования могли, в соответствии с ними, разрабатывать устройства совместимые друг с другом.

Стандарты IEEE 802.x сопоставляются с моделью МОС/ВОС следующим образом (рис. 3.2):

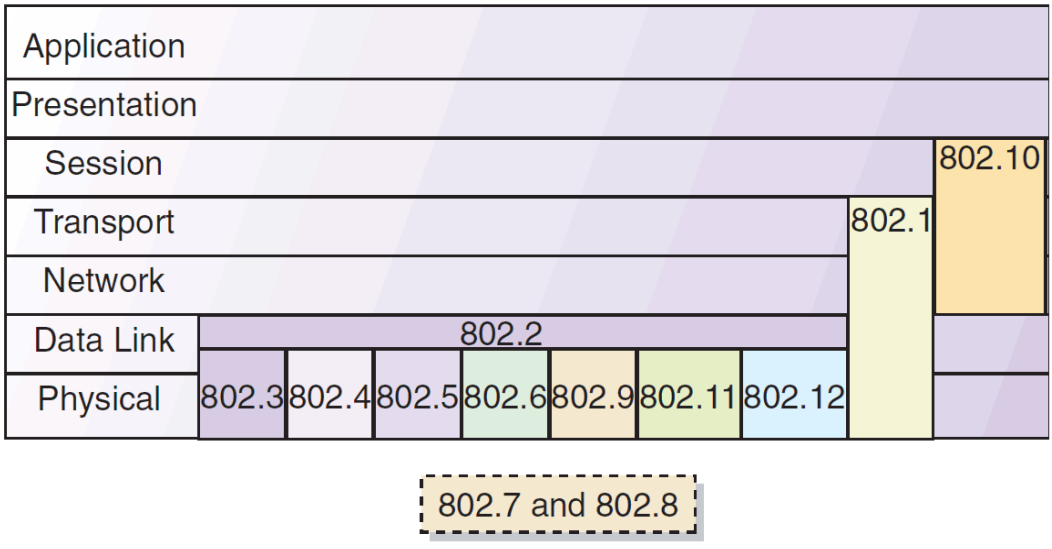

Рис. 3.2. Модель МОС/ВОС и стандарты IEEE 802.x

В следующих таблицах приведен список стандартов IEEE 802.x.

Таблица 3.2. Действующие группы разработки и изучения стандартов IEEE 802.x.

№ группы	Описание
802.1	Higher Layer LAN Protocols Working Group
802.3	Ethernet Working Group
802.11	Wireless LAN Working Group
802.15	Wireless Personal Area Network (WPAN) Working Group
802.16	Broadband Wireless Access Working Group
802.18	Radio Regulatory TAG
802.19	Wireless Coexistence Working Group
802.21	Media Independent Handover Services Working Group
802.22	Wireless Regional Area Networks
802.24	Smart Grid TAG

Таблица 3.3. Приостановленные и расформированные группы IEEE 802.x.

№ группы	Описание
802.2	Logical Link Control Working Group
802.4	Token Bus Working Group
802.5	Token Ring Working Group
802.6	Metropolitan Area Network Working Group
802.7	Broadband TAG
802.8	Fiber Optic TAG
802.9	Integrated Services LAN Working Group
802.10	Security Working Group
802.12	Demand Priority Working Group
802.14	Cable Modem Working Group
802.17	Resilient Packet Ring Working Group
802.20	Mobile Broadband Wireless Access (MBWA) Working Group
802.23	Emergency Services Working Group

Методы доступа к среде передачи

В свое время получили распространение три метода управления доступом к среде передачи данных:

- Carrier Sense Multiple Access With Collision Avoidance (CSMA/CA)
- Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
- Token Passing

Carrier Sense Multiple Access With Collision Avoidance (CSMA/CA)

Carrier Sense Multiple Access With Collision Avoidance (CSMA/CA) – множественный доступ с прослушиванием несущей и избежанием коллизий – это метод, который применяли для избежания коллизий при взаимодействии устройств в сети.

Перед тем как послать пакет с информацией, исходное устройство посылало широковещательный сигнал для прослушивания сетевого трафика и предупреждения других устройств о возможном начале передачи данных. Другие станции должны были при этом воздержаться от передачи данных. Этот метод доступа оказался существенно медленнее, чем CSMA/CD, потому что требовалось дополнительное время на предупреждающее широковещательное послание.

Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

Carrier Sense Multiple Access with Collision Detection (CSMA/CD) – множественный доступ с прослушиванием несущей и обнаружением коллизий – этот метод допускал коллизии, но позволял быстро их обнаружить и повторно послать данные при свободной среде передачи.

Станция, прежде чем начать передачу данных прослушивала канал и, если в этот момент он был свободен, начинала свою передачу. В большинстве случаев передача происходила без помех со стороны других узлов в сети.

Проблема возникала, если два устройства практически одновременно начинали свои передачи. В этом случае возникала коллизия (столкновение) и данные не могли быть распознаны. Поскольку все устройства при этом прослушивают среду, то передающие станции обнаруживали проблему и прекращали передачу. После этого они выжидали случайный промежуток времени и пытались возобновить передачу своих данных. Если коллизия повторялась, то время ожидания увеличивалось. Алгоритм выжидания увеличивал шансы на успешную передачу.

Такой метод хорошо работал в мало- и средненагруженных сетях, но становился малоэффективным при больших нагрузках.

Token Passing

Token Passing – передача маркера – метод доступа, при котором право передачи данных четко регламентируется и передавать данные имеет право только то устройство, которое владеет маркером. После передачи данных станция должна вернуть маркер и передать его следующему устройству. Если у нее есть данные для передачи, то она может начать свою пересылку, если нет, то передавала маркер следующему устройству.

Таким образом не допускались коллизии, но требовались большие усилия для управления маркером, например, специальные центральные устройства. Такой варрант был дороже в исполнении, но очень хорошо проявлял себя в высоконагруженных сетях, так как общая производительность сети мало деградировала.

Выбор подходящего стандарта для проектирования сети

Сейчас широко используются несколько стандартов IEEE 802.x:

- Типы передачи сигнала
- IEEE 802.3 – Ethernet
- IEEE 802.11x – беспроводные соединения

Типы передачи сигнала

По типу передачи сигнала в среде современные сетевые технологии делятся на:

- Занимающие всю полосу пропускания (без модуляции каналов, монополосная – baseband)
- Широкополосная

Монополосная

Монополосные передачи широко используются в современных сетях, благодаря их относительно простой реализации.

При этом вся среда передачи используется как один единственный канал, который занимает всю доступную физическую полосу пропускания. Сигнал принимает только три состояния: ноль, один и «не используется». Таким образом, трансиверы должны распознать все три состояния одного сигнала.

Широкополосная

Широкополосная передача более сложная. В этом случае в одной физической среде создаются несколько каналов, обычно на разных несущих частотах. Процесс создания множества каналов называется частотным мультиплексированием или частотным уплотнением.

Широкополосные трансиверы должны распознавать три состояния сигнала по всем каналам.

По такой технологии работают кабельные и ADSL-модемы.

IEEE 802.3 – Ethernet

Ethernet (от англ. ether «эфир») — пакетная технология передачи данных преимущественно локальных компьютерных сетей.

Стандарты Ethernet определяют проводные соединения и электрические сигналы на физическом уровне, формат кадров и протоколы управления доступом к среде — на канальном уровне модели OSI. Ethernet в основном описывается стандартами IEEE группы 802.3. Ethernet стал самой распространённой технологией ЛВС в середине 1990-х годов, вытеснив такие устаревшие технологии, как Arcnet, FDDI и Token ring.

Технология Ethernet была разработана вместе со многими первыми проектами корпорации Xerox PARC. Общепринято считать, что Ethernet был изобретён 22 мая 1973 года, когда Роберт Меткалф (Robert Metcalfe) составил докладную записку для главы PARC о потенциале технологии Ethernet. Но законное право на технологию Меткалф получил через несколько лет. В 1976 году он и его ассистент Дэвид Боггс (David Boggs) издали брошюру под названием «Ethernet: Distributed Packet-Switching For Local Computer Networks».

Меткалф ушёл из Xerox в 1979 году и основал компанию 3Com для продвижения компьютеров и локальных вычислительных сетей (ЛВС). Ему удалось убедить DEC, Intel и Xerox работать совместно и разработать стандарт Ethernet (DIX). Впервые этот стандарт был опубликован 30 сентября 1980 года.

Комитет IEEE 802.3 установил несколько стандартов, относящихся кабельному стандарту Ethernet:

- Для коаксиального кабеля
  - 10BASE-2, 10BASE-5

- Для витой пары:
  - 10BASE-T, 100BASE-TX, 1000BASE-T
- Для оптоволокна:
  - 10BASE-FL, 100BASE-FX, 1000BASE-SX, 1000BASE-LX, 10GBASE-SR, 10GBASE-LR, 10GBASE-ER

Также приняты в качестве стандарта 802.3ba 40Gb/s и 100Gb/s Ethernet. Работа на этих скоростях предполагает использование оптоволокна.

Стандарты 802.11

При описании стандарта, в скобках указан год его принятия.

- 802.11 — Изначальный 1 Мбит/с и 2 Мбит/с, 2,4 ГГц и ИК стандарт (1997)
- 802.11a — 54 Мбит/с, 5 ГГц стандарт (1999, выход продуктов в 2001)
- 802.11b — Улучшения к 802.11 для поддержки 5,5 и 11 Мбит/с (1999)
- 802.11c — Процедуры операций с мостами; включен в стандарт IEEE 802.1D (2001)
- 802.11d — Интернациональные роуминговые расширения (2001)
- 802.11e — Улучшения: QoS, включение packet bursting (2005)
- 802.11F — Inter-Access Point Protocol (2003)
- 802.11g — 54 Мбит/с, 2,4 ГГц стандарт (обратная совместимость с b) (2003)
- 802.11h — Распределенный по спектру 802.11a (5 GHz) для совместимости в Европе (2004)
- 802.11i — Улучшенная безопасность (2004)
- 802.11j — Расширения для Японии (2004)
- 802.11k — Улучшения измерения радио ресурсов
- 802.11l — Зарезервирован
- 802.11m — Поддержание эталона; обрезки
- 802.11n — Увеличение скорости передачи данных (600 Мбит/с). 2,4-2,5 или 5 ГГц. Обратная совместимость с 802.11a/b/g.
- 802.11o — Зарезервирован
- 802.11p — WAVE — Wireless Access for the Vehicular Environment (Беспроводной Доступ для Транспортной Среды, такой как машины скорой помощи или пассажирский транспорт)
- 802.11q — Зарезервирован, иногда его путают с 802.1Q
- 802.11r — Быстрый роуминг
- 802.11s — ESS Mesh Networking (Extended Service Set — Расширенный Набор Служб; Mesh Network — Ячеистая Сеть)
- 802.11T — Wireless Performance Prediction (WPP, Предсказание Производительности Беспроводного Оборудования) — методы тестов и измерений
- 802.11u — Взаимодействие с не-802 сетями (например, сотовые сети)
- 802.11v — Управление беспроводными сетями
- 802.11x — Зарезервирован и не будет использоваться. Не нужно путать со стандартом контроля доступа IEEE 802.1X

- 802.11y — Дополнительный стандарт связи, работающий на частотах 3,65-3,70 ГГц. Обеспечивает скорость до 54 Mb/c на расстоянии до 5000 м на открытом пространстве.
- 802.11w — Protected Management Frames (Защищенные Управляющие Фреймы)
- 802.11ac — Новый, разрабатываемый IEEE стандарт. Скорости передачи данных до 1.3 Гбит/с, энергопотребление по сравнению с 802.11n снижено до 6 раз. Обратная совместимость с 802.11a/b/g/n. Финальная версия стандарта ожидается к концу 2012 года, а устройства, реализующие новый стандарт уже представлены.
- 802.11ad — Модификация стандарта 802.11ac, работающая в 60Ghz.

Примечания:
802.11F и 802.11T являются рекомендациями, а не стандартами, поэтому используются заглавные буквы.
Названия стандартов укорочены.

Наиболее распространенными стандартами являются:
802.11a – 54 Мбит/с, 5 ГГц, около 50 м
802.11b – 11 Мбит/с, 2,4 ГГц, около 100 м
802.11g – 54 Мбит/с, 2,4 ГГц, около 100 м
802.11n – до 600Мбит/с (реально до 450), 2,4/5 ГГц (в двухдиапазонном исполнении), около 100 м. Обратно совместим с 802.11a/b/g. Может использовать технологию мультиплексирования каналов (Multiple Input, Multiple Output – MIMO) при наличии нескольких антенн (от 2 до 4, 150 Мбит/с на канал).

Контрольные вопросы к 3-й главе.

1. Перечислите 7 уровней эталонной модели МОС/ВОС.

№	Название
7	
6	
5	
4	
3	
2	
1	

2. Каковы общепринятые форматы записи MAC-адреса:
   a. 00-32-FD-34-7C-12
   b. 11:F2:67:CB:00:23
   c. 00/5E/23/AA/12/CD
   d. 23AF09BCC561
3. Какой стандарт Ethernet позволяет создать сеть со скоростью 100 Мбит/с:
   a. 10BASE-FL

b. 100BASE-TX
c. 10BASE-5
d. 1000BASE-SX

4. В каких частотных диапазонах может работать беспроводная карта поддерживающая стандарт 802.11n:
   a. 49 МГц
   b. 2,4 ГГц
   c. 22 МГц
   d. 5 ГГц

4. Среда передачи данных и топология

Ниже будет рассказано о том, как выбрать среду передачи сигналов, соединительные устройства и топологию для сети [5].

Основные темы

- Среда передачи сигналов
- Сетевая аппаратура
- Сетевая топология

Введение

Для планирования сети необходимо знать какие типы сред передачи данных могут быть использованы для соединения элементов сети. Это позволит выбрать наиболее подходящую среду для каждой сети.

Так же понадобятся различные соединительные элементы и сетевые устройства для подключения узлов к сети и объединения сетей между собой.

Способ организации среды передачи данных и разнообразных сетевых устройств называется *топологией сети*.

Среда передачи сигналов

При выборе среды передачи данных стоит принять во внимание следующие факторы:

- Стоимость инсталляции
- Сложность инсталляции
- Скорость передачи данных
- Затухание
- Устойчивость к помехам

При создании сетей используются такие среды:

- Коаксиальный кабель
- Кабель из витых пар
- Оптоволоконный кабель
- Беспроводная связь

Коаксиальный кабель

Коаксиальный кабель – это среда передачи электрического сигнала состоящая из нескольких слоев различных материалов. По центру круглого кабеля рас-

полагается сердечник из цельного или многожильного провода (чаще медного) окруженного диэлектрической оболочкой, поверх которой находится проводящий экранирующий слой из фольги, проволочной оплетки или и того и другого. Все это помещено во внешнюю защитную диэлектрическую оболочку. Устройство коаксиального кабеля приведено на рисунке 4.1.

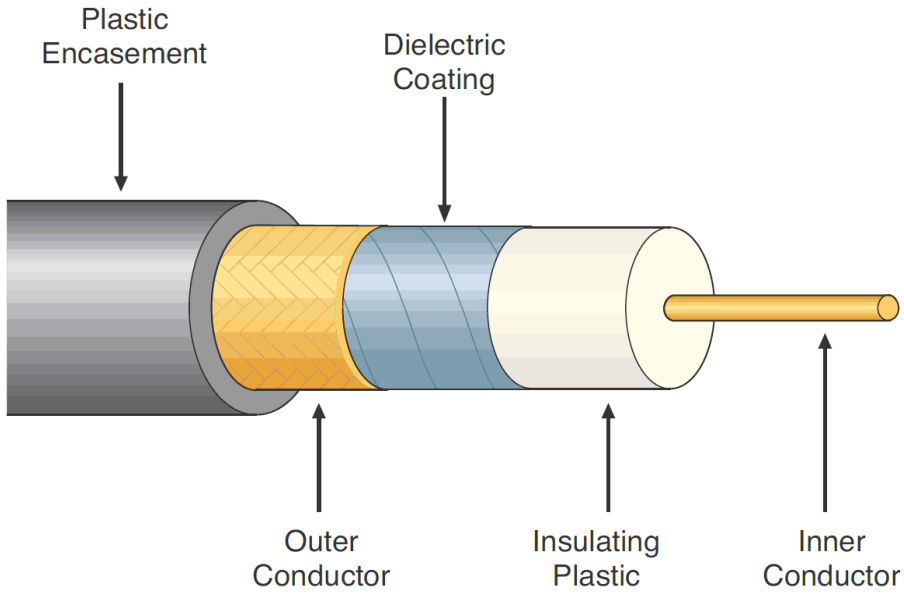

Рис. 4.1. Устройство коаксиального кабеля

Коаксиальный кабель, как и другие среды передачи данных, имеет конечную общую полосу пропускания. *Полоса пропускания* – это количество данных, которые можно передать за определенный промежуток времени.

Ниже представлены два типа коаксиального кабеля:

Толстый Ethernet (Thicknet). Это довольно жесткий кабель толщиной около 1 см (полдюйма) с толстым цельным сердечником (рис. 4.2). По такому кабелю данные можно было передавать на расстояние до 500 м и подключать к нему до 100 узлов.

Часто такой кабель изготавливался с желтой внешней оболочкой, за что получил второе название «желтый Ethernet».

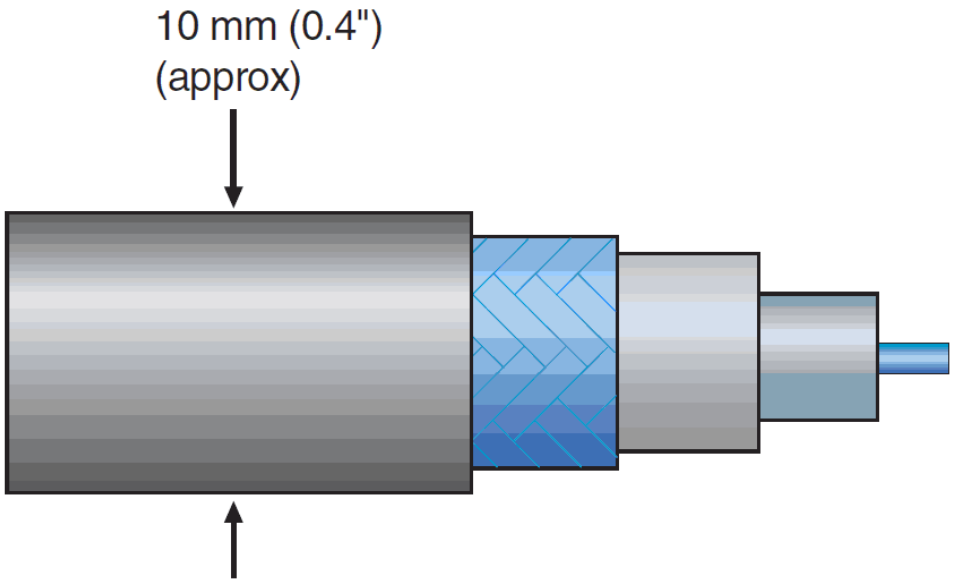

Рис. 4.2. Толстый коаксиальный кабель

Тонкий Ethernet (Thinnet). Это гибкий кабель толщиной около 5-6 мм (четверть дюйма) с цельным или многожильным сердечником (рис. 4.3). По такому кабелю данные можно было передавать на расстояние до 185 м и подключать к нему до 30 узлов. Отдельные куски кабеля и сетевые устройства подключались с помощью BNC-соединителей.

Такой кабель стоил значительно дешевле толстого и имел другое название «Chippernet» (дешевый Ethernet).

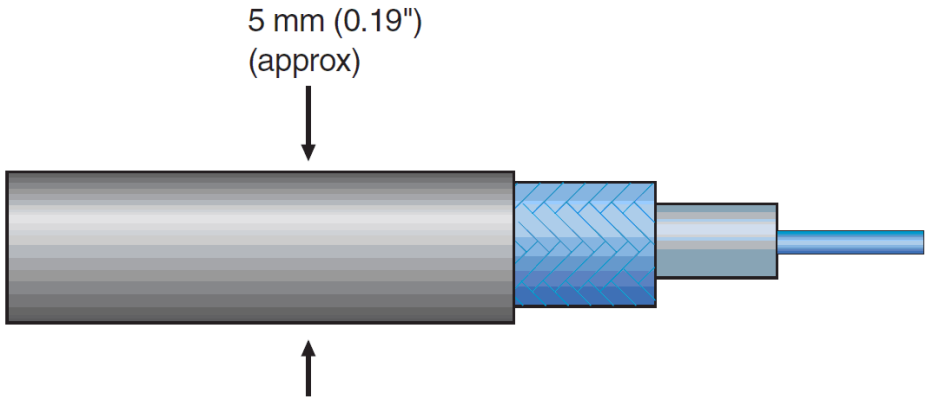

Рис. 4.3. Тонкий коаксиальный кабель

Кабель из витых пар

Витая пара состоит из двух медных изолированных проводов с цельным или многожильным сердечником скрученных друг с другом с определенным шагом скрутки. Одна или несколько (обычно 2 или 4 пары) в общей диэлектрической защитной оболочке составляют кабель из витых пар (рис. 4.4). Однопарный или двухпарный кабель часто применяли в телефонии за рубежом.

Медь используется потому, что она хорошо проводит электрические сигналы, а диэлектрическая изоляция служит защитой от замыкания, но она не защищает от высокочастотных помех, которые называют перекрестными наводками. Для уменьшения этих помех пары и свивают вдоль оси.

Такой кабель дешевле в изготовлении, чем коаксиальный, и проще в инсталляции и эксплуатации.

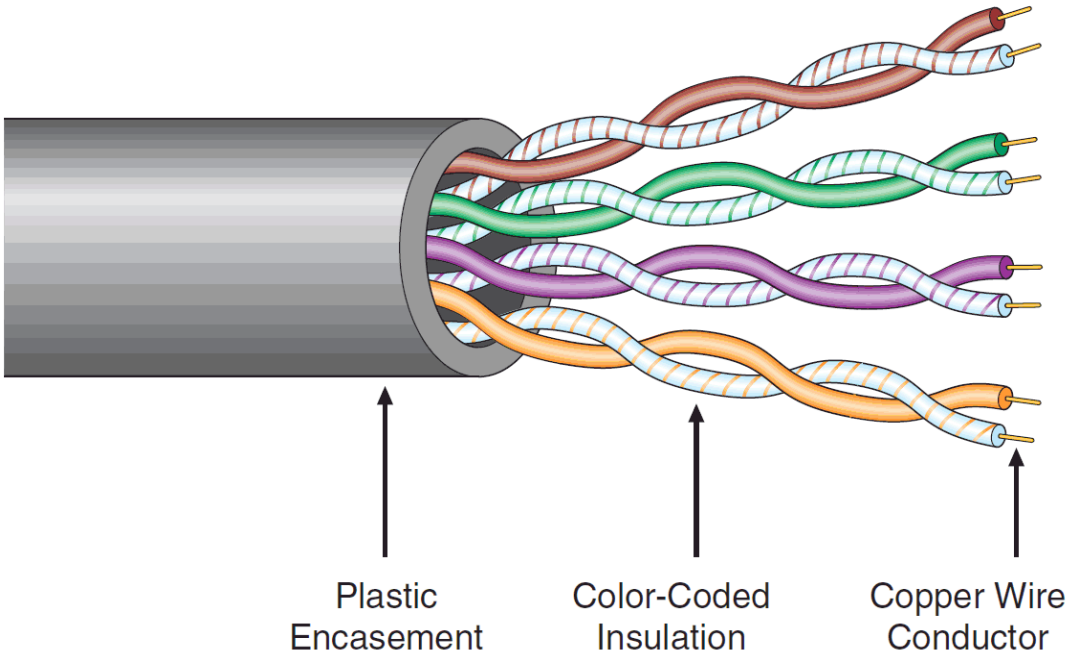

Рис. 4.4. Устройство кабеля из витых пар

Кабели из витых пар были нескольких типов:

- неэкранированная витая пара (UTP — Unshielded twisted pair) — без защитного экрана;
- фольгированная витая пара (FTP — Foiled twisted pair), также известна как F/UTP) — присутствует один общий внешний экран в виде фольги;
- экранированная витая пара (STP — Shielded twisted pair) — присутствует защита в виде экрана для каждой пары и общий внешний экран в виде сетки;
- фольгированная экранированная витая пара (S/FTP — Screened Foiled twisted pair) — внешний экран из медной оплетки и каждая пара в фольгированной оплетке;
- незащищенная экранированная витая пара (SF/UTP —Screened Foiled Unshielded twisted pair).Отличие от других типов витых пар заключается в наличии двойного внешнего экрана, сделанного из медной оплётки, а также фольги.

Кабели из витых пар еще классифицируются по категориям, которые нумеруются от CAT1 до CAT7 и определяют эффективный пропускаемый частотный диапазон. Кабель более высокой категории обычно содержит больше пар проводов и каждая пара имеет больше витков на единицу длины. Категории неэкрани-

рованной витой пары описываются в стандарте EIA/TIA 568 (Американский стандарт проводки в коммерческих зданиях) и в международном стандарте ISO 11801, а также приняты ГОСТ Р 53246-2008 и ГОСТ Р 53245-2008.

- **CAT1** (полоса частот 0,1 МГц) — телефонный кабель, всего одна пара (в России применяется кабель и вообще без скруток — «лапша» — у нее характеристики не хуже, но больше влияние помех). В США использовался ранее, только в «скрученном» виде. Используется только для передачи голоса или данных при помощи модема.
- **CAT2** (полоса частот 1 МГц) — старый тип кабеля, 2 пары проводников, поддерживал передачу данных на скоростях до 4 Мбит/с, использовался в сетях Token ring и Arcnet. Сейчас иногда встречается в телефонных сетях.
- **CAT3** (полоса частот 16 МГц) — 4-парный кабель, используется при построении телефонных и локальных сетей 10BASE-T и token ring, поддерживает скорость передачи данных до 10 Мбит/с или 100 Мбит/с по технологии 100BASE-T4 на расстоянии не дальше 500 метров [источник не указан 47 дней]. В отличие от предыдущих двух, отвечает требованиям стандарта IEEE 802.3.
- **CAT4** (полоса частот 20 МГц) — кабель состоит из 4 скрученных пар, использовался в сетях token ring, 10BASE-T, 100BASE-T4, скорость передачи данных не превышает 16 Мбит/с по одной паре, сейчас не используется.
- **CAT5** (полоса частот 100 МГц) — 4-парный кабель, использовался при построении локальных сетей 100BASE-TX и для прокладки телефонных линий, поддерживает скорость передачи данных до 100 Мбит/с при использовании 2 пар.
- **CAT5e** (полоса частот 125 МГц) — 4-парный кабель, усовершенствованная категория 5. Скорость передач данных до 100 Мбит/с при использовании 2 пар и до 1000 Мбит/с при использовании 4 пар. Кабель категории 5e является самым распространённым и используется для построения компьютерных сетей. Иногда встречается двухпарный кабель категории 5e. Преимущества данного кабеля в более низкой себестоимости и меньшей толщине.
- **CAT6** (полоса частот 250 МГц) — применяется в сетях Fast Ethernet и Gigabit Ethernet, состоит из 4 пар проводников и способен передавать данные на скорости до 1000 Мбит/с и до 10 гигабит на расстояние до 50 м. Добавлен в стандарт в июне 2002 года.
- **CAT6a** (полоса частот 500 МГц) — применяется в сетях Ethernet, состоит из 4 пар проводников и способен передавать данные на скорости до 10 Гбит/с и планируется использовать его для приложений, работающих на скорости до 40 Гбит/с. Добавлен в стандарт в феврале 2008 года.
- **CAT7** (полоса частот 600—700 МГц) — спецификация на данный тип кабеля утверждена только международным стандартом ISO 11801, скорость передачи данных до 10 Гбит/с. Кабель этой категории имеет общий экран

и экраны вокруг каждой пары. Седьмая категория, строго говоря, не UTP, а S/FTP (Screened Fully Shielded Twisted Pair).

- **CAT7a** (полоса частот 1200 МГц) - разработана для передачи данных на скоростях до 40 Гбит/с.

Каждая отдельно взятая витая пара, входящая в состав кабеля, предназначенного для передачи данных, должна иметь волновое сопротивление 100±15 Ом, в противном случае форма электрического сигнала будет искажена и передача данных станет невозможной. Причиной проблем с передачей данных может быть не только некачественный кабель, но также наличие «скруток» в кабеле и использование розеток более низкой категории, чем кабель.

Оптоволоконные кабели

Оптоволоконные кабели представляют собой одно или несколько двухслойных оптических волокон в пластиковой оболочке объединенных в общем внешнем кожухе (рис. 4.5). Оптическое волокно бывает стеклянным и пластиковым.

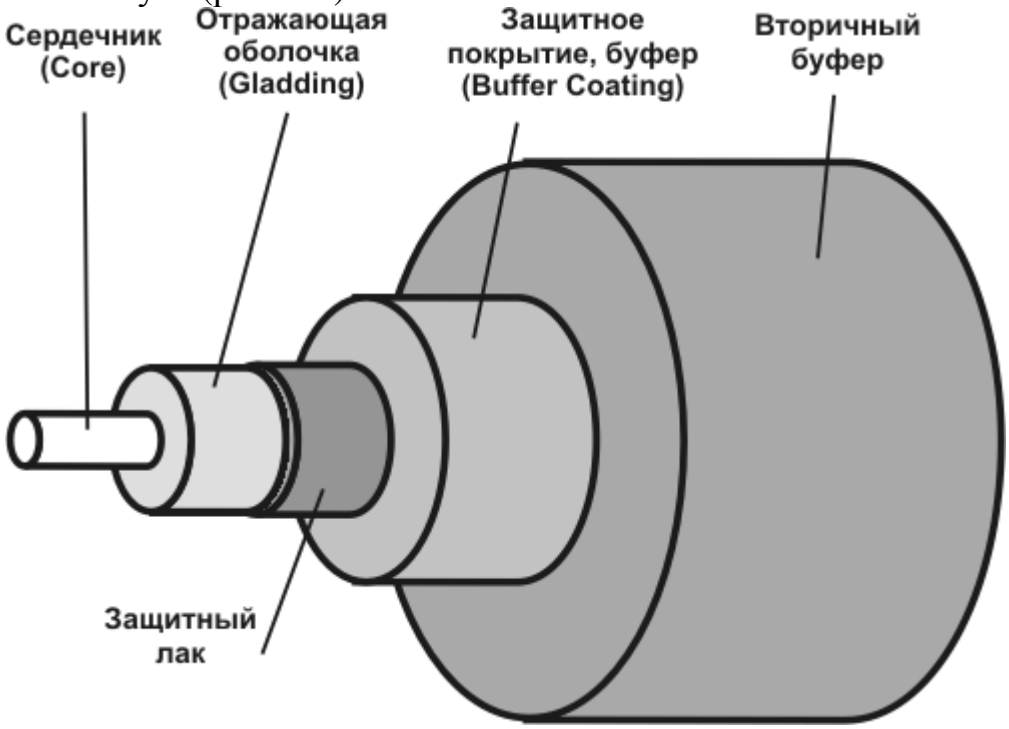

Рис. 4.5. Структура оптоволокна

При передаче оптического сигнала по оптоволокну используется эффект полного отражения луча на границе сред с разными коэффициентами преломления. Это позволяет уменьшить рассеяние светового пучка и передавать его на большие расстояния. Разные типы волокон представлены на рисунке 4.6.

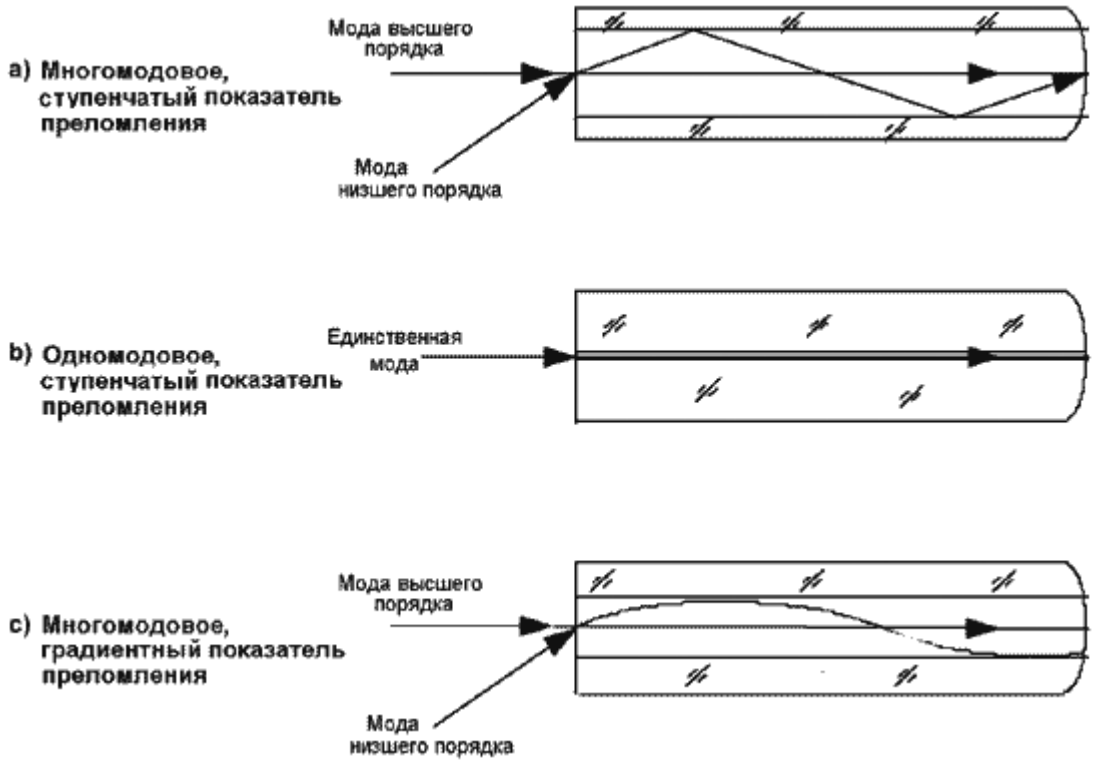

Рис. 4.6. Эффект полного отражения в разных типах оптических волокон

В зависимости от условий прокладки и эксплуатации кабеля внешние оболочки могут быть усилены стальной обмоткой, а промежутки между отдельными волокнами и внутренними оболочками могут быть заполнены водоотталкивающим гелем.

Оптоволоконные кабели бывают двух типов:

- Одномодовые (Single-Mode Fiber – SMF)
- Многомодовые (Multi-Mode Fiber – MMF)

Одномодовое оптоволокно

Одномодовое оптоволокно (Single-Mode Fiber – SMF) имеет сердечник очень малого диаметра – всего 10 микрон и даже менее, например, 9 микрон, и поэтому пропускает свет одной моды (образно говоря – однонаправленный пучок света). Для этого используются источники света с очень узким пучком излучения, например, дорогие лазеры.

Многомодовое оптоволокно

В многомодовом волокне (Multi-Mode Fiber – MMF) сердцевина волокна больше и обычно составляет 50 или 62,5 микрона. Поэтому свет может распространяться по нескольким путям (модам) с разными углами входа пучка света в начало волокна. В качестве излучателей могут применяться лазерные диоды и более дешевые светодиоды. Одномодовое и многомодовое оптоволокно приведены на рисунке 4.7.

Рис. 4.7. Одномодовое и многомодовые волокна

В следующей таблице 4.1 приведены Длины волн и расстояния, на которые передается сигнал в зависимости от типа волокна и излучателя.

Таблица 4.1. Длины волн и дальность передачи сигнала по оптоволокну.

Длина волны, нм	Расстояние	Тип волокна	Тип излучателя
850	550 м (до 2 км)	MMF	SX
1310	10 км	SMF	LX
1550	40 км	SMF	XD
1550	80 км	SMF	ZX
1550	120 км	SMF	EX или EZX

При передаче данных в телекоммуникационных сетях могут быть использованы различные скорости в зависимости от применяемых технологий:
Ethernet: 10 Mbps, 100 Mbps, 1 Gbps, 1,25 Gbps, 10 Gbps
SDH: STM-1 (155 Mbps), STM-4 (622 Mbps), STM-16 (2,488 Gbps)
Fibre Channel: 1, 2, 4, 8 Gbps

Основные преимущества оптоволокна перед медными кабелями – это высокая скорость, большие расстояния и невосприимчивость к электромагнитным помехам.

Беспроводная связь

Беспроводная связь бывает разных типов, но получила наибольшее распространение (и чаще всего ассоциируется с этим названием) радиосвязь между компьютерными устройствами.

Беспроводная сеть Wi-Fi

Большинство беспроводных компьютерных радио-сетей попадают под действие стандартов 802.11. Наиболее распространенными являются:

- 802.11a
- 802.11b

- 802.11g
- 802.11n

Сначала появились сети стандарта 802.11b, работавшие на частоте 2,4 ГГц на скоростях до 11 Мбит/с. Потом появился стандарт 802.11a, который описывал работу сетей на частоте 5 ГГц на скоростях до 54 Мбит/с. Третьим появился вариант 802.11g, который сочетал в себе лучшие наработки стандартов a и b, опорной частотой были 2,4 ГГц, а скорость стала 54 Мбит/с. Некоторые производители предлагали «ускоренные» реализации, с пропускной способностью до 108 Мбит/с.

Затем был ратифицирован стандарт 802.11n, который дает возможность множественный ввод/вывод (Multiple Input/Multiple Output –MIMO), и по 4 каналам может передавать данные на скорости до 600 Мбит/с, но чаще встречаются реализации максимум с тремя каналами и скоростью до 300 Мбит/с. Стандарт позволяет использовать частоты 2,4-2,5 ГГц и 5 ГГц. Обратно совместим со стандартами 802.11a,b,g.

Более подробно беспроводные сети будут рассмотрены в Главе 6 «Беспроводные сети».

В дополнение к беспроводным сетям с использованием радиоволн применяются и некоторые другие среды передачи сигнала без проводов:

- Микроволны
- Инфракрасное излучение
- Радиоволны близкого радиуса действия (Bluetooth, ZigBee)

Сетевая аппаратура

После выбора среды передачи данных можно определяться с устройствами, обеспечивающими соединения в сети. Такие устройства обеспечивают подключение компьютеров, принтеров и других подобных устройств к сети, а также соединяются разные сегменты сети.

Сегмент – это отрезок (диапазон, область действия) среды передачи данных, ограниченный максимальной длиной, на которой устойчиво распознается сигнал, и подключенный к повторителю, концентратору, коммутатору, маршрутизатору и предоставляющий доступ к сетевым ресурсам для клиентов и серверов, подключенных к этому отрезку.

Соединительные устройства могут быть классифицированы в зависимости от выполняемых функций на следующие категории:

- Соединители (разъемы, коннекторы)
- Коммутационные устройства локальных сетей
- Коммутационные устройства глобальных сетей

Соединители

Каждый тип среды передачи данных (имеются ввиду кабельные среды) должен иметь возможность каким-то способом присоединиться к коммутационному устройству или другому отрезку среды. Соединители (media connectors) на

конце кабеля предоставляют физическое взаимодействие между средой передачи данных и устройством.

Каждая среда передачи данных может оснащаться одним или несколькими типами соединителей.

Ниже приведен список распространенных соединителей для разных сред и устройств:

- Байонетный (BNC)
- Соединитель F-типа
- RJ-45
- RJ-11
- Fiber-Optic Straight Tip (ST) Connector
- Fiber-Optic Standard Connector (SC)
- Fiber-Optic Local Connector (LC)
- Mechanical Transfer Registered Jack (MTRJ)
- IEEE1394 (FireWire, i.Link)
- Universal Serial Bus (USB)
- Thunderbolt

Коммутационные устройства локальных сетей

Коммутационные устройства локальных вычислительных сетей соединяют сегменты сетей и подключают устройства к сети. Ниже приведены типы устройств локальных сетей:

- Сетевая интерфейсная карта (Network Interface Card – NIC)
- Модем (modem)
- Повторитель (repeater)
- Концентратор (hub)
- Мост (bridge)
- Коммутатор (switch)
- Точка беспроводного доступа (Wireless Access Point – WAP)
- Мультиплексор (multiplexer)
- Трансивер (transceiver)
- Брандмауэр (firewall)

Сетевая интерфейсная карта

Сетевая интерфейсная карта (Network Interface Card – NIC) – отдельная вставляемая плата или интегрированное устройства, которое содержит все необходимые микросхемы для создания физического и логического соединения между компьютером и средой передачи данных (рис.4.9).

Каждая сетевая карта при производстве получает свой уникальный адрес управления доступом к среде (Media Access Control (MAC) address).

MAC адрес является идентификатором, который служит физическим адресом сетевой платы.

48-битный MAC адрес представляется 12-символьным шестнадцатеричным идентификатором разделенным по два символа двоеточием или, иногда, дефисом. Например:
00:34:EA:73:CD:54

Рис. 4.9. Сетевая интерфейсная карта

Модем (modem)

Модем (modem) – сокращение от «модулятор-демодулятор» - преобразовывает цифровые электрические сигналы в аналоговые или электромагнитные сигналы и обратно.

На сегодняшний день модемы бывают трех типов:

- Традиционные – для телефонных линий.
- Модемы цифровых абонентских линий (Digital Subscriber Line – DSL).
- Кабельные.

Традиционный модем

Модемы для телефонных линий работают в голосовом частотном диапазоне. Скорость передачи до 56 кбит/с.

Модем цифровой абонентской линии (DSL-modem)

Цифровые абонентские линии (DSL) бывают с симметричной и несимметричной скоростью передачи от узла связи к абоненту, и называются, соответственно, Symmetric DSL – SDSL, и Asymmetric DSL – ADSL. Могут работать по обычным или выделенным телефонным линиям, но в повышенном частотном диапазоне. Скорости могут достигать до 12 Мбит/с в симметричном канале и 8/24 Мбит/с – в ассиметричном.

Кабельный модем

Кабельные модемы в качестве среды передачи данных часто используют телевизионный антенный кабель. Скорость передачи может достигать 36 Мбит/с.

Повторитель (repeater)

Повторители (repeater) увеличивали дистанцию для выбранной среды передачи данных усиливая или регенерируя входящие сигналы:

- **Усилители** – усиливали все входящие сигналы, включая помехи. Усилители обычно используются для аналоговых сигналов.
- **Регенераторы** – получая сигнал, удаляли из него шум, восстанавливали уровень сигнала и передавали его на выход. Регенераторы использовались для цифровых сигналов.

Повторители также использовались и как преобразователи среды (media converter), подключаясь к кабелям разных типов.

Концентратор (hub)

Концентраторы бывают нескольких типов:

- **Активный.** Активный концентратор (его еще называют многопортовым повторителем) регенерирует или усиливает входящий сигнал и рассылает его по всем своим портам. Активный концентратор может увеличить длину сети, подключая к себе дополнительные кабельные сегменты. Такой концентратор требует внешнего электропитания для усиления сигналов.
- **Пассивный.** Пассивный концентратор иногда называют делителем (splitter), потому что делит входящий сигнал между своими выходами не усиливая его. Служит для подключения устройств к сети. Пассивный концентратор передает сигнал на меньшие расстояния, чем активный. Он может применяться для подключения разных типов кабелей.
- **Интеллектуальный.** Интеллектуальный концентратор – активное устройство, которое кроме передачи данных может следить за трафиком и имеет функции управления сетью.
- **Коммутирующий.** Коммутирующий концентратор имеет некоторые интеллектуальные возможности и для определенных портов (не всех) может считывать адрес источника и получателя и перенаправлять пакет в группу портов, где он доставляется как обычным концентратором – то есть по всем портам в этой группе.

Мост (bridge)

Мосты использовались для соединения сетевых сегментов одного типа, например, Token Ring или Ethernet.

Мосты увеличивали максимальную дистанцию сети, объединяя два сегмента. Основываясь на MAC-адресах получаемого пакета, мост пересылал его в другой сегмент сети, если источник и получатель пакета находились по разные стороны моста.

Мосты создают отдельные коллизионные домены на своих портах. Так что коллизии (столкновения сигналов) в одном сегменте не мешают передаче сигналов в другом сегменте.

Таблица. 4.2. Разделение MAC адресов в мосте.

Сегмент 1	Сегмент 2
MAC адреса	MAC адреса
00:45:70:5C:12:ED	AC:78:F4:17:09:E3
23:AB:01:56:FA:42	22:18:60:EE:05:14
05:78:BD:45:80:16	03:AA:95:27:17:62

Коммутатор (switch)

Коммутатор объединил в себе функции концентратора и моста, будучи многопортовым устройством. Он регенерирует сигнал и посылает пакет в тот порт, к которому подключен его получатель.

Поскольку к каждому порту коммутатора подключено только одно устройство, то, фактически, создается отдельный кабельный сегмент между коммутатором и этим устройством. Это позволят избежать коллизий (столкновений) и использовать всю полосу пропускания на этом участке между двумя устройствами. В отличие от концентратора, где полоса пропускания делится между всему подключенными к нему устройствами, в коммутаторе доступна вся полоса пропускания на каждом порту. Кроме того витой пары или оптоволокна появляется возможность использовать передачу в двух направлениях одновременно – полный дуплекс.

Коммутаторы не ограничивают прохождения широковещательных пакетов.

Точка беспроводного доступа (Wireless Access Point – WAP)

Точка беспроводного доступа (Wireless Access Point – WAP) используется для организации согласованной работы нескольких беспроводных устройств. Если точка доступа подключена к проводной сети, то она может служить средством подключения беспроводных устройств к проводной сети.

Одна точка доступа может обслуживать несколько клиентов. Их количество, скорость и дальность работы сильно зависят от условий распространения сигнала на охватываемой территории.

Большинство точек доступа не могут работать друг с другом напрямую, поэтому для объединения двух беспроводных сетей может понадобиться беспроводной мост.

Мультиплексор (multiplexer)

Мультиплексор используется для объединения двух и более сигналов для передачи их по среде передачи. Мультиплексоры применяются совместно с демультиплексорами, которые на принимающей стороне расщепляют сигнал из среды передачи на несколько исходных сигналов.

В сетях мультиплексоры могут использоваться, если среда передачи предоставляет большую пропускную способность, чем занимает один сигнал. В этом случае мультиплексоры могут одновременно принимать и передавать сигналы в разных направлениях, что повышает эффективность среды передачи.

Трансивер (transceiver)

Трансиверы могут одновременно принимать и передавать аналоговые или цифровые сигналы.

Большинство современных сетевых карт имеют встроенные трансиверы.

Трансиверы могут быть преобразователями сигнала для разных сред передачи (media converter).

Брандмауэр (firewall)

Брандмауэр (firewall) – это система, которая призвана защищать сеть от внешних угроз. Брандмауэр может быть аппаратным, программным или программно-аппаратным комплексом.

Брандмауэр устанавливают на границе сети для предотвращения неуполномоченного проникновения в сеть извне и для ограничения исходящего трафика из сети.

Коммутационные устройства глобальных сетей

К коммутационным устройствам глобальных сетей (ГВС – WAN) относят:

- Маршрутизатор
- Шлюз
- Channel Service Unit/Digital Service Unit (CSU/DSU)
- Integrated Service Digital Network (ISDN)
- 3G, 4G/LTE

Маршрутизатор

Маршрутизатор – это устройство, которое соединяет две и более сетей с разными адресами сетей. Адрес сети – это идентификатор кабельного сегмента (среды передачи данных), к которому подключены сетевые устройства. Адрес сети отличает сети друг от друга в межсетевом взаимодействии.

Также маршрутизаторы служат для разделения сети на меньшие сегменты. Маршрутизатор пересылает данные в ту сеть, для которой они предназначены.

Тогда как коммутаторы анализируют MAC адреса отправителя и получателя, маршрутизаторы должны анализировать логические адреса более высокого сетевого уровня. Как результат, маршрутизаторы, производящие больше обработки пакета, медленнее коммутаторов.

Маршрутизаторы используют таблицы маршрутизации для принятия решения о том, куда пересылать пакет. Таблица маршрутизации (рис. 4.10) содержит информацию о сетях и адресах сетевых устройств для пересылки предназначенных им пакетов.

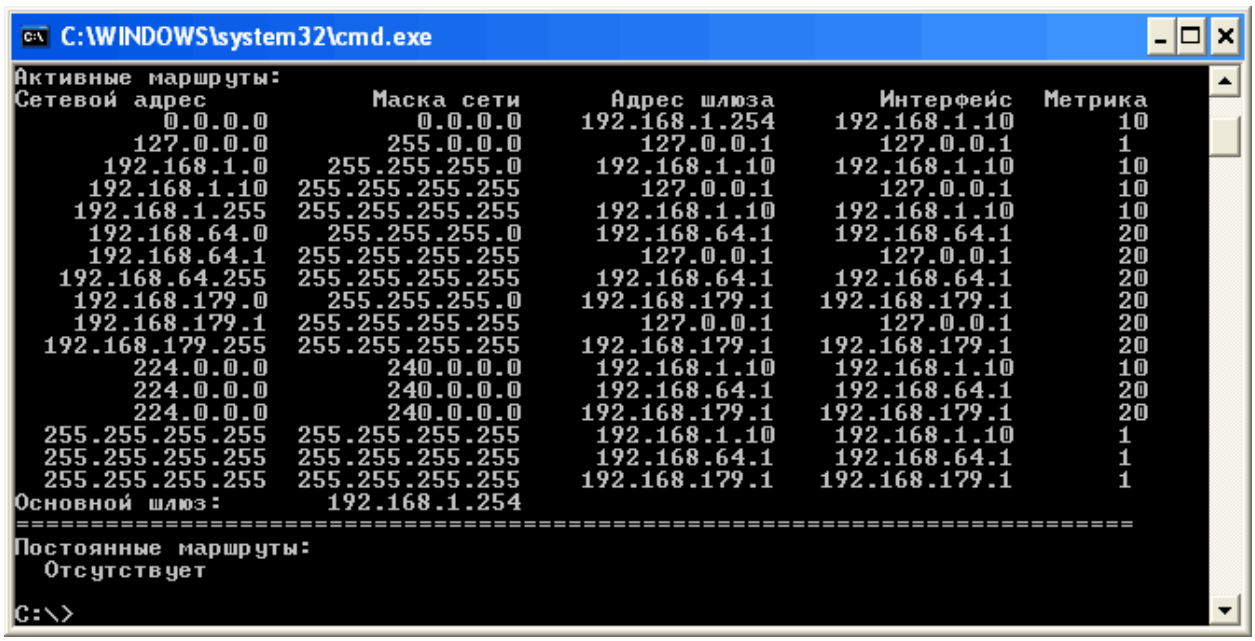

Рис. 4.10. Таблица маршрутизации

Маршрутизаторы обмениваются информацией об известных им маршрутах с другими маршрутизаторами. Обновляя свои таблицы маршрутизации полученной информацией, маршрутизаторы строят схему окружающих сетей и связей между ними.

Маршрутизаторы не пересылают широковещательные пакеты за пределы сети, в которой они были созданы, таким образом ограничивая широковещательный домен и не допускают распространения широковещательных штормов.

Шлюз

Шлюз – это специализированное устройство или программа, которые служат для соединения сетей, использующих различные протоколы или разные типы физического подключения. Шлюзы осуществляют преобразование протоколов.

Например, шлюз может обеспечить взаимодействие сетей, в одной из которых используется протокол TCP/IP, а в другой – IPX/SPX.

3G, 4G/LTE

Мобильная связь поколения строится на основе пакетной передачи данных. Сети третьего поколения 3G работают на частотах дециметрового диапазона, как правило, в диапазоне около 2 ГГц, передавая данные со скоростью до 3,6 Мбит/с.

В сетях 3G обеспечивается предоставление двух базовых услуг: передача данных и передача голоса. Согласно регламентам ITU (International Telecommunications Union — Международный Союз Электросвязи) сети 3G должны поддерживать следующие скорости передачи данных:

- для абонентов с высокой мобильностью (до 120 км/ч) — не более 144 кбит/с;
- для абонентов с низкой мобильностью (до 3 км/ч) — 384 кбит/с;
- для неподвижных объектов — 2048 Кбит/с.

Сети 4G/LTE (Long Term Evolution) должны обеспечить более высокую скорость и дальность передачи данных и обладать большим функционалом.

Сетевые топологии

После выбора среды передачи данных и коммутационных устройств для сети нужно выбрать топологию сети. Топология – это способ размещения и подключения сетевых устройств, а также их взаимное расположение относительно друг друга. Выбор подходящей сетевой топологии позволит создать эффективную, надежную и экономически выгодную сеть.

Топология может быть реальным физическим расположением сети или же логическим представлением информационных потоков:

- Физические сетевые топологии
- Логические сетевые топологии

Физические сетевые топологии

Ниже перечислены физические сетевые топологии:

- Шина
- Звезда
- Кольцо
- Полносвязанная сеть (ячеистая)
- Беспроводная

Логические сетевые топологии

Ниже перечислены логические сетевые топологии:

- Топология звезда шин
- Топология кольцо в звезде

5. Удаленный доступ

Возможность подключить две сети, которые физически не соединены, или подключить рабочую станцию к сети за пределами рабочего места называется удаленный доступ (remote access) [6].

Удаленное подключение к сетям условно можно поделить на три типа:

- Подключение рабочей станции к сети компании
- Подключение небольшого офиса
- Подключение к глобальным сетям

Подключение рабочей станции к сети компании

Технологии доступа:

- Телефонная сеть общего назначения (PSTN)
- Цифровая абонентская линия (DSL)
  - Симметричная линия (SDSL)
  - Асимметричная линия (ADSL)
- Кабельный модем
- Беспроводная связь
- Сотовая связь 3G/4G

Телефонная сеть

Старейший метод подключения к удаленной сети – это использование модемов на традиционных телефонных каналах. Компьютер с подключенным к нему модемом соединяется по телефонным линиям с таким же удаленным компьютером с модемом.

Модемы преобразуют цифровой сигнал с компьютера в аналоговый сигнал, который передается по телефонным сетям до точки назначения. Другой модем производит обратное преобразование принятого аналогового сигнала в цифровой код, понятный компьютеру.

Применение телефонных линий для удаленного доступа носило название сети передачи данных по коммутируемым каналам (Dial-Up Networking – DUN). Максимальная скорость такого соединения составляла 56 кбит/с.

Хотя модемное соединение все еще используется сегодня, но новые технологии, более быстрые, более надежные, с каждым днем все активнее вытесняют его из современных сетей.

Цифровая абонентская линия (DSL)

Цифровые абонентские линии используют те же или сходные линии связи, что и традиционные телефонные линии, но посылают цифровые сигналы, а не аналоговые, как обычные модемы.

Симметричная цифровая абонентская линия (SDSL)

Симметричная цифровая абонентская линия (SDSL) – это высокоскоростное, цифровое, выделенное (то есть не требующее телефонного номера) соединение, которое обеспечивает одинаковую входящую и исходящую скорость.

SDSL – хороший выбор для тех абонентов, которые примерно в равной пропорции принимают и отправляют данные.

Асимметричная цифровая абонентская линия (ADSL)

Асимметричная цифровая абонентская линия (ADSL) – это высокоскоростное, цифровое, выделенное (то есть не требующее телефонного номера) соединение, которое имеет высокую входящую скорость (до 24 Мбит/с) и более низкую (несимметричную) исходящую скорость (до 8 Мбит/с).

ADSL дешевле, чем SDSL, и более соответствует стилю работы домашних и небольших офисов, в которых большая часть информации закачивается из Интернет, что и послужило причиной его широкого распространения.

ADSL и SDSL используют те же телефонные провода, что и обычные телефонные коммутируемые линии.

Кабельный модем

Кабельные модемы используют в качестве среды передачи данных телевизионные коаксиальные антенные кабели или кабели операторов кабельного телевидения. Как и в случае цифровых абонентских линий они передают цифровой сигнал и чаще предоставляют ассиметричную скорость подключения.

Беспроводная связь

Для беспроводной связи отдельных потребителей предлагались различные технологии – Radio Ethernet, микроволновые приемопередатчики и инфракрасные лазерные излучатели. Все эти варианты требовали установки специального оборудования на крыше здания или на наружной стене и протягивания сетевого провода к абоненту.

Из-за дороговизны устройств и сложного монтажа не получили широкого распространения среди индивидуальных пользователей, но обеспечивали иногда единственно возможную связь для удаленных филиалов или складов компаний.

Беспроводная сотовая связь WiMax заменяется связью 4G/LTE.

Сотовая связь 3G/4G

С увеличением вычислительных мощностей сотовых телефонов, карманных ПК (КПК) и смартфонов, им потребовались большие скорости для взаимодействия с существующими сетями и Интернетом. Постепенно цифровая сотовая связь стандарта GSM повышала скорости цифрового доступа абонентских устройств. В зависимости от скорости и используемых технологий этапы (G от generation) стали получать номера, в том числе и промежуточные (2G, 2.5G, 3G, 3.5G, 4G/LTE).

Кроме встроенных и внешних модемов производитель стали выпускать и беспроводные маршрутизаторы WiFi-3G, WiFi-4G, что позволило подключать через сотовые сети не только отдельных пользователей, но и небольшие рабочие коллективы.

Теоретически скорость в сети 4G/LTE может достигать 100 Мбит/с.

Протоколы доступа к сетевым ресурсам:

- Internet Connection Sharing (ICS)
- Network File System (NFS)
- Server Message Block (SMB) или Samba
- Common Internet File System (CIFS)
- NetWare Core Protocol (NCP)
- Apple Filing Protocol (AFP)

Internet Connection Sharing (ICS)

Internet Connection Sharing (ICS, в русской версии ОС Windows переводится как «Общий доступ подключения к Интернету») — возможность, появившаяся в ОС Windows, начиная с версии Windows 98 Second Edition, заключающаяся в

совместном использовании одного подключения к Интернету несколькими компьютерами, находящимися в локальной сети.

ICS должен быть установлен на компьютере, имеющем подключение к Интернет. Фактически ICS представляет собой один из вариантов трансляции сетевых адресов (Network Address Translation – NAT).

Network File System (NFS)

Сетевая файловая система (Network File System - NFS) позволяет UNIX- и Linux-клиентам работать файлами и каталогами на сервере NFS так, как будто они находятся на локальном компьютере.

Server Message Block (SMB) или Samba

Блок серверных сообщений (Server Message Block - SMB) — сетевой протокол прикладного уровня для удалённого доступа к файлам, принтерам и другим сетевым ресурсам, а также для межпроцессного взаимодействия. Первая версия протокола была разработана компаниями IBM, Microsoft, Intel и 3Com в 1980-х годах; вторая (SMB 2.0) была создана Microsoft и появилась в Windows Vista и Windows Server 2008; третья версия (SMB 3.0) реализована в Windows 8 и Windows Server 2012. В настоящее время SMB связан главным образом с операционными системами Microsoft Windows, где используется для реализации «Сети Microsoft Windows» (Microsoft Windows Network) и «Совместного использования файлов и принтеров» (File and Printer Sharing).

В 1992 году появилась Samba — свободная реализация протокола SMB для UNIX-подобных операционных систем (изначально для SunOS). Поскольку Microsoft не опубликовала документацию значительной части своих дополнений к SMB, разработчикам Samba пришлось провести обратную разработку протокола. Сейчас чаще используется в операционных системах Linux.

Common Internet File System (CIFS)

Общая межсетевая файловая система (Common Internet File System - CIFS) – это открытый вариант протокола SMB, который Microsoft опубликовала в 1996 году и стала использовать новое название для дополненной версии протокола, которая использовалась в Windows NT 4.0. SMB и CIFS фактически стали синонимами. Microsoft некоторое время пыталась превратить CIFS в международный стандарт через IETF, но после 2000 года прекратила работу по стандартизации.

Сейчас CIFS реализован практически на всех современных операционных системах и позволяет обмениваться файлами и предоставлять простой сервис сетевой печати.

Apple Filing Protocol (AFP)

Файловый протокол Apple (Apple Filing Protocol - AFP) был предназначен для сетевого файлового доступа компьютеров Apple Macintosh, но сейчас практически вытеснен NFS и CIFS.

Протоколы и службы удаленного доступа:

- Служба удаленного доступа (Remote Access Service – RAS)
  - Клиент удаленного доступа (Remote Access Client)
  - Сервер удаленного доступа (Remote Access Server)
- Протокол точка-точка (Point-to-Point Protocol – PPP)
- Межсетевой протокол по последовательным линиям (Serial Line Internet Protocol – SLIP)
- Виртуальная частная сеть (Virtual Private Network – VPN)
  - Соединение клиент-сервер
  - Соединение сервер-сервер
- Протокол точка-точка поверх Ethernet (Point-to-Point Protocol over Ethernet – PPPoE)
- Туннелированный протокол точка-точка (Point-to-Point Tunneling Protocol – PPTP)
- DirectAccess
- Протокол удаленного рабочего стола (Remote Desktop Protocol – RDP)

Служба удаленного доступа (RAS)

Служба удаленного доступа (Remote Access Service – RAS) подключает удаленных или мобильных сотрудников в сети своей организации. Такие сотрудники инициируют соединение с сервером удаленного доступа с помощью программ удаленного доступа, установленных на их компьютерах. Удаленные пользователи могут работать так, как если бы их компьютеры были напрямую подключены к сети.

- Клиент удаленного доступа

Клиенты удаленного доступа под управлением ОС Windows, UNIX и Macintosh могут подключаться к серверу удаленного доступа RRAS. Чаще всего для этого используются обычные аналоговые модемы для традиционных телефонных линий. Клиент удаленного доступа создает запрос к серверу удаленного доступа, а тот обрабатывает запрос.

- Сервер удаленного доступа

Сервер удаленного доступа RRAS принимает подключения удаленного доступа и пересылает пакеты между клиентами удаленного доступа и сетью, к которой этот сервер присоединен. Серверы удаленного доступа оснащаются либо модемными пулами, а при большей нагрузке их подключают с помощью специального оборудования напрямую к цифровому потоку с телефонной станции.

Протокол точка-точка (PPP)

Протокол точка-точка (Point-to-Point Protocol – PPP) - двухточечный протокол канального уровня (Data Link) сетевой модели OSI. Обычно используется для установления прямой связи между двумя узлами сети, причем он может обеспечить аутентификацию соединения, шифрование (с использованием ECP, RFC 1968) и сжатие данных. Используется на многих типах физических сетей: нуль-модемный кабель, телефонная линия, сотовая связь и т. д.

Часто встречаются подвиды протокола PPP такие, как Point-to-Point Protocol over Ethernet (PPPoE), используемый для подключения по Ethernet, и иногда через DSL; и Point-to-Point Protocol over ATM (PPPoA), который используется для подключения по ATM Adaptation Layer 5 (AAL5), который является основной альтернативой PPPoE для DSL.

PPP может использовать различные механизмы аутентификации для безопасной регистрации пользователей на сервер удаленного доступа.

Архитектура PPP позволяет по такому соединению пропускать такие сетевые протоколы, как IPX/SPX, TCP/IP, NetBEUI и AppleTalk.

Одним из вариантов PPP стал PPTP - PPTP (Point-to-Point Tunneling Protocol) — туннельный протокол типа точка-точка, позволяющий компьютеру устанавливать защищённое соединение с сервером за счёт создания специального туннеля в стандартной, незащищённой сети. PPTP помещает (инкапсулирует) кадры PPP в IP-пакеты для передачи по глобальной IP-сети, например Интернет. PPTP может также использоваться для организации туннеля между двумя локальными сетями. PPTP использует дополнительное TCP-соединение для обслуживания туннеля.

Межсетевой протокол по последовательным линиям (SLIP)

Межсетевой протокол по последовательным линиям (Serial Line Internet Protocol – SLIP) — устаревший сетевой протокол канального уровня эталонной сетевой модели OSI для доступа к сетям стека TCP/IP через низкоскоростные линии связи путём простой инкапсуляции IP-пакетов. Используются коммутируемые соединения через последовательные порты для соединений клиент-сервер типа точка-точка. В настоящее время вместо него используют более совершенный протокол PPP.

Виртуальная частная сеть (Virtual Private Network – VPN)

Виртуальная частная сеть (Virtual Private Network – VPN) – это технология создания частной сети путем ее наложения на существующие общедоступные публичные сети. С помощью такой частной сети сотрудники могут получать доступ к сети организации, используя практически любой доступный способ соединения, например, через Интернет.

Виртуальные частные сети (ВЧС) используют туннелирование для установления соединение и шифрование передаваемого по такой сети трафика.

ВЧС бывают двух типов:

- **Соединение клиент-сервер (сеть).** В этом случае отдельный ВЧС-клиент подключается к ВЧС-серверу, а тот предоставляет доступ к своим или сетевым ресурсам внутри компании. Сейчас это наиболее распространенный способ подключения удаленных, мобильных и надомных сотрудников к сети компании.
- **Соединение сервер-сервер (сеть-сеть).** В этом случае соединяются два сервера (маршрутизатора), которые, по сути, соединяют две и более сетей друг с другом. Для внутренних клиентов таких сетей соединение является прозрачным и не требует каких-либо дополнительных настроек.

DirectAccess

DirectAccess - новая технология, введенная в Windows 7 и Windows Server 2008 R2, которая предоставляет мобильным пользователям компьютера, работающим удаленно, такую же рабочую среду, как если бы они находились офисе. С DirectAccess удаленные пользователи могут получить доступ к корпоративным ресурсам, таким как общие файлы, почтовые серверы, интранет-веб-сайты или внутренние приложения, без необходимости предварительного установления соединения с виртуальной частной сетью (VPN). DirectAccess автоматически, и без вмешательства со стороны пользователя, устанавливает двунаправленную связь от компьютеров клиента до корпоративной сети, с подтверждением подлинности компьютера. Еще до того, как пользователь входит в систему, компьютер полностью доступен для ИТ-службы, позволяя управлять конфигурацией и настройками безопасности, как будто компьютер был связан непосредственно с корпоративной сетью.

Протокол удаленного рабочего стола (RDP)

Протокол удаленного рабочего стола (Remote Desktop Protocol – RDP) - протокол прикладного уровня, купленный Microsoft у Citrix, использующийся для обеспечения удалённой работы пользователя с сервером, на котором запущен сервис терминальных подключений. Клиенты существуют практически для всех версий Windows (включая Windows CE и Mobile), Linux, FreeBSD, Mac OS X, Android, Symbian. По умолчанию используется порт TCP 3389. Официальное название Майкрософт для клиентского ПО — Remote Desktop Connection или Terminal Services Client (TSC).

С помощью протокола RDP пользователи могут подключаться к удаленным компьютерам и серверам и использовать внутренние сетевые ресурсы и запускать прикладные программы, как рабочее станции внутри компании.

Подключение небольшого офиса

Для подключения небольшого или домашнего офиса можно применять такие технологии доступа:

- Телефонная сеть общего назначения (PSTN)
- Цифровая абонентская линия (DSL)
  - Симметричная линия (SDSL)
  - Асимметричная линия (ADSL)
- Кабельный модем
- Спутниковая связь
  - Односторонняя (обратная связь по модему)
  - Двусторонняя
- Беспроводная связь
- Сотовая связь 3G/4G

Протоколы и службы удаленного доступа:

- Служба удаленного доступа (Remote Access Service – RAS)
  - Клиент удаленного доступа (Remote Access Client)

    - Сервер удаленного доступа (Remote Access Server)
- Протокол точка-точка (Point-to-Point Protocol – PPP)
- Межсетевой протокол по последовательным линиям (Serial Line Internet Protocol – SLIP)
- Виртуальная частная сеть (Virtual Private Network – VPN)
    - Соединение сервер-сервер
- Протокол точка-точка поверх Ethernet (Point-to-Point Protocol over Ethernet – PPPoE)
- Туннелированный протокол точка-точка (Point-to-Point Tunneling Protocol – PPTP)

Подключение к глобальным сетям

Два типа подключения к глобальным сетям:

- Выделенное подключение
- Коммутируемое подключение:
    - Коммутация каналов
    - Коммутация пакетов

Технологии глобального доступа:

- Операторские системы E- и T-классов (E1/T1/J1 и E3/T3/J3)
- X.25
- Цифровая сеть с интегрированными услугами (Integrated Service Digital Network – ISDN)
- Синхронная оптическая сеть (Synchronous Optical Network – SONET) и стандарты оптических операторов (Optical Carrier – OCx)

6. Беспроводные сети

Типы беспроводных сетей

Большинство беспроводных компьютерных радио-сетей попадают под действие стандартов 802.11. Наиболее распространенными являются:

- 802.11a
- 802.11b
- 802.11g
- 802.11n

В дополнение к беспроводным сетям с использованием радиоволн применяются и некоторые другие среды передачи сигнала без проводов:

- Микроволны
- Инфракрасное излучение
- Радиоволны близкого радиуса действия (Bluetooth, ZigBee)

802.11a

IEEE 802.11a — стандарт сетей Wi-Fi. Использует частотный диапазон 5 ГГц. Это не первый стандарт, как можно было бы подумать по буквенному индексу – первым является 802.11b.

Несмотря на то, что эта версия используется не так часто из-за стандартизации IEEE 802.11b и внедрения 802.11g, она также претерпела изменения в плане частоты и модуляции. Мультиплексирование с ортогональным частотным разделением каналов (Orthogonal frequency-division multiplexing —OFDM) позволяет передавать данные параллельно на множественных подчастотах. Это позволяет повысить устойчивость к помехам и поскольку отправляется более одного потока данных, реализуется высокая пропускная способность.

IEEE 802.11a может развивать скорость вплоть до 54 Мб/с в идеальных условиях. В менее идеальных условиях (или при чистом сигнале) устройства могут вести связь со скоростью 48 Мб/с, 36 Мб/с, 24 Мб/с, 18 Мб/с, 12 Мб/с и 6 Мб/с.

Из-за высокой частоты сигналу трудно преодолевать препятствия, встречающиеся на пути, такие как стены или другие большие предметы, поэтому лучшее соединение обеспечивается лишь в пределах прямой видимости устройств.

Высокая стоимость, короткая дистанция и необходимость прямой видимости сузили применимость этого стандарта, несмотря на его более высокую пропускную способность.

Стандарт IEEE 802.11a несовместим с 802.11b и 802.11g.

802.11b

Стандарт IEEE 802.11b, принятый в 1999 году, является одним из первых стандартов для беспроводных сетей. В нем используется технология широкополосной модуляции с прямым расширением спектра (Direct Sequence Spread Spectrum - DSSS точнее, его улучшенная версия HR-DSSS) против OFDM в 802.11a. Стандарт предусматривает использование нелицензируемого диапазона частот 2,4 ГГц. Скорость передачи до 11 Мбит/с.

Продукты стандарта IEEE 802.11b, поставляемые разными изготовителями, тестируются на совместимость и сертифицируются организацией Wireless Ethernet Compatibility Alliance (WECA), которая в настоящее время больше известна под названием Wi-Fi Alliance. Совместимые беспроводные продукты, прошедшие испытания по программе «Альянса Wi-Fi», могут быть маркированы знаком Wi-Fi.

Долгое время IEEE 802.11b был распространённым стандартом, на базе которого было построено большинство беспроводных локальных сетей. Сейчас его место занял стандарт G, постепенно вытесняемый более совершенным N.

802.11g

Проект стандарта IEEE 802.11g был утверждён в октябре 2002 г. Этот стандарт предусматривает использование диапазона частот 2,4 ГГц, обеспечивая скорость соединения 54 Мбит/с и превосходя, таким образом, стандарт IEEE 802.11b, который обеспечивает скорость соединения 11 Мбит/с. Кроме того, он гарантирует обратную совместимость со стандартом 802.11b. Обратная совместимость стандарта IEEE 802.11g может быть реализована в режиме модуляции DSSS, и тогда скорость соединения будет ограничена одиннадцатью мегабитами в секунду либо в режиме модуляции OFDM, при котором скорость составляет 54 Мбит/с.

Следующая таблица (табл. 6.1) представляет сравнительные характеристики стандартов 802.11 a, b и g.

Таблица 6.1. Сравнительные характеристики стандартов 802.11.

Стандарт	Скорость	Частота	Тип передачи
802.11a	54 Мбит/с	5 ГГц	OFDM
802.11b	11 Мбит/с	2,4 ГГц	DSSS
802.11g	54 Мбит/с	2,4 ГГц	OFDM – выше 20 Мбит/с DSSS – ниже 20 Мбит/с

802.11n

Стандарт 802.11n повышает скорость передачи данных практически вчетверо по сравнению с устройствами стандартов 802.11g (максимальная скорость которых равна 54 Мбит/с), при условии использования в режиме 802.11n с другими устройствами 802.11n. Теоретически 802.11n способен обеспечить скорость передачи данных до 600 Мбит/с, применяя передачу данных сразу по четырем антеннам. По одной антенне — до 150 Мбит/с.

Устройства 802.11n работают в диапазонах 2,4—2,5 или 5,0 ГГц.

Кроме того, устройства 802.11n могут работать в трёх режимах:

- наследуемом (Legacy), в котором обеспечивается поддержка устройств 802.11b/g и 802.11a;
- смешанном (Mixed), в котором поддерживаются устройства 802.11b/g, 802.11a и 802.11n;
- «чистом» режиме — 802.11n (именно в этом режиме и можно воспользоваться преимуществами повышенной скорости и увеличенной дальностью передачи данных, обеспечиваемыми стандартом 802.11n).

Ключевой компонент стандарта 802.11n под названием MIMO (Multiple Input, Multiple Output — много входов, много выходов) предусматривает применение пространственного мультиплексирования с целью одновременной передачи нескольких информационных потоков по одному каналу, а также многолучевое отражение, которое обеспечивает доставку каждого бита информации соответствующему получателю с небольшой вероятностью влияния помех и потерь данных. Именно возможность одновременной передачи и приема данных определяет высокую пропускную способность устройств 802.11n.

Общие характеристики беспроводных сетей

Топология

Беспроводные радиосети могут различаться по размеру охватываемой ими территории. Часто такую территорию называют ячейкой или сотой (рис. 6.1). Каждая такая ячейка представляет область сети, где действует определенное соединение. В зависимости от размеров площади, покрываемой излучением передающей станции, такие ячейки делятся на:

- Соты
- Микросоты
- Фемтосоты

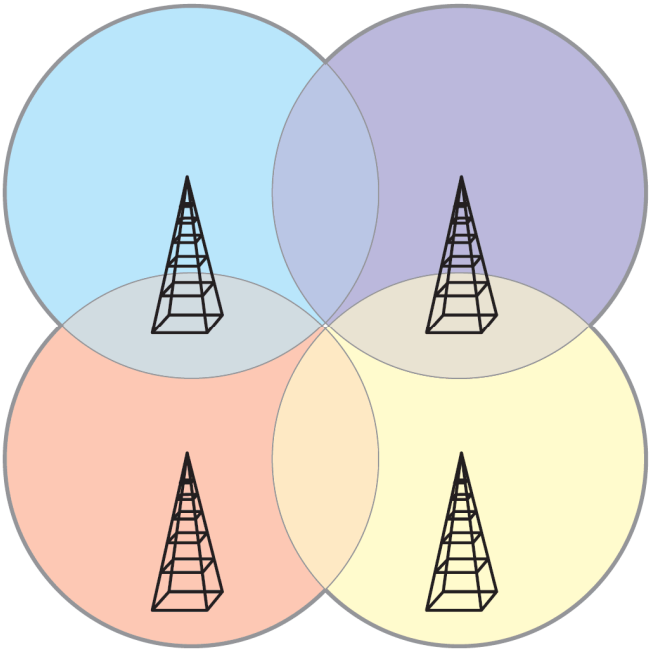

Рис. 6.1. Беспроводная ячеистая топология

Базовые станции могут соединяться друг с другом либо посредством радиосигнала, тогда такая связь называется мостом, либо проводами с помощью коммутаторов. В любом случае беспроводная топология зависит не от межсоединительных кабелей, а от взаимного расположения базовых станций.

При этом беспроводные устройства могут перемещаться из одной ячейки в другую и оставаться на связи.

Беспроводные устройства

Есть несколько типов периферийного оборудования, которые обеспечивают беспроводные соединения:

- Беспроводный адаптер
- Точка беспроводного доступа (Wireless Access Point – WAP)
- Беспроводный мост
  - Точка-точка
  - Точка-многоточка

Беспроводный адаптер

Беспроводный адаптер обеспечивает соединение между материнской платой компьютера и беспроводной сетью. В принципе беспроводный адаптер является ни чем иным, как сетевой картой для беспроводных сетей.

Беспроводные адаптеры могут быть как внутренними, так и внешними устройствами. Внутренние адаптеры могут встраиваться в материнскую плату и часто встречаются в ноутбуках и других мобильных устройствах. Внешние адаптеры могут подключаться к компьютеру через USB-порт или PCMCIA- или CardBus-разъем.

Точка беспроводного доступа (Wireless Access Point – WAP)

Точка беспроводного доступа (Wireless Access Point – WAP) применяется для подключения одного или более беспроводных устройств к проводной сети, а также координирует работу беспроводных устройств между собой.

Точка беспроводного доступа обеспечивает соединение с проводной сетью, так что каждый клиент может получить доступ к серверным ресурсам и другим клиентам в сети.

Точка доступа может обслуживать несколько клиентов. Количество клиентов зависит от числа и типа передающих средств.

Поскольку большинство точек доступа не могут взаимодействовать друг с другом напрямую, то для соединения двух беспроводных ячеек в одну сеть требует применения беспроводного моста.

Простейшая точка беспроводного доступа по сути является концентратором, работающим на 1-м уровне модели ВОС (OSI). Большинство современных точек доступа сочетают в себе функции концентратора, моста, коммутатора и маршрутизатора и даже брандмауэра, работающих на нескольких уровнях модели ВОС (OSI).

Беспроводный мост

Беспроводный мост используется для соединения нескольких беспроводных сегментов сетей друг с другом. Действует он точно так же как и проводные мосты.

Беспроводные мосты делятся на две категории:

- Точка-точка. Мосты точка-точка могут соединяться только с одним другим мостом для объединения всего двух сегментов друг с другом.
- Точка-многоточка. Мосты точка-многоточка могут соединяться с более чем одним мостом, что они служат для объединения нескольких сегментов друг с другом.

Безопасность беспроводных сетей

Поскольку данных в беспроводных сетях чаще распространяются электромагнитным излучением вокруг, а не передаются по определенной фиксированной среде передачи данных, то, в общем, беспроводные сети менее защищены, чем проводные или оптоволоконные сети.

Для обеспечения безопасности беспроводных сетей надо знать:

- Идентификатор сети (Service Set Identifier – SSID)
- Фильтрация MAC-адресов
- Шифрование данных
    - Wired Equivalent Privacy (WEP)
    - Wi-Fi Protected Access (WPA)
    - Advanced Encryption Standard (AES)
- Управление доступом по стандарту 802.1x

Поиск и устранение проблем в беспроводных сетях

Проблемы, которые могут возникнуть в беспроводных сетях можно сгруппировать в следующие категории:

- Аппаратные проблемы
- Программные проблемы
- Проблемы связи

Аппаратные проблемы

Большинство аппаратных проблем в беспроводных сетях являются результатом неправильной инсталляции или сбоя оборудования.

Перед тем как заменить или переконфигурировать устройство, сначала стоить проверить следующее:

- Проверьте физические соединения
- Проверьте беспроводной адаптер

Программные проблемы

Среди основных проблем беспроводных сетей, связанных с программным обеспечением можно выделить:

- Проблемы микропрограммного обеспечения
- Проблемы драйвера

Проблемы связи

Проблемы со связью чаще всего возникают из-за:

- Интерференции
- Большого расстояния
- Состояния ближайшего окружения (стены, погода, статическое электричество)
- Конфигурационных ошибок

7. Сетевые протоколы

Сетевой протокол определяет набор правил передачи данных по сети. Сетевые протоколы задают различные аспекты передачи данных, включая как, когда и сколько данных может быть отправлено по сети.

Не так давно распространенными протоколами являлись:

- Transmission Control Protocol / Internet Protocol - TCP/IP
- Internetwork Packet eXchange / Sequenced Packet eXchange - IPX/SPX
- NetBIOS Extended User Interface - NetBEUI
- AppleTalk

Сейчас наибольшее распространение получил протокол IPv4, а IPv6 идет ему на замену, но не очень быстрыми темпами.

Internetwork Packet eXchange / Sequenced Packet eXchange

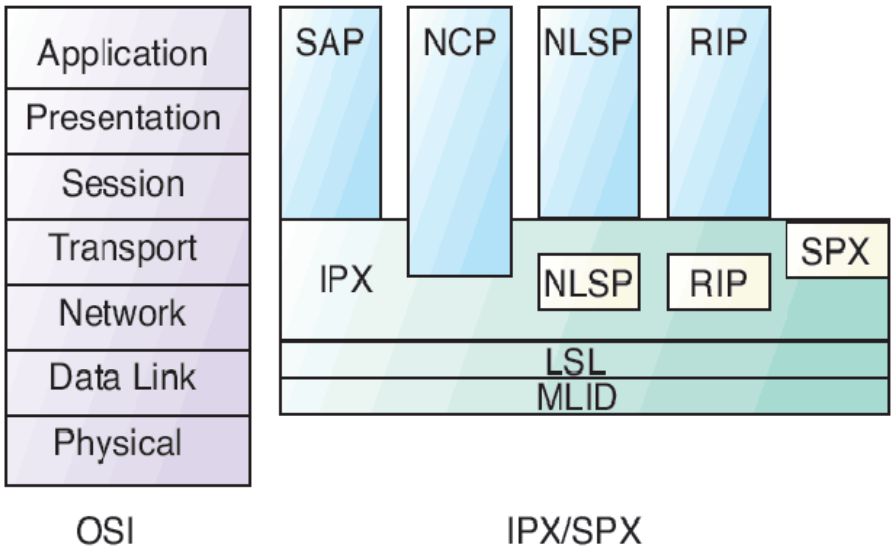

Рис. 7.1. Internetwork Packet eXchange / Sequenced Packet eXchange

На рисунке 7.1. представлено соотношение модели МОС/ВОС и стека протоколов IPX/SPX.

Протоколы нижнего уровня:

- Multiple Link Interface Driver (MLID)
- Link Support Layer (LSL)

Протоколы среднего уровня:

- Internetwork Packet eXchange (IPX)
- Sequenced Packet eXchange (SPX)
- Routing Information Protocol (RIP)
- NetWare Link Services Protocol (NLSP)

Протоколы верхнего уровня:

- NetWare Core Protocol (NCP)
- Service Advertising Protocol (SAP)

Протокол NetBEUI

NetBEUI (NetBIOS Extended User Interface) — расширенный пользовательский интерфейс дейтаграммной передачи NetBIOS. В середине 1990-х годов широко использовался для небольших ЛВС, затем постепенно был вытеснен TCP/IP.

Комбинированный протокол L3/L4, используемый как механизм передачи для NetBIOS на основе широковещательных рассылок. Этот протокол является реализацией стандарта NetBIOS.

Транспортной частью NetBEUI является NBF (NetBIOS Frame Protocol). Сейчас вместо NetBEUI обычно применяется NetBIOS over TCP/IP (NBT), так как поддержка NetBEUI в Windows прекращена с Windows 2003. Samba (SMB-

файловый сервер под Unix) имеет только реализацию NBT, не поддерживая ни IPX, ни NetBEUI.

Протокол NetBEUI вследствие своей примитивности требует меньше всего ресурсов и обеспечивает наивысшую скорость работы, но из-за ряда присущих ему недостатков, таких как невозможность маршрутизации и сильная зашумлённость в большой сети, NetBEUI можно эффективно использовать только в небольших локальных сетях (IBM разработала протокол NetBEUI для локальных сетей, содержащих порядка 20 — 200 рабочих станций). Так как NetBEUI не маршрутизируемый, то он не позволяет создавать глобальные сети, объединяя несколько локальных сетей. Сети, основанные на протоколе NetBEUI, легко реализуются, но их трудно расширять, так как протокол NetBEUI не маршрутизируемый.

Протокол AppleTalk

AppleTalk — это стек протоколов, разработанных Apple Computer для компьютерной сети. Он был изначально включён в Macintosh (1984), сейчас компания отказалась от него в пользу TCP/IP (рис. 7.2).

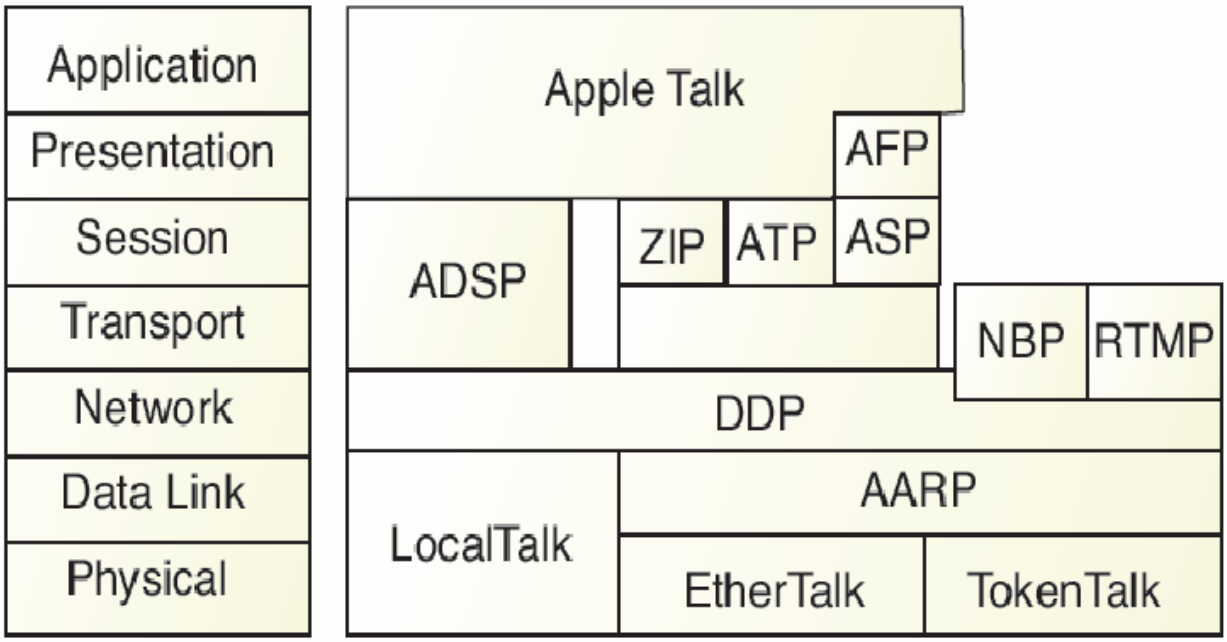

Рис. 7.2. Протокол AppleTalk

Протоколы маршрутизации

Протоколы маршрутизации служат для обмена информацией об известных или действующих маршрутах между маршрутизаторами. Обмениваясь такой информацией друг с другом, маршрутизаторы строят карту маршрутов для достижения той или иной сети. Получив пакет, который требует пересылки в другую сеть, маршрутизатор анализирует свою карту и направляет пакет по одному из известных ему маршрутов. Для выбора пути маршрутизатор руководствуется множеством параметров, таких, как скорость соединения, стоимость передачи пакета, общая длина маршрута, его загруженность и т.д.

В сетях часто можно встретить два основных типа протоколов маршрутизации:

- На основе метода вектора расстояния – RIP;
- С учетом состояния канала связи – OSPF и NLSP.

Routing Information Protocol – RIP

Протокол маршрутной информации (Routing Information Protocol - RIP) — один из протоколов маршрутизации. Применяется в небольших компьютерных сетях, позволяет маршрутизаторам динамически обновлять маршрутную информацию (направление и дальность в переходах (hop)), получая ее от соседних маршрутизаторов. При выборе маршрута для пересылки пакета маршрутизатор выбирает маршрут с наименьшим количеством переходов (маршрутизаторов) до сети назначения.

Максимальное количество переходов, разрешенное в RIP — 15 (метрика 16 означает «бесконечно большую метрику»). Каждый RIP-маршрутизатор по умолчанию вещает в сеть свою полную таблицу маршрутизации раз в 30 секунд, довольно сильно нагружая низкоскоростные линии связи. RIP работает на прикладном уровне стека TCP/IP, используя UDP порт 520.

В современных сетевых средах RIP — не самое лучшее решение для выбора в качестве протокола маршрутизации, так как его возможности уступают более современным протоколам, таким как EIGRP, OSPF. Ограничение на 15 переходов не дает применять его в больших сетях. Преимущество этого протокола — простота конфигурирования.

Этот протокол маршрутизации был реализован для протоколов IPX/SPX и TCP/IP.

Алгоритм маршрутизации RIP (алгоритм Беллмана — Форда) был впервые разработан в 1969 году, как основной для сети ARPANET.

В 1994 году был разработан протокол RIP2 (RFC 2453), который является расширением протокола RIP, обеспечивающим передачу дополнительной маршрутной информации в сообщениях RIP и повышающим уровень безопасности.

Для работы в среде IPv6 была разработана версия RIPng.

NetWare Link Services Protocol – NLSP

NetWare Link Services Protocol (NLSP) - протокол маршрутизации с учетом состояния канала связи (link state). Он предназначен, в первую очередь, для больших сетей IPX/SPX, где RIP уже не справлялся.

NLSP более совершенный протокол маршрутизации, чем RIP, и в дополнение к такому параметру, как метрика расстояния, в расчет принималось состояние канала связи, скорость интерфейса и объем трафика.

Также преимуществом этого протокола была быстрая сходимость (т.е. распространение информации о сетевых связях), реагирование на изменение состояния канала и компактные таблицы маршрутизации.

Open Shortest Path First – OSPF

Open Shortest Path First (OSPF) [7] — протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (link-state technology) и использующий для нахождения кратчайшего пути Алгоритм Дейкстры (Dijkstra’s algorithm).

Протокол OSPF был разработан IETF в 1988 году. Последняя версия протокола представлена в RFC 2328. Протокол OSPF представляет собой протокол внутреннего шлюза (Interior Gateway Protocol — IGP). Протокол OSPF распространяет информацию о доступных маршрутах между маршрутизаторами одной автономной системы.

OSPF – протокол маршрутизации с учетом состояния канала связи для TCP/IP.

OSPF имеет следующие преимущества:

- Высокая скорость сходимости по сравнению с дистанционно-векторными протоколами маршрутизации;
- Поддержка сетевых масок переменной длины (VLSM);
- Оптимальное использование пропускной способности (т. к. строится минимальный остовный граф по алгоритму Дейкстры).

Протоколы оповещения о сетевых сервисах

Для того, чтобы клиенты и сетевые устройства могли узнавать о предлагаемых сервисах в сети и находить соответствующие серверы, существуют протоколы оповещения о сервисах.

Такие протоколы позволяют создавать самонастраивающееся клиентское программное обеспечение и позволяют выбирать пользователю необходимые ему сетевые услуги из готового списка.

Service Advertising Protocol (SAP)

Протокол оповещения о сервисах (Service Advertising Protocol - SAP) позволяет серверам и маршрутизаторам в сети заявлять о своем присутствии и о предоставляемых ими сетевых сервисах. Это осуществляется путем создания и поддержания в актуальном состоянии серверной информационной таблицы, также известной как таблица сервисов. SAP работает на сеансовом и прикладном уровне модели ВОС (OSI).

Серверная информационная таблица содержит информацию о всех серверах в сети и об их предназначении, например, файловый сервер, сервер печати и т.д. Эта информация включает в себя название сервера, адреса и типы предоставляемых сервисов.

Клиенты могут получить эту информацию у ближайшего к себе SAP-маршрутизатора (которым может быть и сервер). SAP-маршрутизаторы периодически посылали широковещательные сообщения о своей сервисной таблице, так что клиенты и другие SAP-маршрутизаторы получали информацию о всех доступных сервисах в сети довольно оперативно (раз в 60 секунд).

SAP работал совместно с сетевым протоколом IPX/SPX.

Service Location Protocol (SLP)

В первых сетях TCP/IP предполагалось, что пользователи знают, где находятся те или иные сетевые ресурсы и сервисы. С ростом и широким распространением сетей TCP/IP возникла необходимость донести эти сведения до потреби-

телей сетевых услуг. Так появились разнообразные и независимые (и разрозненные) протоколы поиска сервисов в сетях на IP-протоколе.

Протокол обнаружения сервисов (Service Location Protocol - SLP) — протокол обнаружения сервисов, который позволяет компьютерам и иным устройствам находить сервисы в локальной вычислительной сети без предварительной конфигурации. SLP был разработан, чтобы работать как в небольших ненастраиваемых сетях, так и в больших корпоративых сетях. Он определен в RFC 2608.

SLP описывает три роли для устройств. Устройство может иметь две или даже три роли одновременно:

- User Agents (UA) — устройства, которые ищут сервисы
- Service Agents (SA) — устройства, анонсирующие один или несколько сервисов
- Directory Agents (DA) — устройства, кеширующие сервисы. Они используются в больших сетях для уменьшения количества трафика и позволяют SLP масштабироваться. Существование DA в сети является необязательным, но если он присутствует, то UA и SA должны использовать его вместо прямых коммуникаций.

Сейчас большинство реализаций действуют как UA и SA. Также они могут быть настроены для работы в качестве DA.

8. Стек протоколов TCP/IP

Стек протоколов TCP/IP состоит из множества протоколов, каждый их которых выполняет какую-то определенную функцию. Ниже перечислены некоторые из этих протоколов:

- Internet Protocol (IP)
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Internet Control Message Protocol (ICMP)
- Bootstrap Protocol (BOOTP)
- Address Resolution Protocol (ARP)
- Reverse Address Resolution Protocol (RARP)
- File Transfer Protocol (FTP)
- HyperText Transfer Protocol (HTTP)

Модели МОС/ВОС (ISO/OSI) и DoD

Протокол TCP/IP был разработан научным подразделением Министерства Обороны США (U.S. Department of Defense) до разработки эталонной модели взаимодействия открытых систем (МОС/ВОС). Но модели DoD и МОС/ВОС могут быть сопоставлены (рис. 8.1).

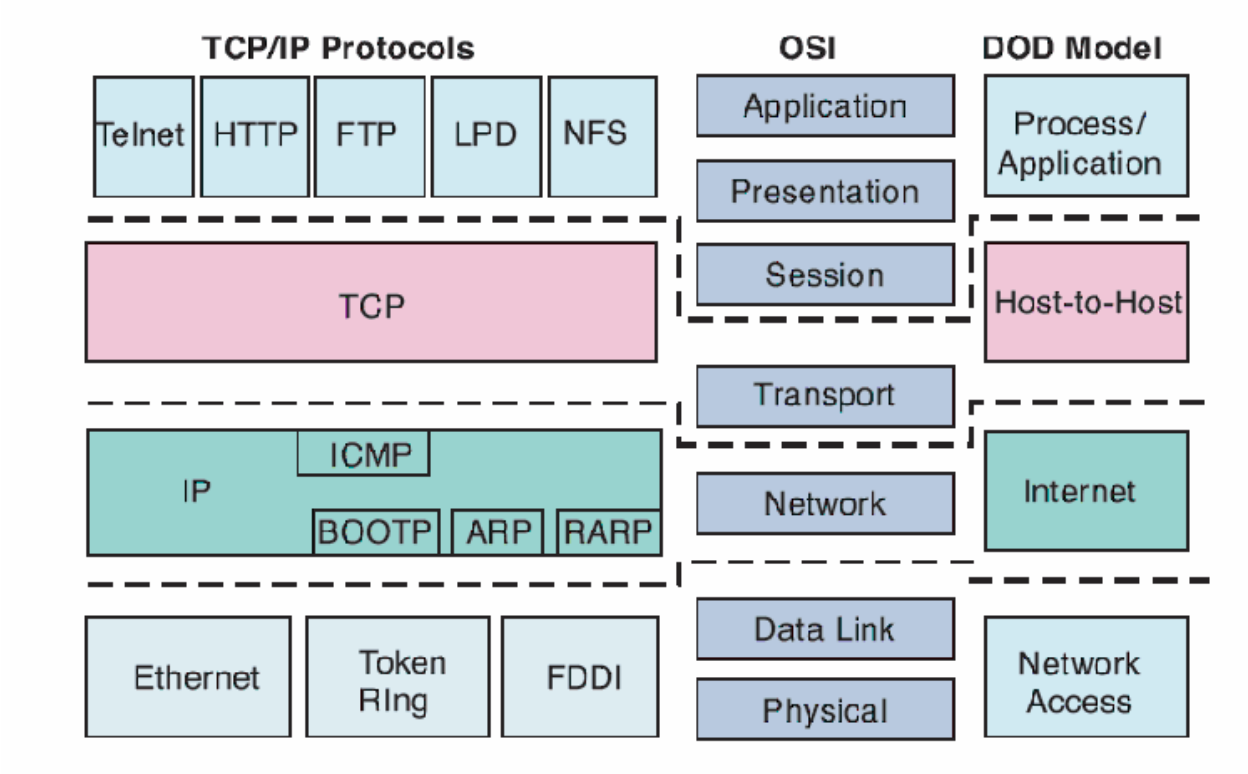

Рис. 8.1. TCP/IP на моделях MOC/BOC и DoD

Функции некоторых протоколов стека TCP/IP

Каждый из протоколов стека TCP/IP выполняю присущую ему функцию. Рассмотрим назначение некоторых из них.

Internet Protocol (IP)

Internet Protocol (IP) — межсетевой протокол. Относится к маршрутизируемым протоколам сетевого уровня семейства TCP/IP. IP предоставляет спецификации, которые позволяют осуществлять маршрутизацию, фрагментацию и последующую сборку пакетов. Неотъемлемой частью протокола является адресация сети.

IP объединяет сегменты сети в единую сеть, обеспечивая доставку данных между любыми узлами сети. Он классифицируется как протокол третьего уровня по сетевой модели OSI. IP не гарантирует надёжной доставки пакета до адресата. В частности, пакеты могут прийти не в том порядке, в котором были отправлены, продублироваться (приходят две копии одного пакета), оказаться повреждёнными (обычно повреждённые пакеты уничтожаются) или не прийти вовсе. Гарантию безошибочной доставки пакетов дают некоторые протоколы более высокого уровня — транспортного уровня сетевой модели OSI, — например, TCP, которые используют IP в качестве транспорта.

Internet Control Message Protocol (ICMP)

Протокол межсетевых управляющих сообщений ICMP (Internet Control Message Protocol) является обязательным стандартом TCP/IP, описанным в документе RFC 792, «Internet Control Message Protocol (ICMP)». Используя ICMP, узлы и маршрутизаторы, связывающиеся по протоколу IP, могут сообщать об ошибках

и обмениваться ограниченной управляющей информацией и сведениями о состоянии.

ICMP-сообщения обычно автоматически отправляются в следующих случаях:

- IP-дейтаграмма не может попасть к узлу назначения.
- IP-маршрутизатор (шлюз) не может перенаправлять дейтаграммы с текущей скоростью передачи.
- IP-маршрутизатор перенаправляет узел-отправитель на другой, более выгодный маршрут к узлу назначения.

Internet Group Management Protocol (IGMP)

Протокол управления группами Интернета (Internet Group Management Protocol - IGMP) — протокол управления групповой (multicast) передачей данных в сетях, основанных на протоколе IP. IGMP используется маршрутизаторами и IP-узлами для организации сетевых устройств в группы.

Этот протокол является частью спецификации групповой передачи пакетов в IP-сетях. IGMP расположен на сетевом уровне. Он во многом аналогичен ICMP для односторонней передачи.

Что такое многоадресная IP-рассылка

Многоадресный IP-трафик направляется по одному адресу, но обрабатывается несколькими узлами. Многоадресная IP-рассылка похожа на подписку на информационный бюллетень. Когда бюллетень выходит в свет, его получают только подписчики; аналогично, только узлы, входящие в группу многоадресной рассылки, получают и обрабатывают IP-трафик, посылаемый по зарезервированному IP-адресу группы. Набор узлов, принимающих трафик с данным многоадресным IP-адресом, называется группой многоадресной рассылки.

Вот другие важные характеристики многоадресной IP-рассылки.

- Членство в группах динамическое, что позволяет узлам присоединяться к группе и покидать ее в любое время.
- Присоединение узлов к группам многоадресной рассылки обеспечивается с помощью IGMP-сообщений.
- Группы не ограничены по размеру и их члены могут быть разбросаны по различным IP-сетям (если маршрутизаторы, которыми соединены эти сети, поддерживают распространение многоадресного IP-трафика и информации о членстве в группах).
- Узел может отправлять IP-трафик по IP-адресу группы, не будучи сам членом этой группы.

Адреса для многоадресной рассылки

IP-адреса для многоадресной рассылки зарезервированы и назначаются из диапазона адресов класса D: с 224.0.0.0 по 239.255.255.255. В следующей таблице 8.1 приведен частичный список адресов класса D, зарезервированных для

многоадресной IP-рассылки и зарегистрированных в IANA (Internet Assigned Numbers Authority).

Таблица 8.1. Адреса многоадресной рассылки.

IP-адрес для многоадресной рассылки	Описание
224.0.0.0	Базовый адрес (зарезервирован).
224.0.0.1	Многоадресная группа «All Hosts» (все узлы), содержащая все системы данного сегмента сети.
224.0.0.2	Многоадресная группа «All Routers» (все маршрутизаторы), содержащая все маршрутизаторы данного сегмента сети.
224.0.0.5	Адрес AllSPFRouters протокола OSPF (Open Shortest Path First). Используется для рассылки маршрутизирующей информации OSPF всем OSPF-маршрутизаторам сегмента сети.
224.0.0.6	Адрес AllDRouters протокола OSPF. Используется для рассылки маршрутизирующей информации OSPF выделенным OSPF-маршрутизаторам сегмента сети.
224.0.0.9	Групповой адрес протокола RIP версии 2. Используется для рассылки маршрутизирующей информации RIP всем RIP v2-маршрутизаторам сегмента сети.
224.0.1.24	Групповой адрес WINS-сервера. Используется для поддержки автоопределения и динамической настройки репликации WINS-серверов.

Address Resolution Protocol (ARP)

Протокол определения адреса (Address Resolution Protocol — ARP) — протокол канального уровня, предназначенный для определения MAC-адреса по известному IP-адресу. Наибольшее распространение этот протокол получил благодаря повсеместности сетей IP, построенных поверх Ethernet.

Существуют следующие типы сообщений ARP: запрос ARP (ARP request) и ответ ARP (ARP reply). Система-отправитель при помощи запроса ARP запрашивает физический адрес системы-получателя. Ответ (физический адрес узла-получателя) приходит в виде ответа ARP.

Перед тем как передать пакет сетевого уровня через сегмент Ethernet, сетевой стек проверяет кэш ARP, чтобы выяснить, не зарегистрирована ли в нём уже нужная информация об узле-получателе. Если такой записи в кэше ARP нет, то выполняется широковещательный запрос ARP. Этот запрос для устройств в сети имеет следующий смысл: «Кто-нибудь знает физический адрес устройства, обладающего следующим IP-адресом?» Когда получатель с этим IP-адресом примет этот пакет, то должен будет ответить: «Да, это мой IP-адрес. Мой физический адрес следующий: …» После этого отправитель обновит свой кэш ARP и будет способен передать информацию получателю.

Transmission Control Protocol (TCP)

Протокол управления передачей (Transmission Control Protocol - TCP) — один из основных сетевых протоколов Интернета, предназначенный для управления передачей данных в сетях и подсетях TCP/IP.

Выполняет функции протокола транспортного уровня модели OSI.

TCP — это транспортный механизм, предоставляющий поток данных, с предварительной установкой соединения, за счёт этого дающий уверенность в достоверности получаемых данных, осуществляет повторный запрос данных в случае потери данных и устраняет дублирование при получении двух копий одного пакета (см. также T/TCP). В отличие от UDP гарантирует целостность передаваемых данных и уведомление отправителя о результатах передачи.

Реализация TCP, как правило, встроена в ядро ОС, хотя есть и реализации TCP в контексте приложения.

Когда осуществляется передача от компьютера к компьютеру через Интернет, TCP работает на верхнем уровне между двумя конечными системами, например, браузером и веб-сервером. Также TCP осуществляет надежную передачу потока байтов от одной программы на некотором компьютере к другой программе на другом компьютере. Программы для электронной почты и обмена файлами используют TCP. TCP контролирует длину сообщения, скорость обмена сообщениями, сетевой трафик.

User Datagram Protocol (UDP)

Протокол пользовательских датаграмм (User Datagram Protocol — UDP) — один из ключевых элементов Internet Protocol Suite, набора сетевых протоколов для Интернета. С UDP, компьютерные приложения могут посылать сообщения (в данном случае называемые дейтаграммами) другим хостам по IP-сети без необходимости предварительного сообщения для установки специальных каналов передачи или путей данных. Протокол был разработан Дэвидом П. Ридом в 1980 году и официально определен в RFC 768.

UDP использует простую модель передачи, без установления соединения для обеспечения надежности, упорядочивания или целостности данных. Таким образом, UDP предоставляет ненадежный сервис, и дейтаграммы могут прийти не по порядку, дублироваться или вовсе исчезнуть без следа. UDP подразумевает, что проверка ошибок и исправление либо не необходимы, либо должны исполняться в приложении. Чувствительные ко времени приложения часто используют UDP, так как предпочтительнее сбросить пакеты, чем ждать задержавшиеся пакеты, что может оказаться невозможным в системах реального времени. При необходимости исправления ошибок на сетевом уровне интерфейса приложение может задействовать TCP, разработанный для этой цели.

Природа UDP как протокола без сохранения состояния также полезна для серверов, отвечающих на небольшие запросы от огромного числа клиентов, например DNS и потоковые мультимедийные приложения вроде IPTV, Voice over IP, протоколы туннелирования IP и многие онлайн-игры.

Функции порта

В стеке протоколов TCP/IP порт играет роль конечной точки логического соединения. Номер порта сопоставляется с сервисной программой, работающей

на сервере, к которой подключаются клиентские компьютеры. Поскольку на одном сервере может работать несколько служебных программ (сервисов), то для их идентификации служат списки зарегистрированных за программами портов, которые ведет Администрация адресного пространства Интернет (Internet Assigned Numbers Authority – IANA).

Диапазон портов простирается от 0 до 65536, при этом порты с 0 по 1024, являются зарезервированными для сервисов.

Протоколы прикладного уровня

DNS — система доменных имен

DHCP — Dynamic Host Configuration Protocol

FTP — протокол передачи файлов

Finger — протокол, возвращающий информацию о пользователях на удаленном компьютере

HTTP — Hypertext Transfer Protocol

IMAP — Internet Message Access Protocol

LDAP — Lightweight Directory Access Protocol

MIME — Multipurpose Internet Mail Extensions

NNTP — сетевой протокол передачи новостей

NTP — сетевой протокол времени

POP3 — почтовый протокол версии 3

RADIUS — протокол аутентификации, авторизации и работы с учетными записями записями

Rlogin — протокол удаленного входа в UNIX

rsync — протокол передачи файлов для резервного копирования, копирования и зеркалирования

RTP — Real-time Transport Protocol

RTSP — Real-time Transport Streaming Protocol

SSH — Secure Shell

SIP — Session Initiation Protocol, сигнальный протокол

SMTP — Simple Mail Transfer Protocol

SNMP — Simple Network Management Protocol

SOAP— Simple Object Access Protocol

Telnet — протокол удаленного доступа к терминалу

TFTP — Trivial File Transfer Protocol, простой протокол передачи файлов

WebDAV — Web Distributed Authoring and Versioning

Маршрутизация и протоколы маршрутизации

- Таблицы маршрутизации
- Статические маршруты
- Динамические маршруты
- Протоколы маршрутизации:
  - Routing Information Protocol (RIP)
  - Open Shortest Path First (OSPF)

9. IP v4

Ниже рассматривается IP протокол версии 4.

- Структура IP адреса
- Классы IP адресов
- IP адреса для частного применения
- Получение зарегистрированного адреса
- Методы присвоения IP-адреса
- Статическая адресация
- Динамическая адресация
- Самоназначенные адреса
- Получение доменного названия
- Способы преобразования названий узлов в IP-адреса
- Создание подсетей
- Создание надсетей (суперсетей) – бесклассовая междоменная маршрутизация
- Преобразование сетевых адресов (Network Address Translation – NAT)

Структура IP адреса

Адрес состоит из двух частей – номер сети и номер узла в сети. IP-адрес версии 4 имеет длину 4 байта и сейчас чаще записывается в виде четырех десятичных чисел, разделенных точками.

Кроме этого встречаются и такие варианты записи адреса:

Двоичное

10100100 00010111 00010001 10011110

Десятичное

164.23.17.158

Шестнадцатеричное

A4.17.11.9E

Адрес и маска подсети:

- Определяет уникальный идентификатор компьютера, т. е. идентификатор узла.
- Определяет подсеть, в которой находится компьютер, т. е. идентификатор подсети.
- Позволяет находящимся в сети компьютерам взаимодействовать друг с другом в среде с использованием маршрутизаторов.

Классы IP адресов

Для определения, какие байты принадлежат номеру сети, а какие номеру узла существует несколько подходов.

Одним из подходов был классовый метод адресации (таб. 9.1).

Таблица 9.1. Классы IP-адресов.

Класс	Первые биты	Наименьший номер	Наибольший номер
A	0	1.0.0.0	126.0.0.0
B	10	128.0.0.0	191.255.0.0
C	110	192.0.0.0	223.255.255.0
D	1110	224.0.0.0	239.255.255.255

E	11110	240.0.0.0	247.255.255.255

IP адреса для частного применения

К частным относятся IP-адреса из следующих сетей:

10.0.0.0/8

172.16.0.0/12

192.168.0.0/16

Также для внутреннего использования предназначены:

127.0.0.0/8

169.254.0.0/16 - Automatic Private IP Addressing (APIPA) используется для автоматической настройки сетевого интерфейса в случае отсутствия DHCP.

Получение зарегистрированного адреса

Организации, уполномоченные регистрировать адреса:

- ICANN
- IANA
- Национальные регистраторы

Internet Corporation for Assigned Names and Numbers, или ICANN — международная некоммерческая организация, созданная 18 сентября 1998 года при участии правительства США для регулирования вопросов, связанных с доменными именами, IP-адресами и прочими аспектами функционирования Интернета.

В рамках развития системы адресации корпорация ICANN последовательно расширяла список доменов общего пользования — сейчас их уже 18, тогда как в 1998 году было всего три (.com, .net, .org). С 2001 года корпорация внедрила доменные зоны .info, .biz, .name, .coop, .museum, .aero, .pro, .travel, .jobs, .cat, .asia, .eu, .mobi, .tel, .tv. При этом в ICANN намерены и в дальнейшем следовать политике расширения адресного пространства за счёт создания новых доменов верхнего уровня, в том числе с использованием символов национальных алфавитов.

На прошедшей в Каире 2-7 ноября 2008 года 33-й конференции ICANN было принято Решение о выделении России кириллического домена верхнего уровня «.рф»[8] . 4 февраля 2011 года IPv4 адреса стали подходить к концу. ICANN уже начала внедрять новую серию IPv6 адресов.

Internet Assigned Numbers Authority (IANA) — «Администрация адресного пространства Интернет» — американская некоммерческая организация, управляющая пространствами IP-адресов, доменов верхнего уровня, а также регистрирующая типы данных MIME и параметры прочих протоколов Интернета. Находится под контролем ICANN.

Координационный центр национального домена сети Интернет (сокращенное название - Координационный центр доменов RU/РФ) - это администратор национальных доменов верхнего уровня .RU и .РФ. Выполняет функции национальной регистратуры. Обладает полномочиями по выработке правил регистрации доменных имен в доменах .RU и .РФ, аккредитации регистраторов и исследованию перспективных проектов, связанных с развитием российских доменов верхнего уровня. Основной задачей Координационного центра является

обеспечение надежного и стабильного функционирования DNS-инфраструктуры российского сегмента сети Интернет.

Методы присвоения IP-адреса

Статическая адресация

Статическую конфигурацию IPv4-адреса можно вручную задать для любого компьютера сети. Типичные конфигурации протокола IPv4 включают следующие элементы.

- IPv4-адрес.
- Маска подсети.
- Шлюз по умолчанию.
- DNS-сервер.

Динамическая адресация

Протокол DHCPv4 позволяет автоматически задавать конфигурации IPv4-адресов для большого числа компьютеров без необходимости настраивать каждый компьютер отдельно. Служба DHCP получает запросы на настройку IPv4 от компьютеров, в параметрах которых указано, что они должны автоматически получать IPv4-адреса. Кроме того, она назначает IPv4-адреса из диапазонов, определенных для каждой из подсетей сети. Служба DHCP определяет подсеть, из которой получен запрос, и назначает IP-адрес из соответствующего диапазона.

Самоназначенные адреса

Automatic Private IP Addressing (APIPA) используется для автоматической настройки сетевого интерфейса в случае отсутствия DHCP. Это адреса из диапазона 169.254.0.0/16.

Получение доменного названия

Организации, уполномоченные регистрировать названия доменов:

- ICANN
- IANA
- Национальные регистраторы

Способы преобразования названий узлов в IP-адреса

Разрешение имен — это процесс преобразования имен компьютеров в IP-адреса. Разрешение имен — неотъемлемый компонент компьютерной сети, поскольку пользователям легче запоминать имена, чем такие абстрактные числа, как IPv4-адрес.

Файл Hosts

Файл Hosts содержит таблицу соответствий IP-адресов названиям узлов в сети. Это обычный текстовый файл, который находится на каждом компьютере, поэтому в больших сетях обновлять централизовано информацию в этих файлах затруднительно. Файл hosts загружается в кэш распознавателя DNS.

DNS

DNS — это служба, которая управляет разрешением имен узлов в IPадреса. Протокол TCP/IP определяет исходный и конечный компьютеры по их адресам IPv4 или IPv6. Однако, поскольку пользователям легче запоминать имена, чем

числа, IP-адресам компьютеров ставятся в соответствие понятные имена. Наиболее распространенный тип записи — название узла.

WINS

WINS предоставляет централизованную базу данных для регистрации динамических сопоставлений NetBIOS-имен, используемых в сети. Сохраняется поддержка WINS для обеспечения обратной совместимости.

LMHOSTS

Файл Lmhosts на всех компьютерах. Использование файла Lmhosts для разрешения NetBIOS-имен требует больших усилий по обслуживанию, поскольку этот файл необходимо поддерживать вручную на всех компьютерах.

Создание подсетей

Маски подсетей (рис. 9.1).

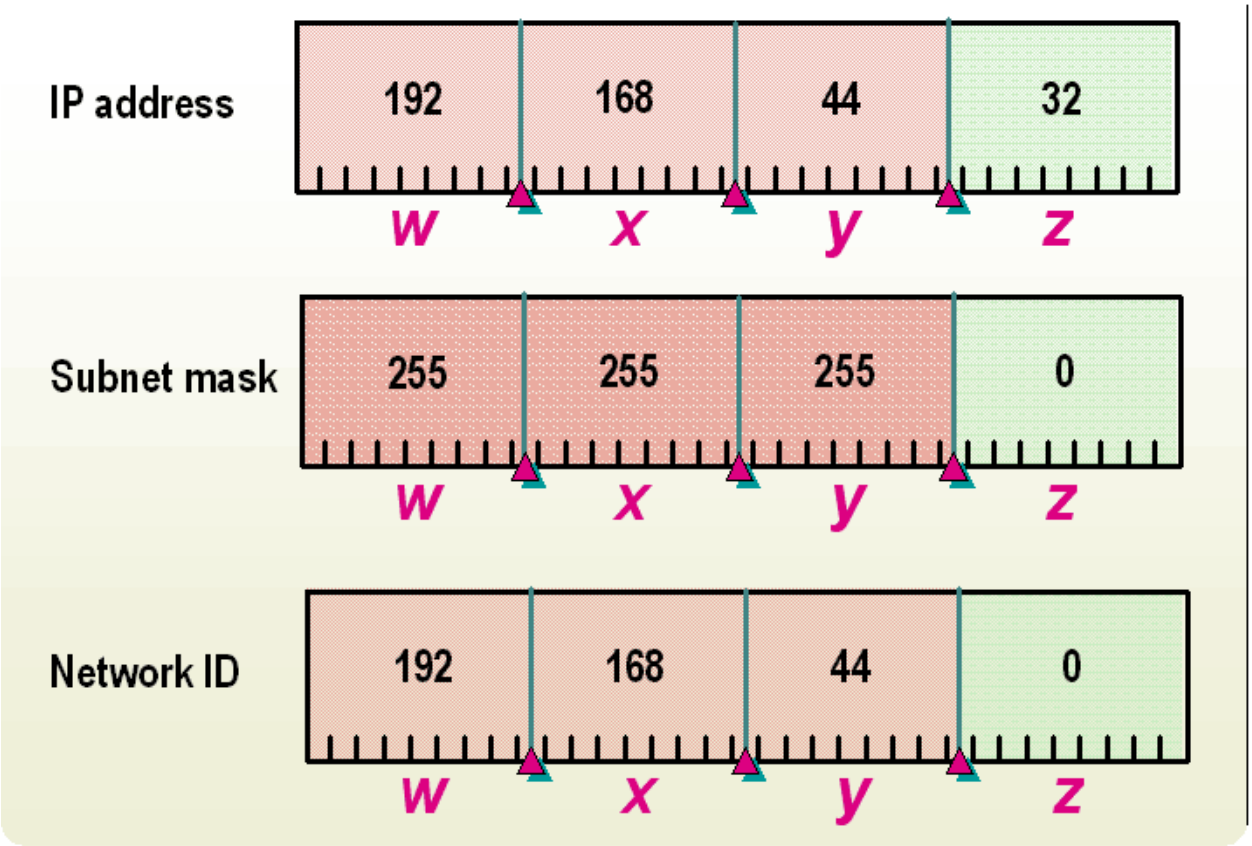

Рис. 9.1. Маска подсети

В простых сетях маски подсетей состоят из четырех октетов, каждый из которых имеет значение 255 или 0. Если октет равен 255, он является частью идентификатора сети. Если октет равен 0, он является частью идентификатора узла.

В сложных сетях маску подсети можно преобразовать в двоичный формат и использовать для определения маски каждый бит. Маска подсети состоит из непрерывных областей единиц и нулей. В левой части маски находится ряд единиц, который продолжается непрерывно, пока не сменится всеми нулями.

Идентификатор сети определяется положением единиц в маске подсети. Идентификатор узла определяется положением нулей. Все биты идентификатора узла, добавляемые к идентификатору сети, должны находиться непосредственно рядом с исходным идентификатором сети.

Каждый бит, равный 1, является частью идентификатора сети. Каждый бит, равный 0, является частью идентификатора узла. Математический процесс сравнения IP-адреса с маской подсети называется применением операции логического И.

Увеличение числа битов в маске подсети позволяет создать большее число подсетей, но уменьшает число узлов в каждой подсети. Использование большего числа битов, чем требуется, позволяет создавать новые подсети, но ограничивает возможности по созданию новых узлов. Использование меньшего числа битов, чем требуется, позволяет создавать новые узлы, но ограничивает возможности по созданию новых подсетей.

Можно рассчитать число битов в маске подсети, требуемое для конкретной сети. Воспользуйтесь формулой 2^n, где n — число битов. Она позволяет получить число подсетей, которое требуется создать в сети. Количество узлов рассчитывается по формуле 2^n-2, где n — число битов, оставшихся для номеров узлов.

Создание надсетей (суперсетей)

Бесклассовая междоменная маршрутизация (Classless Inter-Domain Routing - CIDR) не использует маски подсетей стандартной длины, как это было принято в сетях классов A, B и C, а задействует все 32-битное пространство IPv4-адреса и маски переменной длины. Для такого варианта более подходит тип записи, при котором указывается длина маски в битах, а не в явной десятичной или шестнадцатеричной нотации, например, 192.168.2.0/24, где число «24» означает 24 бита для маски подсети. Такой подход позволил не только увеличивать маску подсети, но и сокращать ее (по сравнению со стандартной маской), увеличивая тем самым количество узлов в одной подсети.

В методе CIDR используются объединение подсетей. Стратегия объединения подсетей состоит в объединении нескольких адресов среды с поклассовой адресацией в единый идентификатор сети среды с бесклассовой маршрутизацией. Благодаря данной методике, несколько смежных идентификаторов сети класса C объединяются в один идентификатор CIDR сети.

Преобразование сетевых адресов (Network Address Translation – NAT*)*

Преобразование сетевых адресов (Network Address Translation — NAT) — это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов. Также имеет названия IP Masquerading, Network Masquerading.

Основные причины, по которым NAT был задействован очень широко это:

- Исчерпание IP-адресов IPv4.
- Безопасность сетей

Исчерпание IP-адресов IPv4

Публичные сети классов A и B были выданы довольно давно и в последние годы можно было получить только сети класса C, емкости которых большим предприятиям было недостаточно. Позволяет сэкономить IP-адреса (только в случае использования NAT в режиме PAT), транслируя несколько внутренних IP-адресов в один внешний публичный IP-адрес (или в несколько, но меньшим

количеством, чем внутренних). По такому принципу построено большинство сетей в мире.

1 февраля 2011 года были распределены по региональным регистраторам последние блоки адресов IPv4. [2]

Безопасность сетей

NAT позволяет предотвратить или ограничить обращение снаружи ко внутренним хостам, оставляя возможность обращения изнутри наружу. При инициации соединения изнутри сети создаётся трансляция. Ответные пакеты, поступающие снаружи, соответствуют созданной трансляции и поэтому пропускаются. Если для пакетов, поступающих снаружи, соответствующей трансляции не существует (а она может быть созданной при инициации соединения или статической), они не пропускаются.

NAT позволяет скрыть внутреннюю структуру сети, выставляя наружу только один зарегистрированный IP-адрес. Так же может скрывать некоторые сервисы внутренних хостов/серверов. По сути, выполняется та же указанная выше трансляция на определённый порт, но возможно подменить внутренний порт официально зарегистрированной службы (например, 80-й порт TCP (HTTP-сервер) на внешний 30080-й).

10. IP v6

Эта глава рассматривает IP протокол версии 6 [9]. Новые функции IPv6-адресов позволяют обойти многие ограничения протокола IPv4. 6 июня 2012 года состоялся Всемирный запуск IPv6 [10]. С этого момента IPv6 переведен из опытного в эксплуатационный режим.

- Преимущества IPv6
- Структура IPv6 адреса
- Типы адресов IPv6
- IP адреса для частного применения
- Получение зарегистрированного адреса и доменного названия
- Методы присвоения IP-адреса
- Статическая адресация
- Динамическая адресация
- Самоназначенные адреса
- Способы преобразования названий узлов в IP-адреса
- Создание подсетей
- Сосуществование IPv4 и IPv6

Преимущества IPv6

Список новых возможностей, которые дают преимущество протоколу IPv6 приведен ниже:

- большее адресное пространство. Протокол IPv6 использует 128-битное адресное пространство, что значительно увеличивает число адресов по сравнению с IPv4;
- более эффективную маршрутизацию. Организация IANA предоставляет глобальные адреса Интернета для поддержки иерархической

маршрутизации. Это уменьшает число маршрутов, которое должно обрабатываться магистральными маршрутизаторами Интернета, и повышает эффективность маршрутизации;

- более простую настройку узлов. Протокол IPv6 поддерживает динамическую настройку клиентов с использованием протокола DHCPv6. Протокол IPv6 также позволяет маршрутизаторам динамически настраивать узлы;
- встроенные методы обеспечения безопасности. В IPv6 имеется встроенная поддержка IPsec. Это гарантирует, что все узлы будут шифровать передаваемые данные;
- усовершенствованная поддержка приоритетной доставки. В соответствии с протоколом IPv6 в заголовки пакетов включается метка потока, обеспечивающая поддержку приоритетной доставки. Это позволяет компьютерам обмениваться пакетами с различным уровнем приоритета, не полагаясь на номера портов, используемые приложениями. Кроме того, приоритет назначается пакетам, данные в которых шифруются с помощью IPsec.
- переработанный заголовок. Структура заголовка пакетов IPv6 является более эффективной с точки зрения обработки и расширяемости. В соответствии с протоколом IPv6 неважные и необязательные поля переносятся в расширенные заголовки для более эффективной обработки пакетов. Расширенные заголовки не превышают полный размер пакета IPv6, что позволяет включить в пакет больший объем информации по сравнению со стандартными 40-байтовыми заголовками пакетов IPv4.

Структура IP адреса

Адрес состоит из двух частей – номер сети и номер узла в сети. IP-адрес версии 6 имеет длину 16 байтов, записывается в виде серии четырех шестнадцатеричных чисел, разделенных двоеточиями.

2001:0db8:11a3:09d7:1f34:8a2e:07a0:765d

Чтобы еще больше сократить отображаемые IPv6-адреса, можно опустить нули в начале адреса или использовать уплотнение за счет нулей. Внутри каждой группы из четырех знаков можно опустить начальные нули и отображать группы из четырех нулей как один ноль. Уплотнение за счет нулей позволяет представлять несколько последовательных групп нулей в виде сдвоенных двоеточий. Пример представления приведен в таблице 10.1.

Таблица 10.1. Запись адреса IPv6.

Описание	Пример
Полный IPv6-адрес	2001:0DB8:0000:0000:02AA:00FF:FE28:9C5A/64
IPv6-адрес с опущенными начальными нулями	2001:DB8:0:0:2AA:FF:FE28:9C5A/64
IPv6-адрес, в котором опущены непрерывные группы нулей и началь-	2001:DB8::2AA:FF:FE28:9C5A/64

ные нули	

Типы адресов IPv6

Типы IPv6-адресов аналогичны типам IPv4-адресов.

Типы IPv6-адресов:

- Одноадресные. IPv6-адреса одноадресной рассылки эквивалентны IPv4-адресам одноадресной рассылки. Их можно использовать для передачи данных между узлами «один-к-одному». У каждого IPv6-узла имеется несколько адресов одноадресной рассылки. Имеется три типа адресов одноадресной рассылки:
  - глобальный адрес одноадресной рассылки. Он эквивалентен публичному IPv4-адресу. Эти адреса глобально маршрутизируемы и доступны в сегменте Интернета, работающем по протоколу IPv6;
  - публичная топология. Первые 48 бит глобального адреса одноадресной рассылки называются публичной топологией. Публичная топология является уникальной в масштабах всего Интернета. Это набор крупных и мелких поставщиков услуг Интернета, обеспечивающих доступ к Интернету по протоколу IPv6. Организация IANA назначает поставщикам услуг Интернета по одному уникальному адресу в глобальном префиксе маршрутизации;
  - топология сайта. Поставщик услуг Интернета может разделить сетевой адрес, полученный от IANA, на подсети, используя следующие 16 бит, которые называются топологией сайта. 16 бит топологии сайта позволяют поставщику услуг Интернета создать до 65536 подсетей максимально эффективным способом, соответствующим базе клиентов этого поставщика.
- локальные адреса каналов. Узлы используют локальные адреса каналов при взаимодействии с соседними узлами, использующими тот же канал. Например, в IPv6-сети с одним каналом и без маршрутизатора узлы взаимодействуют с помощью локальных адресов каналов.

Локальные IPv6-адреса каналов эквивалентны IPv4-адресам APIPA. В случае сбоя DHCP-серверов функция APIPA выделяет адреса в частном диапазоне от 169.254.0.1 до 169.254.255.254. Клиенты проверяют уникальность своих адресов в локальной сети с помощью протокола ARP. Когда у DHCP-сервера снова появляется возможность обрабатывать запросы, клиенты автоматически обновляют свои адреса.

Локальные адреса каналов также обладают следующими особенностями:

- локальные адреса каналов всегда начинаются с FE80.
- IPv6-маршрутизатор никогда не перенаправляет трафик локальных каналов за пределы этих каналов;
- адреса APIPA автоматически назначаются IPv4-узлам. Использование этих адресов ограничено взаимодействием внутри локальной подсети,

и они обычно применяются, когда другие подходящие адреса недоступны;

- уникальные локальные адреса одноадресной рассылки. Они эквивалентны частным адресным пространствам IPv4, например 10.0.0.0/8. Все уникальные локальные адреса одноадресной рассылки имеют префикс FD00::/8;
- глобальный идентификатор занимает следующие 40 бит. Глобальный идентификатор уникальным образом представляет организацию. Этот идентификатор следует создавать случайным образом, чтобы максимизировать уникальность организации. Это бывает полезно при слиянии двух организаций;
- При использовании уникальных глобальных идентификаторов маршрутизация между организациями происходит без изменения конфигурации сети. Следующие 16 бит следует использовать внутри организации, чтобы создавать подсети для маршрутизации между расположениями и внутри них. Выделенные 16 бит позволяют организации создать доя 65536 подсетей для внутреннего использования.
- Адреса произвольной рассылки. Адрес произвольной рассылки — это IPv6-адрес одноадресной рассылки, назначенный нескольким компьютерам. Если пакет отправляется на IPv6-адрес произвольной рассылки, отвечает только ближайший узел. Обычно такая рассылка используется для обнаружения служб или ближайшего маршрутизатора.
- Многоадресные. IPv6-адреса многоадресной рассылки эквивалентны IPv4-адресам многоадресной рассылки. Их следует использовать для отправки данных от одного компьютера множеству компьютеров, определенных с использованием такого же адреса многоадресной рассылки.

Согласно протоколу IPv4 узлу обычно назначался один адрес одноадресной рассылки. Но протокол IPv6 позволяет назначить каждому узлу несколько адресов одноадресной рассылки. Чтобы проверить процессы обмена данными по сети, необходимо знать, для каких целей в протоколе IPv6 используется каждый из этих адресов.

IP адреса для частного применения

К частным относятся IP-адреса локального интерфейса (link local).

Получение зарегистрированного адреса и доменного названия

Организации, уполномоченные регистрировать адреса и названия доменов:

- ICANN
- IANA
- Национальные регистраторы

Методы присвоения IP-адреса

- Статическая адресация
- Динамическая адресация

- Самоназначенные адреса

Статическая адресация

Статическую конфигурацию IPv6-адреса можно вручную задать для любого компьютера сети. Типичные конфигурации протокола IPv6 включают следующие элементы.

• IPv6-адрес
• Длину префикса
• Шлюз по умолчанию
• DNS-сервер

Динамическая адресация

DHCPv6 — это служба, обеспечивающая автонастройку узлов IPv6 с отслеживанием состояния. Она может автоматически предоставлять узлам IPv6 IPv6-адрес и другие сведения о конфигурации, например сведения о DNS-серверах. Эта служба эквивалентна службе DHCPv4

Самоназначенные адреса

Автонастройка — это метод автоматического назначения IPv6-адреса интерфейсу. Автонастройка может быть с отслеживанием состояния или без отслеживания состояния. Служба DHCPv6 обеспечивает автонастройку с отслеживанием состояния, а объявления RA (Router Advertisement) — настройку без отслеживания состояния.

Способы преобразования названий узлов в IP-адреса

Файл Hosts
DNS

Файл Hosts

Файл Hosts содержит таблицу соответствий IP-адресов названиям узлов в сети. Это обычный текстовый файл, который находится на каждом компьютере, поэтому в больших сетях обновлять централизовано информацию в этих файлах затруднительно. Файл hosts загружается в кэш распознавателя DNS.

DNS

DNS — это служба, которая управляет разрешением имен узлов в IPадреса. Протокол TCP/IP определяет исходный и конечный компьютеры по их адресам IPv4 или IPv6. Однако, поскольку пользователям легче запоминать имена, чем числа, IP-адресам компьютеров ставятся в соответствие понятные имена. Поскольку адреса IPv6 очень длинные и запомнить их еще труднее, то в сетях IPv6 серверы DNS будут эксплуатироваться очень интенсивно.

DNS серверы должны поддерживать новые адресные записи (AAAA) (обязательно) и записи указателей (PTR — Pointer) в обратном домене IP6.ARPA (необязательно). Кроме того, нужно обеспечить поддержку DNS-серверами динамических обновлений DNS для AAAA-записей, чтобы узлы IPv6 могли автоматически регистрировать свои имена и IPv6-адреса.

Создание подсетей

Для определения идентификатора сети в каждом IPv6-адресе используется префикс. Этот префикс можно использовать вместо маски подсети аналогично использованию бесклассовой междоменной маршрутизации в протоколе IPv4.

Префикс представляет собой прямую косую черту, после которой указывается число битов в идентификаторе сети. В приведенных в таблице 10.1 примерах этот префикс указывает, что идентификатор сети состоит из 64 бит.

В IPv6 для зарегистрированных адресов предусмотрен диапазон 16 бит для создания подсетей в компании, получившей зарегистрированный адрес сети, этого должно хватить на 65536 подсетей.

Сосуществование IPv4 и IPv6

Протокол IPv6 разрабатывался с учетом того, что он будет постепенно замещать протокол IPv4 на протяжении нескольких лет. Для этого были созданы несколько решений:

- **ISATAP**. Intra-Site Automatic Tunnel Addressing Protocol - Протокол автоматической внутрисайтовой адресации туннелей, позволяющий передавать между сетями IPv6 пакеты через сети IPv4
- **6to4**. 6to4 это переходный механизм, позволяющий передавать IPv6 пакеты через IPv4 сети, и не требующий создания двусторонних туннелей. Это, как правило, используется, когда конечный пользователь или сайт хотят получить соединение с IPv6 Интернетом, но не могут получить его от провайдера.
- **Teredo**. Teredo — сетевой протокол, предназначенный для передачи IPv6 пакетов через сети IPv4, в частности через устройства, работающие по технологии NAT, путём их инкапсуляции в UDP дейтаграммы.
- **PortProxy**. Сервис PortProxy – это шлюз уровня приложения для тех узлов, которые не поддерживают IPv6. PortProxy облегчает взаимодействие узлами или приложениями, которые не могут общаться по одному протоколу IPv4 или IPv6.

11. Обеспечение безопасности передачи данных

В этой главе рассматриваются вопросы сетевой безопасности, методы усиления защиты и роль различных протоколов в обеспечении безопасности [11].

Основные темы:

- Вопросы безопасности данных
- Определение методов обеспечения безопасности
- Протоколы аутентификации
- Протоколы безопасности
- Применение преобразования сетевых адресов (NAT)
- Выгоды использования виртуальных локальных сетей (VLAN)

Вопросы безопасности данных

Вопросы безопасности данных могут возникать из-за того, что неизвестные пользователи могут воздействовать на ваши коммуникации следующими способами:

- Прослушивание
- Выдавание себя за другого
- Изменение или подделка данных

- Вредоносные программы:
  - Вирусы
  - Черви
  - Троянские кони
  - Шпионские программы
  - Перехватчики клавиатуры
  - Перехватчики браузеров
  - «Звонилки»

Прослушивание

Практически все сетевые карты поддерживают возможность перехвата пакетов, передаваемых по общему каналу локальной сети. При этом рабочая станция может принимать пакеты, адресованные другим компьютерам того же сегмента сети. Таким образом, весь информационный обмен в сегменте сети становится доступным злоумышленнику. Для успешной реализации этой атаки компьютер злоумышленника должен располагаться в том же сегменте локальной сети, что и атакуемый компьютер. Прослушивание затруднено в сетях с коммутаторами (большинство современных сетей).

Прослушивание также может вестись в общедоступных сетях, например, Интернете, поэтому важные данные передают в зашифрованном виде и по шифрованным каналам, например, виртуальным частным сетям.

Выдавание себя за другого

Имперсонализация или кража цифровой личности - это действие направленное на совершение неправомочных действий сторонними лицами от имени другого (часто уполномоченного) пользователя.

Различают три формы имперсонализации:

- **Spoofing (мистификация, обман).** В этом случае один человек выдает себя за другого. В сетях обычно используются поддельные адреса источника.
- **Misrepresentation (неверное представление).** В этом случае человек или организация представляют себе тем, кем на самом деле не являются.
- **Phishing (выуживание).** Способ получения злоумышленниками учетных записей и паролей пользователей путем рассылки электронной почты от имени доверенных компаний или перенаправления пользователей на ложный вэб-сайт, очень похожий на оригинальный.

Изменение или подделка данных

Изменение или замена информации при передаче данных. Например, в заявке может быть увеличено число заказанного оборудования.

Вредоносные программы

Вредоносное программное обеспечение – это любые программы, которые скрытно устанавливаются на компьютере с целью испортить, похитить данные, нарушить работу компьютера, неправомочно использовать его ресурсы.

Вредоносные программы представляются в нескольких формах. Вот некоторые из них:

- Вирусы
- Черви
- Троянские кони
- Шпионские программы
- Перехватчики клавиатуры
- Перехватчики браузеров
- «Звонилки»

Определение методов обеспечения безопасности

Хэширование
Шифрование/расшифровка
Цифровая подпись
Цифровой сертификат
Антивирусные программы
Фильтрация или блокировка портов (брандмауэр)

Протоколы аутентификации

Password Authentication Protocol (PAP)
Challenge Handshake Authentication Protocol (CHAP)
Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)
Extensible Authentication Protocol (EAP)
Remote Authentication in Dial-In User Service (RADIUS)
Kerberos

Протоколы безопасности

IPSec
Secure Socket Layer (SSL)
Layer 2 Tunneling Protocol (L2TP)

Применение преобразования сетевых адресов (NAT)

NAT – это технология преобразования частных адресов для доступа в Интернет по одному зарегистрированному IP-адресу.

Скрывает внутреннюю организацию сети и уменьшает потребность в регистрированных IP-адресах.

NAT бывает:

- Статический
- Динамический

Выгоды использования виртуальных локальных сетей (VLAN)

Виртуальные локальные сети (VLAN) группируют компьютеры и сетевые ресурсы таким образом, что они взаимодействуют так, как будто находятся в одной сети, хотя могут находится в разных и изолируют эти группы друг от друга.

Виртуальные локальные сети (VLAN) предоставляют такие удобства:

- Гибкая сегментация
- Упрощенное администрирование
- Лучшая производительность

- Усиленная сетевая безопасность

12. Методы защиты сетей

Сетевая безопасность подвергается атакам происходящими из Интернета, так и из внутренней сети компании. Организациям важно обеспечивать безопасность сети, защищая свои сети от нарушителей.

Можно внедрить сетевую защиту с помощью:

- Брандмауэра
- Прокси-сервера
- Безопасности для сетевых ресурсов

Брандмауэр

Брандмауэр (еще межсетевой или сетевой экран) — комплекс программно-аппаратных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

Основной задачей брандмауэра является защита компьютерных сетей или отдельных узлов от несанкционированного доступа.

Различные виды брандмауэров могут работать на разных уровнях модели ВОС (OSI). В простых вариантах межсетевые экраны называют фильтрами, так как их основная задача — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации.

Некоторые сетевые экраны также позволяют осуществлять трансляцию адресов — динамическую замену внутрисетевых (для частного применения) адресов или портов на внешние, используемые за пределами ЛВС.

Основные функции брандмауэра:

- Фильтрация коммуникаций
- Блокировка портов
- Блокировка IP-адресов источников
- Аудит сетевого трафика

Рекомендации по внедрению брандмауэра:

- Исключите нежелательные регистрации
- Защищайте все входящие порты
- Знайте и понимайте возможные ограниченности функционала

Брандмауэр не является защитой от всех угроз для сети. В частности, он:

- не может защищать узлы сети от проникновения через «люки» (back doors) или уязвимости ПО;
- не обеспечивает защиту от многих внутренних угроз, в первую очередь — утечки данных;
- не защищает от вредоносных программ, в том числе вирусов;
- не может защищать от абсолютно новых угроз.

Прокси-сервер

Большинство домашних и небольших офисных сетей используют удаленное соединение или соединение с помощью модема для подключения к поставщику

услуг Интернета, который, в свою очередь, подключает их к Интернету. Поставщик услуг Интернета выделяет каждой сети единственный IP-адрес для подключения к Интернету. Кроме того, каждому компьютеру в сети требуется IP-адрес для подключения к Интернету. Вместо того, чтобы использовать отдельный IP-адрес для каждого компьютера, экономически более выгодно использовать один IP-адрес для нескольких компьютеров. Прокси-сервер - это компонент брандмауэра, который позволяет подключать к Интернету несколько объединенных в сеть компьютеров с использованием единственного IP-адреса.

Прокси-серверы выполняют две основные функции: повышение быстродействия сети и фильтрацию клиентских запросов.

- **Повышение быстродействия.** Прокси-серверы уменьшают время, требующееся для ответа на запросы, сделанные группой пользователей. Это происходит благодаря тому, что прокси-сервер кэширует, или сохраняет, результаты всех запросов, сделанных в течение определенного промежутка времени. Если пользователю требуется повторно вывести запрошенную ранее веб-страницу, прокси-сервер просто возвращает эту страницу, а не пересылает запрос на веб-сервер с последующей повторной загрузкой этой страницы.
- **Фильтрация клиентских запросов.** Прокси-серверы можно также использовать для фильтрации клиентских запросов на определенные подключения к Интернету. Например, компания может использовать прокси-сервер для того, чтобы исключить возможность подключения к определенным веб-узлам для своих служащих.

Основные преимущества сервера-посредника (прокси-сервера):

- Улучшенная производительность сети
- Фильтрация запросов
- Слежение за использованием Интернет
- Обеспечение сетевой безопасности
- Упрощение администрирования
- Фильтрация содержимого

Безопасность для сетевых ресурсов

В дополнение к брандмауэрам и прокси-серверам для защиты сети стоит ввести средства защиты для сетевых ресурсов.

Обеспечение целостности и безопасности данных является фундаментальной функцией сети. Первым уровнем безопасности данных в сетевой среде является назначение пользователям и группам соответствующих разрешений для ресурсов, к которым им необходимо получить доступ.

В зависимости от места применения средств защиты они относятся к двум моделям:

- Защита на уровне ресурсов
- Защита на уровне пользователей

Защита на уровне ресурсов

Если к сетевому ресурсу открывается общий доступ (доступ из любого другого места в сети), этому ресурсу назначается отдельный набор разрешений, который управляет доступом к соответствующим свойствам или функциям этого ресурса с сетевых компьютеров.

В одноранговых сетях, где нет централизованной системы управления, каждому общему ресурсу приходится присваивать индивидуальный набор разрешения для его использования. В этом случае ведется локальный учет внешних пользователей и их прав доступа. Часто для подключения к такому ресурсу требуется ввести пароль, который владелец ресурса предоставляет своим потенциальным потребителям.

Защита на уровне пользователей

В сетях с централизованной системой управления учетные записи пользователей, ресурсов и распределение прав доступа к ним ведутся центральной базой данных специального назначения, еще называемой **службой каталога**.

Назначение прав происходит централизовано в соответствии с выполняемыми пользователем должностными обязанностями.

В модели защиты на уровне пользователя прежде чем получить доступ к ресурсу, пользователь должен зарегистрироваться в сети, а затем его учетные данные и права доступа будут переданы сетевому ресурсу. В этом случае пользователь должен ввести имя и пароль только один раз, а права доступа к различным ресурсам хранятся и проверяются централизованно.

13. Сетевые операционные системы

Применительно к сетевым возможностям операционные системы (ОС) можно разделить на три группы:

- **Клиентские ОС.** Клиентские операционные системы работают на клиентских рабочих станциях и обеспечивают базовую функциональность для ежедневной работы. Примером таких ОС могут служить: Microsoft Windows XP, Vista, Windows 7 и 8, MacOS, SUSE Linux Enterprise Desktop, Red Hat Enterprise Linux Desktop.
- **Сетевые (серверные) ОС.** Сетевые операционные системы (Network Operating System – NOS), еще называют серверными ОС, работают на серверах и предоставляют расширенный функционал, например, базы данных, совместное использование файлов и других ресурсов, электронную почту и прочее. Такими сетевыми операционными системами являются: Novell Open Enterprise Server (NetWare и SLES), Microsoft Windows Server 2003, 2008 и 2012, SUSE Linux Enterprise Server 9, 10 и 11, Red Hat Enterprise Linux Server 5 и 6, Apple OS X Server, разнообразные UNIX-системы.
- **Комбинированные ОС.** Некоторые ОС могут содержать компоненты как клиентские, так и некоторые серверные функции, например, для организации одноранговых сетей. К таким систеама можно отнести Microsoft Windows XP, Vista, Windows 7, настольные варианты MacOS X и многие Linux-системы.

Некоторые серверные операционные системы:

- UNIX
- Linux
- Microsoft Windows
- Apple OS X Server
- Novell NetWare и Open Enterprise Server (OES)

UNIX

UNIX был разработан в начале 1970-х годов группой программистов из Bell Laboratories. Изначально эта ОС проектировалась быть компактной, гибкой системой для использования программистами.

UNIX позволяет нескольким пользователям одновременно подключаться к одному компьютеру и использовать совместно его ресурсы.

Поскольку UNIX разрабатывался быть переносимой на разные платформы операционной системой, гибкой и недорогой, то он быстро завоевал признание в университетах.

При большом разнообразии UNIX-систем наиболее популярными были Sun Solaris, SCO UNIX, BSD, SVR4, AIX, SVID, XENIX, HP-UX.

Linux

В 1991 году финский студент Линус Торвальдс создал свободную версию UNIX-подобной операционной системы. Названная им ОС Linux стала разрабатываться по модели открытого исходного кода.

Торвальдс сделал исходный код ядра Linux доступным для изучения и изменения через Интернет. Это означало, что текущая разрабатываемая версия всегда свободно доступна всем.

И хотя Linux в чем-то схож с UNIX по функционалу и общим принципам работы, но это совершенно отдельная ОС и ее базовый код разрабатывался независимо.

Сегодня Linux имеет множество вариантов и дистрибутивов. Не претендуя на полноту списка приведем лишь некоторые из них: SUSE Linux, Red Hat Linux, Ubuntu, Debian, Slackware, Mandriva и другие.

Microsoft Windows

Изначально Microsoft разработала Windows как графическую операционную систему для персональных компьютеров. Позже была разработана серверная версия этой ОС, которая получила название Windows NT.

В современных версиях Windows Server предлагаются наиболее часто используемые функции почти всех общих требований к обработке данных сервером. В них реализованы функции Server Core, Hyper-V и DirectAccess, а также такие возможности уровня предприятия, как кластеризация, расширенный удаленный доступ и виртуализация для критических бизнес-приложений и крупномасштабной реализации виртуализации.

Apple OS X Server

Mac OS X Server — UNIX-подобная, серверная операционная система. Серверная редакция имеет архитектуру аналогичную Mac OS X, но включает в себя программы администрирования и управления рабочими группами. Эти программы обеспечивают упрощённый доступ к сетевым сервисам, таким как почтовый сервер, Samba сервер, LDAP, DNS и другим. Также включает в себя многочисленные дополнительные сервисы и программы для их управления, например, веб-сервер, вики-сервер, чат-сервер, календарь-сервер и множество других. OS X Server — вариант операционной системы Mac OS X для серверов.

В OS X используется ядро Darwin, основанное на микроядре Mach и содержащее код, написанный самой Apple и код, полученный из операционных систем NeXTSTEP и FreeBSD. OS X выпускалась для компьютеров Macintosh (Макинто́ш) на базе процессоров PowerPC и Intel. Начиная с версии 10.6, OS X работает только на процессорах от Intel, поддержка архитектуры PowerPC прекращена.

Novell NetWare и Open Enterprise Server (OES)

NetWare - это программное решение сервисов Сети, которое значительно увеличивает возможности Вашей компании для обеспечения взаимодействия в Вашей сети и в Интернете. Благодаря постоянному взаимодействию, защите Сети и высокой доступности, NetWare осуществляет сервис хранения файлов, печати, Каталога, электронной почты и ресурсов баз данных на основе единой Се-

ти One Net, объединяющей все типы сетей - корпоративных и общих, проводных и беспроводных, систем хранения данных и рабочих столов клиентов [12].

На платформу NetWare 6 были портированы популярные UNIX программы, такие как WEB Server Apache, SQL сервер MySQL, PHP, ssh и другие приложения. Была улучшена поддержка симметричной многопроцессорной обработки (SMP — несколько процессоров в одном сервере), представлены iFolder (синхронизация файлов локальной папки с сервером и предоставления защищённого доступа к ним в локальной сети и через Интернет), iManager (веб-утилита администрирования NetWare и других продуктов), Native File Access Pack (NFAP — компонент, предоставляющих доступ к ресурсам сервера NetWare клиентам Windows, Macintosh и UNIX-подобных систем по протоколам соответствующих сетей), NetDrive (утилита, позволяющая назначать буквы дисков на HTTP- и FTP-ресурсы, а также на серверы iFolder), а также веб-сервер по умолчанию был заменён с Netscape Enterprise Server на Apache. Также база данных Btrieve (используемая с предыдущих версиях NetWare) была заменена на Pervasive PSQL, представляющего собой развитие того же Btrieve.

Novell Open Enterprise Server (OES) — новая сетевая операционная система компании Novell. OES включает в себя Novell NetWare, SUSE Linux Enterprise Server и набор сетевых служб (файловые службы, принт-сервер, службы каталогов, службы кластера, службы хранения данных, службы управления сетью и серверами, веб-приложения и т. д.), которые могут использоваться как с ядром Linux, так и с ядром NetWare. Продукт был разработан таким образом, чтобы обе операционные системы могли взаимодействовать друг с другом, а клиенты могли создавать смешанные среды для оптимального удовлетворения своих потребностей. В том числе создавать смешанные кластеры, в которых ресурсы при сбое могут перемещаться с сервера NetWare на сервер Linux и наоборот.

Конфигурирование клиентских ОС для подключения к серверам

Подключение клиентских компьютеров к серверам может осуществляться под управлением операционных систем:

- Linux
- Microsoft Windows
- Apple OS X

14. Предоставление сетевой поддержки

Средства отказоустойчивости для сетевых данных

Средства восстановления после катастроф для сетевых данных

Средства отказоустойчивости для сетевых данных

Отказоустойчивость – это свойство системы обеспечить целостность и доступность данных при сбое или поломке оборудования.

Отказоустойчивость обеспечивается избыточностью оборудования и повышается организационными мерами.

При организации отказоустойчивости сетевых ресурсов стоит обратить особое внимание на такие системы:

- Хранение данных

- Электроснабжение
- Запасные каналы связи

Хранение данных

Есть несколько способов обеспечения целостности сетевых данных при использовании дополнительных устройств хранения. Один из распространенных способов – это организация массива независимых исков (Redundant Area of Independent Disks – RAID).

Для эффективного применения RAID-технологии надо знать:

- Как работает RAID
- Преимущества дисковых массивов
- Семь уровней RAID
- Выбор применения RAID
- Преимущества и недостатки разных уровней RAID
- Использование «горячего» и «холодного» резервов для защиты данных

Электроснабжение

Проблемы электропитания:

- Повышенное напряжение и всплески
- Пониженное напряжение
- Отключение

Обеспечение бесперебойного электроснабжения:

- Дополнительный ввод электроснабжения
- Источники бесперебойного питания и стабилизаторы
- Источники автономного питания (генераторы)

Запасные каналы связи

Запасной канал связи лучше реализовать на другой коммуникационной технологии, например, SDSL или беспроводная связь.

Средства восстановления после катастроф для сетевых данных
Рекомендации по подготовке к возможным катастрофам
Резервное копирование и восстановление данных

Нормальное или полное резервное копирование
Инкрементальное резервное копирование
Дифференциальное резервное копирование
Прямое копирование или зеркальное резервное копирование
Ежедневное резервное копирование

Запасные площадки и центры обработки данных

Запасные площадки разной степени готовности:

- «Горячие»
- «Теплые»

- «Холодные»

Восстановление после катастрофы

Кроме стандартных средств восстановления после катастрофы есть еще несколько дополнительных, которые нужно иметь ввиду:

- Использование сторонних утилит для восстановления данных
- Обращение в профессиональные центры восстановления данных

15. Поиск и устранение сетевых проблем

Выбор подходящих инструментов для кабельных работ

Кабельные работы включают прокладку и разделку кабелей, оконцовывание соответствующими вилками и розетками, тестирование готовых кабельных сегментов.

Для проведения кабельных работ служат следующие инструменты:

- Инструмент для снятия изоляции
- Обжимной инструмент (для вилок)
- Забивной инструмент (для розеток и коммутационных панелей)
- Кабельные тестеры
- Разнообразные инструменты и приборы для работы с оптоволокном
- Оптические тестеры

С широким распространением беспроводных сетей необходимым инструментом в арсенале стали беспроводные сканеры и анализаторы сигналов.

Понимание видимых признаков для определения проблем в сети

Видимыми индикаторами работы сети являются светодиоды и, например, жидкокристаллические экраны, на сетевых устройствах. Они помогают сетевому администратору оценивать состояние и работоспособность сети, а также обнаруживать и диагностировать проблемы с сетью.

Часто встречаются такие индикаторы:

- **Индикатор наличия связи.** Если он горит, то установлено физическое соединение двух сетевых устройств. Различная цветовая индикация может показывать скорость установленного соединения.
- **Индикатор скорости.** Иногда для разных скоростей сетевого устройства использовались отдельные световые индикаторы, а не цветовая кодировка.
- **Индикатор дуплексного режима.** Этот индикатор показывал режим установленного канала связи – полу- или полнодукплексный.
- **Индикатор трафика**. Этот индикатор мигает при приеме или передаче данных.
- **Индикатор коллизий.** Этот индикатор сигнализировал о возникновении столкновений в сети с шинной топологией. Большое количество коллизий говорило насыщении сетевого сегмента станциями или о проблемах. Сейчас такой индикатор практически не применяется.

Выбор сетевых утилит для поиска и устранения проблем со связью в сети

Для поиска и устранения проблем в сетях с использованием протокола TCP/IP можно применять такие утилиты [13]:

- Ping
- Tracert
- Netstat
- Nbtstat
- Arp
- Config/ifconfig/ipconfig/winipcfg/ip/netsh
- Route
- Nslookup/dig/host

Определение влияния добавления, удаления и изменения сетевых сервисов

Перед внедрением новых сетевых сервисов в сетях TCP/IP нужно учитывать их влияние на сеть и уже развернутые сервисы. Некорректное применение сервисов TCP/IP может пагубно сказаться на сетевой производительности.

Тремя важными сервисами TCP/IP, которые имеют глобальное воздействие на сеть, являются:

- DHCP
- DNS
- WINS

Описание пошаговой модели поиска и устранения неисправностей

1. Определите симптомы и потенциальные последствия
2. Определите область воздействия
3. Узнайте, что изменилось
4. Выберите наиболее вероятную причину
5. Выполните восстанавливающие действия по плану с учетом потенциального влияния
6. Протестируйте результат
7. Определите результат и эффект выполненного решения
8. Задокументируйте решение и процесс

Устранение проблем, связанных со средой передачи данных

Устранение неисправностей, связанных со средой передачи данных, требует решений таких проблем:

- **Плохой кабель.** Надо убедиться, что используемый кабель подходит для этой сети. Неверно выбранный кабель может привести к:
  - **Большому затуханию сигнала**. Это свойство электромагнитных волн терять амплитуду или искажаться при передаче.
  - **Чрезмерной фрагментации пакетов**. Это происходит, когда на принимающей стороне пакеты приходят урезанными или неполными.
  - **Кабельные наводки или помехи.** Это воздействие сигналов, проходящих в одном кабеле, на сигналы, передаваемые по соседнему или близко расположенному другому кабелю, а также сильных внешних электромагнитных излучений или импульсов.

Такие помехи приводят к ошибкам в контрольной сумме пакетов в Ethernet-сетях.

- **Сетевое оборудование.** Неправильно работающее или сбойное сетевое оборудование может приводить к нечеткому сигналу, а также уменьшению расстояния, на котором сигнал уверенно принимается. В этом случае устройство следует заменить на исправное.