Московская финансово-промышленная академия

Кафедра Информационных систем

Власенко В.И.

Интернет-курс по дисциплине «Информационные сети»

Москва
2010

Содержание

Аннотация к дисциплине

Дисциплина «Информационные сети» входит в цикл общепрофессиональных дисциплин государственного образовательного стандарта 230200 «Информационные системы». Она позволяет обеспечить получение знаний об основах передачи данных в компьютерных сетях, стековой организации сетевого программного обеспечения, основах проектирования компьютерных сетей различных уровней; теории, принципах, методах и алгоритмах передачи данных в компьютерных сетях; методах и технологиях оптимизации производительности сетей; основах технологий проектирования и разработки сетевых приложений. Рассматриваются основные характеристики информационных сетей, разновидности телекоммуникационных каналов, кодирование и сжатие информации, режимы переноса информации, архитектуры сетей, цифровые сети интегрального обслуживания, сопряжение разнородных сетей.

Цели и задачи дисциплины:

Целью дисциплины «Информационные сети» является теоретическая и практическая подготовка студентов в области передачи информации в такой степени, чтобы они могли выбирать необходимые оборудование, технологии и программные средства передачи данных, уметь объяснить их работу и правильно эксплуатировать, а также приобретение студентами знаний о принципах построения современных сетей; основ организации информационных сетей, формирование у студентов базовой системы знаний и навыков по методам коммутации и маршрутизации информационных потоков, обучение студентов приемам и методам работы в локальных и глобальных вычислительных сетях с использованием сетевых операционных систем.

Задачи изучения дисциплины:

· ознакомление с общим подходом к стандартизации и построению существующих и перспективных информационных сетей;

· формирование у студентов минимально необходимых знаний в области передачи информации;

· ознакомление с методами и средствами, технологиями, протоколами передачи информации в локальных, городских, глобальных информационных сетях;

· выработка практических навыков аналитического и экспериментального исследования процесса передачи информации, создания программных средств передачи информации в информационных сетях, проектирования протоколов передачи информации, проектирование информационных сетей различного масштаба.

В результате изучения дисциплины обучаемый должен:

иметь представление:

· о базовой эталонной модели OSI;
· об основных видах информационных сетей;
· о различных структурах сетей;
· о классификации сетевых протоколов;
· об устройствах объединения сетей: концентраторах, мостах, коммутаторах и маршрутизаторах, сетевых адаптерах;
· о технических аспектах информационной безопасности;
· о методах оценки эффективности информационных сетей;

знать:

· основные понятия об информационных сетях;
· назначение и структуру локальной вычислительной сети;
· компоненты локальной вычислительной сети, ее топологию;
· структуру сетевых операционных систем;
· основные компоненты и утилиты сетевых операционных систем;

уметь:

· оценивать производительность и стабильность работы сети;
· осуществлять разработку проекта сети;
· давать рекомендации по улучшению производительности и надёжности сети;
· входить в сеть и использовать ее ресурсы;
· настраивать компоненты сети;
· работать с утилитами сетевой операционной системы;
· выявлять и исправлять возможные сбои и ошибки в сети;

приобрести навыки:

· принятия решений;
· планирования временных затрат на решение поставленной задачи;
· выбора критериев средств информационной системы.

Тема 1. Основные понятия информационных сетей как открытых информационных систем

Цели:

- Научиться классифицировать тип и вид сети.
- Научиться идентифицировать одноранговые сети и сети на основе сервера.
- Понять функции серверов.
- Получить представление об открытых информационных системах.

Информационная сеть (Information network) - сеть, предназначенная для обработки, хранения и передачи данных. Информационная система это материальная система, организующая, хранящая и преобразующая информацию. Информационная сеть состоит из:

- абонентских и административных систем;
- связывающей их коммуникационной сети.

Коммуникационная сеть; Сеть передачи данных; (Communication network) - сеть, основной задачей которой является передача данных без ошибок и искажения. Коммуникационная сеть является ядром информационной сети, обеспечивающим передачу и некоторые виды обработки данных.

Вычислительная сеть; Сеть ЭВМ; Компьютерная сеть (Computer network) - вычислительный комплекс, включающий территориально распределенную систему компьютеров и их терминалов, объединенных в единую систему. Система компьютеров, объединенных каналами передачи данных называется информационно-вычислительная сеть.

1.1.Одноранговые сети и сети на основе сервера.

Сеть— это взаимодействующая совокупность объектов, связанных друг с другом линиями. Основные характеристики сети, её структура и особенности определяются архитектурой. Наибольшее распространение получила архитектура взаимодействия открытых систем. Также широко используются архитектуры крупных фирм-изготовителей.

Все сети имеют некоторые общие компоненты, функции и характеристики. В их числе:

- серверы (server) — компьютеры, предоставляющие свои ресурсы сетевым пользователям;
- клиенты (client) — компьютеры, осуществляющие доступ к сетевым ресурсам, предоставляемым сервером;
- среда (media) передачи данных — способ соединения компьютеров;
- ресурсы (resources), предоставляемые серверами — файлы, принтеры и другие элементы, используемые в сети.

Несмотря на определенные сходства, сети разделяются на два типа: одноранговые (peer-to-peer); на основе сервера (server based). Различия между одноранговыми сетями и сетями на основе сервера имеют принципиальное значение, поскольку определяют разные возможности этих сетей. Выбор типа сети зависит от многих факторов: размера предприятия; необходимого уровня безопасности; вида бизнеса; уровня доступности административной поддержки; объема сетевого трафика; потребностей сетевых пользователей; финансовых затрат.

1.1.1. Одноранговые сети

В одноранговой сети все компьютеры равноправны: нет иерархии среди компьютеров и нет выделенного (dedicated) сервера. Каждый компьютер функционирует и как клиент, и как сервер. Все пользователи самостоятельно решают, какие данные на своем компьютере сделать общедоступными по сети. Чтобы ресурс стал общим, его необходимо отдать в общее пользование, используя службы удаленного доступа. В зависимости от того, как будет установлена защита данных, другие пользователи смогут пользоваться файлами сразу же после их создания.

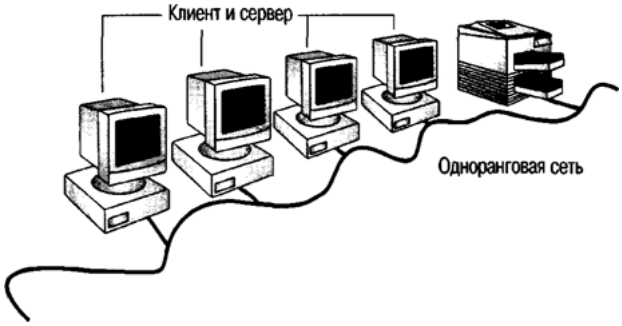


Рис. 1.1. В одноранговой сети компьютеры –это и клиенты и серверы

Одноранговые сети относительно просты и значительно дешевле, но требуют более мощных компьютеров. Одноранговые сети называют также рабочими группами. ***Рабочая группа*** - это небольшой коллектив, менее 15 компьютеров. В одноранговой сети требования к производительности и к уровню защиты для сетевого программного обеспечения, ниже, чем в сетях с выделенным сервером. Сетевую безопасность одновременно можно применить только к одному ресурсу, и пользователь должен помнить столько паролей, сколько сетевых ресурсов. Одноранговая сеть характеризуется рядом стандартных решений:

- компьютеры расположены на рабочих столах пользователей;
- пользователи расположены компактно и сами выступают в роли администраторов и обеспечивают защиту информации;
- для объединения компьютеров в сеть применяется простая кабельная система (в последнее время и беспроводная связь).

1.1.2. Пиринговые сети

Пиринговые сети— это компьютерные сети, основанные на равноправии участников. В таких сетях отсутствуют выделенные серверы, а каждый узел (peer) является как клиентом, так и сервером. В отличие от архитектуры клиент-сервера, такая организация позволяет сохранять работоспособность сети при любом количестве и любом сочетании доступных узлов. Участниками сети являются пиры. Впервые фраза «peer-to-peer» была использована в 1984 году Парбауэллом Йохнухуйтсманом.

Помимо чистых P2P-сетей, существуют так называемые гибридные сети, в которых существуют сервера, используемые для координации работы, поиска или предоставления информации о существующих машинах сети и их статусе (on-line, off-line ит.д.). Гибридные сети сочетают скорость централизованных сетей и надёжность децентрализованных благодаря гибридным схемам с независимыми индексационными серверами, синхронизирующими информацию между собой. При выходе из строя одного или нескольких серверов, сеть продолжает функционировать. К частично децентрализованным файлообменным сетям относятся например EDonkey, BitTorrent. В современных файлообменных сетях информация загружается сразу с нескольких источников. Ее целостность проверяется по контрольным суммам. Несмотря на то, что большие одноранговые (пиринговые) сети намного устойчивее многоранговых (клиент-серверных), надежность не является их главным преимуществом. Для конечного пользователя, намного важнее тот факт, что скорость обмена файлами в P2P-сетях на порядок выше, чем в традиционных. Главной проблемой для многих пользователей пиринговых сетей является необходимость постоянно держать свой компьютер, подключенным к Интернету, – P2P- сеть будет работать и без этого, но скорость загрузки будет снижена. Во всех пиринговых сетях действует железный принцип «скачал сам – отдай другим».

Известные децентрализованные и гибридные (пиринговые) сети

ED2K (eDonkey2000)— сеть децентрализованного типа. Поиск выполняют специализированные серверы, связанные между собой. Клиенты самостоятельно обмениваются по протоколу MFTP. Компания MetaMachine, разработчик исходной концепции и первого клиента, основанного на веб-интерфейсе (Edonkey 2000 v1.4.5), в 2005 году прекратила поддержку этого проекта, однако сеть продолжает функционировать за счет более совершенного и более мощного клиента *eMule*, который использует механизмы *Kademlia* для построения децентрализованного сегмента eD2k . ***TC (***полное название ***TrueChat)***— малоизвестная сеть, в основном для общения использующая сервер (обычно с публичным IP) для связи клиентов (peer-hub-peer). ***Overnet, Kad***— децентрализованные технологии на базе протокола Kademlia, обслуживающие поиск по сети eDonkey2000 (eD2k). ***BitTorrent***— технология распределённого распространения файлов, как правило, большого объёма. Отличается высокой скоростью и централизованностью. Некоторые BitTorrent-клиенты поддерживают DHT и могут работать без центрального сервера (т.н. трекера). ***FastTrack, iMesh***(англ.)— первоначально была реализована в KaZaA. ***OpenFT***— открытое продолжение сети FastTrack. Поддерживается клиентами giFT (KCeasy), mlDonkey. ***Advanced Direct Connect***— представляет собой слабо связанные между собой выделенные сервера для поиска (хабы). Хабы Direct Connect очень удобны для организации файлового обмена в локальных сетях. ***Gnutella***— полностью децентрализованная сеть, использующая протокол, разработанный компанией Nullsoft, основанный на HTTP-загрузках. Самоорганизация сети происходит за счет автоматического взаимообмена данными нод-листа между соединенными клиентами . Клиенты: Shareaza, BearShare , LimeWire, Gnucleus, Phex. ***Ares***— файлообменная сеть для любых файлов. ***Soulseek***— проприетарный протокол. Весь поиск происходит через центральный сервер, на котором есть бесплатная регистрация и платная подписка (официальный сайт). Клиенты: Soulseek, mlDonkey, SolarSeek. ***Freenet, GNUnet, Entropy***— файлообменные анонимные сети, устойчивые к интернет-цензуре. ***MP2P (Manolito P2P)***— поддерживается клиентами Blubster, Piolet, RockItNet. ***Nodezilla***— файлообменная анонимная сеть. ***JXTA***— стандартизация P2P спецификаций и протоколов http://www.jxta.org. ***RShare***— открытая анонимная сеть P2P. ***Peer2Mail***— принципиально это даже не пиринговая сеть, а разновидность ПО позволяющего передавать файлы между двумя хостами (peer-to-peer), используя почтовые сервисы в качестве роутера. Технология передачи файлов основана на инкапсуляции в SMTP-протокол. ***Ants p2p***— открытая P2P-сеть 3-го поколения повышенной безопасности. Java-клиент. ***Rodi***— поддерживает поиск по содержанию файлов. Java-клиент. ***BeShare***— сеть, ориентированная на BeOS. ***Skype***— P2P-телефония. ***WiPeer***— сеть, действующая напрямую между компьютерами, минуя оборудование провайдера. Таким образом, сеть полностью свободна от цензуры. ***SKad*** или ***OpenKAD***— модификация протокола Kademlia. Полностью децентрализованые сети. Первым шагом в этом направлении стала программа en:Winny. Дальнейше развитие этой сети в сторону сетевой анонимности привело к появлению программы en:Share. И на сегодняшний день существует и третья версия под управлением программы Perfect Dark. ***Usenet***— глобальная доска объявлений. ***Poisoned***— программа для работы с файлообменными сетями Gnutella, OpenFT, FastTrack в среде операционной системы Mac OS X. Представляет собой графический интерфейс для фонового приложения giFT. ***Netsukuku***— сеть нового поколения, представляет собой ячеистую сеть передачи данных, заменяет 3-й уровень современной модели OSI другим протоколом маршрутизации. Протокол Netsukuku выстраивает структуру сети в виде фрактала. Сеть является распределённой, масштабируемой, анонимной и не контролируемой, отдельно от Интернета, без поддержки каких-либо служб и государственных каналов. Для расчёта всех необходимых путей связи узла со всеми остальными узлами протокол использует алгоритм Quantum Shortest Path Netsukuku (QSPN).

1.1.3. Сети на основе сервера

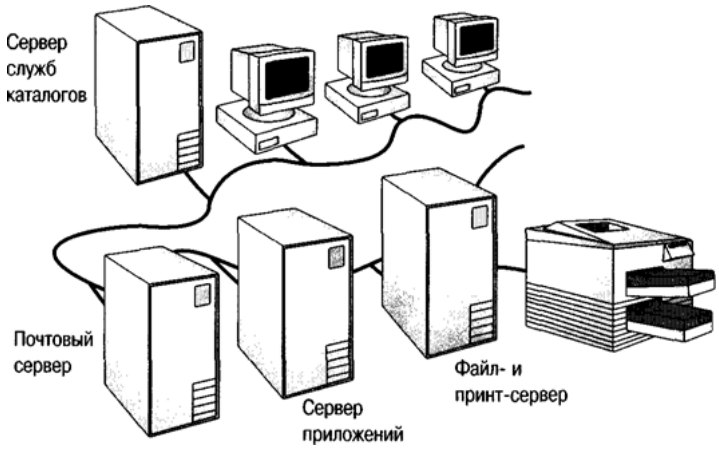


Рис. 1.2. Специализированные серверы

Выделенным называется такой сервер, который функционирует только как сервер (исключая функции клиента или рабочей станции). Они специально оптимизированы для быстрой обработки ***запросов*** от сетевых клиентов и для управления защитой файлов и каталогов. Сети на основе сервера стали промышленным стандартом. ***Сервер –*** это компьютер, предоставляющий свои ресурсы (диски, принтеры, каталоги, файлы и т.п.) другим пользователям сети. С увеличением размеров сети и объема сетевого трафика необходимо увеличивать количество серверов. Распределение задач среди нескольких серверов гарантирует, что каждая

задача будет выполняться самым эффективным способом из всех возможных. Чтобы приспособиться к возрастающим потребностям пользователей, серверы в больших сетях стали ***специализированными*** (specialized).

· ***Файл-серверы и принт-серверы***

· ***Терминальный сервер,*** объединяющий группу терминалов, упрощающий переключения при их перемещении.

· ***Коммуникационные серверы—*** управляют потоком данных и почтовых сообщений между этой сетью и другими сетями, мэйнфреймами или удаленными пользователями через модем и телефонную линию. Выполняют функции терминального сервера, но осуществляющий также маршрутизацию данных. Служба каталогов предназначена для поиска, хранения и защиты информации в сети. Windows NT Server объединяет компьютеры в логические группы - ***домены*** (domain), - система защиты которых наделяет пользователей различными правами доступа к любому сетевому ресурсу.

В расширенной сети использование серверов разных типов приобретает особую актуальность. Необходимо поэтому учитывать все возможные нюансы, которые могут проявиться при разрастании сети, с тем, чтобы изменение роли определенного сервера в дальнейшем не отразилось на работе всей сети. По мере усложнения возлагаемых на серверы функций и увеличения числа обслуживаемых ими клиентов происходит все большая специализация серверов. Существует множество типов серверов.

· ***Первичный контроллер домена, сервер,*** на котором хранится база бюджетов пользователей и поддерживается политика защиты. ***Вторичный контроллер домена,*** сервер, на котором хранится резервная копия базы бюджетов пользователей и политики защиты. ***Универсальный сервер,*** предназначенный для выполнения несложного набора различных задач обработки данных в локальной сети.

· ***Сервер базы данных,*** выполняющий обработку запросов, направляемых базе данных.

· ***Серверы приложений.*** На серверах приложений выполняются прикладные части клиент-серверных приложений, а также находятся данные, доступные клиентам. Например, чтобы упростить извлечение данных, серверы хранят большие объемы информации в структурированном виде. Файл или данные целиком копируются на запрашивающий компьютер. А в сервере приложений на запрашивающий компьютер пересылаются только результаты запроса. Приложение-клиент на удаленном компьютере получает доступ к данным, хранимым на сервере приложений. Однако вместо всей БД на Ваш компьютер с сервера загружаются только результаты запроса.

· ***Почтовые серверы***

· ***Proxy сервер,*** подключающий локальную сеть к сети Internet. ***Web–сервер,*** предназначенный для работы с web –информацией. ***Сервер защиты данных,*** оснащенный широким набором средств обеспечения безопасности данных и, в первую очередь, идентификации паролей.

· ***Сервер удаленного доступа***, обеспечивающий сотрудникам, работающим дома торговым агентам, служащим филиалов, лицам, находящимся в командировках, возможность работы с данными сети. ***Сервер доступа,*** дающий возможность коллективного использования ресурсов пользователями, оказавшимися вне своих сетей (например, пользователями, которые находятся в командировках и хотят работать со своими сетями). Для этого пользователи через коммуникационные сети соединяются с сервером доступа и последний предоставляет нужные ресурсы, имеющиеся в сети.

· ***Видеосервер,*** который в наибольшей степени приспособлен к обработке изображений, снабжает пользователей видеоматериалами, обучающими программами, видеоиграми, обеспечивает электронный маркетинг. Имеет высокую производительность.

1.1.4. Комбинированные сети

Существуют и комбинированные типы сетей, совмещающие лучшие качества одноранговых сетей и сетей на основе сервера. Многие администраторы считают, что такая сеть наиболее полно удовлетворяет запросы, так как в ней могут функционировать оба типа ОС, но для их эксплуатации необходимы определенные знания и навыки планирования.

Одноранговые сети и сети на основе сервера объединяет общая цель – разделение ресурсов. А вот различия определяют:

· требования к аппаратному обеспечению;

· способ поддержки пользователей.

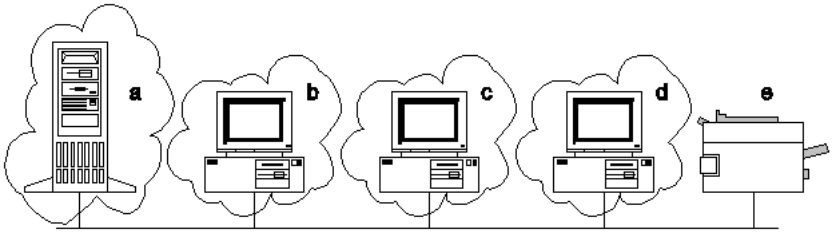


Рис. 1.3. Комбинированная ИС
*(**a** – сервер (компьютер с ОС Windows NT Server), **b** – клиент и сервер (компьютер с ОС Windows NT Workstation), **c** - клиент и сервер (компьютер с ОС Windows), **d** - клиент и сервер (компьютер с ОС Windows для рабочих групп), **e** – сетевой принтер [принт-сервер])*

1.1.5. Выводы

Сеть позволяет совместно использовать ресурсы, например файлы и принтеры, а также работать с интерактивными приложениями, например планировщиками и e-mail. В настоящее время компьютерные сети выходят за пределы ЛВС и вырастают в глобальные компьютерные сети. Использование компьютерных сетей сулит множество преимуществ:

· снижение затрат благодаря совместному использованию данных и периферийных устройств;

· стандартизацию приложений и своевременное получение данных;

· более эффективное взаимодействие и планирование рабочего времени.

1.2. Классификация сетей.

В зависимости от технологии передачи данных различают (см. рис. 1.4.):
- сети с маршрутизацией данных (каждый блок данных передаётся только одной системе-адресату)
- сети с селекцией данных (каждый блок данных передаётся всем системам).

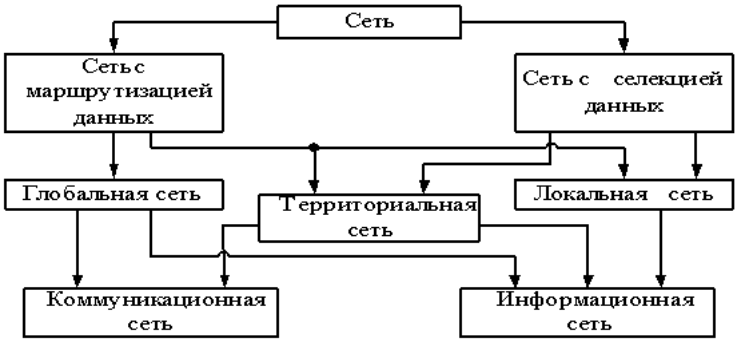


Рис. 1.4. Классификация ИС по технологии

По территориальному признаку сети делятся на: локальные; территориальные; глобальные; смешанные.

Коммуникационная сеть предназначена для передачи данных. Кроме того, она может обеспечивать выполнение задач, связанных с преобразованием данных (сборкой символов в пакеты, обеспечение достоверности передачи и т.д.).

Информационная сеть получается подключением к коммуникационной сети абонентской системы. При этом на базе коммуникационной сети может быть построена не одна, а группа информационных сетей.

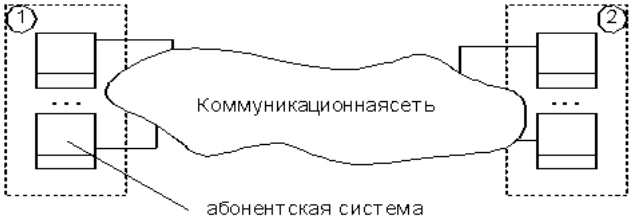


Рис. 1.5. ИС = КС+АС

Современные сети являются пассивными, поэтому в них вводятся компоненты активной диагностики и управления ресурсами. Последние становятся всё более распространёнными, увеличивая надёжность и гибкость функционирования сетей. Любая сеть создаётся для удовлетворения запросов её пользователей. Поэтому наряду с многопрофильными (универсальными) сетями распространение получают сети специализированные, предназначенные для выполнения определённых целей (сеть библиотек, банковская сеть, исследовательская сеть, сеть Аэронет).

Информационные сети, принадлежащие государству, называют ***общественными сетями***. Информационные сети, созданные концернами, объединениями, фирмами, именуются ***частными сетями***. Различают ***интегрированные сети, неинтегрированные сети*** и ***подсети***. Интегрированная вычислительная сеть (интерсеть) представляет собой взаимосвязанную совокупность многих вычислительных сетей, которые в интерсети называются подсетями. В автоматизированных системах крупных предприятий подсети включают вычислительные средства отдельных проектных подразделений. Интерсети нужны для объединения таких подсетей, а также для объединения технических средств автоматизированных систем проектирования и производства в единую систему комплексной автоматизации (CIM - Computer Integrated Manufacturing). Развитие интерсетей заключается в разработке средств сопряжения разнородных подсетей и стандартов для построения подсетей, изначально приспособленных к сопряжению. Сети также различают в зависимости от используемых в их протоколов и по способам коммутации. Еще одним популярным способом классификации информационных сетей является их классификация по масштабу производственного подразделения, в пределах которого действует сеть. Различают сети отделов, сети кампусов и корпоративные сети.

Архитектура сети определяет основные элементы сети, характеризует ее общую логическую организацию, техническое обеспечение, программное обеспечение, описывает методы кодирования. Архитектура также определяет принципы функционирования и интерфейс пользователя. С помощью сетей можно разделять ресурсы и информацию. Компьютерная сеть позволит совместно использовать периферийные устройства: принтеры; дисковые накопители; стримеры; сканеры; и др. Компьютерная сеть позволяет совместно использовать информационные ресурсы: каталоги; файлы; прикладные программы; игры; БД; текстовые процессоры.

1.3. Открытая система.

Система— это совокупность объектов и отношений между ними, образующая единое целое. В информатике системой называют совокупность, состоящую из одного либо нескольких компонентов, соответствующих средств программирования, операторов, физических процессов, средств телекоммуникации и других образующих автономное целое, способное осуществлять обработку и передачу данных. *Взаимодействие открытых систем* – это правила сопряжения систем с открытой архитектурой, создаваемых различными производителями.

1.1.3. Типы и виды систем. Технология открытых систем

Система может быть создана в одном устройстве или в группе устройств, установленных в данном месте. Такая система называется одноточечная. Она может быть создана во множестве взаимосвязанных устройств, установленных в различных местах (многоточечная). Многоточечная система образует сеть. Существо технологии открытых систем состоит в формировании среды, включающей программное обеспечение, аппаратные средства, службы связи, интерфейсы, форматы данных и протоколы, обеспечивающей переносимость, взаимосвязь и масштабируемость приложений и данных. Совокупность указанных качеств достигается за счет использования развивающихся, общедоступных и общепризнанных стандартов на продукты информационных технологий, составляющих среду открытой системы. "Открытая спецификация" определяется как "общедоступная спецификация, которая поддерживается открытым, гласным согласительным процессом, направленным на постоянную адаптацию новой технологии, и соответствует стандартам". То есть, открытая спецификация не зависит от конкретной технологии, не зависит от конкретных технических и программных средств или продуктов отдельных производителей. Число продуктов информационных технологий, составляет много тысяч, соответственно, велико и число стандартов. Для облегчения взаимопонимания между указанными группами специалистов целесообразно использовать какую-то единую модель среды открытых систем. Такой моделью служит эталонная модель OSE/RM среды открытых систем (Open System Environment Reference Model).

1.1.4. Открытая система

На сегодня не существует однозначно устоявшегося определения термина "открытые системы". Различные организации формулируют его по-разному, исходя из своих конкретных задач. Принципы открытых систем применяются в настоящее время при построении большинства классов систем: вычислительных, информационных, телекоммуникационных, систем управления в реальном масштабе времени, встроенных микропроцессорных систем. В условиях перехода к интегрированным вычислительно-телекоммуникационным системам принципы открытых систем составляют основу технологии интеграции. ***Открытая система (OSI)—*** это система, использующая соответствующие международные стандарты. По определению комитета IEEE открытая система – это система, реализующая открытые спецификации (стандарты) на интерфейсы, службы и форматы данных, достаточное для того, чтобы обеспечить:

- возможность переноса (мобильность) прикладных систем с минимальными изменениями на широкий диапазон систем;
- совместную работу (интероперабельность) с другими прикладными системами на локальных и удалённых платформах;
- взаимодействие с пользователями в системе, облегчающее переход от системы к системе (мобильность пользователей).

Главное здесь – переход от множества платформ, поддерживаемых только их создателями, к общепринятым стандартам, поддерживаемым всем компьютерным сообществом. Масштабный переход к архитектурам и технологиям открытых систем начался более 10 лет назад и был обусловлен, в основном, двумя проблемами: проблемой мобильности программ и массивов данных; проблемой создания распределенных информационных инфраструктур, обеспечивающих организацию удаленного взаимодействия программно-аппаратных средств и массивов данных. В качестве классического примера открытой системы можно привести операционную систему UNIX, базовая версия которой была разработана в конце 60-х г.г. К. Томпсоном и Д. Ритчи. Несмотря на большое количество разных реализаций UNIX, их форматы файлов полностью совместимы друг с другом, и, как правило, совместимо также программное обеспечение. Каждая открытая система предназначена для выполнения двух задач: обработки и передачи данных. Первая часть – это прикладные процессы, предназначенные для обработки данных и в первую очередь для нужд пользователей. Вторая часть – область взаимодействия, которая обеспечивает передачу данных между прикладными процессами, расположенными в различных системах.

Рис. 1.6. Выполнение задач в открытой системе

Контрольные вопросы:

1. Чем отличается коммуникационная сеть от информационной сети?
2. Как разделяются сети по территориальному признаку?
3. Что такое совокупность правил, устанавливающих процедуры и формат обмена информацией?
4. Чем отличается рабочая станция в сети от обычного персонального компьютера?
5. Какие элементы входят в состав сети?
6. Как называется описание физических соединений в сети?
7. Что такое архитектура сети?
8. Чем отличается одноранговая архитектура от клиент серверной архитектуры?
9. Что такое Proxy–сервер?
10. Что такое открытая система?

Практические задания:

ЗАДАНИЕ № 1.1. Описание работы в сети. Подберите для каждого понятия соответствующее определение.

Понятие:	Определение:

1. Полнодуплексная сеть.	a. Среда, по которой можно передавать несколько сигналов одновременно.
2. Широкополосная сеть.	b. Технология, в которой канал для связи устанавливается до начала передачи данных.
3. Коммутация каналов.	c. Сеть, в которой системы выполняют только назначенные им роли.
4. Клиент-серверная сеть.	d. Среда, способная осуществлять трафик одновременно в обоих направлениях.
5. Узкополосная сеть.	e. Среда, по которой можно одновременно передавать только один сигнал.

ЗАДАНИЕ № 1.2. Сетевые операционные системы. Сопоставьте сетевой ОС в левой колонке наиболее точное описание из правой.

Сетевая ОС	Описание
1. Linux	a. Использует регистрационную базу данных для хранения учетных записей пользователей
2. Windows NT	b. Современная версия первого варианта UNIX, разработанного AT&T
3. Macintosh	c. Доступна в версиях Server, Advanced Server и Datacenter
4. UNIX System V	d. Первая версия Windows, не основанная на MS-DOS
5. NetWare 3.x	e. Изначально использовал собственный протокол канального уровня
6. Windows 2000	f. Версия UNIX в рамках проекта Open Source

ЗАДАНИЕ № 1.3. Классы сетей. Сопоставьте какой класс сети в левой колонке наиболее точно соответствует IP из правой.

Класс сети	IP:
1. Сети класса A	a. номера в диапазоне от 240.0.0.0 до 247.255.225.225.
2. Сети класса B.	b. номера в диапазоне от 224.0.0.0 до 239.255.225.225.
3. Сети класса C.	c. номера в диапазоне от 192.0.1.0 до 223.255.225.0.
4. Сети класса D.	d. номера в диапазоне от 128.0.0.0 до 191.255.0.0.
5. Сети класса E.	e. номера в диапазоне от 1.0.0.0 до 126.0.0.0.

Рис. 1.7. Классы IP-адресов

ЗАДАНИЕ № 1.4. Изобразить соотношение понятий: информационное общество, информационное пространство, информационная инфраструктура, технология открытых систем, относительно социально-эномического и политического развития общества.

Решение:

Перечень литературы и Интернет-ресурсов:

1. Аппаратное обеспечение вычислительных систем / Д.В. Денисов, В.А. Артюхин, М. Ф. Седненков; под ред. Д.В. Денисова. – М.: Маркет ДС, 2007 – 184 с.

2. Архитектура компьютерных систем и сетей: Учеб. пособие / Т.П. Барановская, В.И. Лойко, М.И. Семенов; Под ред. В.И. Лойко. М.: Финансы и статистика, 2003. – 256 с.: ил.

3. Барфилд, Эд , Уолтерс, Брайен. Программирование "клиент-сервер" в локальных вычислительных сетях; Учебник:Пер.с англ. . -М.:Филинъ,1997-423с.

4. Базовые технологии локальных сетей - http://www.citforum.ru/nets/protocols2/index.shtml.

5. Введение в IP-сети — http://www.citforum.ru/nets/ip/contents.shtml

6. Дуглас Тумбс Разбираясь с DNS, — Открытые системы, Windows IT Pro №02, 2006.

7. Жеретинцева Н. Курс лекций по компьютерным сетям.Владивосток: ДВГМА, 2000. 158 с.

8. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. (рекомендовано Мин. образования РФ). СПб: Питер, 2001,668 с.

9. Пиринговые сети - http://www.compress.ru/Archive/CP/2005/10/39/

10. Стефан Лоусон Серьезных препятствий для DNS не предвидится, — Открытые системы, Computerworld №28-29, 2003.

11. Черняк Л. Юбилей TCP/IP. Computerworld. — Открытые системы, 2003. — № 2.

12. Якубайтис Э.А. Информационные сети и системы: Справочная книга. – М.: Финансы и статистика, 1996.

13. Якубайтис Э.А. Открытые информационные сети. – М.:Радио и связь,1991.–208 с.

Тема 2. Модели и структуры информационных систем

Цели:

· Получить представление об ЛВС и ГВС.
· Сформировать знания о различных архитектурах в ЛВС.
· Понять характерные особенности и различия между различными структурами сетей.
· Получить представление о виртуальных сетях – нового поколения сетей

В зависимости от расстояния между абонентскими системами, информационные сети подразделяются на глобальные, территориальные и локальные. Различают универсальные и специализированные информационные сети.

Иерархия компьютерных сетей может быть представлена в следующем виде:

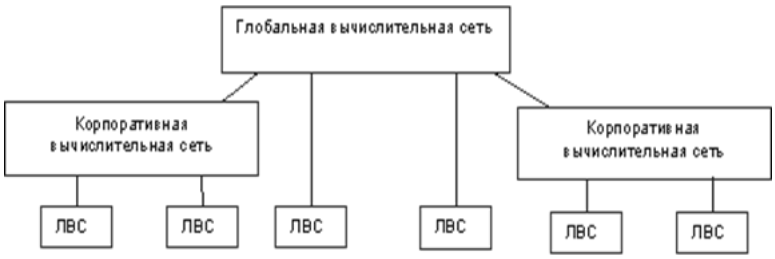


Рис. 2.1. Иерархия компьютерных сетей

2.1. Локальная сеть (ЛВС).

Локальная сеть – это сеть, системы которой расположены на небольшом расстоянии друг от друга. Она охватывает небольшое пространство, как правило, одно здание и характеризуется высокими скоростями передачи данных. Каналы такой сети имеют высокое качество и принадлежат одной организации.

Применяются две архитектуры локальных сетей:

· архитектура «клиент-сервер» (позволяет эффективно использовать ресурсы сетей). В них выделяется один или несколько узлов (их название - серверы), выполняющих в сети управляющие или специальные обслуживающие функции, а остальные узлы (клиенты) являются терминальными, в них работают пользователи. Сети клиент/сервер различаются по характеру распределения функций между серверами, другими словами по типам серверов (например, файл-серверы, серверы баз данных). При специализации серверов по определенным приложениям имеем сеть распределенных вычислений;

· одноранговая архитектура предполагает взаимодействие равноправных абонентских систем. Все узлы равноправны; поскольку в общем случае под клиентом понимается объект (устройство или программа), запрашивающий некоторые услуги, а под сервером - объект, предоставляющий эти услуги. Поэтому каждый узел в одноранговых сетях может выполнять функции и клиента, и сервера.

В зависимости от используемых физических средств соединения выделяют

· кабельные локальные сети;
· беспроводные локальные сети.

Технология удалённого доступа обеспечивает подключение систем к локальной сети через территориальную сеть либо радиоканал. Такие задачи возникают при работе сотрудников на дому и в командировках, а также при взаимодействии локальных сетей. Удалённый доступ обеспечивается серверами удалённого доступа.

С одной стороны, серверы удалённого доступа подключены к локальной сети, с другой – к территориальной коммутационной сети. Он обеспечивает маршрутизацию блоков данных при их передаче через территориальную сеть.

Коммутируемая локальная сеть (КЛС) – это локальная сеть, состоящая из сегментов, которые с помощью коммутирующего комплекса соединяются в единое целое. Деление локальной сети на сегменты позволяет: отключать от сети повреждённые сегменты; не пропускать блоки данных в другие сегменты, если они адресованы системе того же сегмента; создавать коммуникационную локальную сеть.

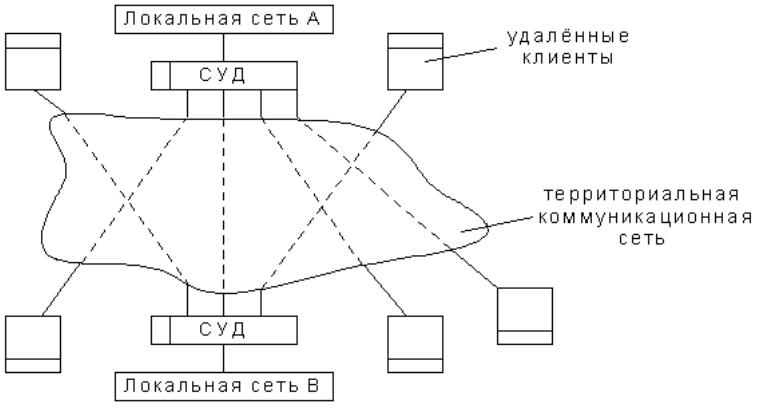


Рис. 2.2. Технология удалённого доступа

Объединение сетей друг с другом позволяет создавать крупные ассоциации локальных сетей. Ассоциация создаётся благодаря включению между локальными сетями ретрансляционных систем, которые часто должны обеспечивать преобразование форматов блоков данных, изменение порядка передачи в них битов управления и пересчёт проверочной суммы. Ассоциация создается благодаря включению между локальными сетями ретрансляционных систем, в том числе - коммутаторов, маршрутизаторов, концентраторов. Так, ассоциация шести сетей (1-6), может быть соединена тремя ретрансляционными системами (a, c, e), см рис.

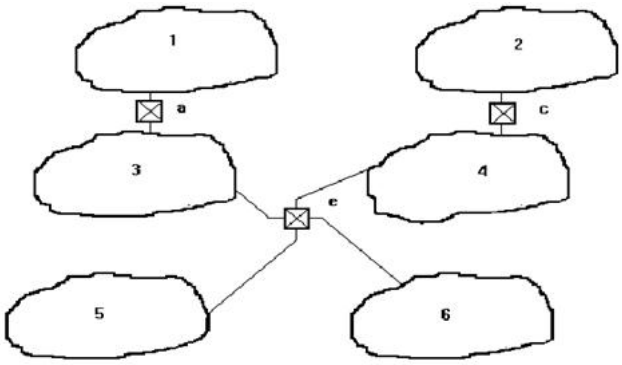


Рис. 2.3. Соединение тремя ретрансляционными системами (a, c, e), ассоциации шести сетей (1-6)

Каждая из последних связывает две или более сетей. Тип используемой ретрансляционной системы зависит от того, в какой степени отличаются стандарты соединяемых сетей. Задача соединения большого числа разнотипных ЛС упрощается, если имеется одна базовая сеть, обеспечивающая их взаимодействие (сеть АТМ, ЦСИО). Ассоциация локальных сетей используется для решения разнообразных задач в науке, промышленности и бизнесе.

2.1.1. Соединения

Соединение **–** это ассоциация функциональных блоков, устанавливаемая для передачи данных. В соответствии с семью уровнями области взаимодействия открытых систем, существует 7 видов соединений, которые обозначаются в соответствии с названием уровня. Каждое соединение i-го уровня обеспечивает взаимодействие объектов этого уровня через логические каналы. Указанные каналы проходят через все уровни, расположенные ниже i-го уровня, и физические средства соединения. Соединения создаются только на время сеанса взаимодействия объектов, при этом согласуются процедуры подтверждения передаваемых блоков данных, а также происходит управление их потоком, чтобы скорости работы соответствовали возможностям партнеров. Вместе с этим нередко экономически целесообразно обойтись и без организации соединений. В этом случае, передача данных между объектами происходит без предварительной договоренности между ними. Объект отправитель отправляет по логическому каналу объекту адресату блоки данных сразу же , как только появиться необходимость. Если же адресат не готов к приему, то эти блоки выбрасываются. Отправитель, не получив подтверждение о приеме блоков, хранит из копии и, если нужно, вновь отправляет их к адресату. При взаимодействии с установлением соединения осуществляется резервирование средств в сети для поддержки исходящего диалога во время существования соединения. При взаимодействии без установления соединения эти средства не резервируются.

Физические средства соединений **–** это совокупность физической среды аппаратных и программных средств, обеспечивающие передачу сигналов между системами. Их основой является используемая физическая среда: витая пара, плоский кабель, коаксиал, оптический кабель, эфир, и т.д.

Они делятся на 2 вида:

· пассивные **–** именуются соединения, предназначенные только для передачи сигналов;

· активные **–** не только передают сигналы, но и обеспечивают несложные виды их обработки: модуляцию, демодуляцию, контроль занятости канала, и т.д.

2.1.2. Канал

Канал **–** средство или путь, по которому передаются сигналы, либо данные. Современная технология передачи данных, исходя из экономических посылок, обеспечивает по одному физическому каналу одновременные взаимодействия группы пар систем, которые ведут передачу данных независимо друг от друга. Это приводит к необходимости рассмотрения пути, по которому данные передаются от источника к адресату. Этот путь определятся логическим каналом, которые может использовать частотную полосу или интервалы времени, выделенные в физическом канале. Виртуальные каналы являются важным звеном в общей классификации каналов. Они прокладываются через физический уровень, канальный уровень, и в ряде случаев сетевой уровень, а также последовательности физических каналов коммуникационной сети. Каждому из них присваивается номер. В блоках, отправляемых по виртуальному каналу, может не быть явных адресов отправителя и получателя, они заключены в номерах виртуальных каналов, что позволяет значительно сократить адресный блок. Различают асинхронный и синхронный каналы. В синхронном канале обеспечивается синхронизация процесса передачи, а в асинхронном она отсутствует. Различают симплексные (сигналы передаются в одном направлении), полудуплексные (сигналы передаются в двух направлениях, но по очереди), дуплексные каналы.

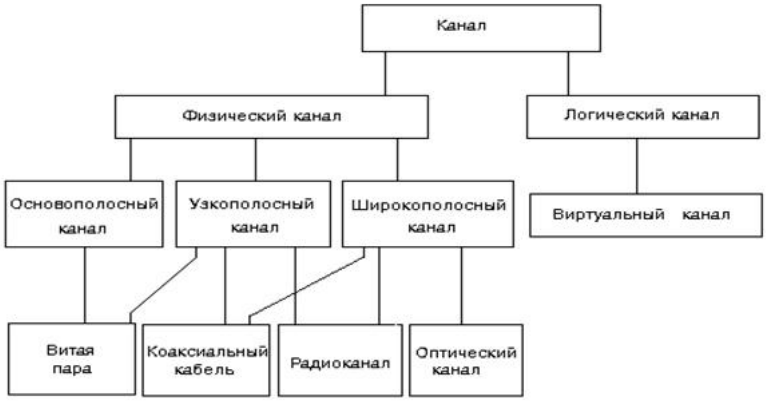


Рис. 2.4. Виды каналов передачи данных

2.1.3. Порт

Порт – точка доступа к устройству, либо программе. Различают физические и логические порты. Первые из них являются местами подключения физических объектов. Логические порты создаются на границах программных уровней, прикладных процессов, функциональных блоков. В портах начинаются и заканчиваются логические каналы и соединения, проложенные на любом уровне области взаимодействия.

2.2. Глобальная сеть.

Глобальная сеть — это сеть, абонентские системы которой расположены в разных странах. Они были созданы, как объединение территориальных сетей. Стремление к предоставлению сетевых служб и ресурсов большому числу пользователей привело к объединению территориальных сетей и созданию глобальных сетей. Благодаря своим большим размерам каждая из них предоставляет своим пользователям тысячи Баз Данных (БД), межконтинентальную электронную почту, возможность обучения практически любым специальностям. Кроме этого, глобальная сеть является связующим звеном большого числа небольших сетей. Глобальную сеть, состоящую из группы взаимодействующих территориальных сетей, называют также метасетью. Пример: сеть Internet. Создание глобальных сетей привело к появлению архитектуры компьютер-сеть, в которой простые и высокоэффективные сетевые компьютеры стали компонентами этих сетей и предназначены для использования их больших возможностей. Абонентские системы, позволили их обладателям интегрироваться в мировую информационную инфраструктуру.

2.3. Территориальная сеть.

Территориальная сеть — это сеть, системы которой расположены в различных географических точках. Она охватывает большое пространство (от района до группы стран). В случае, если она охватывает континенты, то используется название глобальной сети. Характерной особенностью является применение протяжённых широкополосных каналов, большого числа узлов коммутации или спутников связи. Она должна удовлетворять следующим основным требованиям:

- включать большое число абонентских систем (до нескольких тысяч);
- покрывать большой географический район; гарантировать безопасность данных;
- обеспечивать широковещание и доставку сообщений группам и отдельным адресатам;
- иметь высокую пропускную способность (до десятков Гбит/с);
- обладать большой надёжностью в работе; передавать разнообразные виды данных:

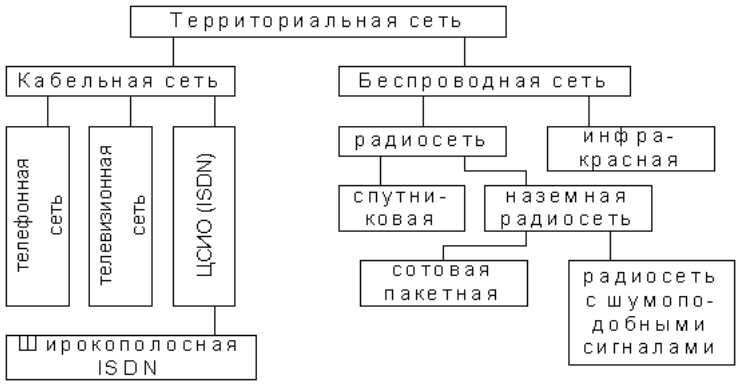


Рис. 2.5. Классификация территориальных сетей

2.4. Виртуальная сеть (VPN).

Виртуальная сеть – это сеть, характеристики которой в основном определяются её программным обеспечением.
Причины создания виртуальных сетей:

· необходимость создания оперативных изолированных от других пользователей рабочих групп. Рабочая группа – это совокупность пользователей, имеющих общие ресурсы и права использования этих ресурсов. Рабочая группа создаётся в сети для выполнения комплекса задач, определяемых функциональными обязанностями пользователей (разработка проекта, проведение электронного маркетинга и т.д.);

· желание облегчить процедуры перемещения, удаления объектов сети;

· стремление предоставить оперативную возможность смены ролей, чтобы клиент, когда это необходимо, мог выступать в роли сервера;

· возможность обеспечения безопасности данных путём локализации трафика в рамках изолированной группы.

Для этого в коммуникационной сети устанавливается интеллектуальное устройство (узлы коммутации, концентраторы, мосты и т.д.), которое в соответствии с указаниями административной системы соединяет друг с другом логические каналы, образуя закрытую для других абонентов локальную сеть. В одной большой ассоциации физических сетей может быть создано значительное число виртуальных сетей, функционирующих независимо друг от друга. Виртуальная технология обладает большой гибкостью, позволяющей динамически менять число и состав виртуальных сетей сколько угодно раз.

2.1.4. Варианты построения VPN

Можно выделить четыре основных варианта построения сети VPN, которые используются во всем мире. Данная классификация предлагается компанией Check Point Software Technologies, которая считается законодателем моды в области VPN.

Вариант "Intranet VPN", который позволяет объединить в единую защищенную сеть несколько распределенных филиалов одной организации, взаимодействующих по открытым каналам связи. Именно этот вариант получил широкое распространение во всем мире, и именно его в первую очередь реализуют компании-разработчики.

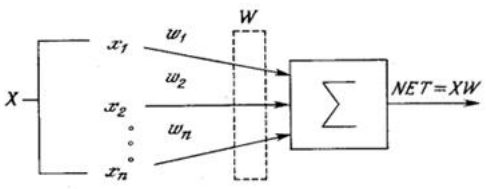
Вариант "Remote Access VPN", который позволяет реализовать защищенное взаимодействие между сегментом корпоративной сети (центральным офисом или филиалом) и одиночным пользователем, который подключается к корпоративным ресурсам из дома (домашний пользователь) или через notebook (мобильный пользователь). Данный вариант отличается от первого тем, что удаленный пользователь, как правило, не имеет статического адреса, и он подключается к защищаемому ресурсу не через выделенное устройство VPN, а прямиком со своего собственного компьютера, на котором и устанавливается программное обеспечение, реализующее функции VPN. Компонент VPN для удаленного пользователя может быть выполнен как в программном, так и в программно-аппаратном виде. В первом случае программное обеспечение может быть как встроенным в операционную систему (например, в Windows 2000), так и разработанным специально (например, АП "Континент-К"). Во втором случае для реализации VPN используются небольшие устройства класса SOHO (Small Office\Home Office), которые не требуют серьезной настройки и могут быть использованы даже неквалифицированным персоналом. Такие устройства получают сейчас широкое распространение за рубежом.

Вариант "Client/Server VPN", который обеспечивает защиту передаваемых данных между двумя узлами (не сетями) корпоративной сети. Особенность данного варианта в том, что VPN строится между узлами, находящимися, как правило, в одном сегменте сети, например, между рабочей станцией и сервером. Такая необходимость очень часто возникает в тех случаях, когда в одной физической сети необходимо создать несколько логических сетей. Например, когда надо разделить трафик между финансовым департаментом и отделом кадров, обращающихся к серверам, находящимся в одном физическом сегменте.

Последний вариант "Extranet VPN" предназначен для тех сетей, к которым подключаются так называемые пользователи "со стороны" (партнеры, заказчики, клиенты и т.д.), уровень доверия к которым намного ниже, чем к своим сотрудникам. Хотя по статистике чаще всего именно сотрудники являются причиной компьютерных преступлений и злоупотреблений.

2.5. Искусственные нейронные сети.

Искусственные нейронные сети чрезвычайно разнообразны по своим конфигурациям. Несмотря на такое разнообразие, сетевые парадигмы имеют много общего. Развитие искусственных нейронных сетей вдохновляется биологией. То есть рассматривая сетевые конфигурации и алгоритмы, исследователи мыслят их в терминах организации мозговой деятельности. ***Искусственный нейрон*** имитирует в первом приближении свойства биологического нейрона. На вход искусственного нейрона поступает некоторое множество сигналов, каждый из которых является выходом другого нейрона. Каждый вход умножается на соответствующий вес, аналогичный синаптической силе, и все произведения суммируются, определяя уровень активации нейрона. На рисунке представлена модель, реализующая эту идею. Хотя сетевые парадигмы весьма разнообразны, в основе почти всех их лежит эта конфигурация. Здесь множество входных сигналов, обозначенных x_1, x_2,…,x_n, поступает на искусственный нейрон. Эти входные сигналы, в совокупности обозначаемые вектором **X**, соответствуют сигналам, приходящим в синапсы биологического нейрона. Каждый сигнал умножается на соответствующий вес w_1, w_2,…, w_n, и поступает на суммирующий блок, обозначенный ?. Каждый вес соответствует «силе» одной биологической синаптической связи. (Множество весов в совокупности обозначается вектором **W**.) Суммирующий блок, соответствующий телу биологического элемента, складывает взвешенные входы алгебраически, создавая выход, который мы будем называть NET. В векторных обозначениях это может быть компактно записано следующим образом:



2.1.5. Однослойные и многослойные искусственные нейронные сети

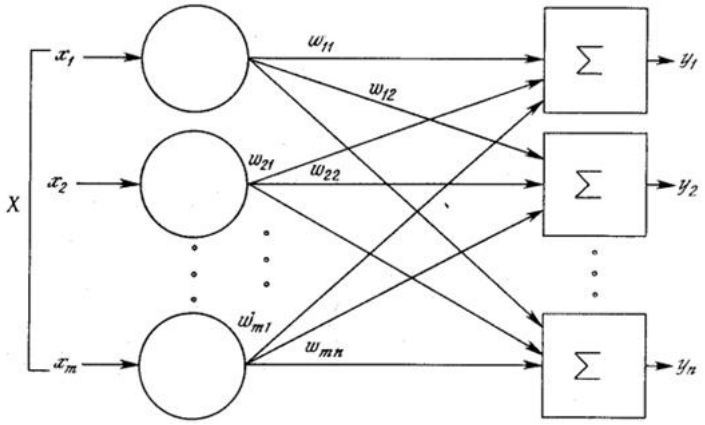


Рис. 2.6. Однослойная нейронная сеть

Хотя один нейрон и способен выполнять простейшие процедуры распознавания, сила нейронных вычислений проистекает от соединений нейронов в сетях. Простейшая сеть состоит из группы нейронов, образующих слой, как показано в правой части рис.1.5. Отметим, что вершины-круги слева служат лишь для распределения входных сигналов. Они не выполняют каких- либо вычислений, и поэтому не будут считаться слоем. По этой причине они обозначены кругами, чтобы отличать их от вычисляющих нейронов, обозначенных квадратами. Каждый элемент из множества входов **X** отдельным весом соединен с каждым искусственным нейроном. А каждый нейрон выдает взвешенную сумму входов в сеть. В искусственных и биологических сетях многие соединения могут отсутствовать, все соединения показаны в целях общности. Могут иметь место также соединения между выходами и входами элементов в слое. Удобно считать веса элементами матрицы **W**. Матрица имеет *m* строк и *n* столбцов, где m – число входов, а n – число нейронов. Например, $w_{2,3}$ – это вес, связывающий третий вход со вторым нейроном. Таким образом, вычисление выходного вектора **N**, компонентами которого являются выходы OUT нейронов, сводится к матричному умножению **N** =**XW,** где **N** и **X** – векторы-строки.

2.1.6. Сети встречного распространения

Возможности сети встречного распространения, превосходят возможности однослойных сетей. Время же обучения по сравнению с обратным распространением может уменьшаться в сто раз. Встречное распространение не столь общо, как обратное распространение, но оно может давать решение в тех приложениях, где долгая обучающая процедура невозможна. Будет показано, что помимо преодоления ограничений других сетей встречное распространение обладает собственными интересными и полезными свойствами.

Во встречном распространении объединены два хорошо известных алгоритма: самоорганизующаяся карта Кохонена и звезда Гроссберга Их объединение ведет к свойствам, которых нет ни у одного из них в отдельности. Методы, которые подобно встречному распространению, объединяют различные сетевые парадигмы как строительные блоки, могут привести к сетям, более близким к мозгу по архитектуре, чем любые другие однородные структуры. Похоже, что в мозгу именно каскадные соединения модулей различной специализации позволяют выполнять требуемые вычисления. Сеть встречного распространения функционирует подобно столу справок, способному к обобщению. В процессе обучения входные векторы ассоциируются с соответствующими выходными векторами. Эти векторы могут быть двоичными, состоящими из нулей и единиц, или непрерывными. Когда сеть обучена, приложение входного вектора приводит к требуемому выходному вектору. Обобщающая способность сети позволяет получать правильный выход даже при приложении входного вектора, который является неполным или слегка неверным. Это позволяет использовать данную сеть для распознавания образов, восстановления образов и усиления сигналов.

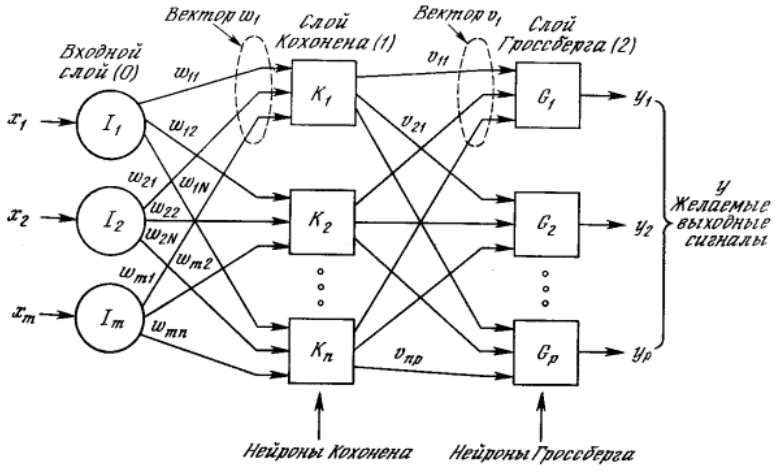


Рис. 2.7. Сеть с встречным распознаванием без обратных связей

2.1.7. Оптические нейронные сети

Взаимное соединение нейронов с помощью световых лучей не требует изоляции между сигнальными путями, световые потоки могут проходить один через другой без взаимного влияния. Более того, сигнальные пути могут быть расположены в трех измерениях. Плотность путей передачи ограничена только размерами источников света, их дивергенцией и размерами детектора. Потенциально эти размеры могут иметь величину в несколько микрон. Наконец, все сигнальные пути могут работать одновременно, тем самым обеспечивая огромный темп передачи данных. В результате система способна обеспечить полный набор связей, работающих со скоростью света. Оптические нейронные сети могут также обеспечить важные преимущества при проведении вычислений. Величина синаптических связей может запоминаться в голограммах с высокой степенью плотности; некоторые оценки дают теоретический предел в 10^{12} бит на кубический сантиметр. Хотя такие значения на практике не достигнуты, существующий уровень плотности памяти очень высок. Кроме того, веса могут модифицироваться в процессе работы сети, образуя полностью адаптивную систему.

Контрольные вопросы:

1. Что такое локальная сеть?
2. Чем отличаются глобальные от территориальных сетей?
3. Изобразите схематически иерархию компьютерных сетей.
4. Расскажите о классификации территориальных сетей.
5. Какие виды каналов передачи данных Вы знаете?
6. Что из себя представляет глобальная сеть?
7. Что такое виртуальная сеть?
8. Какие виды нейронных сетей Вы знаете?
9. Какой протокол описывает свойства беспроводных сетей?
10. Что такое порт?

Практические задания:

ЗАДАНИЕ № 2.1. Основы работы с Network Monitor.

Network Monitor: установка, приемы работы, перехват трафика в локальной сети.

Задание:

1) из каталога Снифферы\Netmon_SMS2003 на компакт-диске произведите установку полной версии Network Monitor и убедитесь, что он работает;

2) настройте в Network Monitor фильтр таким образом, чтобы перехватывались только данные, которые передаются между вашим и преподавательским компьютером (LONDON);

3) выполните в командной строке команду.

ping LONDON

перехватите и просмотрите эти пакеты.

Решение:

1) из каталога NetMon_SMS2003\I386 запустите программу NETMONSETUP.EXE (Внимание! На одном уровне с каталогом NetMon_SMS2003 должен находиться каталог SMSSETUP) и произведите установку Network Monitor;

2) из меню Start -> Programs -> Microsoft Network Monitor запустите Microsoft Network Monitor. В ответ на приглашение Please specify the network... нажмите OK и выберите сетевое соединение Local Computer -> Local Area Connection, а затем еще раз нажмите OK. В меню Capture выберите Start и убедитесь, что Network Monitor перехватывает сетевые пакеты. В меню Capture выберите Stop и остановите перехват;

3) выполните в командной строке команду;

PING LONDON

чтобы узнать IP-адрес компьютера преподавателя. Затем в Network Monitor в меню Capture выберите Filter и в окне Capture Filter нажмите на кнопку Edit. Откроется окно Address Expression.

4) В окне Address Expression и нажмите на кнопку Edit Addresses. Откроется окно Address Database. В этом окне нажмите на кнопку Add и введите информацию об адресе:

Name: LONDON;

флажок Permanent Name: установлен;

Type: IP;

Address: IP-адрес компьютера преподавателя (который вы узнали в п.3);

Comment: Trainer computer.

Нажмите OK, а затем Close. В оба списка в окне Address Expression будет добавлен созданный вами адрес.

5) В левой части окна Address Expression в столбце Station 1 выберите Local и IP-адрес вашего сетевого соединения. Затем в правой части окна в столбце Station 2 выберите созданный вами адрес. Убедитесь, что в столбце Direction стоит знак "оба направления" (<->) и нажмите OK. В окне Capture Filter должна появиться дополнительная строка;

INCLUDE имя_вашего_компьютера(IP) <-> LONDON(IP)

6) В окне Capture Filter выделите строку *INCLUDE *ANY <-> *ANY* и нажмите на кнопку Delete, чтобы осталась только созданная вами строка. Затем нажмите на кнопку OK, чтобы закрыть окно Capture Filter с сохранением сделанных изменений;

7) В меню Capture выберите Start, чтобы начать перехват данных. Затем в командной строке еще раз выполните команду *PING LONDON*. После этого в меню Capture выберите Stop and View и просмотрите захваченные данные.

ЗАДАНИЕ № 2.2. Основы работы с IRIS.

Сниффер EEYE IRIS, перехват трафика в сети, настройка фильтров, реконструкция сеансов, статистика по протоколам, компьютерам, загрузке сети и размеру пакетов.

Задание:

1) из каталога Снифферы\IRIS на компакт-диске произведите установку IRIS и убедитесь, что он работает;

2) настройте в IRIS фильтр для перехвата только трафика HTTP;

3) из Internet Explorer откройте начальную страницу Web-сайта на компьютере LONDON. Перехватите этот трафик из IRIS и реконструируйте в IRIS сеанс обращения на Web-сервер (в IRIS должна быть видна та страница, к которой вы обращались из Internet Explorer);

4) получите из IRIS информацию о распределении трафика по протоколам, по компьютерам, по размеру пакетов и по загрузке сети.

Решение:

1) Из каталога Снифферы\Iris запустите файл Iris407Demo.exe и произведите установку с параметрами по умолчанию. После окончания установки запустите Iris и выберите ваш сетевой адаптер.

2) В меню Filters выберите Edit Filter и в окне Edit Filter Settings выберите строку Layer 2,3. В столбце Frame установите флажок напротив 0x0800 DoD IP, в столбце Layer 3+ (IP) - флажок напротив 0x06 (TCP). Затем щелкните по строке Ports, чтобы открыть вкладку Ports.

3) На вкладке Ports в списке Known Ports дважды щелкните по строке HTTP 80, чтобы добавить протокол HTTP в список портов фильтра. Нажмите на кнопку OK.

4) В меню Capture выберите Start, чтобы начать перехват пакетов.

5) Откройте у себя на компьютере Internet Explorer и в его адресной строке введите London. Если возникло предупреждение системы безопасности, добавьте этот адрес в Internet Explorer в список доверенных.

6) Вернитесь в окно Iris и в меню Capture выберите Stop, чтобы остановить перехват данных. Затем в меню выберите команду Send buffer to Decode. Откроется окно Decode.

7) В окне Host Activity выберите сеанс вашего компьютера (могут быть перехвачены и сеансы других компьютеров), затем в нижнем правом окне воспользуйтесь кнопкой Select displaying format (зеленого цвета), чтобы отобразить трафик данного сеанса в разных режимах (пакетов, ASCII, HTML). Затем нажмите на кнопку с надписью GO (красного цвета). В окне Select Items to be retrieved from Internet выберите строку со слэшем (/) и нажмите кнопку Go get it! Просмотрите страницу в окне IRIS.

8) В меню View выберите Protocol Distribution, Top Hosts, Size distribution, Bandwith и Traffic report. Обратите внимание, что для первых трех пунктов бесплатная версия Iris показывает случайные данные.

ЗАДАНИЕ № 2.3. Перехват парольных хэшей NTLMv2 и их расшифровка.

Хэши Windows NTLM V2 при аутентификации по сети, перехват и расшифровка программой Cain&Abel.

Задание:

1) создайте на своем компьютере несколько локальных пользователей с паролями разной длины и сложности. При создании пользователей лучше снять флажок User must change password at next logon. Также создайте на своем компьютере общий каталог (например, Test) и предоставьте этим пользователям (или просто группе Everyone) права на него;

2) установите программу Cain&Abel на своем компьютере и запустите на ней сниффер паролей;

3) попросите соседа подключиться к вашему компьютеру по сети от имени созданных вами пользователей (удобнее всего это сделать через Map Network Drive -> Connect using a different user name, не забывайте сразу удалять созданные вами сетевые диски);

4) при помощи Cain просмотрите пойманные парольные хэши и постарайтесь подобрать пароли;

5) протестируйте вручную при помощи Cain пароли для пойманных вами хэшей (подходит данный пароль к хэшу или нет). Используйте при тестировании правильные и неправильные пароли.

Примечание: утилита Cain находится в настоящий момент на стадии бета-тестирования, а реальный взлом паролей NTLMv2 (особенно грубой силой) может потребовать очень большого количества времени. Поэтому вполне допускается возникновение проблем в работе программы, или вам не удастся взломать пароли созданных вами пользователей. Постарайтесь в этом случае просто познакомиться с возможностями Cain.

Примечание 2: при обращении пользователя по протоколу NTLMv2 передаются также хэши LanManager и NTLM, которые не привязаны к паролю и взламывать которые бессмысленно. В ответе будет использована попытка взломать хэши NTLM+Challange для целей демонстрации, взломать пароли при помощи нее, скорее всего, не получится.

Решение:

1) После создания пользователей запустите из каталога Снифферы\Cain&Abel файл cain25b56.exe и произведите установку этой программы с параметрами по умолчанию. По окончании установки Cain примите предложение установить драйвер WinPCAP. завершите установку и перезагрузите компьютер.

2) Запустите Cain и нажмите на пункт меню Configure. На вкладке Sniffer выберите ваш сетевой адаптер и нажмите OK. Затем нажмите на кнопку Start Sniffer (крайняя левая кнопка в панели инструментов) и перейдите на вкладку Sniffer, а в ней - на еще одну вкладку (внизу) Passwords. В ней показывается информация о перехваченных паролях.

3) Попросите соседа подключиться к вашему компьютеру от имени созданных вами пользователей (и сами выполните те же действия для его компьютера). Это можно сделать так: щелкните правой кнопкой мыши по иконке "My Computer", в контекстном меню выберите Map Network Drive, затем введите путь к сетевому каталогу на компьютере пользователя (например, \\vancouver\test) и щелкните по ссылке Connect using a different username. Далее введите имя пользователя и пароль, потом удалите созданный сетевой диск - и так несколько раз. Убедитесь, что количество пойманных парольных хэшей в Cain в контейнере SMB растет.

4) Щелкните правой кнопкой мыши по пойманным парольным хэшам и в контекстном меню выберите Send all to Cracker. Перейдите на вкладку Cracker и выделите (с клавишей Shift) пойманные вами хэши. Затем щелкните по ним правой кнопкой

мыши и в контекстном меню выберите Dictionary Attack (NTLM + Challenge). Откроется окно Dictionary Attack с информацией о количестве загруженных хэшей.

5) В окне Dictionary Crack нажмите на кнопку Add и выберите файл Wordlists.txt в каталоге Wordlists, а затем нажмите на кнопку Open, чтобы вернуться в окно Dictionary Crack. Нажмите на кнопку Start и просмотрите, как происходит перебор паролей по словарю.

6) После окончания перебора по словарю можно запустить перебор грубой силой - пункт контекстного меню Brute-Force Attack (NTLM + Challenge) и посмотреть, как оценит необходимое время для перебора Cain. Дожидаться окончания перебора грубой силой не рекомендуется.

7) Чтобы протестировать пароль, можно выбрать в контекстном меню команду Test Password и ввести свой пароль. Если пароль правильный, то строка будет помечена рисунком ключа, если нет - замка.

ЗАДАНИЕ № 2.4. Просмотр сетевых соединений и открытых портов.

Просмотр сетевых соединений и открытых портов на компьютере Windows, утилита TCPView.

Задание:

При помощи утилиты TCPView из каталога "Мониторинг локальных соединений" просмотрите текущие сетевые соединения и открытые порты своего компьютера и определите, какая программа открыла это соединение/порт. Получите информацию как в виде имен компьютеров и названий служб, так и в виде IP-адресов и номеров портов.

Решение:

Запустите файл TCPView.exe из каталога Мониторинг локальных соединений\TCP View на компакт-диске. Просмотрите свойства процессов, которые работают с портами и сетевыми соединениями. Чтобы переключиться между режимами показа, в меню Options снимите/установите флажок Resolve Names.

ЗАДАНИЕ № 2.5. Шифрование трафика при помощи IPSec.

IPSec в Windows, создание и активация политики IPSec, проверка шифрования данных.

Примечание: эта лабораторная работа выполняется в паре. Перед ее выполнением найдите партнера, с которым вы будете ее выполнять.

Ситуация: в связи с особенностями сетевого приложения между двумя компьютерами под управлением Windows 2003 Server в вашей сети открытым текстом передается важная информация. Вы должны сделать невозможным перехват всего трафика между этими двумя компьютерами. Весь трафик с другими компьютерами может передаваться в обычном режиме .

Задание:

1) Установите на оба компьютера в паре Internet Information Server в конфигурации по умолчанию и убедитесь, что вы видите на компьютере партнера страницу Under Construction.

2) Настройте на обоих компьютерах принудительное шифрование всего IP-трафика между этими двумя компьютерами с использованием Preshared key.

3) Настройте получение информации о статистике передачи пакетов IPSec.

4) Еще раз обратитесь на Web-сайт на компьютере партнера и убедитесь при помощи IRIS и Network Monitor, что данные сеанса теперь просмотреть невозможно. Сравните данные, представляемые IRIS и Network Monitor.

5) Отключите применение IPSec на обоих компьютерах в паре.

Решение:

1) Откройте Панель управления -> консоль Add/Remove Programs -> Add/Remove Windows Components и установите флажок напротив Application Server (флажок должен быть затененным - выбранным частично). Если компьютер не сможет найти путь к дистрибутиву Windows 2003 Server самостоятельно, обратитесь за дистрибутивом к преподавателю.

2) После окончания установки у партнера обратитесь на его компьютер из Internet Explorer. Вы должны увидеть страницу "Under construction".

3) В командной строке выполните команду MMC. Откроется оболочка Microsot Management Console. В меню File выберите Add/Remove Snap-In и добавьте две консоли: IP Security Policy Managenet (для локального компьютера) и IP Security Monitor. Нажмите на кнопку Add, а затем OK, чтобы вернуться в основное окно консоли. Для удобства созданную вами консоль можно сохранить, например, на рабочем столе под именем IPSec.msc.

4) В созданной вами консоли раскройте узел IP Security Policies on Local Computer, щелкните по этому узлу правой кнопкой мыши и в контекстном меню выберите Create IP Security Policy. Запустится мастер создания политики IP Security.

5) На первом экране мастера введите имя политики (например, TestPolicy) и нажмите Next.

6) На втором экране (Requests for Secure Communication) снимите флажок Activate the default response rule и нажмите Next.

7) На последнем экране мастера убедитесь, что флажок Edit Properties установлен и нажмите Finish. Откроется экран свойств вашей политики. Нажмите в нем на кнопку Add, чтобы добавить новое правило для вашей политики. На первом экране мастера создания правил нажмите Next.

8) На втором экране мастера (Tunnel Endpoint) убедитесь, что переключатель стоит в положении This rule does not specify a tunnel и нажмите Next.

9) На экране Network Type оставьте переключатель в положении All network connections и нажмите Next.

10) На экране IP Filter list нажмите на кнопку Add. Откроется окно создания нового фильтра. В этом окне введите название фильтра (например, имя компьютера партнера_filter) и нажмите Add. Откроется еще один мастер - создания фильтров. На его первых двух экранах нажмите Next.

11) На экране IP Traffic Source оставьте в качестве адреса источника My IP Address и нажмите Next.

12) На экране IP Traffic Destination выберите в списке адресов назначения A specific IP address и укажите IP-адрес вашего партнера. На остальных экранах этого мастера оставьте значения по умолчанию. Вы опять вернетесь в окно IP Filter List, в котором будет присутствовать созданный вами фильтр. Нажмите в нем OK и в окне Security Rule Wizard на экране IP Filter List установите переключатель напротив созданного вами фильтра. Нажмите Next.

13) На следующем экране (Filter Action) установите переключатель в положение Require Security и нажмите Next.

14) На следующем экране (Authentification Method) установите переключатель в положение Use this string to protect the key exchange (preshared key) и в поле внизу введите текстовое значение, например, TEST. Это значение должно совпадать с тем значением, которое ввел у себя партнер. Нажмите Next, на последнем экране снимите флажок Edit Properties и нажмите Finish. Затем в окне консоли MMC щелкните правой кнопкой мыши по созданной вами политике и в контекстном меню выберите Assign. Дождитесь, пока партнер завершит выполнение аналогичных действий на своем компьютере.

15) Раскройте узел IP Security Monitor -> имя вашего компьютера -> Active Policy и просмотрите информацию о назначенной вами политике и о статистике взаимодействия по IPSec (под Main Mode).

16) Запустите Iris и в меню Filters выберите команду Clear Filters. Запустите IRIS на перехват сетевого трафика и обратитесь к Web-сайту вашего партнера. Затем остановите перехват, в меню Decode выполните команду Send buffer to Decode и просмотрите трафик сеанса вашего компьютера. IRIS не сможет расшифровать никакие данные выше протокола IP.

17) Запустите Network Monitor и настройте в нем фильтр для перехвата трафика только между ваши компьютером и компьютером партнера (аналогично тому, как это делалось в перовой лабораторной). Network Monitor покажет служебную информацию протокола ESP.

18) Вернитесь в созданную вами консоль IPSec, щелкните правой кнопкой мыши по созданной вами политике и в контекстном меню выберите Un-assign. Дождитесь пока, ту же операцию выполнит ваш партнер, и убедитесь, что вы опять можете обратиться на его Web-сервер.

ЗАДАНИЕ № 2.6. Обнаружение снифферов в локальной сети.

Выявление снифферов в локальной сети, применение утилиты ProDetect.

Задание:
При помощи утилиты ProDetect выявите работающие снифферы в локальной сети.

Примечание: утилита ProDetect находится на стадии бета-версии и работает только с библиотекой WinPCAP версии 2.3 (версии 3.0 и старше не подходят).

Решение:

1) Откройте панель управления -> Add/Remove Programs и найдите там библиотеку WinPCAP 3.0 (она должна появиться после установки Cain). Удалите ее и обязательно перезагрузите компьютер.

2) Из каталога Снифферы\WPCAP на компакт-диске запустите файл WinPcap_2_3.exe и произведите установку этой библиотеки.

3) Из каталога Антисниффинг\ProDetect на компакт-диске произведите установку утилиты ProDetect.

4) Откройте каталог C:\Program Files\ProDetect\Binaries и запустите оттуда файл prodetect.exe.

5) В меню Options выберите Network Interface Setup и в списке Network Interface выберите ваш сетевой адаптер (в нем не должно быть слов NdisWan). Нажмите на кнопку Accept.

6) В меню Options выберите Preferences и добавьте в него перечень сканируемых IP-адресов локальной сети (например, 192.168.5.200 - 192.168.5.220). Просмотрите возможности на вкладке Alert Options, затем нажмите на кнопку Accept.

7) В меню File выберите Start. В ходе сканирования и по окончании его можно просматривать информацию об обнаруженных компьютерах, работающих в promiscuous mode, при помощи вкладки Report.

Перечень литературы и Интернет-ресурсов:

1. Бройдо В.Л. Вычислительные системы, сети и телекоммуникации: Учебник для вузов. 2-е изд. – СПб.: Питер, 2005. – 703 с.: ил.

2. Бэрри Нанс. Компьютерные сети пер. с англ. – М.: БИНОМ, 1996.

3. Гайсина Л.Ф. Сети ЭВМ и телекоммуникации: Учебное пособие. - Оренбург: ГОУ ОГУ, 2004. - 160 с.

4. Компьютерные сети: Учебный курс Microsoft Corporation – М.: Издательский отдел «Русская редакция», 1999.

5. Кульгин М. Практика построения компьютерных сетей. Для профессионалов. – СПб.: Питер, 2001. – 320 с.

6. Новиков Ю.В., Кондратенко С.В. Локальные сети: архитектура, алгоритмы, проектирование.- М.: Издательство ЭКОМ, 2000.- 312 с.

7. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. (рекомендовано Мин. образования РФ). СПб: Питер, 2001,668 с.

8. Основы локальных сетей - http://www.intuit.ru/department/network/baslocnet/

9. Пятибратов А.П., Гудыно Л.П. Вычислительные системы, сети и телекоммуникации. – М.: Финансы и статистика, 2001. – 512 с.

10. Столлингс В. Современные компьютерные сети. – СПб.: Питер, 2003. – 783 с.

11. Уоссермен Ф. Нейрокомпьютерная техника: Теория и практика. Пер. с англ., 1992. 118 с.

12. Учебник по компьютерным сетям. Сетям — http://kompset.narod.ru/siteunior.html

13. Якубайтис Э.А. Информационно-вычислительные сети. – М.: Финансы и статистика, 1984. – 232 с.

14. Якубайтис Э.А. Локальные информационно-вычислительные сети. – Рига: Зинатне, 1985. – 284 с.

Тема 3. Информационные ресурсы и теоретические основы современных информационных систем

Цели:

· Сформировать основные представления о базах данных, как информационном хранилище знаний.
· Уметь применять различные поисковые системы для получения информации.
· Разобраться в ключевой роли анализа сетей теории очередей (называемой также теорией массового обслуживания).

3.1. Ресурсы, базы данных и базы знаний, информационное хранилище.

Ресурсы – это данные, приложения (программы) и периферийные устройства (принтер, плоттер, сканер, модем и т.п.). Понятие ***интерактивной связи*** компьютеров подразумевает обмен сообщениями в реальном режиме времени.

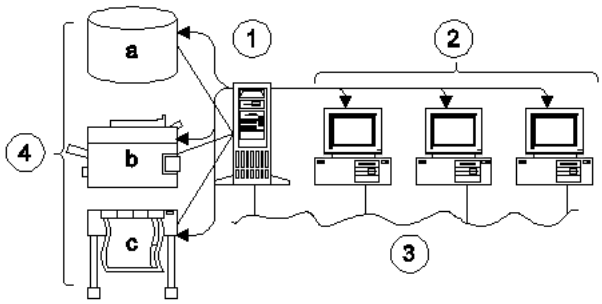


Рис. 3.1. Пример разделения общих ресурсов в ИС

(**1 –** сервер, **2 –** клиенты, **3 –** среда передачи данных **–** сетевой кабель, **4 –** разделяемые ресурсы: **a –** данные (файлы, базы данных), **b,c –** периферийные устройства (принтер, плоттер))

Ресурс – это объект системы или сети, предоставленный процессу. Объекты делятся на физические и логические. К первым относятся процессоры, внешние устройства, физические каналы, узлы коммутации, ... Логическими ресурсами являются программы, навигаторы, трансляторы, языки, платформы, интерфейсы, память, логические каналы и т.д.. Ресурс может использоваться одним либо одновременно несколькими процессами. В последнем случае необходимо организовать такое обращение к ресурсу, которое без каких-либо конфликтов распределяет его между процессами. Основной информационный ресурс сетей – находящаяся на объектах системы информация. Доступ к информационным ресурсам сети осуществляется с помощью транзакций.

Транзакция — короткий во времени цикл взаимодействия объектов, включающий запрос - выполнение задания - ответ. Информация в основном расположена в базе данных.

База Данных - совокупность взаимосвязанных данных, организованная по определенным правилам. Строго говоря, базой данных является специальным образом организованные один либо группа файлов. Для работы с ними используется СУБД. При этом подразумевается, что база данных определена по схеме, не зависящей от программ, которые к ней обращаются. БД характеризуется ее концепцией - совокупностью требований, определяемых представлениями пользователей о необходимой им информации. На основе баз данных создаются разнообразные системы, например, электронные библиотеки.

Распределённая база данных – это БД, содержимое которой расположено в нескольких абонентских системах информационной сети. Это позволяет располагать данные так, что последние с одной стороны находятся в пунктах наибольшего их спроса, а с другой стороны обеспечивается доступ к любым данным, не зависимо от того, где они находятся. Распределённая база данных, создаваемая заново, является однородной. Вместе с этим, нередко она образуется как совокупность группы баз данных, уже функционирующих в ряде систем. В этом случае возникает неоднородная распределённая база данных. Оба типа баз погружаются в Систему Управления Распределенной Базой Данных (СУРБД).

Характерными особенностями распределённой базы данных являются:

· использование распределенного словаря, содержащего сведения о характере имеющихся данных, их размещении и способе доступа к ним;
· выполнение транзакций или обеспечение работы электронной почты между всеми абонентскими системами;
· пространственная прозрачность, дающая возможность не знать, где расположены компоненты базы. Перемена места хранения файла не приводит к изменению способа и процедуры доступа к этому файлу;
· прозрачность распределения, позволяющая размещать данные в любых абонентских системах;
· полная функциональность, т.е. возможность выполнения всех тех же операций, которые возможны в базе, находящейся в одной системе;
· целостность данных, обеспечиваемая функциями слежения за данными, исправления ошибок;
· независимость от типов используемых в системах устройств.
· работа с частью базы данных, расположенной в одной системе, не может быть прервана обращением из другой системы;
· администратор части базы, находящейся в одной системе работает независимо от администраторов частей базы, расположенных в других системах.

Информационное хранилище – это программная платформа, опирающаяся на большое количество баз данных и представляющая пользователям и прикладным программам подготовленную нужным образом информацию.

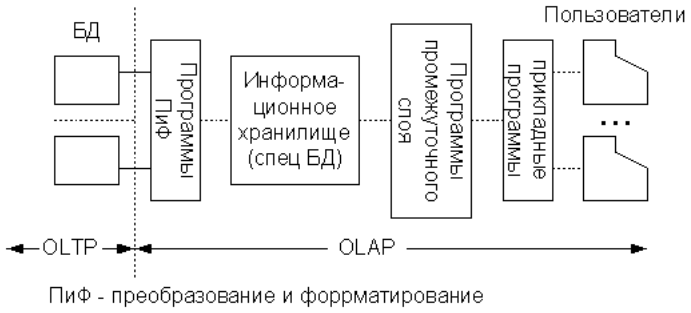


Рис. 3.2. Структура

Здесь процесс обработки данных физически разделяется на 2 этапа: первый из них связан с обработкой транзакций в реальном времени (OLTP), в результате чего в базе данных накапливается первичная информация (например, функционировании финансового банка). На втором этапе осуществляется аналитическая обработка в реальном времени (OLAP) (например, анализ снятия наличности со счетов, планирование объёма оказываемых услуг, показатели эффективности работы отделений и всего банка и т.д.).

Знания – это накопленные человечеством факты, истины и прочие объекты познания. Поэтому в отличии от базы данных в базе знаний располагаются сведения, содержащиеся в документах, книгах, статьях и отчётах.

Элементы знаний, благодаря концептуальным связям, предоставляемых гиперсредой, объединяются, образуя базу знаний. Такие связи бывают четырёх видов:

- общность – связь двух элементов по содержанию их характеристик;
- партитивность – соотношение целого и его частей;
- противопоставление – встречается в элементах, которые имеют положительные и отрицательные характеристики;
- взаимосвязь – отражает взаимную зависимость элементов.

Базы знаний – это организованная совокупность знаний, относящихся к какой-нибудь предметной области. Базы знаний применяются при решении задач искусственного интеллекта. Доступ к информации может быть осуществлён, например, через электронную библиотеку, электронную биржу, информационный киоск, с помощью видеотекса, телетекста и т.д.

«**Научно-техническая информация**»(Scienceandtechnicalinformation, STI) означает документированную информацию, возникающую в результате научного и технического развития, а также информацию, необходимую руководителям, научным, инженерным и техническим работникам в процессе их деятельности, включая специализированную экономическую и нормативно-правовую информацию.

3.2. Поиск и отбор информации в информационных системах.

Поиск - процесс, в ходе которого в той или иной последовательности производится соотнесение отыскиваемого с каждым объектом, хранящимся в массиве. Цель любого поиска заключается в потребности, необходимости или желании находить различные виды информации, способствующие получению лицом, осуществляющим поиск, нужных ему сведений, знаний и т.д. для повышения собственного профессионального, культурного и любого иного уровня; создания новой информации и формирования новых знаний; принятия управленческих решений и т.п.

Существуют различные толкования термина "поиск информации" или "информационный поиск". Термин "информационный поиск" (англ. "information retrieval") ввёл американский математик К. Муэрс. Он заметил, что побудительной причиной такого поиска является *информационная потребность*, выраженная в форме информационного запроса. К объектам информационного поиска К. Муэрс отнес документы, сведения об их наличии и (или) местонахождении, фактографическую информацию.

Решать проблемы фактографического поиска первыми стали представители библиотек. Они разработали средства информационного поиска, получившие название "справочно-поисковый аппарат" (каталоги, библиографические указатели и др.). В профессиональной отечественной печати данный термин используется с 1970-х годов. Библиотекари определяют "информационный поиск" как нахождение в информационном *массиве документов*, соответствующих *информационному запросу пользователей*.

С точки зрения использования компьютерной техники ***информационный поиск*** - совокупность логических и технических операций, имеющих конечной целью нахождение документов, сведений о них, фактов, данных, релевантных запросу потребителя.

Релевантность - устанавливаемое при информационном поиске соответствие содержания документа информационному запросу или поискового образа документа поисковому предписанию.

Системы, обеспечивающие реализацию подобного поиска информации, называются **поисковыми системами** (ПС). В традиционных технологиях ПС представляют картотеки и каталоги, адресные и иные справочники, указатели, энциклопедии, справочный аппарат к изданиям и другие материалы.

Поисковые системы осуществляют поиск среди документов базы или иных массивов машиночитаемых данных, содержащих заданные слова. Электронные ПС с помощью обычных или интеллектуальных терминалов (ПЭВМ) дают возможность пользователям производить поисковые запросы при помощи формальных и описывающих содержание элементов и с применением специальных логических операторов; осуществляют поиск среди документов базы или иных массивов машиночитаемых данных, содержащих заданные слова. Поисковые системы позволяют осуществлять только поисковые процедуры и связанные с ними процессы.

Информационно-поисковые системы Поисковые системы с большим набором функций и возможностей обычно входят в состав СУБД и именуются информационно-поисковыми системами. Они также создаются и используются для эффективного нахождения пользователями необходимых им данных, в том числе в Интернете. Система, обеспечивающая поиск и отбор

необходимых данных на основе информационно-поискового языка и соответствующих правил поиска, а **база данных** - как совокупность средств и методов описания, хранения и манипулирования данными, облегчающих сбор, накопление и обработку больших информационных массивов. Организация различных БД отличается видом объектов данных и отношений между ними.

Терминологически "**информационно-поисковая система**" (англ. "information retrieval system", IRS) - представляет систему, предназначенную для поиска и хранения информации; пакет программного обеспечения, реализующий процессы создания, актуализации, хранения и поиска в информационных базах и банках данных.

Функционирование современных ИПС основано на двух предположениях:

· документы, необходимые пользователю, объединены наличием некоторого признака или комбинации признаков;

· пользователь способен указать этот признак.

Автоматизированные ИПС (АИПС), используют компьютерные программно-технические средства и технологии и предназначаются для нахождения и выдачи пользователям информации по заданным критериям.

ИПС делятся на: традиционные (ручные, механические, электромеханические) и автоматизированные (электронные). Информационно-поисковые системы предназначены для поиска информации в базе данных. По характеру выдаваемой информации они делятся на 2 типа:

· документальные системы по заданию пользователя выдают необходимые ему документы (книги, законы, статьи и т.д.);

· фактографические: её задача – поиск в документах интересующих пользователя сведений (например, типы, характеристики и технологии изготовления стали).

3.3. Электронные документы, книги и библиотеки. Электронный офис.

Электронный документ - документ, представленный в электронной форме (оцифрованный или подготовленный на компьютере), имеющий электронную подпись, идентифицирующую (подтверждающую) его подлинность.

Электронные тексты - электронные (машиночитаемые) документы, хранящиеся на любых машинных носителях данных, доступные для использования в компьютерных программно-технических устройствах и системах.

Электронное издание - это издание, представляющее электронную запись информации (произведение) на каком-либо машиночитаемом носителе информации и рассчитанное на использование с помощью электронных технических устройств.

Электронная книга - это вид книги, хранящийся в электронном форме на любом машиночитаемом электронном носителе и включающий специальные средства навигации в ней.

Электронная библиотека (от англ. "digital library" - "цифровая библиотека") - вид, как правило, общедоступной автоматизированной информационной системы, содержащей машиночитаемые (электронные) документы. ЭБ помогают обучаемым и преподавателям экономить время на получение нужной им литературы, что очень важно при работе в режимах активного (в том числе дистанционного) обучения. Подобная библиотека функционирует на сайте МФПА.

Практически в любых организациях, предприятиях, учреждениях, ведомствах, фирмах, учебных заведениях и т.п. функционируют различные информационные потоки. Если деятельность таких организаций в значительной степени связана с использованием компьютерных информационных технологий, средств и методов преобразования информации, то их обычно называют ***электронными офисами***. Они представляют собой систему автоматизации работы учреждения, основанную на применении компьютерной техники. Использование Интернета позволило создать разновидность электронного офиса, получившую название “*виртуальный офис*”. В этом случае основные функции информационного обслуживания управленческой деятельности и информационные ресурсы не сосредоточены в реальном офисе с соответствующими атрибутами (помещением, оборудованием, персоналом и т. п.), а пространственно распределены в различных узлах информационной сети.

3.4. Электронная биржа и информационный киоск. Видеотекс, телетекс и факс.

По определению МСЭ-Т "***телематические службы*** - службы электросвязи (кроме телефонной, телеграфной и служб передачи данных), которые организуются с целью обмена информацией через сети электросвязи". Первая телематическая служба Телетекс появилась в начале 80-х годов. ***Телетекс*** - буквенно-цифровая система передачи деловой корреспонденции, предназначенная для обслуживания учреждений и предприятий. Эта система несколько напоминает систему ***Телекс*** (абонентский телеграф - АТ), но отличается от нее сохранением формы текста, значительно большим набором знаков, большей скоростью передачи, высокой достоверностью (одна ошибка на 400 страниц печатного текста), возможностью редактировать подготовляемую к передаче документацию. ***Телетекс –*** это сетевая служба передачи текстовых документов. Является простейшей разновидностью электронной почты. Функционирует в телефонной сети.

Телерукопись - служба передачи графической информации, которая отображается на приемном конце согласно движениям "пера", пишущего на передающем конце. Сообщения, наносятся отправителем на бумагу, лежащую на специальном планшете.

Электронная биржа – это биржа, ведущая торги с использованием информационной сети. Брокеры-посредники могут находиться в различных географических пунктах и странах. ***Информационный киоск —*** автоматизированный программно-аппаратный комплекс, предназначенный для предоставления справочной информации.

Видеотекс – сетевая служба доступа терминалов к базе данных и сервисам, предоставляемым сетью. Работает в общественной телефонной сети. Различают три видеотекса:

· справочная служба;

· служба передачи сообщений;

· диалоговая служба.

Все они в первую очередь предназначены для конторской деятельности. В последнее время стал использоваться и для широких пользователей.

Факсимильная связь – это передача через коммуникационную сеть неподвижных изображений и текста. Для устранения недостатков созданы компьютерные факсимильные системы, включаемые в сеть при помощи факсимильных плат. Эти системы, соединяясь друг с другом, способны, не пользуясь бумагой, передавать точные копии документов. Рассматриваемая интеграция обеспечивает также шифрование передаваемой информации.

Служба телеконференции позволяет проводить в реальном масштабе времени конференции между пользователями, расположенными в разных местах, с помощью терминалов и сетей электросвязи. Различают *аудиографические* и *видеоконференции*.

3.5. Теоретические основы современных информационных сетей.

Рассматриваются два характерных типа сетей: с коммутацией пакетов и коммутацией каналов. В первом случае, через сеть от источника к получателю по некоторому маршруту, выбор которого определяется проектом сети, передаются пакеты, т.е. блоки данных переменной длины. В случае коммутации каналов, для пары пользователей устанавливается маршрут передачи от одного конца к другому. Такие параметры, как число и длина пакетов, поступающих в сеть или проходящих через неё в любой момент времени, число вызовов, поступающих на вход сети за заданное время, продолжительность занятия (ресурса) – в общем случае подвержены статистическим изменениям. Поэтому для изучения их воздействия на сеть и получения соответствующих количественных характеристик должны применяться вероятностные методы.

Ключевую роль в анализе сетей играет теория очередей (называемая также теорией массового обслуживания). Для сетей с коммутацией пакетов проблема очередей возникает совершенно естественно. Пакеты, поступающие на вход сети или промежуточного узла, на пути к пункту назначения накапливаются, обрабатываются с целью выбора подходящего канала передачи к следующему узлу, а затем считываются в этот канал, когда наступит время их передачи. Время, затраченное на ожидание передачи в накопителе, является важной мерой, характеризующей работу сети. Оно зависит от времени обработки в узле и длины пакета, а также от пропускной способности канала передачи и дисциплины обслуживания, применяемой при обработке пакета. Теория очередей возникает также при исследовании сетей с коммутацией каналов. Во-первых, при изучении обработки вызовов, во-вторых, при анализе зависимости между числом доступных каналов и вероятностью того, что вызов, требующий установление соединения, будет заблокирован или поставлен в очередь для ожидания обслуживания.

Рассмотрим простейшую модель обслуживания:

В качестве пакетов будем рассматривать пакеты данных для случая коммутации пакетов или вызовы для систем с коммутацией каналов. Пакеты поступают случайным образом со скоростью λ в единицу времени. Они ожидают обслуживания в накопителе, и обслуживаются в соответствии с некоторой конкретной дисциплиной со средней скоростью μ пакетов в единицу времени. На рисунке показана одна обслуживающая линия. В более же общем случае могут быть доступны несколько обслуживающих линий, и в этом случае одновременно могут обслуживаться несколько пакетов. В контексте сети передачи данных обслуживающая линия — это средство передачи (исходящий канал или линия, передающие пакеты или, в случае систем с коммутацией каналов, обрабатывающие вызовы), которое передает данные с предписанной скоростью C блоков данных в единицу времени. Таким образом, процесс обслуживания определяется длиной пакета или продолжительностью соединения.

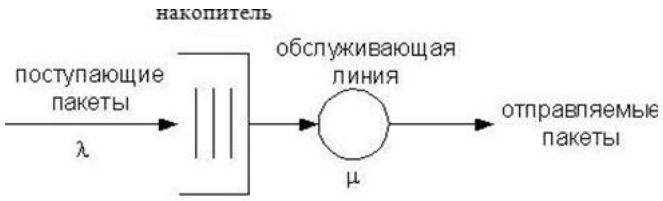


Рис. 3.3. Модель обслуживания

Если интенсивность поступления λ приближается к скорости обработки пакетов μ, очередь начинает расти. При накопителе конечной ёмкости очередь достигает наибольшей допустимой величины, а при переполнении накопителя поступление всех последующих пакетов будет заблокировано. Для однолинейных систем обслуживания стабильность обеспечивается при $\lambda<\mu$. Введём параметр $\rho=\lambda/\mu$. Его называют коэффициентом использования канала или интенсивностью нагрузки. Когда ρ приближается к 1 или превышает её, возникает область перегрузки, и поступающие пакеты блокируются более часто. Характеристики сети (время задержки, вероятность блокировки и т.д.) зависит также от вероятности состояний очереди. Для расчёта вероятностей состояния должны быть известны следующие характеристики:

· процесс поступления пакетов (статистика входящих потоков);

· распределение длин пакетов (распределение времени обслуживания);

· дисциплина обслуживания (обслуживание в порядке поступления – ОПП или FIFO, некоторые дисциплины обслуживания с приоритетами).

Для многолинейных систем вероятности состояний зависят также от числа обслуживающих линий. В теории массового обслуживания принято моделировать процесс поступления вызовов с помощью Пуассоновского процесса.

3.5.1. Пуассоновский процесс

Рассмотрим бесконечно малый промежуток времени Δt ($\Delta t\to 0$), проходящий между моментами t и $t+\Delta t$. При определении пуассоновского процесса используются три основные предпосылки:

1. вероятность одного поступления в течение времени Δt определяется в виде: $\lambda\Delta t+O(\Delta t)$, где $O(\Delta t)$ – члены более высокого порядка, которыми мы можем пренебречь при $\Delta t\to 0$;

2. вероятность нулевого поступления в течение времени Δt равна $1-\lambda\Delta t$;

3. поступление – без последействия (без памяти), т.е. поступление в течение Δt не зависит от предыдущих поступлений.

Если теперь рассмотреть большой промежуток времени T, то вероятность $p(k)$ того, что в промежутке T произойдут k поступлений, равна:

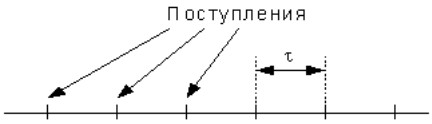
$$p(k)=\frac{(\lambda T)^k e^{-\lambda T}}{k!},\ \text{где } k=0,\ 1,\ 2,\ \ldots$$

Это равенство называется распределением Пуассона. Оно нормировано:

$$\sum_{k=0}^{\infty} p(k) = 1$$ и его среднее значение имеет вид: $$E(k) = \sum_{k=0}^{\infty} Kp(k) = \lambda T.$$

Дисперсия распределения: $\sigma^2 = E(k) = \lambda T$.

Теперь рассмотрим большой промежуток времени и отметим на нём моменты, в которые наступили события Пуассоновского процесса.



Очевидно, что τ - это положительная случайная величина с непрерывным распределением. Оказывается, что для Пуассоновского распределения величина τ распределена по показательному закону:

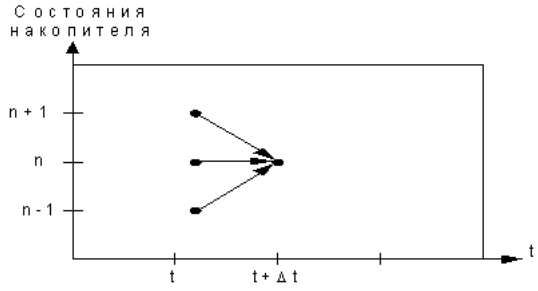
$$f(\tau) = \lambda e^{-\lambda\tau},\ \tau \geq 0$$

Среднее значение показательного распределения:

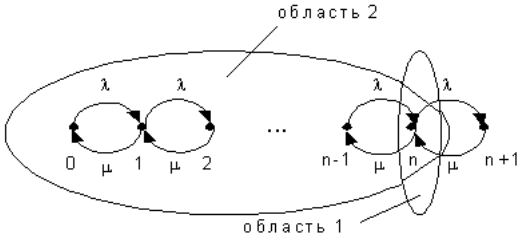
$$E(t) = \int_0^{\infty} \tau f(\tau) d\tau = 1 / \lambda,$$ а дисперсия $\sigma_\tau^2 = 1 / \lambda^2$.

3.5.2. Система обслуживания M/M/1

Система обслуживания M/M/1 – это система с одной обслуживающей линией, Пуассоновским входящим потоком, показательным распределением обслуживания и дисциплиной ОПП (обслуживание в порядке поступления). Диаграмма изменений состояний во времени для системы может быть изображена следующим образом:



Рассмотрим диаграмму состояний для системы M/M/1:



Пусть процессы поступления и обслуживания определяются соответственно параметрами λ и μ. Определим вероятность $p_n(t+\Delta t)$ того, что в момент времени $t+\Delta t$ в системе будет находиться n клиентов (пакетов или вызовов). Из диаграммы видно, что в момент времени t система могла находиться только в состоянии $n-1$, n или $n+1$. Тогда мы можем записать:

$$p_n(t+\Delta t) = p_n(t)\left[(1-\lambda\Delta t)(1-\mu\Delta t) + \mu\Delta t \cdot \lambda\Delta t\right] +$$
$$+p_{n-1}\left[\lambda\Delta t \cdot (1-\mu\Delta t)\right] + p_{n+1}\left[\mu\Delta t \cdot (1-\lambda\Delta t)\right]$$

Вероятности перехода из одного состояния в другое получены в результате рассмотрения путей, по которым происходят эти переходы, и расчёта соответствующих вероятностей. Например, если система осталась в состоянии n, то могли произойти либо уход и одно поступление с вероятностью $\mu\Delta t$, либо ни одного ухода или поступления с вероятностью $(1-\lambda\Delta t)(1-\mu\Delta t)$, что и показано в первом случае.

Производя упрощения, используя разложение $p_n(t+\Delta t)$ в ряд Тейлора, можно получить следующее уравнение:

$$\frac{dp_n(t)}{dt} = -(\lambda+\mu)p_n(t) + \lambda p_{n-1}(t) + \mu p_{n+1}(t).$$

Для стационарного состояния вероятность $p_n(t)$ приближается к некоторому постоянному значению, поэтому $\frac{dp_n(t)}{dt} = 0$. Тогда последнее уравнение для стационарного случайного процесса упрощается и принимает вид:

$$(\lambda + \mu)p_n(t) = \lambda p_{n-1}(t) + \mu p_{n+1}(t) \quad (1)$$

Форма уравнения (1) показывает, что при работе системы действует стационарный принцип равновесия: левая часть описывает интенсивность уходов из состояния n, а правая часть – интенсивность приходов в состояние *n* из *n-1* или *n+1*. Чтобы существовали вероятности стационарного состояния, эти две интенсивности должны быть равны.

Контрольные вопросы:

1. Что такое «Система обслуживания M/M/1», нарисовать диаграмму изменения состояний?
2. Записать формулу равенства называется распределения Пуассона.
3. Что такое информационный киоск?
4. Дать определения электронного текста, электронной книги, электронной библиотеке.
5. Что такое релевантность?
6. В чём разница между информационно-поисковыми системами и автоматизированными системами поиска?
7. На какие традиционные группы делятся ИПС?
8. На какие группы делятся ИПС по характеру выдаваемой информации?
9. В чём разница между базами знаний и базами данных?
10. Что такое информационное хранилище?

Практические задания:

ЗАДАНИЕ № 3.1. Естественно-языковый поиск. Проверьте справедливость указанных правил по трактовке слов в поисковых машинах Yandex, Rambler, Google, Aport.

Знаки «+» и «-». Если вы хотите, чтобы слова из запроса обязательно были найдены, поставьте перед каждым из них «+». Если вы хотите исключить какие-либо слова из результата поиска, поставьте перед каждым из них «-».

*Например, запрос «**частные объявления продажа велосипедов**», выдаст много ссылок на сайты с разнообразными частными объявлениями. А запрос с «+» «**частные объявления продажа +велосипедов**» покажет объявления о продаже именно велосипедов.*

*Если вам нужно описание Парижа, а не предложения многочисленных турагентств, имеет смысл задать такой запрос «**путеводитель по парижу -агентство –тур**».'*

Обратите внимание на знак «-». Это именно минус, а не тире и не дефис. Знак «-» надо писать через пробел от предыдущего и слитно с последующим словом, вот так: «**рак –гороскоп**». Если написать «**рак-гороскоп**» или «**рак – гороскоп**», то знак «-» будет проигнорирован.

ЗАДАНИЕ № 3.2. Основные операторы. Проверьте справедливость указанных выше правил по естественно-языковому поиску в поисковых машинах Yandex, Rambler, Google, Aport.

Несколько набранных в запросе слов, разделенных пробелами, означают, что все они должны входить в одно предложение искомого документа. Тот же самый эффект произведет употребление символа '**&**'.

*Например, при запросе **'лечебная физкультура'** или **'лечебная & физкультура'**), результатом поиска будет список документов, в которых в одном предложении содержатся и слово **'лечебная'**, и слово **'физкультура'**. (Эквивалентно запросу **'+лечебная +физкультура'**)*

Между словами можно поставить знак '|', чтобы найти документы, содержащие любое из этих слов. (Удобно при поиске синонимов).

*Запрос вида **'фото | фотография | фотоснимок | снимок | фотоизображение'** задает поиск документов, содержащих хотя бы одно из перечисленных слов.*

Еще один знак, тильда '~', позволит найти документы с предложением, содержащим первое слово, но не содержащим второе.

*По запросу **'банки ~ закон'** будут найдены все документы, содержащие слово **'банки'**, рядом с которым (в пределах предложения) нет слова **'закон'**.*

Чтобы подняться на ступеньку выше, от уровня предложения до уровня документа, просто удвойте соответствующий знак. Одинарный оператор (**&**, ~) ищет в пределах предложения, двойной (**&&**, ~~) - в пределах документа.

*Например, по запросу **'рецепты && (плавленый сыр)'** будут найдены документы, в которых есть и слово **'рецепты'** и словосочетание **'(плавленый сыр)'** (причем **'(плавленый сыр)'** должен быть в одном предложении. А запрос **'руководство Visual C ~~ цена'** выдаст все документы со словами **'руководство Visual C'**, но без слова **'цена'***

ЗАДАНИЕ № 3.3. Поиск с расстоянием. Проверьте справедливость указанных выше правил по использованию основных операторов в поисковых машинах Yandex, Rambler, Google, Aport.

Часто в запросах ищут устойчивые словосочетания. Если поставить их в кавычки, то будут найдены те документы, в которых эти слова идут строго подряд.

*Например, по запросу **«красная шапочка»** будут найдены документы с это фразой. (При этом контекст «а шапочка у нее была красная» найден не будет.)*

Как *Яndex* адресует слова? Если все слова в тексте перенумеровать по порядку их следования, то расстояние между словами a и b - это разница между номерами слов a и b. Таким образом, расстояние между соседними словами равно 1 (а не 0), а

расстояние между соседними словами, стоящими «не в том порядке», равно -1. То же самое относится и к предложениям.

Если между двумя словами поставлен знак '/', за которым сразу напечатано число, значит, требуется, чтобы расстояние между ними не превышало этого числа слов.

*Например, задав запрос **'поставщики /2 кофе'**, вы требуете найти документы, в которых содержатся и слово **'поставщики'** и слово **'кофе'**, причем расстояние между ними должно быть не более двух слов и они должны находиться в одном предложении. (Найдутся "поставщики колумбийского кофе", "поставщики кофе из Колумбии" и т.д.)*

Если порядок слов и расстояние точно известны, можно воспользоваться пунктуацией '/+**n**'. Так, например, задается поиск слов, стоящих подряд.

*Запрос **'синяя /+1 борода'** означает, что слово **'борода'** должно следовать непосредственно за словом **'синяя'**. (К тому же результату приведет запрос **"синяя борода"**)*

В общем виде ограничение по расстоянию задается при помощи пунктуации вида '**/(n m)**', где '**n**' минимальное, а '**m**' максимально допустимое расстояние. Отсюда следует, что запись '**/n**' эквивалентна '**/(-n +n)**', а запись '**/+n**' эквивалентна '**/(+n +n)**'.

*Запрос **'музыкальное /(-2 4) образование'** означает, что **'музыкальное'** должна находиться от **'образование'** в интервале расстояний от 2 слов слева до 4 слов справа*

Практически все знаки можно комбинировать с ограничением расстояния.

*Например, результатом поиска по запросу **'вакансии ~ /+1 студентов'** будут документы, содержащие слово **'вакансии'**, причем в этих документах слово **'студентов'** не следует непосредственно за словом **'вакансии'**.*

Когда знаки ограничения по расстоянию стоят после двойных операторов, то употребленные там числа - это расстояние не в словах, а в предложениях. Расстояние в абзацах определяется аналогично расстоянию в словах.

*Запрос **'банк && /1 налоги'** означает, что слово **'налоги'** должно находиться в том же самом, либо в соседнем со словом **'банк'** предложении.*

ЗАДАНИЕ № 3.4. Синтаксис языка запросов (строгий поиск) Проверьте справедливость указанных выше правил по ранжированию результатов поиска в поисковых системах Yandex, Rambler, Google, Aport.

Синтаксис	Что означает оператор	Пример запроса
пробел или &	логическое И (в пределах предложения)	лечебная физкультура
&&	логическое И (в пределах документа)	рецепты && (плавленый сыр)
|	логическое ИЛИ	фото | фотография | снимок | фотоизображение
+	обязательное наличие слова в найденном документе (работает также в применении к стоп-словам)	+быть или +не быть
( )	группирование слов	(технология | изготовление) (сыра | творога)
~	бинарный оператор И НЕ (в пределах предложения)	банки ~ закон
~~ или -	бинарный оператор И НЕ (в пределах документа)	путеводитель по парижу ~~ (агентство | тур)
/(n m)	расстояние в словах (-назад +вперед)	поставщики /2 кофе; музыкальное /(-2 4) образование; вакансии ~ /+1 студентов
«a»	поиск фразы	"красная шапочка" (эквивалентно красная /+1 шапочка)
&&/(n m)	расстояние в предложениях (-назад +вперед)	банк && /1 налоги

Поиск в элементах

Синтаксис	Что означает оператор	Пример запроса
$title (выражение)	поиск в заголовке	$title (CompTek)
$anchor (выражение)	поиск в тексте ссылок	$anchor (CompTek | Dialogic)
#keywords=(выражение)	поиск в ключевых словах	#keywords=(поисковая система)
#abstract=(выражение)	поиск в описании	#abstract=(искалка | поиск)
#image="значение"	поиск файла изображения	#image="tort*"
#hint=(выражение)	поиск в подписях к изображениям	#hint=(lenin | ленин)
#url="значение"	поиск на заданном сайте (странице)	#url="www.comptek.ru*"
#link="значение"	поиск ссылок на заданный URL	#link="www.yandex.ru*"

Советы по проведению поиска:

· Можно обойтись без механизма поиска, если то, что вы ищете, вам хорошо знакомо. Достаточно ввести предполагаемый адрес, например www.cocacola.com, www.harrypotter.com или www.billbradley.com.

· Экономьте время, ограничив область поиска конкретной категорией.

· Не щелкайте по ссылкам на полученных страницах. Вместо этого щелкните на ссылке правой клавишей мыши и выберите пункт меню **Open in New Window** (*Открыть в новом окне*) или перенесите ссылки мышью во второе окно браузера.

· Избегайте специальных компьютерных терминов, таких, как *file*, *folder*, *disk* и *memory*, если вы не обозначаете ими компьютерные понятия.

· При поиске имени собственного используйте режим поиска «точно по фразе» и кавычки, если это возможно.

· Если в результате было обнаружено слишком мало страниц, переключитесь из режима поиска «точно по фразе» в режим поиска по всем словам, из него – в режим поиска по одному из слов или используйте меньше ключевых слов.

· Если в результате поиска было обнаружено слишком много страниц, то переключитесь из режима поиска по одному из слов в режим поиска по всем словам или добавьте больше ключевых слов.

· Для того чтобы узнать ответы на простые вопросы (например, какова высота Эйфелевой башни), обратитесь на узел, воспринимающий вопросы на разговорном английском языке.

· Следите за правописанием.

ЗАДАНИЕ № 3.5. Поиск в зонах. Проверьте справедливость указанных выше правил по использованию в запросе скобок в поисковых системах Yandex, Rambler, Google, Aport.

Можно искать информацию в «зонах» - заголовках (имя «зоны»: **Title**), ссылках (имя «зоны»: **Anchor**) и адресе (имя «зоны»: **Address**).

Синтаксис: **$имя_зоны (поисковое выражение)**.

*Запрос **'$title CompTek'** ищет в заголовках документов слово **'CompTek'**.*

*Запрос **'$anchor (CompTek | Dialogic)'** находит документы, в ссылках внутри которых есть одно из слов **'CompTek'** или **'Dialogic'**.*

Поиск в определенных элементах.

Можно ограничить поиск информации списком серверов или наоборот исключить сервера из поиска (url). Можно также искать документы, содержащие ссылки на определенные URL (link), и файлы картинок (image). Если вы хотите работать не с конкретным URL (image), а со всеми, начинающимися с данной последовательности символов, используйте "*".

Синтаксис: **#имя_элемента=«имя_файла (URL)»**.

*По запросу **'CompTek ~~ #url=«www.comptek.ru*»'** будут искаться упоминания компании **'CompTek'** везде, кроме ее собственного сервера (www.comptek.ru). А запрос **'#link=«www.comptek.ru*»'** покажет все документы, которые сослались на сервер компании.*

*Запрос **' #image=«tort*»'** даст ссылки на документы с изображениями тортов (хотя, возможно, найдется и портрет черепахи Тортиллы).*

Можно также искать по ключевым словам (keywords), аннотациям (abstract) и подписям под изображениями (hint).

Синтаксис: **#имя_элемента=(поисковое выражение)**.

*Запросу **'#keywords=(поисковая система) | #abstract=(поисковая система)'** будут искаться все страницы, в meta тегах которых есть эти слова.*

*По запросу **'#hint=(кино)'** будут найдены документы, содержащие изображение с такой подписью.*

Ранжирование результата поиска.

При поиске для каждого найденного документа Яндекс вычисляет величину релевантности (соответствия) содержания этого документа поисковому запросу. Список найденных документов перед выдачей пользователю сортируется по этой величине в порядке убывания. Релевантность документа зависит от ряда факторов, в том числе от частотных характеристик искомых слов, веса слова или выражения, близости искомых слов в тексте документа друг к другу и т.д. Пользователь может повлиять на порядок сортировки, используя операторы веса и уточнения запроса.

Задание веса слова или выражения применяется для того, чтобы увеличить релевантность документов, содержащих «взвешенное» выражение.

Синтаксис: **слово:число** или **(поисковое_выражение):число**

*По запросу **'поисковые механизмы:5'** будут найдены те же документы, что и по запросу **'поисковые механизмы'**. Разница состоит в том, что наверху списка найденного окажутся документы, где чаще встречается именно слово **'механизмы'**.*

*Запрос **'поисковые (механизмы | машины | аппараты):5 '** равнозначен запросу **'поисковые (механизмы:5 | машины:5 | аппараты:5)'**.*

Задание уточняющего слова или выражения применяется для того, чтобы увеличить релевантность документов, содержащих уточняющее выражение.

Синтаксис: **<- слово** или **<- (уточняющее_выражение)**

*По запросу **'компьютер <- телефон'** будут найдены все документы, содержащие слово **'компьютер'**, при этом первыми будут выданы документы, содержащие слово **'телефон'**.*

*Если ни в одном документе со словом **'компьютер'** нет слова **'телефон'**, результат запроса будет эквивалентен запросу **'компьютер'**.*

ЗАДАНИЕ № 3.6. Скобки. Проверьте справедливость указанных выше правил по поиску с расстоянием в поисковых системах Yandex, Rambler, Google, Aport.

Вместо одного слова в запросе можно подставить целое выражение. Для этого его надо взять в скобки.

*Например, запрос **'(история, технология, изготовление) /+1 (сыра, творога)'** задает поиск документов, которые содержат любую из фраз **'история сыра'**, **'технология творога'**, **'изготовление сыра'**, **'история творога'**.*

Перечень литературы и Интернет-ресурсов:

1. Дымарский Я.С., Крутякова Н.П., Яновский Г.Г. Управление сетями связи: принципы, протоколы, прикладные задачи. – М.: Мобильные коммуникации, 2003. – 384 с.

2. Информационные киоски — http://video-in.ru/

3. Информационные технологии и электронные коммуникации — http://emf.ulstu.ru/metod/ITEK/index.htm

4. Муштоватый И.Ф. Самоучитель по работе в Интернете/ Под общ. редакцией М.И. Монастырского. – Ростов н/Д.: “Феникс”, 2001. – 320с.

5. Основы Web-технологий / П.Б. Храмцов, С.А. Брик, А.М. Русак, А.И. Сурин /Под. редакцией П.Б. Храмцова. – М.: ИНТУИТ.РУ ”Интернет-Университет Информационных Технологий, 2003. – 512 с.

6. Основы современных компьютерных технологий под редакцией А.Д. Хомоненко– СПб КОРОНА принт, 1998.

7. Пауэлл Т.А. Полное руководство по HTML / Пер. с англ. А.В. Качанов. – Мн.: ООО Попурри, 2001. – 912 с.

8. Пятибратов А.П. и др. Вычислительные системы, сети и телекоммуникации: Учебник/ Под редакцией А.П. Пятибратова. – М.: Финансы и статистика, 2001. – 512 с.

9. Системы передачи информации — http://kunegin.narod.ru/ref/lec/86.htm

10. Столлингс В. Компьютерные сети, протоколы и технологии Интернета. – СПб.: БХВ-Петербург, 2005. – 832 с.

11. Стэн Шатт Мир компьютерных сетей пер. с англ. – К.: BHV, 1996 – 288 с.

12. Технология корпоративных сетей. М. Кульгин. – СПб ПИТЕР, 1999.

13. Титтел Эд, Хадсон Курт, Дж. Майкл Стюард Networking Essentials – СПб ПИТЕР, 1999.

14. Якубайтис Э.А. Информационные сети и системы: Справочная книга. – М.: Финансы и статистика, 1996.

Тема 4. Базовая эталонная модель международной организации стандартов

Цели:

- Сформировать базовые знания об уровнях модели OSI, на которых функционируют конкретные сетевые компоненты.
- Научиться описывать главные функции каждого уровня модели OSI.
- Научиться определять уровни модели OSI, на которых выполняются конкретные сетевые операции.
- Познакомиться с расширениями модели OSI со стороны IEEE Project 802.

В 1978 году International Standards Organization (ISO) выпустила набор спецификаций, описывающих архитектуру сети с неоднородными устройствами. Исходный документ относился к открытым системам, чтобы все они могли использовать одинаковые протоколы и стандарты для обмена информацией.

В 1984 году ISO выпустила новую версию своей модели, названную эталонной моделью взаимодействия открытых систем (Open System Interconnection reference model, OSI). Версия 1984 года стала международным стандартом: именно ее спецификации используют производители при разработке сетевых продуктов, именно ее придерживаются при построении сетей. Модель OSI стандартизует количество, функции и названия уровней системных средств взаимодействия. Стек OSI стандартизует конкретный набор протоколов.

Эта модель - широко распространенный метод описания сетевых сред. Являясь многоуровневой системой, она отражает взаимодействие программного и аппаратного обеспечения при осуществлении сеанса связи, а также помогает решить разнообразные проблемы.

Базовая эталонная модель взаимодействия открытых систем (БЭМВОС) – это концептуальная основа, определяющая характеристики и средства открытых систем. Она обеспечивает работу в одной сети систем, выпускаемых различными производителями. На базе этой модели описываются правила и процедуры передачи данных между открытыми системами. Она также описывает структуру открытой системы и комплекс стандартов, которым она должна удовлетворять.

Основными элементами модели являются: уровни, объекты, соединения, физические средства соединений.

4.1. Многоуровневая архитектура.

В модели OSI сетевые функции распределены между семью уровнями. Каждому уровню соответствуют различные сетевые операции, оборудование и протоколы. На рис.5.1.

Рис. 4. представлена многоуровневая архитектура модели OSI. На каждом уровне выполняются определенные сетевые функции, которые взаимодействуют с функциями соседних уровней, вышележащего и нижележащего. Например, Сеансовый уровень должен взаимодействовать только с Представительским и Транспортным уровнем и т.п. Все эти функции подробно описаны.

Объединение различных уровней иерархии на одном физическом устройстве, например уровня доступа с уровнем распределения и уровня распределения с уровнем ядра, вполне допустимо. В случае построения небольших ЛВС оно является экономически выгодным. Но в процессе развития сети переход к классическому многоуровневому дизайну неизбежен, поскольку лишь при таком подходе возможно более рациональное использование функциональных возможностей оборудования в узлах сети, что позволит минимизировать стоимость владения.

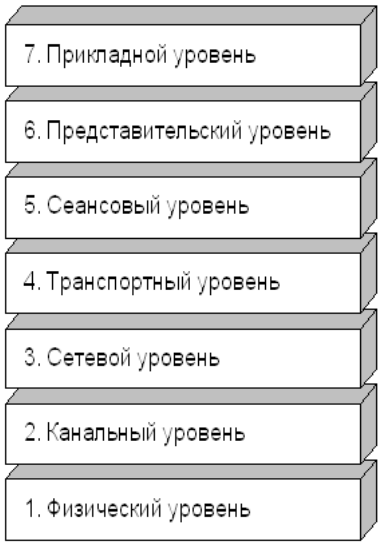


Рис. 4.1. Семь уровней модели OSI

Нижние уровни - 1-й и 2-й - определяют физическую среду передачи данных и сопутствующие задачи (такие, как передача битов данных через плату сетевого адаптера и кабель). Самые верхние уровни определяют, каким способом осуществляется доступ приложений к услугам связи. Чем выше уровень, тем более сложную задачу он решает.

Каждый уровень предоставляет несколько услуг (т. е. выполняет несколько операций), подготавливающих данные для доставки по сети на другой компьютер. Уровни отделяются друг от друга границами - интерфейсами. Все запросы от одного уровня к другому передаются через интерфейс. Каждый уровень использует услуги нижележащего уровня.

4.1.1. Взаимодействие уровней модели OSI

Задача каждого уровня - предоставление услуг вышележащему уровню, «маскируя» детали реализации этих услуг. При этом каждый уровень на одном компьютере работает так, будто он напрямую связан с таким же уровнем на другом компьютере. Эта логическая, или виртуальная, связь между одинаковыми уровнями показана на рис.7.2. Однако в действительности связь осуществляется между смежными уровнями одного компьютера - программное обеспечение, работающее на каждом уровне, реализует определенные сетевые функции в соответствии с набором протоколов. Перед подачей в сеть данные разбиваются на пакеты. Пакет (packet) - это единица информации, передаваемая между устройствами сети как единое целое. Пакет проходит последовательно через все уровни программного обеспечения. На каждом уровне к пакету добавляется некоторая информация, форматирующая или адресная, которая необходима для успешной передачи данных по сети.

Для обеспечения надежности и отказоустойчивости локальных вычислительных сетей используются различные методы, как в самой топологии сети, так и при выборе телекоммуникационного оборудования. Как правило, при построении ЛВС для связи между различными уровнями в топологии сети предусматривают резервные подключения между телекоммуникационным оборудованием.

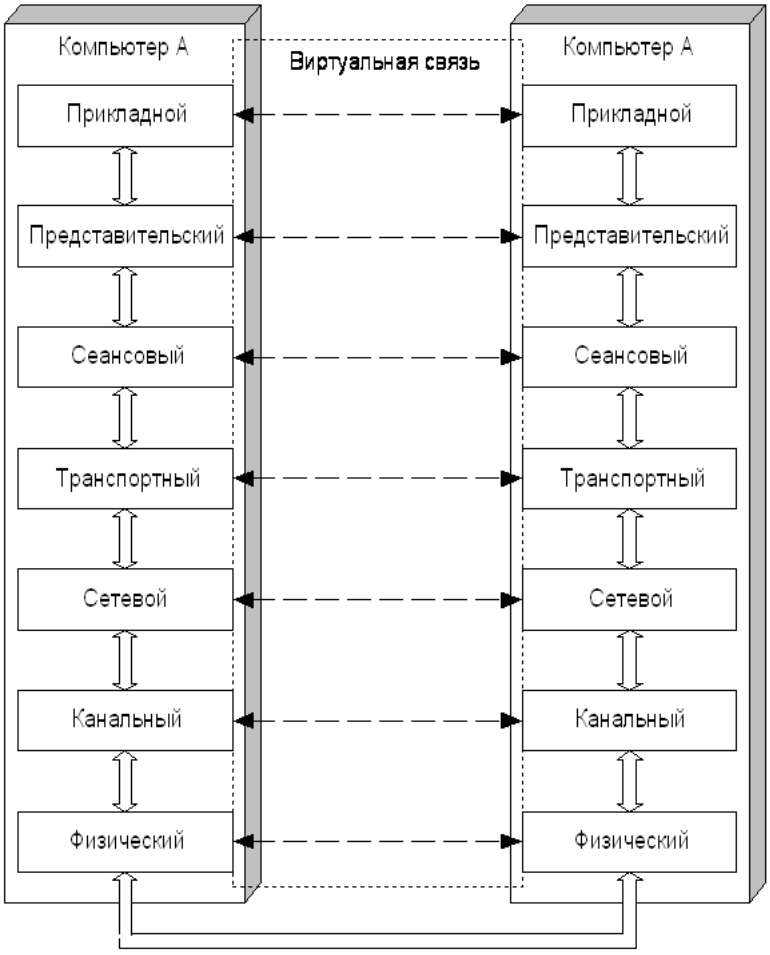


Рис. 4.2. Взаимосвязи между уровнями модели OSI

На принимающей стороне пакет проходит через все уровни в обратном порядке Программное обеспечение на каждом уровне читает информацию пакета, затем удаляет информацию, добавленную к пакету на этом же уровне отправляющей стороной, и передает пакет следующему уровню. Когда пакет дойдет до Прикладного уровня, адресная информация будет удалена, и данные примут свой первоначальный вид.

Таким образом, за исключением самого нижнего уровня сетевой модели, никакой иной уровень не может непосредственно послать информацию соответствующему уровню другого компьютера. Информация на компьютере-отправителе должна пройти через все уровни. Затем она передается по сетевому кабелю на компьютер — получатель и опять проходит сквозь все слои, пока не достигнет того же уровня, с которого она была послана на компьютере-отправителе. Взаимодействие смежных уровней осуществляется через интерфейс. Интерфейс определяет услуги, которые нижний уровень предоставляет верхнему, и способ доступа к ним. Поэтому каждому уровню одного компьютера «кажется», что он непосредственно взаимодействует с таким же уровнем другого компьютера.

4.1.2. Прикладной уровень

Уровень 7, Прикладной (Application), - самый верхний уровень модели OSI. Он представляет собой окно для доступа прикладных процессов к сетевым услугам. Этот уровень обеспечивает услуги, напрямую поддерживающие приложения пользователя, такие, как программное обеспечение для передачи файлов, доступа к базам данных и электронная почта. Нижележащие уровни поддерживают задачи, выполняемые на Прикладном уровне. Прикладной уровень управляет общим доступом к сети, потоком данных и обработкой ошибок.

4.1.3. Представительский уровень

Уровень 6, Представительский (Presentation), определяет формат, используемый для обмена данными между сетевыми компьютерами. Этот уровень можно назвать переводчиком. На компьютере-отправителе данные, поступившие от Прикладного уровня, на этом уровне переводятся в общепонятный промежуточный формат. На компьютере-получателе на этом уровне происходит перевод из промежуточного формата в тот, который используется Прикладным уровнем данного компьютера. Представительский уровень отвечает за преобразование протоколов, трансляцию данных, их шифрование, смену или преобразование применяемого набора символов (кодовой таблицы) и расширение графических команд. Представительский уровень, кроме того, управляет сжатием данных для уменьшения количества передаваемых битов.

На этом уровне работает утилита, называемая редиректором (redirector). Ее назначение - переадресовать операции ввода/вывода к ресурсам сервера.

4.1.4. Сеансовый уровень

Уровень 5, Сеансовый (Session), позволяет двум приложениям на разных компьютерах устанавливать, использовать и завершать соединение, называемое сеансом. На этом уровне выполняются такие функции, как распознавание имен и защита, необходимые для связи двух приложений в сети.

Сеансовый уровень обеспечивает синхронизацию между пользовательскими задачами посредством расстановки в потоке данных контрольных точек (chekpoints). Таким образом, в случае сетевой ошибки, потребуется заново передать только данные, следующие за последней контрольной точкой. На этом уровне выполняется управление диалогом между взаимодействующими процессами, т.е. регулируется, какая из сторон осуществляет передачу, когда, как долго и т.д.

4.1.5. Транспортный уровень

Уровень 4, Транспортный (Transport), обеспечивает дополнительный уровень соединения - ниже Сеансового уровня. Транспортный уровень гарантирует доставку пакетов без ошибок, в той же последовательности, без потерь и дублирования. На этом уровне сообщения переупаковываются: длинные разбиваются на несколько пакетов, а короткие объединяются в один. Это увеличивает эффективность передачи пакетов по сети. На Транспортном уровне компьютера-получателя сообщения распаковываются, восстанавливаются в первоначальном виде, и обычно посылается сигнал подтверждения приема.

Транспортный уровень управляет потоком, проверяет ошибки и участвует в решении проблем, связанных с отправкой и получением пакетов.

4.1.6. Сетевой уровень

Уровень 3, Сетевой (Network), отвечает за адресацию сообщений и перевод логических адресов и имен в физические адреса. Одним словом, исходя из конкретных сетевых условий, приоритета услуги и других факторов здесь определяется маршрут от компьютера-отправителя к компьютеру-получателю. На этом уровне решаются также такие задачи и проблемы, связанные с сетевым трафиком, как коммутация пакетов, маршрутизация и перегрузки.

Если сетевой адаптер маршрутизатора не может передавать большие блоки данных, посланные компьютером-отправителем, на Сетевом уровне эти блоки разбиваются на меньшие, а Сетевой уровень компьютера-получателя собирает эти данные в исходное состояние.

4.1.7. Канальный уровень

Уровень 2, Канальный (Data link), осуществляет передачу кадров (frames) данных от Сетевого уровня к Физическому. Кадры - это логически организованная структура, в которую можно помещать данные. Канальный уровень компьютера-получателя упаковывает «сырой» поток битов, поступающих от Физического уровня, в кадры данных.

На рис.7 3. представлен простой кадр данных, где идентификатор отправителя - адрес компьютера-отправителя, а идентификатор получателя - адрес компьютера- получателя. Управляющая информация используется для маршрутизации, а также указывает на тип пакета и сегментацию. Данные - собственно передаваемая информация. CRC (остаток избыточной циклической суммы) - это сведения, которые помогут выявить ошибки, что, в свою очередь, гарантирует правильный прием информации.

Канальный уровень обеспечивает точность передачи кадров между компьютерами через Физический уровень. Это позволяет Сетевому уровню считать передачу данных по сетевому соединению фактически безошибочной.

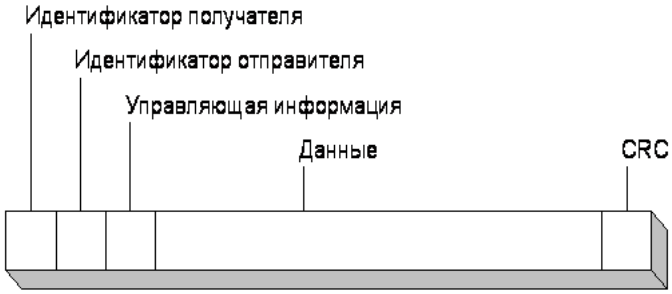


Рис. 4.3. Простой кадр данных

Обычно, когда Канальный уровень посылает кадр, он ожидает со стороны получателя подтверждения приема. Канальный уровень получателя проверяет наличие возможных ошибок передачи. Кадры, поврежденные при передаче, или кадры, получение которых не подтверждено, посылаются вторично.

4.1.8. Физический уровень

Уровень 1, Физический (Physical), - самый нижний в модели OSI. Этот уровень осуществляет передачу неструктурированного, «сырого» потока битов по физической среде (например, по сетевому кабелю). Здесь реализуются электрический, оптический, механический и функциональный интерфейсы с кабелем. Физический уровень также формирует сигналы, которые переносят данные, поступившие от всех вышележащих уровней. На этом уровне определяется способ соединения сетевого кабеля с платой сетевого адаптера, в частности, количество контактов в разъемах и их функции. Кроме того, здесь определяется способ передачи данных по сетевому кабелю.

Физический уровень предназначен для передачи битов (нулей и единиц) от одного компьютера к другому. Содержание самих битов на данном уровне значения не имеет. Этот уровень отвечает за кодирование данных и синхронизацию битов, гарантируя, что переданная единица будет воспринята именно как единица, а не как ноль. Наконец, Физический уровень устанавливает длительность каждого бита и способ перевода бита в соответствующие электрические или оптические импульсы, передаваемые по сетевому кабелю.

4.2. Модель IEEE 802.

В конце 70-х годов, когда ЛВС стали восприниматься в качестве потенциального инструмента для ведения бизнеса, IEEE пришел к выводу: необходимо определить для них стандарты. В результате был выпущен Project 802, названный в соответствии с годом и месяцем своего издания (1980 год, февраль). Хотя публикация стандартов IEEE опередила публикацию стандартов ISO, оба проекта велись приблизительно в одно время и при полном обмене информацией, что и привело к рождению двух совместимых моделей. Project 802 установил стандарты для физических компонентов сети - интерфейсных плат и кабельной системы, - с которыми имеют дело Физический и Канальный уровни модели OSI.

Итак, эти стандарты, называемые 802-спецификациями, распространяются: на платы сетевых адаптеров; компоненты глобальных вычислительных сетей; компоненты сетей, при построении которых используют коаксиальный кабель и витую пару. 802-спецификации определяют способы, в соответствии с которыми платы сетевых адаптеров осуществляют доступ к физической среде и передают по ней данные. Сюда относятся соединение, поддержка и разъединение сетевых устройств.

4.1.9. Категории

Стандарты ЛВС, определенные Project 802, делятся на 12 категорий, каждая из которых имеет свой номер.
802.1 - объединение сетей.
802.2 - Управление логической связью.
802.3 - ЛВС с множественным доступом, контролем несущей и обнаружением коллизий (Ethernet).
802.4 - ЛВС топологии «шина» с передачей маркера.
802.5 - ЛВС топологии «кольцо» с передачей маркера.
802.6 - сеть масштаба города (Metropolitan Area Network, MAN).
802.7 - Консультативный совет по широковещательной технологии (Broadcast Technical Advisory Group).
802.8 - Консультативный совет по оптоволоконной технологии (Fiber-Optic Technical Advisory Group).
802.9 - Интегрированные сети с передачей речи и данных (Integrated Voice/Data Networks).
802.10 - Безопасность сетей.
802.11 - Беспроводная сеть.
802.12 - ЛВС с доступом по приоритету запроса (Demand Priority Access LAN, 100baseVG-AnyLan).

4.1.10. Расширения модели OSI

Два нижних уровня модели OSI, Физический и Канальный, устанавливают, каким образом несколько компьютеров могут одновременно использовать сеть, чтобы при этом не мешать друг другу.

IEEE, подробно описывая Канальный уровень, разделил его на два подуровня:

- Управление логической связью (Logical Link Control, LLC) - контроль ошибок и управление потоком данных;
- Управление доступом к среде (Media Access Control, MAC).

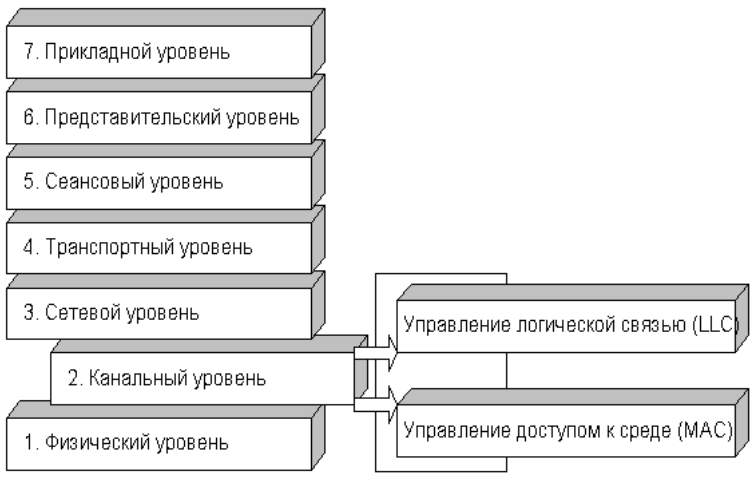


Рис. 4.4. Подуровни: Управление логической связью и доступом к среде

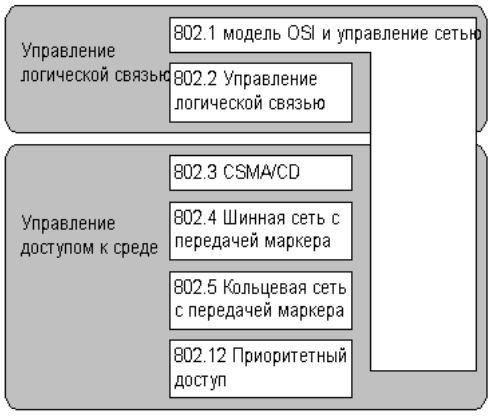


Рис. 4.5. Стандарты Project 802 для подуровней

Контрольные вопросы:

1. Какой уровень управляет общим доступом к сети, потоком данных и обработкой ошибок?
2. Какой уровень на компьютере-получателе переводит промежуточный формат в тот, который используется Прикладным уровнем данного компьютера?
3. Какой уровень определяет маршрут от компьютера-отправителя к компьютеру-получателю?
4. На каком уровне определяется способ соединения сетевого кабеля с сетевым адаптером?
5. На каком уровне модели OSI начинается процесс создания пакета?
6. Какой уровень модели OSI в Project 802 разделен на два подуровня: Управление логической связью и Управление доступом к среде?
7. Что стандартизует модель OSI?
8. Что стандартизует стек OSI?
9. Почему в модели OSI семь уровней?
10. Какой уровень отвечает за доступ приложений в сеть?

Практические задания:

ЗАДАНИЕ № 4.1. Для каждого из перечисленных ниже протоколов, функций или понятий определите уровень модели OSI, к которому он относится.

1. Ethernet.
2. Разделение диалога.
3. Синтаксис передачи данных.
4. Маршрутизация.
5. Сегментация.
6. SMTP.
7. Дифференциальная манчестерская схема.

ЗАДАНИЕ № 4.2. Мониторинг изменений на компьютерах пользователей и проведение инвентаризаций.

Инвентаризации и отслеживание изменений на компьютерах, Systems Management Server, Tivoli, Unicenter, CHECKCFG/AIDA.

Очень администратору предписывается контролировать не только работоспособность серверов/приложений или журналы событий, но и изменения на рабочих станциях пользователей - появление на них новых приложений, несанкционированных изменений в оборудовании, изменений в настройках (например, появление новых сетевых ресурсов) и т.п. Обычно, поскольку все равно собирается информация об оборудовании/программном обеспечении/настройках, в программах, предназначенных для этих целей, предусматривается также возможность проведения инвентаризаций.

Официальная программа для этой цели - Systems Management Server. Однако эта программа является очень ресурсоемкой (требует для работы также установленного SQL Server), дорогостоящей с точки зрения лицензирования, сложной в установке и настройке и не слишком надежной. Кроме того, необходимо на каждый клиентский компьютер ставить дополнительное программное обеспечение клиента SMS. Как правило, развертывание SMS оправданно только на крупных предприятиях, в которых требуется множество функциональных возможностей SMS.

Альтернативные средства - Tivoli от IBM, Unicenter от Computer Associates и т.п. также не отличаются простотой и дешевизной. В то же время одно из лучших решений в этой области - простое, надежное и с русским интерфейсом - абсолютно бесплатно. Это - программа checkcfg. Она не требует установки на клиенте (достаточно запустить ее при запуске рабочей станции, например, через реестр, сценарий подключения или просто autoexec.bat), при запуске сканирует реестр и протоколирует в текстовый файл (по умолчанию он называется именем, совпадающим с MAC-адресом клиентской рабочей станции) на сетевом каталоге значимую информацию о компьютере:

О информацию о всех существенных устройствах - процессор, память, материнская плата, все платы расширения, USB-устройства, жесткие диски и сменные накопители и т.п.;

О информацию об операционной системе, роли компьютера и языке;

О информацию об установленных пакетах обновлений и патчах;

О информацию о всех установленных на компьютере программах;

О информацию об автоматически запускаемых программах;

О информацию о почтовых профилях;

О информацию о сетевых ресурсах;

О информацию о параметрах сетевых и коммутируемых соединений;
О информацию о свободном месте на дисках;
О SMART-информацию винчестеров (например, для оценки их надежности).

Собранную информацию можно в автоматическом режиме анализировать при помощи программы Doberman, которая выдает вам протокол о всех изменениях, которые произошли между запусками программы checkcfg.

Всю собранную информацию можно представлять в графическом виде и генерировать стандартные документы по инвентаризации (предусмотрено большое количество полей атрибутов, история каждого компьютера/устройства, а также еще 10 видов объектов, информация о которых может отслеживаться (принтеры, хабы/свитчи, UPS и т.п.)

ЗАДАНИЕ № 4.3. Мониторинг доступности процесса в режиме реального времени.

Отслеживание работы процесса на удаленном компьютере, утилита ServersCheck.

Примечание: эта лабораторная работа выполняется в паре.

Задание:

A. Установите на свой компьютер программное обеспечение для мониторинга ServersCheck (из каталога Мониторинг\Мониторинг серверов-служб-приложений\ServersCheck).

B. Настройте его для мониторинга доступности процесса calc.exe на компьютере партнера по лабораторной. В случае, если процесс на компьютере партнера будет не обнаружен, ServersCheck должен выдавать на ваш компьютер по NET SEND предупреждающее сообщение.

C. Попросите партнера запустить, а через несколько минут остановить калькулятор на своем компьютере, и убедитесь, что предупреждающие сообщения действительно выдаются.

D. По окончании лабораторной удалите программное обеспечение ServersCheck.

Решение:

1) Из каталога Мониторинг\Мониторинг серверов-служб-приложений\ServersCheck на компакт-диске запустите файл setup.exe и произведите установку с параметрами по умолчанию. После окончания установки в меню Start -> Programs -> ServersCheck выберите команду Start ServersCheck. Откроется окно Internet Explorer с консолью управления ServersCheck и окно Configuration Wizard.

2) В окне Configuration Wizard нажмите на кнопку Start Configuration. На экране Configuration Wizard - Email введите свой адрес электронной почты (например, administrator@vancouverdom.msft) и нажмите на кнопку Verify Email.

3) На экране Configuration Wizard - Email 2 в поле Outgoing SMTP Server введите имя вашего компьютера, а затем свое имя пользователя и пароль и нажмите на кнопку Save Mail Settings.

4) На экране Configuration Wizard - Email 3 нажмите на кнопку Set Security.

5) На экране Configuration Wizard - Security в поле Username введите Administrator, в поле Password - P@ssw0rd. На следующем экране нажмите на кнопку Close Windows.

6) В окне ServersCheck удалите две существующие проверки (для этого необходимо нажать на иконку с изображением корзины в крайнем правом столбце). Затем в окне Servers Check нажмите на кнопку Add New Monitoring Rule.

7) На первом шаге мастера добавления правил мониторинга просмотрите предоставленные возможности и в разделе Windows Based Checks установите переключатель в положение PROCESS: checks if a process is running or not, затем нажмите на кнопку Next Step.

8) На втором шаге мастера в поле Unique name введите значение Calc.exe check, в поле Group оставьте значение None.

9) На третьем шаге мастера в поле How often ... введите значение 1 минута, в поле When the rule failed оставьте значение 3.

10) На четвертом шаге мастера в поле Target Host введите имя компьютера партнера, в поле Process Name введите Calc.exe, в поле Username и Password - соответственно имя учетной записи администратора на этом компьютере и ее пароль (например, DENVERDOM\administrator с паролем P@ssw0rd). Затем нажмите на кнопку Test Settings. Если калькулятор на компьютере партнера не запущен, то результат должен быть Down, если запущен - OK.

11) На пятом экране мастера в поле Alert when: выберите All down cycles, в поле Send a network message to введите имя вашего компьютера, остальные поля оставьте пустыми. Нажмите на кнопку Save monitoring rule, а затем - на кнопку START MONITORING (в верхнем правом углу).

12) Попросите партнера запустить, а через несколько минут остановить калькулятор, и просмотрите, как меняется информация о проверках. Убедитесь, что сообщения по NET SEND передаются (если они не передаются, то проверьте статус служб Alerter и Messenger - они должны быть запущены).

13) После окончания лабораторной работы нажмите на кнопку Stop Monitoring и произведите удаление ServersCheck через Add/Remove Programs, а затем перезагрузите компьютер.

ЗАДАНИЕ № 4.4. Мониторинг событий аудита в режиме реального времени.

Отслеживание доступа к файлу, мониторинг обращения к файлам в реальном времени, программа EventTracker.

Задание:

1) Включите аудит на доступ к объектам на вашем компьютере.

2) Создайте на вашем компьютере текстовый файл C:\confidential.txt и внесите в него какой-либо текст. Настройте для этого текстового файла аудит для обращений на чтение от любых пользователей.

3) Установите на свой компьютер программу EventTracker (из каталога Мониторинг\Event Log Monitoring\EventTracker).

4) Настройте отслеживание событий аудита в EventTracker таким образом, чтобы при любом обращении к файлу c:\confidential.txt на ваш рабочий стол выдавалось соответствующее сообщение по NET SEND.

5) Обратитесь к файлу c:\confidential.txt и убедитесь, что настроенное оповещение срабатывает. По окончании лабораторной отключите оповещение.

Решение:

1) Откройте консоль Active Directory Users and Computers, раскройте узел для своего домена, щелкните правой кнопкой мыши по контейнеру Domain Controllers, в контекстном меню выберите Properties и перейдите на вкладку Group Policy. Выделите строку Default Domain Controller Policy и нажмите на кнопку Edit. Откроется окно Group Policy Object Editor.

2) В окне Group Policy Object Editor раскройте узел Computer Configuration -> Windows Settings -> Secuirty Settings -> Local Policies -> Audit Policies, щелкните по строке Audit object access и установите флажки Success и Failure. Закройте окно редактора групповых политик с сохранением сделанных изменений и выполните в командной строке команду GPUDATE.

3) После создания текстового файла C:\confidential.txt щелкните по нему правой кнопкой мыши, в контекстном меню выберите Properties и перейдите на вкладку Security.

4) Нажмите на кнопку Advanced, перейдите на вкладку Auditing и нажмите на кнопку Add. В поле Enter the object name to select... введите Everyone, нажмите на кнопку Check Names, а затем нажмите OK.

5) В окне Auditing Entry for confidential.txt установите флажки Successful и Failed напротив строки List Folder/Read Data, затем три раза нажмите OK, чтобы закрыть окно свойств файла.

6) Откройте файл confidential.txt в блокноте, затем откройте Event Viewer и просмотрите в журнале событий Security события с EventID 560.

7) Из каталога Мониторинг\Event Log Monitoring\EventTracker на компакт-диске запустите программу ETEwal4-6.exe. Произведите установку с параметрами по умолчанию. На экране Select Applications выберите Enterprise Management Console. На экране Basic Configuration оставьте значения по умолчанию. На экране Get Available Windows Events не устанавливайте флажок Get existing events into Event Tracker.

8) После окончания установки из меню Start -> Programs -> Prism Microsystems -> EventTracker запустите программу Event Tracker Management Console.

9) В Event Tracker Management Console в меню Configure выберите Configure Alerts и нажмите на кнопку Add.

10) На экране Alert Group Configuration введите имя оповещения, например, "Обращение к confidential.txt" и нажмите на кнопку Next.

11) На экране Event Details нажмите на кнопку Add Event и введите:

- в поле Event Type - Audit Success;
- в поле Log Type - Security;
- в поле EventID - 560;
- в поле Match in Event Descr - C:\confidential.txt.

Нажмите на кнопку OK, а затем еще раз нажмите на кнопку Add и введите такое же событие, но для поля Event Type выберите тип Audit Failure.

Нажмите на кнопку Next.

12) На экране Computers выберите свой компьютер и нажмите на кнопку Add, чтобы поместить его в список выбранных компьютеров.

13) На экране Actions установите флажок Send net message и в окне Message введите имя своего компьютера. Затем три раза нажмите на кнопку OK, чтобы завершить создание оповещения.

14) Откройте в блокноте файл confidential.txt, чтобы убедиться, что оповещение срабатывает (при генерации первого сообщения может быть пауза в 10-15 секунд).

15) Чтобы отключить оповещение, еще раз в меню Configure выберите Configure Alerts и снимите флажок в столбце Message напротив вашего оповещения/

ЗАДАНИЕ № 4.5. Мониторинг изменений и инвентаризация оборудования и ПО.

Мониторинг изменений на компьютерах пользователей, инвентаризация оборудования и программного обеспечения, CHECKCFG и DOBERMAN.

Задание:

A. При помощи программы Checkcfg соберите информацию о конфигурации вашего компьютера Windows 2003 Server и виртуального компьютера Windows 98. Обеспечьте на виртуальном компьютере Windows 98 автоматический запуск Checkcfg при запуске компьютера.

B. Удалите с компьютера под управлением Windows 2003 какую-либо установленную программу (например, EventTracker) и при помощи программы Doberman отследите данные изменения.

C. При помощи программы Sklad создайте структуру вашей сети на основе собранных данных и познакомьтесь с возможностями этой программы.

Решение:

1) Скопируйте каталог CheckCfg из каталога Мониторинг\Changes Monitoring на компакт-диске на диск C:\ и разверните файл checkcfg.zip в текущий каталог.

2) Откройте сетевой доступ к каталогу c:\checkcfg как \\имя_вашего_компьютера\checkcfg$ и предоставьте для него права Change для группы EveryOne.

3) Для сбора информации о локальном компьютере в меню Start -> Run выполните команду \\имя_вашего_компьютера\Checkcfg$ и из открывшегося каталога запустите программу Checkcfg.exe.

Примечание: обязательно запускайте программу в первый раз из сетевого каталога (даже несмотря на то, что физически он является локальным), поскольку путь первого запуска прописывается в файл checkcfg.ini.

В этом каталоге появится подкаталог DATE с файлом протокола (название его будет соответствовать номеру MAC-адреса вашего компьютера) и файл конфигурации checkcfg.ini.

4) Для сбора информации о виртуальном компьютере запустите виртуальный компьютер под управлением Windows 98, откройте нем сетевой каталог \\имя_вашего_компьютера\checkcfg$ и запустите в нем программу checkcfg.exe.

5) Для того, чтобы обеспечить автоматический запуск checkcfg.exe на компьютере под управлением Windows 98, можно создать пакетный файл и положить его в папку Автозагрузка, или воспользоваться сценарием подключения, или просто исправить в файле checkcfg.ini значение параметра RunMode на 1 - в этом случае программа будет записана в раздел автозапуска в реестре.

6) Внесите изменения в конфигурацию компьютера Windows 2003 (например, удалите программу EventTracker), и после удаления еще раз запустите файл checkcfg.exe.

7) Разархивируйте (можно в текущий каталог) файл doberman.zip и запустите программу dobernam.exe. В поле "Проверять файлы в каталогах" выберите каталога C:\Checkcfg\DATE и нажмите на кнопку Добавить. Затем нажмите на кнопку "Запустить проверку" в левом нижнем углу. Просмотрите информацию в отчете.

8) Разархивируйте (можно также в текущий каталог) файлы bde_min.zip и skald.zip, и после этого запустите программу SKLAD.EXE. На предложение создать пример дерева структуры вашего предприятия нажмите Yes (чтобы просмотреть пример, в реальной работе его создавать не нужно).

9) В окне Sklad в меню File выберите Обновить данные и добавьте в перечень каталогов каталог C:\Checkcfg\DATE (выберите этот каталог и нажмите на кнопку "Добавить"). Нажмите на кнопку Настройка и просмотрите возможные параметры добавления информации, а затем нажмите на кнопку Пуск. В ответ на приглашение распределить неучтенные компьютеры нажмите No, а затем - выход.

10) Просмотрите поля, которые можно заполнить для импортированных компьютеров, а затем нажмите на кнопку Ins и просмотрите другие объекты, которые можно добавить.

Перечень литературы и Интернет-ресурсов:

1. Блэк Ю. Сети ЭВМ: протоколы, стандарты, интерфейсы. – М.: Мир, 1990.–506 с.
2. Вычислительные сети и сетевые протоколы/Д.Дэвис, Д.Барбер, У.Прайс, С.Соломонидес. – М. : Мир, 1982. – 564 с.
3. Модель OSI Сервер BiLiM Systems Ltd. - http://www.citforum.ru/nets/switche/osi.shtml.
4. Олифер В.Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2007. – 960 с.
5. Протоколы информационно-вычислительных сетей : Справочник / С.А. Аничкин, С.А. Белов, А.В. Бернштейн и др.; Под ред. И.А. Мизина, А.П. Кулешова. – М.: Радио и связь, 1990. – 504 с.
6. Сетевые технологии — http://net.e-publish.ru/p214aa1.html
7. Столлингс В. Компьютерные сети, протоколы и технологии Интернета. – СПб.: БХВ-Петербург, 2005. – 832 с.
8. Таненбаум Э. Компьютерные сети. – СПб.: Питер, 2007. – 992 с.
9. Шварц М. Сети связи: протоколы, моделирование и анализ: В 2-х ч. – М.: Наука. Гл. ред. физ.-мат. лит., 1992.
10. IEEE 802.16 Working Group on Broadband Wireless Access Standards, - http://www.ieee802.org/16/
11. IEEE 802.16 Published Standards and Drafts, — http://www.ieee802.org/16/published.html
12. IEEE - Стандарты — http://grouper.ieee.org/groups/802/11/Reports/tgi_update.htm
13. http://standards.ieee.org/reading/ieee/std/lanman/802.11-1999.pdf
14. http://grouper.ieee.org/groups/802/11/Reports/tgg_update.htm

Тема 5. Компоненты информационной сети

Цели:

· Получить представление о компонентах сети.
· Научиться идентифицировать информационные сети.
· Различать классификацию типа и вида сети.
· Получить представление об открытых информационных систем.
· Научиться определять тип сети, подходящий для решения конкретной задачи

Информационная сеть состоит из трех основных аппаратных компонент и двух программных, которые должны работать согласованно. Для корректной работы устройств в сети их нужно правильно инсталлировать и установить рабочие параметры.

Основные компоненты.

Основными аппаратными компонентами сети являются следующие:

1. Абонентские системы: компьютеры (рабочие станции или клиенты и серверы); принтеры; сканеры и др.
2. Сетевое оборудование: сетевые адаптеры; концентраторы (хабы); мосты; маршрутизаторы и др.
3. Коммуникационные каналы: кабели; разъемы; устройства передачи и приема данных в беспроводных технологиях.

Основными программными компонентами сети являются следующие:

1. Сетевые операционные системы, где наиболее известные из них это: Windows NT; Windows for Workgroups; LANtastic; NetWare; Unix; Linux и т.д.
2. Сетевое программное обеспечение (Сетевые службы): клиент сети; сетевая карта; протокол; служба удаленного доступа.

Существует три основных компонента информационных сетей:

· абонентская система;
· ретрансляционная система;
· административная.

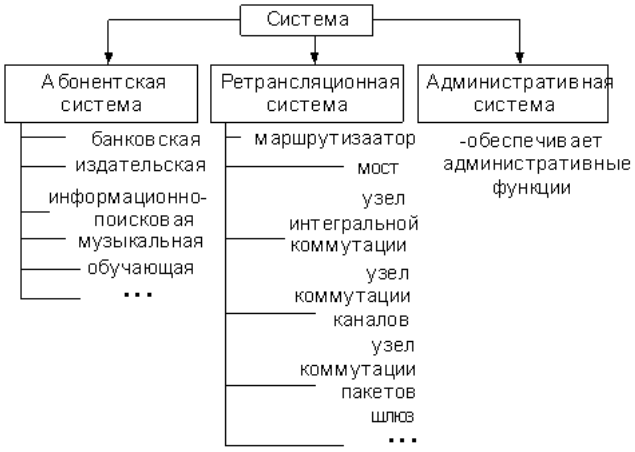


Рис. 5.1. Типы систем

5.1. Абонентская система.

Пользователь — это юридическое или физическое лицо, использующее какие-либо ресурсы сети. Самого пользователя либо систему, с которой он работает, называют абонентом информационной сети. Для удобной и эффективной работы пользователь использует интерфейс пользователя, определяющий взаимодействие пользователя с операционной системой или сетью – совокупность аппаратных и программных средств.

Абонент — это объект, имеющий право взаимодействия с системой или сетью. Ими могут быть терминалы, абонентские системы или локальные сети. Что касается пользователей, то они являются физическими, а предприятия или учреждения – юридическими абонентами сети или системы. Абонентами также могут быть программы, сообщения или устройства.

В обеспечении безопасности данных важную роль играет регистрация абонентов.

Абонентская система (Subscriber system) — в информационных сетях - система, которая является поставщиком или потребителем информации.

АС реализуется в виде одного или нескольких устройств:

Рассматриваемые устройства делятся на 2 группы:

А – выполняют прикладные процессы и часть, либо полностью функции области взаимодействия этих процессов.

В – предназначены лишь для реализации части функций взаимодействия. Они разгружают устройства А для эффективного выполнения ими прикладных программ.

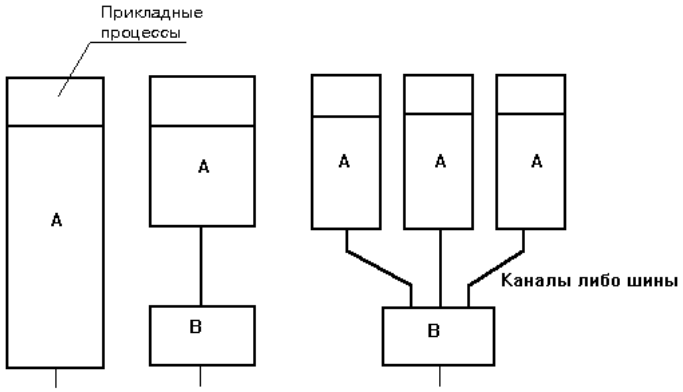


Рис. 5.2. Абонентская система

A и B соединяются друг с другом каналами или шинами.

Устройства B иногда могут находиться в коммуникационной сети, тогда устройства A устанавливаются на рабочих местах пользователей и связываются каналами с коммуникационной сетью, подключаясь к B (например, у пользователей устанавливается лишь терминал).

Абонентские системы могут быть универсальными, но могут также специализироваться на выполнении определенных типов задач (например: банковская система, издательская система, информационно-поисковая, музыкальная, и т.д.).

5.2. Ретрансляционная система.

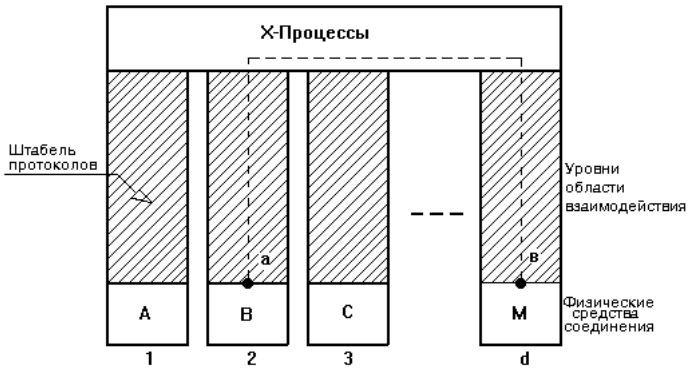
Это система, предназначенная для передачи данных или преобразования протоколов. Необходимость объединения нескольких сетей с разными протоколами, поставило задачу создания таких ретрансляционных систем, которые:

- объединяют сети с различной архитектурой, каждая из которых имеет полную автономию и свои средства управления;
- имеют базовые функциональные блоки, определяющие штабели протоколов для сетей разного типа;
- предусматривают наличие нескольких входных портов с различными скоростями передачи данных.

Для решения возлагаемых на них задач ретрансляционные системы осуществляют:

- коммутацию и маршрутизацию данных;
- согласование протоколов в соединяемых коммуникационных сетях либо частях сетей;
- передачу блоков данных между сетями либо их частями;
- укрупнение либо разукрупнение блоков данных, если в сетях (их частях) они имеют различные размеры;
- управление потоками данных;
- оповещение о переполнениях буферов систем и происходящих неисправностях;
- восстановление работы после отказов и неисправностей;
- определение состояний соединяемых сетей либо их частей;
- учет своей работы и подготовку отчетов об этом.

В соответствии с выполняемыми функциями, логическая структура·каждой из ретрансляционных систем состоит из d+1 частей.



Любая из d частей определяется штабелем протоколов соединяемых сетей либо их частей. Кроме этого, система содержит общую часть, выполняющую X-процессы объединения остальных d частей. Ретрансляционная система опирается на физические средства соединения (A,B,C...,M) в сетях, представленные физическими каналами. Последние соединяются через штабели протоколов и X-процессы (например, a-b).

В зависимости от числа обрабатываемых уровней выделяется четыре типа систем.

Одноуровневые системы включают только физический уровень. Двухуровневые системы к физическому добавляют канальный уровень, а трехуровневые также и сетевой уровень. Семиуровневые системы обрабатывают все уровни области взаимодействия. Кроме этого, ретрансляционные системы, подразделяются на две группы, определяемые выполняемыми функциями:

- коммутация и маршрутизация;

· преобразование штабелей протоколов.

К ретрансляционным системам, осуществляющим коммутацию и маршрутизацию относятся:
· узел интегральной коммутации, который строится на базе баньяновой сети либо матричного коммутатора;
· узел коммутации каналов;
· узел коммутации пакетов;
· узел смешанной коммутации;
· коммутатор.

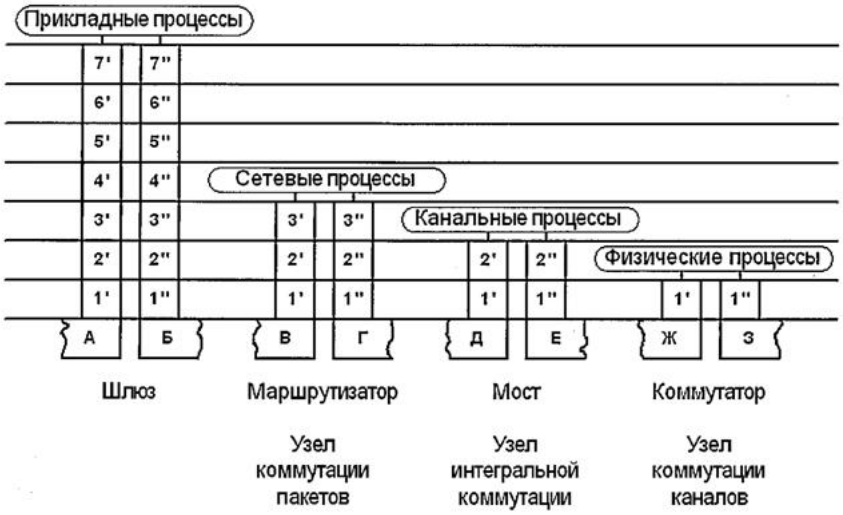


Рис. 5.3. Типы ретрансляционных систем

К ретрансляционным системам, преобразующим протоколы, относятся:
· мост;
· маршрутизатор;
· шлюз.

5.2.1. Ретрансляционные системы, осуществляющие коммутацию и маршрутизацию:

Узел коммутации каналов

Узел коммутации каналов – это ретрансляционная система, устанавливающая по вызову соединение последовательностей каналов между партнерами в течении сеанса. Основная его часть выполняет функции физического уровня и физических процессов, обеспечивающих соединение каналов друг с другом.

Структура основной части узла коммутации каналов:

В зависимости от типов физических средств соединения в каналах, подходящих к узлу, протоколы физического уровня могут быть как различными, так и одинаковыми. Кроме основной узел содержит и вспомогательную часть. Ее задачей является управление узлом и взаимодействие с административной системой. Управляющая часть содержит дополнительно уровни 2-7, а также прикладные процессы управления. Эти процессы и уровни располагаются над физическим уровнем основной части узла.

Физические процессы обеспечивают соединение нужных пар каналов. Все логические каналы, подходящие к узлу, используются при передаче данных монопольно.

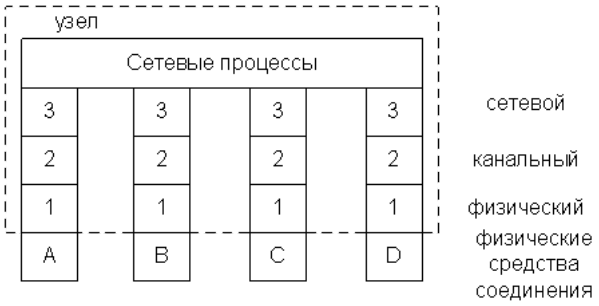
Узел коммутации пакетов

Узел коммутации пакетов – это ретрансляционная система, распределяющая блоки данных в соответствии с их адресацией.

Узел коммутации пакетов имеет достаточно сложную структуру:

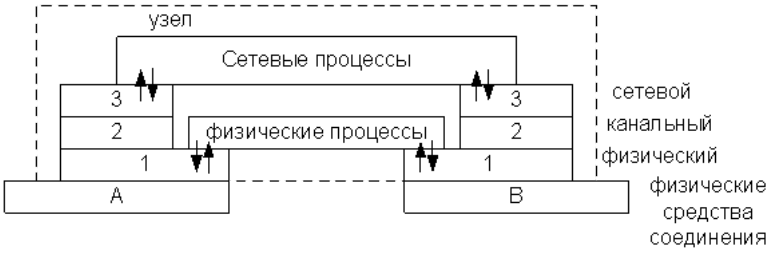
Протоколы на физическом уровне, канальном уровне и сетевом уровне могут быть как одинаковыми, так и различными. Вместе с основной частью узел содержит и управляющую часть, которая обеспечивает управление узлом и взаимодействует с административной системой.

Сетевые процессы обеспечивают коммутацию и маршрутизацию пакетов по адресам их назначения. Все каналы, подходящие к узлу, используются коллективным образом.



Узел смешанной и интегральной коммутации

Узел смешанной коммутации **–** это ретрансляционная система, обеспечивающая как коммутацию каналов, так и коммутацию пакетов. Узел смешанной коммутации имеет комплексную структуру:



Сетевые процессы осуществляют коммутацию пакетов. Коммутация каналов осуществляется физическими процессами.

Узел интегральной коммутации **—** ретрансляционная система, осуществляющая быструю передачу пакетов. Узел интегральной коммутации в отличие от узла коммутации пакетов передает по нужному маршруту кадры либо ячейки без просмотра их содержимого. Осуществляется сквозная коммутация. Операция ретрансляции выполняется только при помощи аппаратуры без использования программного обеспечения. Благодаря этому узел интегральной коммутации обеспечивает скоростную коммутацию данных. Узлы строятся на основе баньяновых сетей либо матричных коммутаторов.

5.2.2. Объединение сетей

Таким образом, ретрансляционные системы реализуют межсетевые, канальные и физические процессы. Задачей является выполнение функций, в том числе преобразований, необходимых для соединения частей сетей либо целых сетей.

Объединение сетей осуществляется на базе одного из двух принципов: с установлением соединения, без установления соединения. Каждое из них имеет определенные преимущества и недостатки. Так, объединение с установлением соединения позволяет заранее распределять буферы и другие ресурсы системы. В этом случае обеспечивается простое и надежное управление потоком информации, проходящими из одной сети в другую. При этом обеспечиваются уведомление о потере блоков данных и упорядочивание этих блоков. Однако организация и поддержание межсетевых соединений требует выполнения сложных протоколов.

Объединение сетей без установления между ними соединения характеризуется простотой протоколов и высокой скоростью работы ретрансляционной системы. Однако при использовании этого способа все преимущества объединения с установлением соединения становятся здесь недостатками. Для их компенсации абонентские системы обеих сетей должны имеет мощные версии транспортных протоколов.

5.3. Административные системы.

Административные системы **–** это системы, обеспечивающие управление сетью либо её частью. На неё возлагаются следующие функции:

· сбора информации и учёта работы компонентов сети (времени работы соединений, сведений о загрузке каналов и ресурсов сети, регистрации ошибок или отказов);

· подготовка отчётов о работе сети;

· осуществление диагностики;

· контроль передачи блоков данных;

· восстановление работы после отказов и неисправностей;

· управление конфигурацией (включение и выключение абонентских систем, ведение справочника сети; создание резервных каналов, изоляция неисправных компонентов);

· осуществление сервиса для пользователей, связанного с показом динамического состояния сети.

Административная система может совмещаться с узлом коммутации либо абонентской системой. Если в сети функционирует несколько абонентских систем, то одна из них назначается главной.

Управление сетью обеспечивает выполнение функций администрирования, из которых в первую очередь **выделяется:**

5.2.3. Управление конфигурацией сети и именованием

Задачи *управления конфигурацией сети и именованием* заключаются в конфигурировании параметров как элементов сети, так и сети в целом. Для элементов сети, таких как маршрутизаторы, мультиплексоры и т. п., с помощью этой группы задач определяются сетевые адреса, идентификаторы (имена), географическое положение и пр. Для сети в целом управление

конфигурацией обычно начинается с построения карты сети, то есть отображении реальных связей между элементами сети и изменении связей между элементами сети - образование новых физических или логических каналов, изменение таблиц коммутации и маршрутизации. Управление конфигурацией (как и другие задачи системы управления) могут выполняться в автоматическом, ручном или полуавтоматическом режимах. Например, карта сети может составляться автоматически, на основании зондирования реальной сети пакетами-исследователями, а может быть построена оператором системы управления вручную. Чаще всего применяются полуавтоматические методы, когда автоматически полученную карту оператор подправляет вручную. Методы автоматического построения топологической карты, как правило, являются фирменными разработками.

Более сложной задачей является настройка коммутаторов и маршрутизаторов на поддержку маршрутов и виртуальных путей между пользователями сети. Согласованная ручная настройка таблиц маршрутизации при полном или частичном отказе от использования протокола маршрутизации (а в некоторых глобальных сетях, например X.25, такого протокола просто не существует) представляет собой сложную задачу. Многие системы управления сетью общего назначения ее не выполняют, но существуют специализированные системы конкретных производителей, например система NetSys компании Cisco Systems, которые решают ее для маршрутизаторов этой же компании.

5.2.4. Обработка ошибок

Группа задач *обработки ошибок* включает выявление, определение и устранение последствий сбоев и отказов в работе сети. На этом уровне выполняется не только регистрация сообщений об ошибках, но и их фильтрация, маршрутизация и анализ на основе некоторой корреляционной модели. Фильтрация позволяет выделить из весьма интенсивного потока сообщений об ошибках, который обычно наблюдается в большой сети, только важные сообщения, маршрутизация обеспечивает их доставку нужному элементу системы управления, а корреляционный анализ позволяет найти причину, породившую поток взаимосвязанных сообщений (например, обрыв кабеля может быть причиной большого количества сообщений о недоступности сетей и серверов). Устранение ошибок может быть как автоматическим, так и полуавтоматическим. В первом случае система непосредственно управляет оборудованием или программными комплексами и обходит отказавший элемент за счет резервных каналов и т. п. В полуавтоматическом режиме основные решения и действия по устранению неисправности выполняют люди, а система управления только помогает в организации этого процесса - оформляет квитанции на выполнение работ и отслеживает их поэтапное выполнение (подобно системам групповой работы). В этой группе задач иногда выделяют подгруппу задач управления проблемами, подразумевая под проблемой сложную ситуацию, требующую для разрешения обязательного привлечения специалистов по обслуживанию сети.

5.2.5. Анализ производительности и надежности

Задачи *анализа производительности и надежности* связаны с оценкой на основе накопленной статистической информации таких параметров, как время реакции системы, пропускная способность реального или виртуального канала связи между двумя конечными абонентами сети, интенсивность трафика в отдельных сегментах и каналах сети, вероятность искажения данных при их передаче через сеть, а также коэффициент готовности сети или ее определенной транспортной службы. Функции анализа производительности и надежности сети нужны как для оперативного управления сетью, так и для планирования развития сети.

Результаты анализа производительности и надежности позволяют контролировать *соглашение об уровне обслуживания* (SLA), заключаемое между пользователем сети и ее администраторами (или компанией, продающей услуги). Обычно в SLA оговариваются такие параметры надежности, как коэффициент готовности службы в течение года и месяца, максимальное время устранения отказа, а также параметры производительности, например средняя и максимальная пропускная способности при соединении двух точек подключения пользовательского оборудования, время реакции сети (если информационная служба, для которой определяется время реакции, поддерживается внутри сети), максимальная задержка пакетов при передаче через сеть (если сеть используется только как транзитный транспорт). Без средств анализа производительности и надежности поставщик услуг публичной сети или отдел информационных технологий предприятия не сможет ни проконтролировать, ни тем более обеспечить нужный уровень обслуживания для конечных пользователей сети.

5.2.6. Управление безопасностью и учёт работы сети

Задачи *управления безопасностью* подразумевают контроль доступа к ресурсам сети (данным и оборудованию) и сохранение целостности данных при их хранении и передаче через сеть. Базовыми элементами управления безопасностью являются процедуры аутентификации пользователей, назначение и проверка прав доступа к ресурсам сети, распределение и поддержка ключей шифрования, управления полномочиями и т. п. Часто функции этой группы не включаются в системы управления сетями, а реализуются либо в виде специальных продуктов (например, систем аутентификации и авторизации Kerberos, различных защитных экранов, систем шифрования данных), либо входят в состав операционных систем и системных приложений.

К задачам *учета работы сети* относится регистрация времени использования различных ресурсов сети — устройств, каналов и транспортных служб. Подобные задачи имеют дело с такими понятиями, как время использования службы и плата за ресурсы — billing. Ввиду специфического характера оплаты услуг у различных поставщиков и различными формами соглашения об уровне услуг эта группа функций обычно не включается в коммерческие системы и платформы управления типа HP Open View, а реализуется.

Контрольные вопросы:

1. Перечислить основные компоненты сети.
2 Дайте определение: абонент и пользователь?
3. Что такое абонентская система в информационных сетях?
4. Для чего служит ретрансляционная система?
5. Назовите какие узлы существуют в ретрансляционных системах?
6. Какими техническими средствами осуществляется соединение информационных сетей?
7. Дайте определение административной системы в информационных сетях и рассказать о её назначении?
8. Расскажите различия между узлами коммутации пакетов и узлами коммутации каналов.

9. Какие устройства, преобразующие протоколы, относятся к ретрансляционным системам?
10. Что такое узел интегральной коммутации?

Практические задания:

ЗАДАНИЕ № 5.1. Создание сети для фирмы с помощью Microsoft ISA 2010.

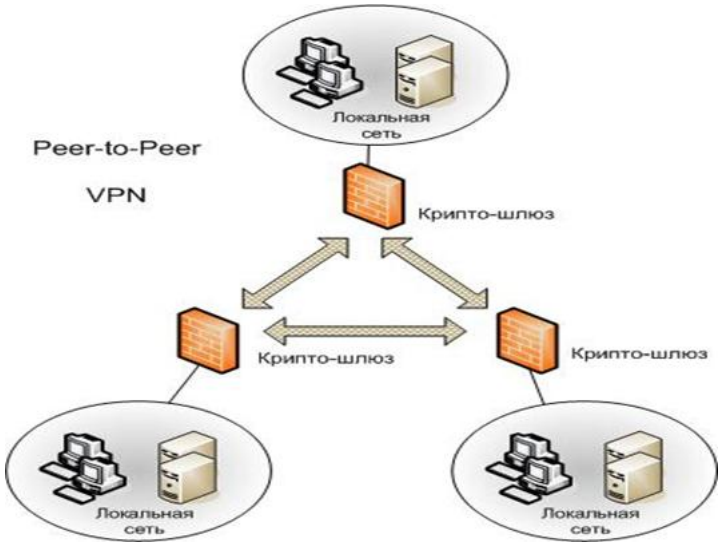
Метод объединения двух сетей с применением технологии VPNв англозязычной литературе называетя "Peer-to-Peer VPN" или "site-to-site VPN". Между двумя сетями устанавливается режим "прозрачного шифрования". Для шифрования и передачи трафика в IP-сетях наиболее часто используют протокол IPSec.

Для организации VPN-соединенией (VPN-туннелей) между центральным офисом и филиаламинебольших компанийрекомендуем использовать аппаратные интернет-шлюзы (firewall) со встроеннойподдержкой VPN. Примером таких шлюзов могут бытьZyXEL ZyWALL, Netgear Firewall, Check Point Safe@Office, и т.п. Данный класс продуктов рассчитан на применение в небольших компаниях со средней численностью персонала от 5 до 100 человек. Эти устройства просты в настройке, обладают высокой надежностью и достаточной производительностью. В головном офисе организации частоустанавливаютпрограммные интегрированные решения по защите сети, такие как"Microsoft Internet Security and Acceleration Server2010"(Microsoft ISA 2010),CheckPoint Express,CheckPoint VPN-1 Edge и другие. Для управления этими средствами защиты необходимо наличиевысококвалифицированного персонала, который, как правило, или имеется в головном офисе или заимствуется у компании-аутсорсера.

Инструкция по установки:

О 1 часть: http://www.isadocs.ru/articles/installing-threat-management-gateway-2010-rtm-enterprise-edition.html
О 2 часть: http://www.isadocs.ru/articles/installing-threat-management-gateway-2010-rtm-enterprise-edition-part2.html

Вне зависимости от применяемого оборудования, общая схема построения Peer-to-Peer VPN для безопасного объединения локальных сетей удаленных офисов в единую сеть, следующая:



Следует также заметить, что существуют специализированные аппаратные крипто-шлюзы,такие какCisco VPN Concentrator, "Континент-К", и др. Их область применения - сети средних и крупных компаний, где необходимо обеспечить высокую производительность при шифровании сетевого трафика, а также специальные возможности.

На что необходимо обратить внимание при выборе оборудования.

Выбирая оборудованиедля организациивиртуальной частной сети (VPN)необходимо обратить внимание на следующие свойства:

1. количество одновременно-поддерживаемых vpn-туннелей;
2. производительность;
3. возможность фильтрации сетевого трафика внутри vpn-туннеля (эта функция реализована далеко не во всех интернет-шлюзах);
4. поддержка управления качеством QoS (очень полезна припередачеголосовоготрафика между сетями);
5. совместимость с имеющимся оборудованием и применяемыми технологиями.

Аппаратные решения.

· Преимущества решений, построенных нанедорогих аппаратных интернет-шлюзах:

о низкая стоимость;

о высокая надежность (нет необходимости в резервном копировании, при отключении питания ничего не выходит из строя);

о простота администрирования;

о малое энергопотребление;

о занимает мало места, можно установить где угодно;

о в зависимости от выбранной платформы для построения VPN,имеется возможность для установки на vpn-шлюздополнительных сервисов: антивирусная проверка интернет-трафика, обнаружение атак и вторжений, и др, что существенноувеличивает общий уровень защищенности сети и уменьшает общую стоимость решения по комплексной защите сети.

· Недостатки:

o решение не масштабируется, увеличение производительности достигается полной заменой оборудования;

o менее гибко в настройках;

o интеграция с Microsoft Active Directory (или LDAP), как правило, не поддерживается.

Программные решения.

u **Преимущества программных решений:** гибкость; масштабируемость, т.е. возможность увеличить производительность по мере необходимости;

u **Недостатки: в**ысокая цена; сложность администрирования.

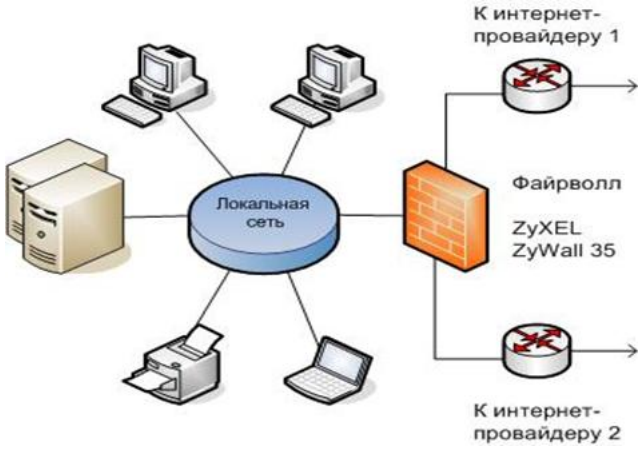
ЗАДАНИЕ № 5.2. Безопасное подключение офиса к Интернет. Решение для малого бизнеса.межсетевой экран.

Данное ИТ-решение используется при следующих условиях:

1. Число пользователей в организации находится в пределах от 10 до 50;
2. В организации есть как удаленные, так и мобильные пользователи.

Предлагаемое решение.

Защита сетевого периметра при подключении к Интернет осуществляется посредством установки аппаратного межсетевого экрана Zyxel.



Межсетевые экраны Zyxel показали свою надежность, гибкость и легкость в управлении. Они имеют возможность подключать средства антивирусной проверки http, ftp и smtp трафика путем установки дополнительных модулей (Аппаратный ускоритель ZyWALL Turbo Card и др.), а также имеют встроенную поддержку виртуальных частных сетей (VPN).

Преимущества использования аппаратного межсетевого экрана по сравнению с программным в небольшой компании сводятся к следующему:

1. Нет необходимости выделять отдельный компьютер для установки программного обеспечения межсетевого экрана и нести, в связи с этим, дополнительные накладные расходы на администрирование базовой операционной системы;
2. Нет нужды покупать операционную систему для установки программного обеспечения межсетевого экрана;
3. В таких устройствах нет жестких дисков, специализированная операционная система загружается из энергонезависимой памяти, как следствие -высокая надежность и производительность. Также нет проблем с резервным копированием, достаточно сохранить текущую конфигурацию устройства во внешний файл.

Межсетевой экран анализирует заголовки пакетов, но не их содержание, где обычно и таится вредоносный код (вирусы и т.п.). Этого недостаточно для надежного обеспечения нормальной работы предприятия. Поэтому многие менеджеры ИТ отдают предпочтение шлюзам, соединяющим функции межсетевого экрана с защитой от вирусов и обнаружением и предотвращением вторжений как наиболее реальному решению задачи защиты корпоративной сети от покушений из Интернета.

Для защиты периметра и поддержки удаленных VPN-соединений можно также использовать аппаратные файрволл компаний Netgear, D-Link, и др. Оборудование Netgear и D-Link несколько дешевле, но надежность,гибкость и качество интерфейса управления у продукции Zyxel, по нашему мнению, все-такисущественно выше. Стоит отметить, что некоторые возможности ZyWALL 35 являются избыточными и не всегда находят применение в небольших компаниях, например аутентификация с помощью внешнего RADIUS-сервера, поддержка демилитаризованной зоны (DMZ) и др. В этом случае, дешевле использовать более простые модели аппаратных файрволл.

Межсетевой экран ZyWALL

Решаемые задачи.

Применение межсетевого экрана в качестве межсетевого экрана при подключении офиса к Интернет позволит решить следующие задачи:

О фильтрация пакетов согласно созданным правилам фильтрации;
О инспекция пакетов с учетом состояния протокола (SPI);
О при подключении к двум провайдерам Интерент - резервирование канала или балансировка нагрузки;
О создание демилитаризованной зоны (DMZ) для изолирования интернет-сервисов;
О авторизация пользователей посредством локальной базы данных или авторизация и подсчет трафика на внешнем RADIUS сервере.

При использовании карты дополнительных услуг: on-line проверка на вирусы потока http, ftp, smtp.

ЗАДАНИЕ № 5.3. Подключаем к нашей новый офис с помощью маршрутизатора D-Link.

VPN предполагает комплексные решения в области защиты данных. Прежде всего, передаваемая информация передается в зашифрованном виде. Для идентификации адресата и отправителя применяются специальные меры. И наконец, проверяется, что данные не были изменены во время движения по публичным сетям, по ошибке или злонамеренно. Итак, построение VPN предполагает создание защищенных от постороннего доступа туннелей между несколькими локальными сетями и/или удаленными клиентами. Для создания и обслуживания подобных туннелей необходимы специальные протоколы, программное обеспечение, специфическое оборудование. На сегодняшний день одним из самых проработанных и совершенных Интернет-протоколов для построения VPN является протокол IPSec (IP Security). Он обеспечивает аутентификацию, проверку целостности и шифрование сообщений на уровне каждого пакета. Для управления криптографическими ключами IPSec использует протокол IKE*. Пожалуй, самым основным преимуществом IPSec является то, что это протокол сетевого уровня. VPN, построенные на его базе, работают абсолютно прозрачно для всех приложений, сетевых сервисов, а также для сетей передачи данных канального уровня. IPSec позволяет маршрутизировать зашифрованные пакеты сетям без дополнительной настройки промежуточных маршрутизаторов, поскольку он сохраняет, принятый в IPv4, стандартный IP-заголовок.

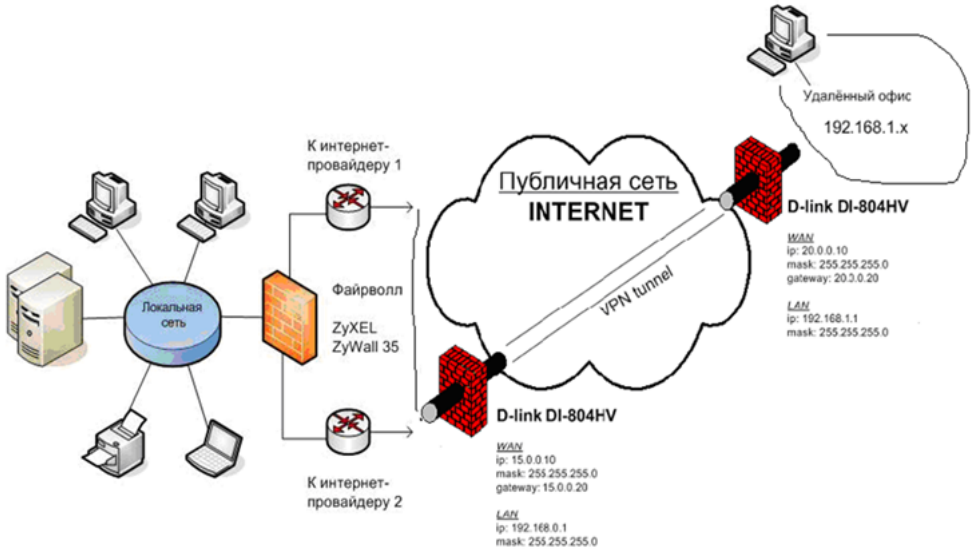
(*) IKE - Internet Key Exchange — протокол обмена Интернет-ключами. Этот протокол предусматривает три метода аутентификации для защиты данных и каналов связи и позволяет кодировать заголовки и содержимое пакетов с помощью ключа, обеспечивая практически абсолютную безопасность линии связи. В соответствии с протоколом IKE пакеты шифруются с помощью секретного ключа, заранее известного обеим сторонам, или с помощью стандартного открытого ключа. Кроме того, IKE поддерживает использование цифровых сертификатов, создаваемых такими специализированными организациями, как VeriSign, и обеспечивающих еще более высокий уровень защиты.

DI-804HV -это высокопроизводительный широкополосный маршрутизатор с функциями безопасной передачи данных, спроектированный специально для применения в связках центральный офис - отделение. Предлагая эффективное решения для подключения удаленных офисов во всем мире к центральному через Интернет , устройство составляет серьезную конкуренцию подключениям типа точка-точка по дорогим выделенным каналам. Маршрутизатор бизнес-класса DI-804HV поддерживает IPSec для обеспечения безопасности соединений, связывая небольшие сети удаленных офисов в единую сеть или позволяя получать дополнительные сервисы вашим доверенным партнерам удаленно. В дополнение, маршрутизатор одновременно выполняет функции Интернет-шлюза, предоставляя доступ в Интернет всем сотрудникам офиса, используя одино единственное подключение к провайдеру через Ethernet WAN порт или подключенный к нему кабельный/DSL модем. Маршрутизатор D-Link DI-804HV полностью поддерживает протокол IPSec. При помощи этого маршрутизатора возможно организовать до 40 туннелей IPSec. Начиная с версии прошивкиver.1.3, включена поддержка Dynamic VPN, позволяющая осуществлять VPN подключение к корпоративной сети мобильным хостам с непостоянными IP-адресами. DI-804HV предоставляет гибкую и недорогую реализацию VPN для обеспечения сохранности корпоративных данных.

УСТАНОВКА!!!

Итак, перед нами стоит задача: объединить при помощи VPN-туннеля сети главного и удалённого офисов, с тем, чтобы обеспечить безопасный обмен корпоративными данными, а также прозрачный защищённый доступ к Intranet-ресурсам сети главного офиса пользователям сети удалённого офиса через небезопасный Интернет. Оба офиса имеют выделенное подключение к Интернет с реальными статическими IP- адресами. Для осуществления задачи у нас есть два маршрутизатора D-link DI-804HV.

Вот как выглядит схема, которую нам предстоит реализовать.



Конфигурируем первый DI-804HV:

Шаг 1. Запускаем браузер, заходим на наш маршрутизатор и настраиваем WAN (внешний IP) и LAN (внутренний IP маршрутизатора).

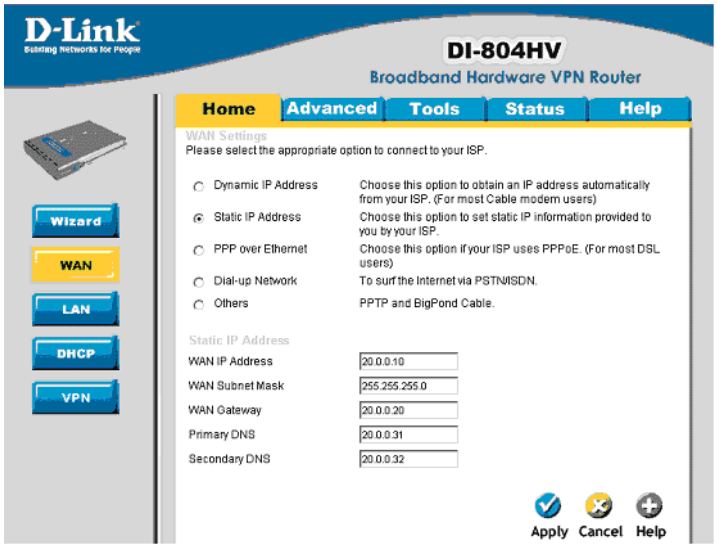
Примечание:

· не забываем отключить в браузере использование прокси-сервера, если таковая настройка имеется;

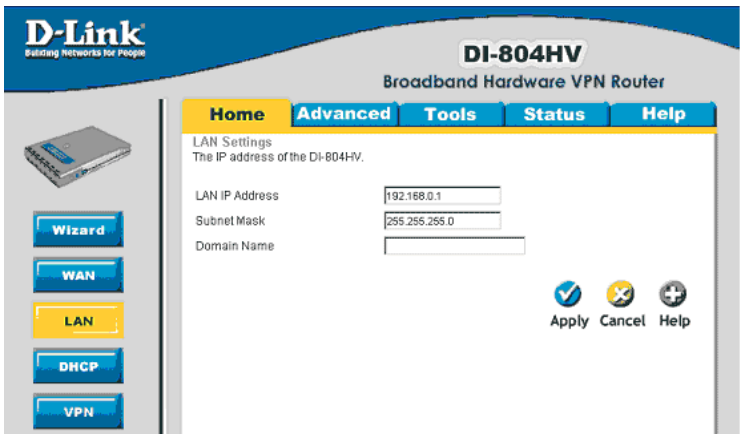
· внутренний IP -адрес у DI-804HV по умолчанию - 192.168.0.1, поэтому компьютеру, с которого конфигурируется DI-804HV, нужно назначить IP- адрес типа 192.168.0.x;

· логин по умолчанию - "Admin" , пароль пустой;

· для того чтобы внести изменения в конфигурацию маршрутизатора, после всех необходимых манипуляций на соответствующей странице веб-интерфейса нужно нажать кнопку "Apply" и затем "Restart".

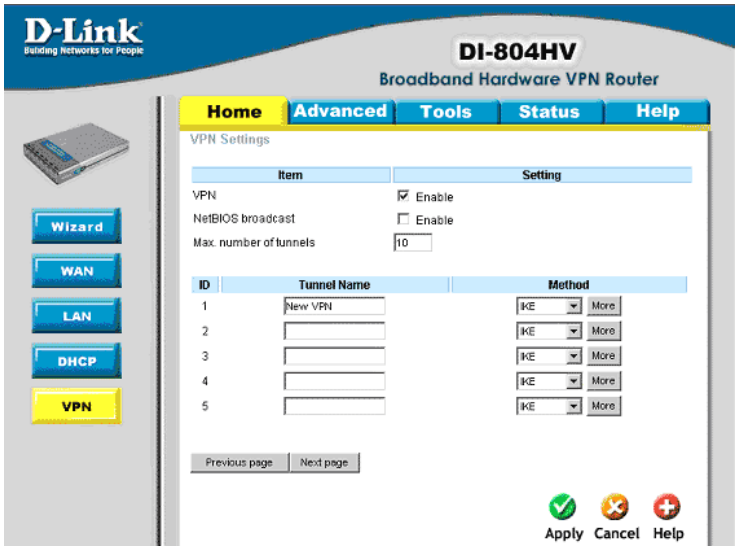


Выбираем статический IP - адрес. Указываем внешний IP, маску подсети, шлюз по умолчанию, первичный и вторичный DNS.

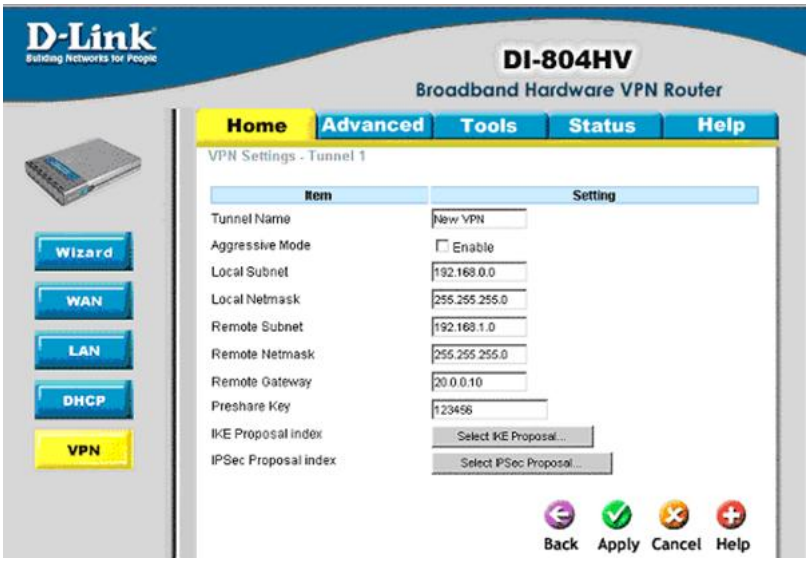


Задаём внутренний IP-адрес маршрутизатора, соответствующую маску подсети.

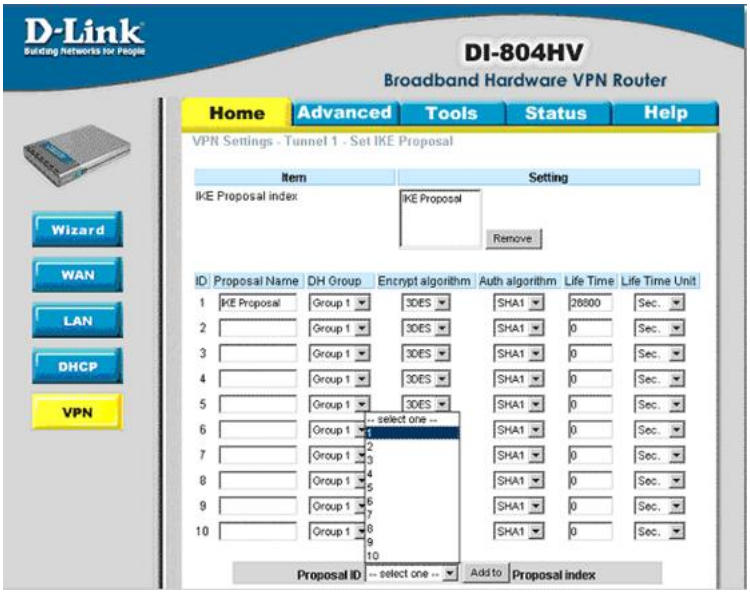
Шаг 2. Настраиваем VPN.



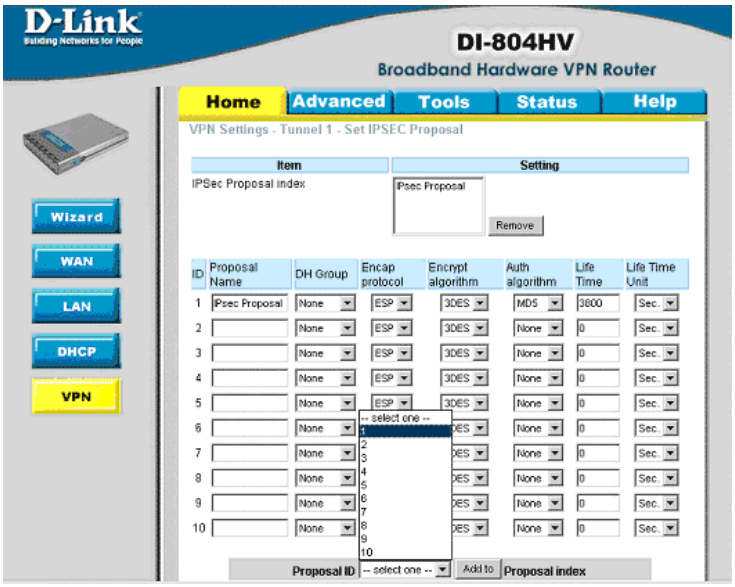
В маршрутизаторе DI-804HV возможно два метода настройки VPN : IKE и Manual. Настроим VPN используя IKE. Напротив ID1 в поле «Tunnel Name» вписываем название нашего туннеля, в выпадающем меню «Method» выбираем IKE, жмём кнопку «More».



Здесь мы задаём: адрес локальной подсети (Local Subnet), маску локальной подсети (Local Netmask), адрес удалённой подсети (Remote Subnet), маску удалённой подсети (Remote Netmask). В поле «Remote Gateway» задаём внешний IP-адрес удалённого VPN маршрутизатора. В поле «Preshare Key» — задаём первичный ключ, который будет использоваться механизмом IKE для организации VPN-туннеля. Этот ключ должен быть одинаковым на обоих концах VPN-туннеля.

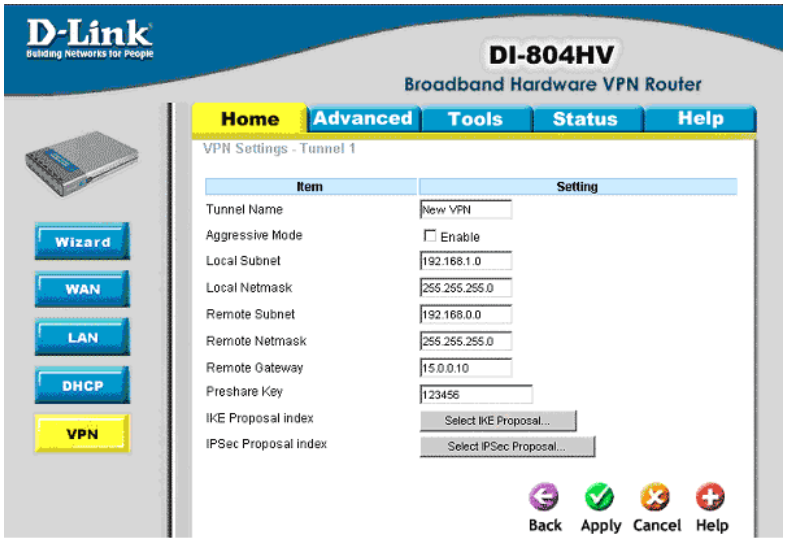


Нажимаем на кнопку «Select IKE Proposal …» и попадаем в меню Set IKE Proposal. Заполняем соответствующие поля, как показано на рисунке. Выбираем в выпадающем меню «Proposal ID» — «1» и нажимаем кнопку «Add to». Далее «Apply».



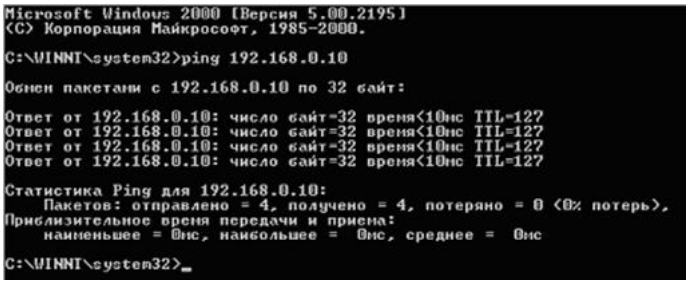
Теперь заходим в меню «Set IPSEC Proposal». Заполняем соответствующие поля, как показано на рисунке. Выбираем в выпадающем меню «Proposal ID» — «1» и нажимаем кнопку «Add to». Далее «Apply».

Шаг 3. Аналогичным образом настраиваем второй DI-804HV.



Настройки «IKE Proposal» и «IPSEC Proposal» у двух маршрутизаторов совершенно идентичны. Настройки VPN-туннеля у второго маршрутизатора немного отличаются.

Для того чтобы инициализировать VPN-туннель даём пинг с одного хоста на другой.



Как мы видим на скриншоте, наличие между хостами VPN-туннеля, проходящего через Интернет, остаётся совершенно незамеченным для утилиты ping. Более того, оно будет незаметно и для всех других сетевых приложений и служб. Это замечательное свойство протокола IPSec, обусловленное, как мы уже говорили, тем, что это протокол сетевого уровня, открывает огромные возможности перед системными администраторами компаний, имеющих более чем один офис.Таким образом мы обледенили 3 офиса..

ЗАДАНИЕ № 5.4. Объеденяем наши 3 офиса с 4 офисом на котором установлена Операционная система Unix.

Шаг 1.Установка в офис интернета - Операционная система Unix.

!ВАЖНО! Настраивать VPN-соединение мы будем по шагам. В конце каждого шага - шаг проверки. Все команды в командной строке вводятся от имени суперпользователя (root)

Что нам нужно для работы

Клиент Linux Mandriva 2010 скачать

Особой разницы в конфигурировании клиентского vpn соединения для различных дистрибутивов Linux нет. Для поднятия и настройки VPN-соединения нам потребуются всего две программы - **ppp** (http://samba.org/ppp/) и **pptp** (http://pptpclient.sourceforge.net/). Программа **ppp** с вероятностью 99% уже стоит в вашем дистрибутиве, пакет, содержащий **pptp**, в разных дистрибутивах называется по-разному, в основном **pptp-linux**. После установки в системе должны присутствовать два исполняемых файла - **/usr/sbin/pppd** и **/usr/sbin/pptp**. Вкратце - **pptp** создает туннель к VPN-серверу, через который **ppp** соединяется и работает как обычное модемное соединение.

Внимание! Файрвол мандривы блокирует все новые сетевые интерфейсы, поэтому в настройках файрвола нужно поставить галочку разрешения, и всё заработает. Настройка VPN PPTP осуществляется с правами администратора.

Естественно, для поднятия соединения нам необходима рабочая локальная сеть и данные провайдера об IP (или имени) VPN-сервера, VPN-логине и VPN-пароле. Также пригодится информация об используемом протоколе аутентификации и о наличии шифрования траффика (если ее нет - ничего страшного). Подавляющее большинство провайдеров используют протокол аутентификации MS-CHAP v2, а о наличии шифрования нам подскажут логи ошибок **pppd**. Подсказка: если у вас стоит MS Windows и там поднято VPN-соединение, его параметры можно посмотреть на вкладке соединения "Сведения". Нас интересуют параметры "Проверка подлинности" и "Шифрование".

Локальная сеть:
IP: 10.167.17.38
Маска подсети: 255.255.0.0.
Шлюз (gateway): 10.167.0.17
DNS1: 195.14.50.1
DNS2: 195.14.50.21
Параметры локальной сети могут получаться нами автоматически.
VPN параметры:
Имя VPN-сервера: vpn.наша.фирма.net
Логин: VPN_LOGIN
Пароль: VPN_PASSWORD

Шаг 2.Проверка работоспособности локальной сети.

Перед началом настройки самого VPN соединения необходимо до конца разобраться с настройками локальной сети: или вписать их вручную, или получить автоматически (не забудьте в последнем случае установить DHCP-клиента, если он еще не установлен, например dhclient, который входит в пакет dhcp-client). Если сеть уже настроена, мы должны увидеть примерно следующее:

```
[root@myhost sergo]# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:13:D4:68:B2:3E
inet addr:10.167.17.38  Bcast:10.167.255.255  Mask:255.255.0.0
inet6 addr: fe80::213:d4ff:fe68:b23e/64 Scope:Link
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:2884 errors:0 dropped:0 overruns:0 frame:0
TX packets:25 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:243742 (238.0 Kb)  TX bytes:2242 (2.1 Kb)
Interrupt:19
```

Или

```
[root@myhost sergo]# ip a sh dev eth0
3: eth0: <BROADCAST,MULTICAST,UP,10000> mtu 1500 qdisc pfifo_fast qlen 1000
link/ether 00:13:D4:68:B2:3E brd ff:ff:ff:ff:ff:ff
inet 10.167.17.38/16 brd 10.167.255.255 scope global eth0
[root@myhost sergo]# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.167.0.0      0.0.0.0         255.255.0.0     U     0      0        0 eth0
0.0.0.0         10.167.0.17     0.0.0.0         UG    0      0        0 eth0
```

Или

```
[root@myhost sergo]# ip r
10.167.0.0/16 dev eth0  proto kernel  scope link  src 10.167.17.38
default via 10.167.0.17 dev eth0 scope link
```

Если ничего подобного не выводится, поднимаем сеть и указываем в качестве шлюза по умолчанию наш шлюз локальной сети, выданный провайдером:

```
ifconfig eth0 10.167.17.38 netmask 255.255.0.0 up
route add default gw 10.167.0.17
```

Если IP DNS-серверов провайдер присылает автоматически, то получаем их из файла **/etc/resolv.conf**, но предварительно отключите все другие интерфейсы, кроме настраиваемого, который включите. Если же IP DNS-серверов провайдер выдал и автоматически не присылает, то их необходимо вписать в файл **/etc/resolv.conf**:

```
[root@myhost sergo]# cat /etc/resolv.conf
nameserver 195.14.50.1
nameserver 195.14.50.21
```

Если сеть работоспособна, должны пинговаться шлюз и VPN-сервер, а также DNS-сервера. Проверяем:

```
[root@myhost sergo]# ping -c5 10.167.0.17
PING 10.167.0.17 (10.167.0.17) 56(84) bytes of data.
64 bytes from 10.167.0.17: icmp_seq=1 ttl=255 time=3.95 ms
64 bytes from 10.167.0.17: icmp_seq=2 ttl=255 time=0.526 ms
64 bytes from 10.167.0.17: icmp_seq=3 ttl=255 time=0.528 ms
64 bytes from 10.167.0.17: icmp_seq=4 ttl=255 time=3.31 ms
64 bytes from 10.167.0.17: icmp_seq=5 ttl=255 time=0.534 ms
[root@myhost sergo]# ping -c5 vpn.someserver.net
PING vpn.corbina.net (195.14.38.8) 56(84) bytes of data.
64 bytes from vpn8-l0.msk.corbina.net (195.14.38.8): icmp_seq=1 ttl=248  time=1.17 ms
64 bytes from vpn8-l0.msk.corbina.net (195.14.38.8): icmp_seq=2 ttl=248 time=1.16 ms
64 bytes from vpn8-l0.msk.corbina.net (195.14.38.8): icmp_seq=3 ttl=248 time=1.19 ms
64 bytes from vpn8-l0.msk.corbina.net (195.14.38.8): icmp_seq=4 ttl=248 time=1.17 ms
64 bytes from vpn8-l0.msk.corbina.net (195.14.38.8): icmp_seq=5 ttl=248 time=1.00 ms
```

Шаг 3.Предварительная настройка роутинга.

Примечание: Предварительная настройка роутинга необходима в том случае, когда VPN и/или DNS-сервера находятся в других подсетях.

Из таблицы маршрутизации (см. выше) мы видим, что в настоящий момент доступ ко всем хостам сети (включая DNS и VPN

Тем не менее часто если маршрутизировать DNS-сервера в шлюз локальной сети, то открытие web-страниц происходит быстрее.

Для начала узнаем IP нашего VPN-сервера с помощью команды **ping**:

```
[root@myhost sergo]# ping -c5 vpn.corbina.net
PING vpn.corbina.net (195.14.38.8) 56(84) bytes of data.
```

Как видно из команды ping, IP VPN сервера 195.14.38.8

Добавляем в нашу таблицу роутинга статические маршруты на VPN и DNS сервера:

```
route add -host 195.14.50.1 gw 10.167.0.17
```

route add -host 195.14.50.21 gw 10.167.0.17
route add -host 195.14.38.8 gw 10.167.0.17
или
ip r a 195.14.50.1 via 10.167.0.17
ip r a 195.14.50.21 via 10.167.0.17
ip r a 195.14.38.8 via 10.167.0.17
Удаляем маршрут по умолчанию:
route del default
или
ip r d default
Таблица маршрутизации будет выглядеть так:
[root@myhost sergo]# route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
195.14.50.21 10.167.0.17 255.255.255.255 UGH 0 0 0 eth0
195.14.50.1 10.167.0.17 255.255.255.255 UGH 0 0 0 eth0
195.14.38.8 10.167.0.17 255.255.255.255 UGH 0 0 0 eth0
10.167.0.0 0.0.0.0 255.255.0.0 U 0 0 0 eth0
Или
[root@myhost sergo]# ip r
195.14.50.21 via 10.167.0.17 dev eth0
195.14.50.1 via 10.167.0.17 dev eth0
195.14.38.8 via 10.167.0.17 dev eth0
10.167.0.0/16 dev eth0 proto kernel skope link src 10.167.17.38
Проверка: мы должны успешно пинговать DNS и VPN сервера:
[root@myhost sergo]# ping -c5 195.14.50.1
PING 195.14.50.1 (195.14.50.1) 56(84) bytes of data.
64 bytes from 195.14.50.1: icmp_seq=1 ttl=56 time=4.45 ms
64 bytes from 195.14.50.1: icmp_seq=2 ttl=56 time=1.30 ms
64 bytes from 195.14.50.1: icmp_seq=3 ttl=56 time=1.22 ms
[root@myhost sergo]# ping -c5 195.14.50.21
PING 195.14.50.21 (195.14.50.21) 56(84) bytes of data.
64 bytes from 195.14.50.21: icmp_seq=1 ttl=56 time=0.982 ms
64 bytes from 195.14.50.21: icmp_seq=2 ttl=56 time=0.954 ms
64 bytes from 195.14.50.21: icmp_seq=3 ttl=56 time=1.02 ms
[root@myhost sergo]# ping -c5 195.14.38.8
PING 195.14.38.8 (195.14.38.8) 56(84) bytes of data.
64 bytes from 195.14.38.8: icmp_seq=1 ttl=248 time=1.34 ms
64 bytes from 195.14.38.8: icmp_seq=2 ttl=248 time=2.60 ms
64 bytes from 195.14.38.8: icmp_seq=3 ttl=248 time=1.09 ms

Шаг 4.Настройка параметров VPN-соединения. Тестовый запуск.

Все параметры нашего VPN соединения мы запишем в файле **/etc/ppp/peers/corbina**. Создадим его и наполним следующим содержанием:

pty "pptp 195.14.38.8 --nolaunchpppd --nobuffer"
remotename pptp
user VPN_LOGIN
password "VPN_PASSWORD"
lock
usepeerdns
nodeflate
nobsdcomp
noauth

Параметры user и password в комментариях не нуждаются.

Обратим внимание на то, что пароль забран в кавычки. При анализе проблем поможет указание параметра debug и чтение логов.

Убеждаемся, что в файлах **/etc/ppp/options**, **~/.ppprc**, **/etc/ppp/options.pppd** нет незакомментированных параметров, которыми бы система могла затереть наши настройки. Если есть - комментируем.

Поднимаем VPN соединение:
pppd call corbina debug nodetach
Появятся логи соединения. Если все прошло успешно, они будут выглядеть примерно так:
[root@myhost sergo]# pppd call corbina debug nodetach
using channel 2
Using interface ppp0
Connect: ppp0 <--> /dev/pts/0
sent [LCP ConfReq id=0x1 <asyncmap 0x0> <magic 0x33368137> <pcomp> <accomp>]
rcvd [LCP ConfReq id=0x1 <auth chap MD5> <magic 0x36da4966>]
sent [LCP ConfAck id=0x1 <auth chap MD5> <magic 0x36da4966>]
sent [LCP ConfReq id=0x1 <asyncmap 0x0> <magic 0x33368137> <pcomp> <accomp>]
rcvd [LCP ConfAck id=0x1 <asyncmap 0x0> <magic 0x33368137> <pcomp> <accomp>]

```
sent [LCP EchoReq id=0x0 magic=0x33368137]
rcvd [CHAP Challenge id=0x1 <f872f6df5542429b46d6cf7e89a3386c>, name = "bras8"]
sent [CHAP Response id=0x1 <ebb4965e871c49a07565b148dc2dbf29>, name = "unicorn2"]
rcvd [LCP EchoRep id=0x0 magic=0x36da4966]
rcvd [CHAP Success id=0x1 ""]
CHAP authentication succeeded
CHAP authentication succeeded
sent [IPCP ConfReq id=0x1 <compress VJ 0f 01> <addr 0.0.0.0>]
rcvd [IPCP ConfReq id=0x1 <addr 195.14.38.8>]
sent [IPCP ConfAck id=0x1 <addr 195.14.38.8>]
rcvd [IPCP ConfRej id=0x1 <compress VJ 0f 01>]
sent [IPCP ConfReq id=0x2 <addr 0.0.0.0>]
rcvd [IPCP ConfNak id=0x2 <addr 89.178.77.182>]
sent [IPCP ConfReq id=0x3 <addr 89.178.77.182>]
rcvd [IPCP ConfAck id=0x3 <addr 89.178.77.182>]
Cannot determine ethernet address for proxy ARP
local  IP address 89.178.77.182
remote IP address 195.14.38.8
Script /etc/ppp/ip-up started (pid 4072)
Script /etc/ppp/ip-up finished (pid 4072), status = 0x0
```

На соседнем терминале убедимся, что VPN-соединение установлено. Должен появиться сетевой интерфейс **ppp0**:

```
[root@myhost sergo]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:13:D4:68:B2:3E
inet addr:10.167.17.38  Bcast:10.167.255.255  Mask:255.255.0.0
inet6 addr: fe80::213:d4ff:fe68:b23e/64 Scope:Link
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:24990 errors:0 dropped:0 overruns:0 frame:0
TX packets:97 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:2327027 (2.2 Mb)  TX bytes:8516 (8.3 Kb)
Interrupt:19
lo        Link encap:Local Loopback
inet addr:127.0.0.1  Mask:255.0.0.0
inet6 addr:::1/128 Scope:Host
UP LOOPBACK RUNNING  MTU:16436  Metric:1
RX packets:13496 errors:0 dropped:0 overruns:0 frame:0
TX packets:13496 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:1387313 (1.3 Mb)  TX bytes:1387313 (1.3 Mb)

ppp0      Link encap:Point-to-Point Protocol
inet addr:89.178.77.182  P-t-P:195.14.38.8  Mask:255.255.255.255
UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
RX packets:4 errors:0 dropped:0 overruns:0 frame:0
TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:3
RX bytes:40 (40.0 b)  TX bytes:46 (46.0 b)
```

Если VPN сервер использует шифрование, соединение закончится ошибкой [ЗДЕСЬ ДОЛЖНЫ БЫТЬ ЛОГИ ОШИБКИ]. В этом случае добавим в файл **/etc/ppp/peers/corbina** строчку

```
require-mppe-128
```

и загрузим соответствующий модуль ядра командой

```
modprobe ppp_mppe
```

- эту команду стоит вписать в файл **/etc/rc.local**, чтобы она выполнялась на этапе загрузки.

Запускаем снова. Все должно заработать.

Обратите внимание на параметр **MTU** интерфейса **ppp0**. По умолчанию он равен 1500. Если ваш провайдер использует другую величину **MTU** (допустим, 1460) - в тот же файл конфигурации **etc/ppp/peers/corbina** добавляем строчку

```
mtu 1460
```

Также замечено, что проблема с соединением может быть из-за неправильной аутентификации, потому могут помочь такие настройки в файле etc/ppp/peers/corbina (показан случай надобности в mschap v2, который чаще всего используется для MS VPN):

```
refuse-eap
refuse-chap
refuse-mschap
```

Шаг 5.Окончательная настройка роутинга.

Итак, мы подняли VPN соединение, но в интернет выйти не можем - машина пока не знает где искать интернет-хосты. Для этого мы должны добавить маршрут по умолчанию через интерфейс **ppp0** в нашу таблицу маршрутизации (помните - старый маршрут по умолчанию мы удалили). В качестве шлюза по умолчанию теперь выступает remote IP address, который нам любезно предоставил VPN сервер - 195.14.38.8 (да-да, в нашем случае он совпадает с IP VPN сервера - но это не всегда так; это лишь шлюз, предоставленный нам VPN сервером и через него доступны интернет хосты). Этот **remote IP address** присутствует как в

логах **pppd** (remote IP address 195.14.38.8), так и в параметрах интерфейса **ppp0**, которые выводятся на экран командой ifconfig (P-t-P:195.14.38.8) - этот адрес мы увидим как шлюз, когда сеть уже будет поднята на интерфейсе ppp0. Вводим:

route add default gw 195.14.38.8
или
route add default dev ppp0
что в данном контексте - одно и то же.
Теперь попробуем пропинговать какой-нибудь интернет-хост:
[root@myhost sergo]# ping -c5 www.ya.ru
PING ya.ru (213.180.204.8) 56(84) bytes of data.
64 bytes from ya.ru (213.180.204.8): icmp_seq=1 ttl=61 time=2.11 ms
64 bytes from ya.ru (213.180.204.8): icmp_seq=2 ttl=61 time=2.23 ms
64 bytes from ya.ru (213.180.204.8): icmp_seq=3 ttl=61 time=2.39 ms
Работает!

Шаг 6.Автоматизация.

Теперь, когда соединение оттестировано, можно подумать и об автоматизации. Когда **pppd** устанавливает соединение, он автоматически выполняет скрипт **/etc/ppp/ip-up.d/ip-up**, когда соединение рвется - выполняется скрипт **/etc/ppp/ip-down.d/ip-down**. Значит, в эти файлы и надо забить весь роутинг, который в предыдущих пунктах мы вводили руками.

Мы не случайно сначала рассмотрели идеальный вариант, когда VPN сервер провайдера представлен в единственном числе и имеет один IP. В этом случае именем хоста (**vpn.наши фирма.net**) можно пренебречь и использовать в настройках только его IP, что мы и сделали. Однако если провайдер большой, под именем VPN сервера скрывается несколько серверов с разными IP, что позволяет провайдеру динамически регулировать нагрузку на них (примечание: вы можете выбрать один из этих IP и работать только с ним, что мы и делали ранее). Для того, чтобы выяснить, какие IP имеет хост **vpn. наши фирма.net**, воспользуемся командой **host** из пакета **bind-utils** (примечание: при повторных запусках команды вывод команды часто может быть иным по сравнению с предыдущими выводами команды, и видно, что при однократном запуске команды часто предоставляется не полный список IP адресов VPN сервера, а только список актуальных на данный момент):

пренебречь и использовать в настройках только его IP, что мы и сделали. Однако если провайдер большой, под именем VPN сервера скрывается несколько серверов с разными IP, что позволяет провайдеру динамически регулировать нагрузку на них (примечание: вы можете выбрать один из этих IP и работать только с ним, что мы и делали ранее). Для того, чтобы выяснить, какие IP имеет хост **vpn. наши фирма.net**, воспользуемся командой **host** из пакета **bind-utils** (примечание: при повторных запусках команды вывод команды часто может быть иным по сравнению с предыдущими выводами команды, и видно, что при однократном запуске команды часто предоставляется не полный список IP адресов VPN сервера, а только список актуальных на данный момент):

[root@myhost sergo]# host vpn.corbina.net
vpn.наша фирма.net has address 195.14.38.19
vpn.наша фирма.net has address 195.14.38.20
vpn.наша фирма.net has address 195.14.38.1
vpn.наша фирма.net has address 195.14.38.2
vpn.наша фирма.net has address 195.14.38.3
vpn.наша фирма.net has address 195.14.38.4
vpn.наша фирма.net has address 195.14.38.5
vpn.наша фирма.net has address 195.14.38.6
vpn.наша фирма.net has address 195.14.38.7
vpn.наша фирма.net has address 195.14.38.8
vpn.наша фирма.net has address 195.14.38.9
vpn.наша фирма.net has address 195.14.38.10
vpn.наша фирма.net has address 195.14.38.11
vpn.наша фирма.net has address 195.14.38.12
vpn.наша фирма.net has address 195.14.38.13
vpn.наша фирма.net has address 195.14.38.14
vpn.наша фирма.net has address 195.14.38.15
vpn.наша фирма.net has address 195.14.38.16
vpn.наша фирма.net has address 195.14.38.17
vpn.наша фирма.net has address 195.14.38.18

Роутинг на всю эту прорву серверов нам нужно один раз внести в файл **/etc/ppp/ip-up.d/ip-up** и привести файл к следующему виду:

```
#!/bin/sh
#
# This script is run by pppd when there's a successful ppp connection.
#
route add -host 195.14.38.1 gw 10.167.0.17
route add -host 195.14.38.2 gw 10.167.0.17
route add -host 195.14.38.3 gw 10.167.0.17
....
route add -host 195.14.38.19 gw 10.167.0.17
route add -host 195.14.38.20 gw 10.167.0.17
route del default
route add default dev ppp0
```

Хотел бы добавить, что часто, но не всегда, в скрипте **/etc/ppp/ip-up.d/ip-up** не обязательно забивать весь этот список, можно обойтись строкой

route add -host $5 gw 10.167.0.17

в скрипте **/etc/ppp/ip-up** перед строкой **exit 0**, т.к. **$5** - переменная, содержащая remote IP address, который часто, но не всегда, совпадает с адресом vpn сервера.

А в скрипт **/etc/ppp/ip-down.d/ip-down** мы запишем строчки, которые вернут нам шлюз по умолчанию после обрыва соединения:

```
#!/bin/sh
#
# This script is run by pppd after the connection has ended.
#
route del default
route add default gw 10.167.0.17
```

Надо вписать в файл **/etc/ppp/ip-up.d/ip-up** строчку **route add default dev ppp0**, иначе нет соединения. В результате наш файл настроек **/etc/ppp/peers/corbina** будет выглядеть следующим образом:

```
pty "pptp vpn.наша.фирма.net --nolaunchpppd --nobuffer"
remotename pptp
user VPN_LOGIN
password "VPN_PASSWORD"
lock
usepeerdns
nodeflate
nobsdcomp
noauth
pppd call наша.фирма
killall pppd (или pptp-command stop)
```

Запускать и прерывать соединение можно также командами

```
pon наша.фирма
poff наша.фирма
```

но предварительно выполнив команды:

```
cp /usr/share/doc/ppp/scripts/pon /usr/sbin/ && chmod u+x /usr/sbin/pon
cp /usr/share/doc/ppp/scripts/poff /usr/sbin/ && chmod u+x /usr/sbin/poff
```

Если есть необходимость запускать соединение от простого пользователя, установите программу **sudo** и в файл **/etc/sudoers** впишите:

```
sergo   myhost = NOPASSWD: /usr/bin/pon, /usr/bin/poff
```

Соответственно, замените **sergo** и **myhost** на имя вашего пользователя и его машины. Он сможет запускать и прерывать соединение командами:

```
sudo pon наша.фирма
sudo poff наша.фирма
```

Автозагрузка интернета при старте системы

Для автозагрузки интернета при старте системы добавьте в конец файла **/etc/rc.d/rc.local** строчку: pppd call corbina

Графические утилиты для настройки VPN в Mandriva

Есть простая графическая программа для настройки VPN в Mandriva для любого DE - vpnpptp (http://code.google.com/p/vpnpptp/), которая включает в себя графический конфигуратор, основанный на этой инструкции, а также программу для дозвона (при этом оба эти приложения достаточно независимы друг от друга).

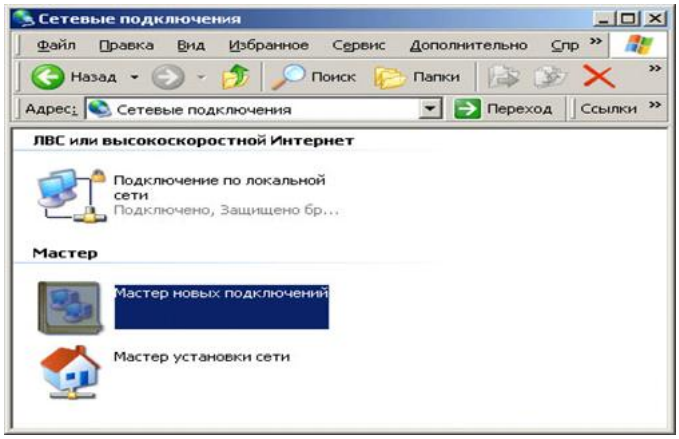
Для KDE есть программа KVpnc.

Заключение.. после всего сделанного до этого у нас в офисе будет доступен интернет..

ЗАДАНИЕ № 5.5. Подключение vpn соединения в windows xp и windows 2000(использованием route).

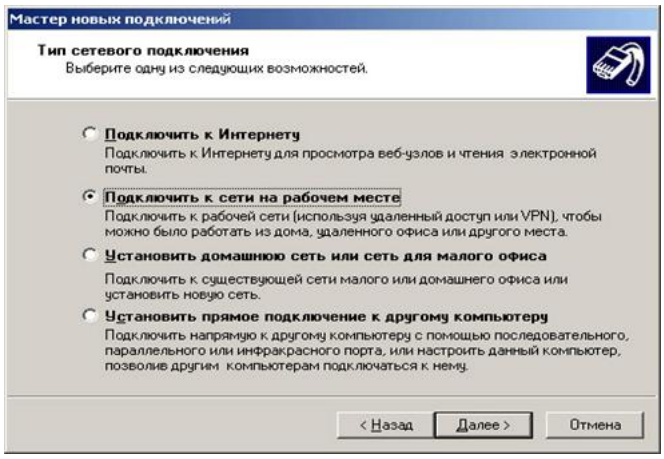
Шаг 1. Создание нового сетевого подключения.

В **Панели управления** Windows (Пуск -> Настройка -> Панель управления) необходимо выбрать папку **Сетевые подключения**. В MS Windows'2000 эта папка называется иначе - **Сеть и удалённый доступ к сети**. Доступ к этой папке может также осуществляться через свойства ярлыка **Сетевое окружение** (обычно находится на **Рабочем столе** Windows). В папке **Сетевые подключения** необходимо выбрать ярлык **Мастер сетевых подключений**.



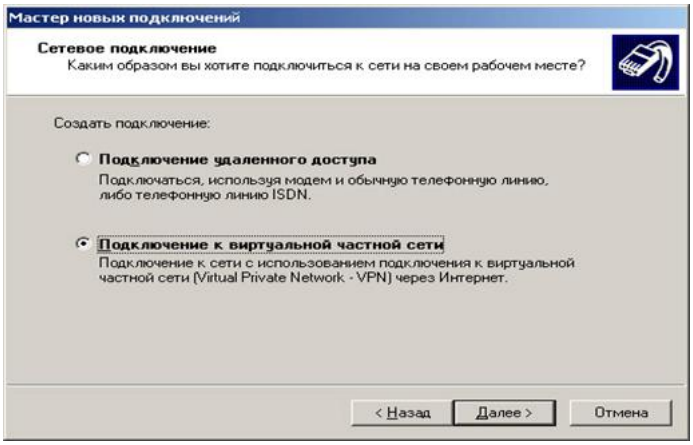
Шаг 2. Диалог «Тип сетевого подключения».

Мастер сетевых подключений предложит выбрать тип сетевого подключения. Необходимо выбрать тип **Подключить к сети на рабочем месте**.



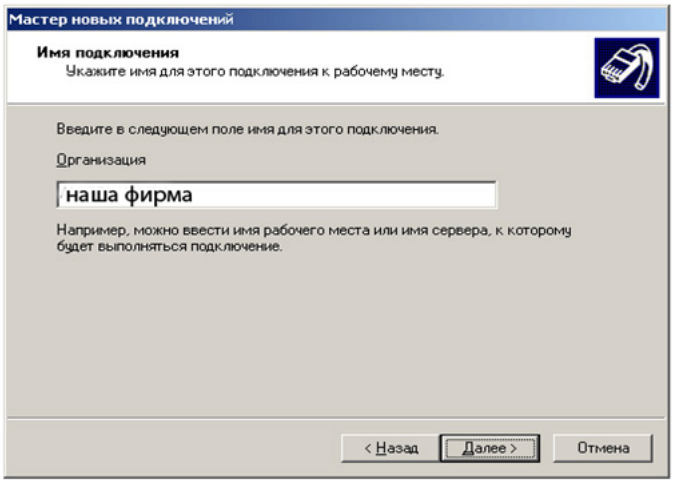
Шаг 3. Диалог «Сетевое подключение».

Следующий пункт определяет способ соединения с VPN-сервером. Необходимо выбрать пункт **Подключение к виртуальной частной сети**.



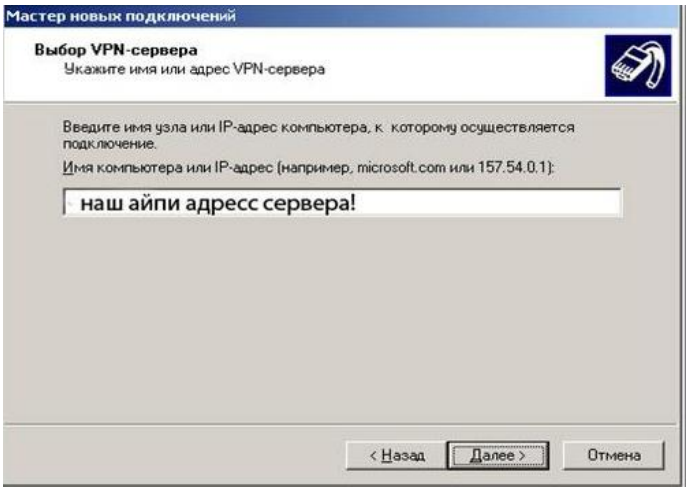
Шаг 4. Диалог «Имя сетевого подключения».

Данный диалог предлагает ввести произвольное имя сетевого подключения. Имя действительно может быть любым. Под этим именем ярлык данного соединения будет отображаться в папке **Сетевые подключения**. Например, ALTERLAN VPN.



Шаг 5. Диалог «Выбор VPN-сервера».

На данном этапе необходимо выбрать VPN-сервер, который позволит зарегистрироваться в VPN-сети. Вписать айпи адрес сервера. Этот адрес необходимо вписать в поле **Имя компьютера или IP-адрес**.

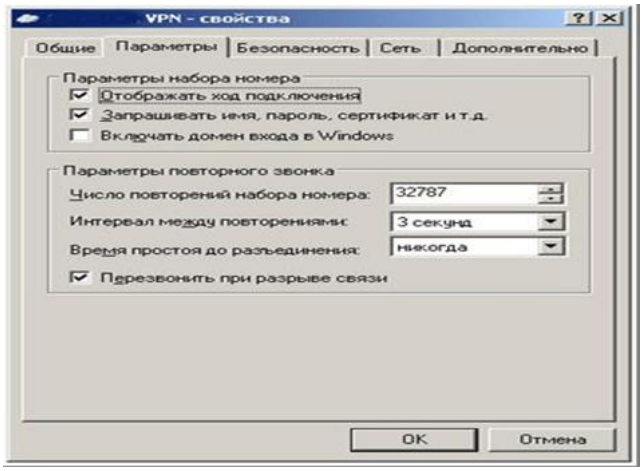


Шаг 6. Диалог «Подключение к VPN».

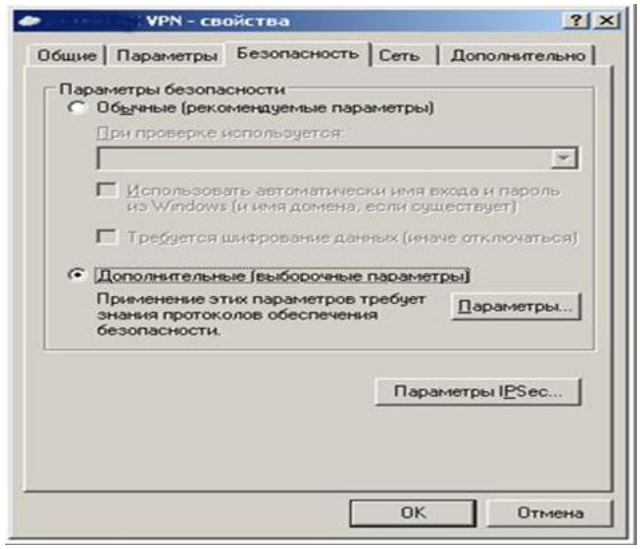
Здесь, в соответствующие поля, необходимо вписать логин и пароль, Кроме того оперируя опциями сохранения пароля, можно установить, будет ли данное подключение использоваться всеми, кто имеет доступ к данному компьютеру, или только владельцем текущей учётной записи.

Шаг 7. Последний штрих - настройка свойств подключения.

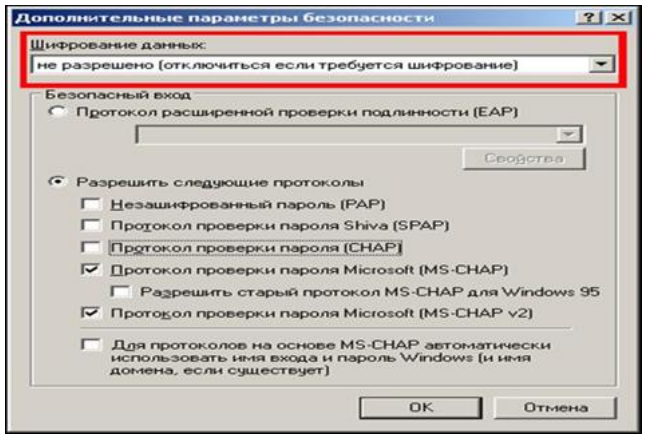
Выполните инструкции, описанные в Шаге 1. Кликните правой кнопкой мыши на ярлыке только что созданного сетевого подключения и выберите опцию **Свойства**. В закладке **Параметры** установите значения в соответствии со скриншотом.



Перейдите к закладке **Безопасность**. Необходимо отметить пункт **«Дополнительные параметры»**.



Далее следует нажать кнопку **Параметры** и в открывшемся окне настроить параметры согласно скриншоту: шифрование данных «не разрешено», разрешённые протоколы: «Протокол проверки пароля Misrosoft(MS-CHAP)» и «Протокол проверки пароля Misrosoft(MS-CHAP v2)».



Дла сохранения настроек следует нажать кнопку **OK**. После этого настройку подключения к VPN-серверу можно считать законченной.

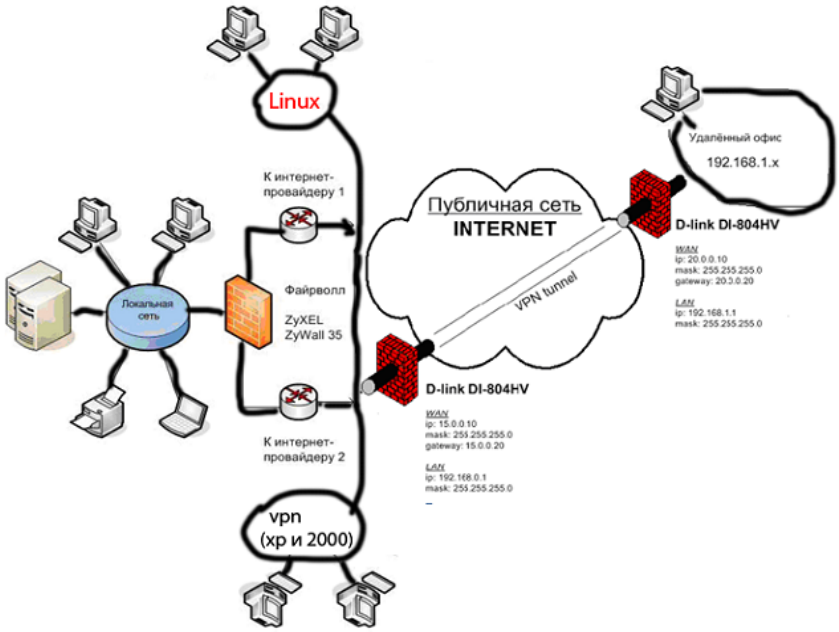
Шаг 7. Настройка роутинга.

Изначально, при включенном VPN-соединении, локальные ресурсы сети недоступны. Для их использования необходимо ручную ввести и выполнить определённую последовательность команд:

route add 10.0.0.0 mask 255.0.0.0 шлюз пользователя
route add 172.16.0.0 mask 255.240.0.0 шлюз пользователя
route add 62.117.94.0 mask 255.255.255.0 шлюз пользователя

Шаг 8. P.S.

После всего сделанного ранее мы с легкостью можем зайти в интернет и одновременно смотреть локальные ресурсы..



вот такое у нас получилось соединение сетей состоящее из 4 офисов подключенных разными методами (описанными ранее).

Внутри офиса компьютеры соединены между друг другом витой парой.

Перечень литературы и Интернет-ресурсов:

1. Microsoft Windows 2000 Server. Учебный курс MCSA/MCSE (3-е изд.) Пер. с англ. — М.: Издательско-торговый дом «Русская редакция», 2002. — 870 с.

2. Microsoft Windows 2000 Active Directory Services. Учебный курс Пер. с англ. — М.: Издательско-торговый дом «Русская редакция», 2001 — 800 с.

3. Вишневский А., Кокорева О., Чекмарев А. Microsoft Windows Server 2003. Русская версия. — С.-Пб.: БХВ-Петербург, 2003 — 1120 с.

4. Власов Ю. В. Терминальные службы Windows 2000. Часть 1 //Windows 2000 Magazine/RE, № 1, 2001 г., с. 56-59.

5. Власов Ю. В. Терминальные службы Windows 2000. Часть 2 //Windows 2000 Magazine/RE, № 2, 2001 г., с. 56-62.

6. Власов Ю. В. Начинаем работать с Windows NT Terminal Server //Windows 2000 Magazine/RE, № 2(5), 2000 г., с. 27-35.

7. Кульгин М. Технологии корпоративных сетей. Энциклопедия. — С.-Пб.:«Питер», 2000, 704 с.

8. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3-е издание — С.-Пб.: «Питер», 2005 — 960 с.

9. Таненбаум Э. Компьютерные сети (3-е изд.) Пер. с англ. — С.-Пб.:«Питер», 2002 — 848 с.

10. Ч. Рассел, Ш. Кроуфорд, Дж. Джеренд Microsoft Windows Server 2003. Справочник администратора. — М.:Эком, 2005 — 1391 с.

11. Уильям Р. Станек, Microsoft Windows Server 2003. Справочник администратора. Пер. с англ. — М.: Издательско-торговый дом «Русская редакция», 2004 - 648 с.

12. Объединение локальных сетей через транзитную ATM-сеть - http://www.citforum.ru/nets/tpns/glava_8.shtml

Тема 6. Коммуникационные и моноканальные сети

Цели:

· Научиться определять тип подсети, подходящий для решения конкретной задачи;
· Получить представление о топологии и структуре моноканала;
· Научиться идентифицировать метод доступа;
· Усвоить основные особенности каждого метода доступа:
О CSMA/CD; CSMA/CA;
О с передачей маркера; по приоритету запроса.

Коммуникационной сетью - называется сеть, основной задачей которой является передача данных. Коммуникационная сеть, именуемая также сетью передачи данных, является ядром информационной сети, обеспечивающим передачу и некоторые виды обработки данных. На базе одной коммуникационной сети можно создать несколько информационных сетей. Задачей коммуникационной сети является доставка адресатам блоков данных, которые при этом не должны терять своей целостности, доставляться без ошибок и искажения. Важными в сети являются также операции по предотвращению больших очередей и переполнения буферов систем, Коммуникационные сети делятся на три класса: сети с маршрутизацией данных, сети с селекцией данных и смешанные сети.

Наряду с сетями, каждая из которых функционирует в соответствии с принятым протоколом, появились многопротокольные сети. Их создание требует больших капиталовложений. Однако затраченные средства быстро окупаются гибкостью работы этих сетей. Высокопроизводительные коммуникационные сети стали именоваться базовыми сетями. Высокие скорости обеспечивают сети ретрансляции кадров.

Соответственно типам передаваемых сигналов различают аналоговые сети и дискретные сети.

Аналоговая сеть - коммуникационная сеть, передающая и обрабатывающая аналоговые сигналы. Необходимость передачи звука, речи и изображений привела к созданию аналоговых сетей, в которых носителем данных является аналоговый сигнал. Для передачи речи были созданы телефонные сети.

Как и любая сеть с маршрутизацией данных, телефонная состоит из узлов коммутации, именуемых Автоматическими телефонными станциями (АТС), а в качестве абонентских систем, в первую очередь, используются телефонные аппараты. Чаще всего, телефонная сеть опирается на кабельную сеть. В настоящее время телефонная сеть быстро переходит на дискретные сигналы. Это дает возможность использовать многопрофильные коммуникационные сети, строить работу телефонных станций на базе микропроцессоров. Дискретная телефонная сеть надежна в работе и обеспечивает высокую помехоустойчивость связи.

Передача движущихся изображений стала осуществляться через телевизионные сети. Телевизионная сеть - сеть, предназначенная для обеспечения функционирования телевидения. На первых этапах своего развития телевизионные сети создавались как аналоговые сети, предназначенные только для передачи движущихся изображений и звукового их сопровождения. Характерной особенностью всех телевизионных сетей является их высокая пропускная способность, достигающая сотен мегабит в секунду. Телевизионная сеть вначале базировалась на использовании одного либо двух древовидных моноканалов, построенных на широкополосных каналах, создаваемых на основе эфира. Теперь большое распространение получают сети кабельного телевидения; особенно с использованием оптических кабелей. Из-за увеличения числа абонентов, наращивания длины магистралей на смену древовидной пришла гнездовая структура. Телевизионная сеть из сети широковещания постепенно превращается в многоцелевую коммуникационную сеть большой пропускной способности.

Однако, вскоре стал ясен первый важный недостаток аналоговых сетей - искажение сигналов и трудности, связанные с восстановлением их первоначальной формы. С появлением компьютеров стал ясен второй недостаток рассматриваемых сетей трудности, связанные с обеспечением взаимодействия компьютеров, которые данные передают с помощью дискретных сигналов.

Развитие коммуникационных сетей показало необходимость интеграции звука, изображений и других типов данных для возможности их совместной передачи. Так как дискретные сети надежней и экономичней аналоговых, то за основу были приняты именно они. В этой связи число аналоговых сетей быстро сокращается и они заменяются дискретными.

Дискретная сеть — коммуникационная сеть, передающая и обрабатывающая дискретные сигналы. Первоначально дискретные принципы использовались в системах обработки данных. В семидесятых годах эти принципы стали применяться и в коммуникационных сетях. Разработка теории, массовое производство разнообразных высокоскоростных Интегральных Схем (ИС), создание дискретной аппаратуры для каналов привели к тому, что обработка и передача данных слились в единое целое. Появились протоколы, определяющие дискретные сети, именуемые также цифровыми сетями. Использование в сетях дискретных сигналов позволило обеспечить различные виды коммутации на базе одних и тех же узлов коммутации и каналов. Эта задача решена международным союзом электросвязи, который разработал модель Цифровой Сети с Интегральным Обслуживанием (ЦСИО или ISDN). Для дискретных сетей созданы дискретные системы, обеспечивающие скоростную передачу сигналов. Дискретные сети по сравнению с прежними (аналоговыми сетями) имеют достаточно много преимуществ. К ним, в первую очередь, относятся: высокая помехоустойчивость, широкое использование микропроцессоров и устройств памяти, простота каналообразующей аппаратуры.

6.1. Сеть с маршрутизацией данных.

Сеть с маршрутизацией данных – тип коммуникационной сети, в которой для передачи данных необходимо выполнение процесса маршрутизации.

Важной особенностью, отличающей сеть с маршрутизацией данных от сети с селекцией данных, является наличие узлов коммутации. Характерно, что в этой сети передача данных от одного источника одновременно возможна только одному адресату. Такая сеть состоит из одного либо группы узлов коммутации (1,2,3), связанных каналами друг с другом, а также с абонентскими системами и административными системами, подключаемыми в точках абонентского интерфейса. Этот интерфейс определяет взаимодействие сети с абонентской либо административной системой. Межузловой интерфейс характеризует в сети взаимодействие узлов коммутации друг с другом. И, наконец, межсетевой интерфейс описывает взаимодействие двух сетей. Простейшим видом рассматриваемой сети является одноузловая звездообразная сеть.

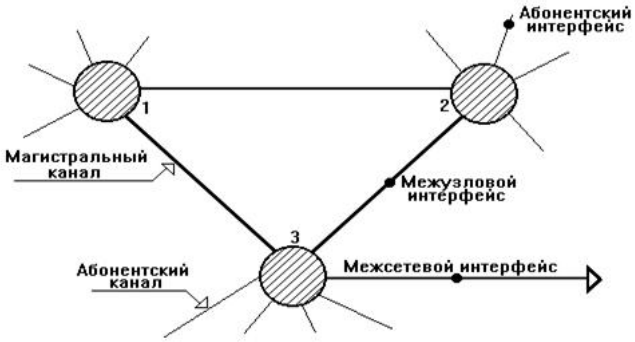


Рис. 6.1. Сеть с маршрутизацией данных

Стратегия передачи данных в сети с маршрутизацией информации строится на следующих принципах. Каждый узел коммутации участвует в процессе маршрутизации, управляя только своей зоной - каналами, связанными с этим узлом. Получая информацию в этой зоне, узел осуществляет маршрутизацию в зоне и коммутацию блоков данных либо каналов. Узлы коммутации могут также сообщать друг другу о состоянии компонентов сети и трафика в различных ее частях. В результате прокладываются маршруты передачи данных в соответствии с адресами их отправления и назначения. Процесс управления сетью распределен между административной системой и всеми узлами. Структура узла разбивается на несколько крупных блоков: Ядром ее является коммуникационный блок, который обеспечивает маршрутизацию и коммутацию пакетов. Непосредственно с коммуникационным блоком взаимодействует административный блок, выполняющий функции управления узлом. К узлу, подходят магистральные каналы и абонентские каналы. Первые соединяют узлы и сети друг с другом, вторые подключаются к абонентским системам и административным системам.

Универсальный интерфейс коммуникационной сети **–** это интерфейс между абонентской или административной системой и коммуникационной сетью. Международный союз по электросвязи утвердил универсальный интерфейс для синхронной работы в общественной коммуникационной сети, определяемый рекомендацией X.21. В ней определяется пара взаимодействующих смежных систем: Оконечное Оборудование Данных ООД (DTE) и Оконечное Оборудование Сети ООС (DCE). Первой является абонентская или административная система; второй **–** связанная с первой ретрансляционная система. Между ними определяется интерфейс на физическом уровне.

6.2. Коммуникационные подсети.

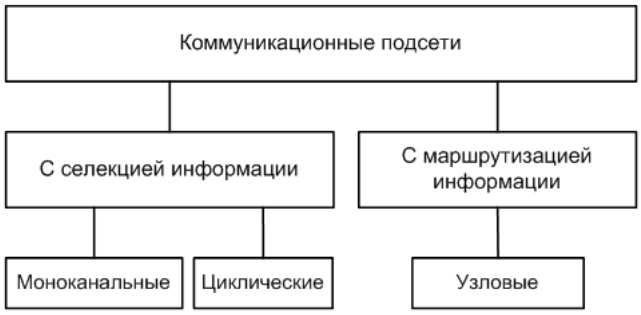


Рис. 6.2. Классификация коммуникационных подсетей

Коммуникационные подсети характеризуются многими свойствами. Важнейшими из них являются те, которые определяют способы поставки информации конкретным адресатам. В этом отношении коммуникационные подсети делятся на два класс. К первому из них относятся *коммуникационные подсети с селекцией информации*. Они характеризуются тем, что в них любой блок данных передается от одной абонентской системы-отправителя всем абонентским системам. Системы, получив очередной блок данных, проверяют адрес его назначения. Система, которой адресован блок, принимает его, остальные системы отвергают этот блок. В результате происходит селекция информации, которая позволяет посылать блоки данных одной группе, а также сразу всем абонентским системам, подключенным к коммуникационной подсети. Подсети с селекцией информации делятся на две группы: *моноканальные* и *циклические*. Они различаются тем, что в подсети первой группы каждый посланный блок данных попадает ко всем абонентским системам практически одновременно, а в подсети второй группы каждый передаваемый блок доставляется всем абонентским системам последовательно (по очереди), проходя мимо каждой из них.

Моноканальная коммуникационная подсеть далее для краткости именуется *моноканалом*. Моноканал строится на основе общего канала, к которому через специальные устройства подключаются все абонентские системы сети. Циклическая коммуникационная подсеть, часто именуемая *циклическим кольцом*, - это канал, имеющий кольцевую форму. В это кольцо врезаются абонентские системы, деля его на сегменты. Ко второму классу относятся *коммуникационные подсети с маршрутизацией информации*. В этих подсетях передача данных в отличие от сетей предыдущего класса осуществляется от одной абонентской системы-отправителя к другой абонентской системе-получателю. Для обеспечения такой доставки информации в коммуникационной подсети используются один либо более узлов коммутации. Поэтому рассматриваемую подсеть далее будем именовать узловой. Каждый узел коммутации принимает блоки данных и передает далее по различным направлениям в зависимости от адресов их назначения. Благодаря этому в подсети осуществляется маршрутизация информации - прокладка через коммуникационную подсеть трактов, связывающих абонентские системы. Моноканальные, циклические и узловые подсети нередко конкурируют друг с другом. При этом, правда, нужно иметь в виду, что моноканальные и узловые подсети могут быть как локальными, так и территориальными. Что же касается циклических подсетей, то они являются только локальными.

6.3. Моноканальные подсети.

Моноканал – это канал, одновременно (с точностью до времени их распространения) передающий сигналы группе систем. Моноканал похож на циклические сети. Моноканал является основой моноканальной сети. Он состоит из одного или нескольких параллельно расположенных общих звеньев, блоков доступа и абонентских звеньев. В зависимости от размеров, топологии, пропускной способности и других характеристик, выделяют несколько типов моноканала: шина, магистральный моноканал, древовидный моноканал.

Моноканальная сеть – это локальная сеть, ядром которой является моноканал. Моноканал в соответствии с базовой эталонной моделью взаимодействия открытых систем выполняет в сети роль физических средств соединения. Блоки доступа и абонентские звенья обеспечивают включение в сеть абонентских систем. В последних физический уровень и канальный уровень определяются характеристиками моноканала. Выбор физических средств моноканала зависит от предъявляемых к ним требований, в первую очередь — скорость передачи сигналов, надежность работы, стоимость средств. В зависимости от способа передачи сигналов по моноканалам, последние делятся на два вида: физические и частотные.

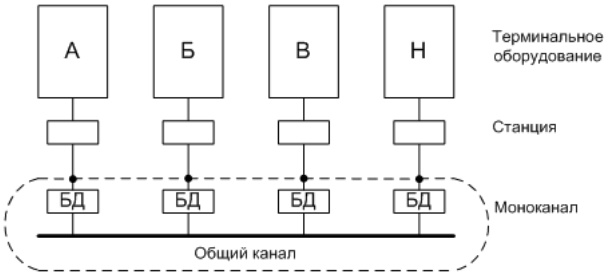


Рис. 6.3. Физический моноканал

Физический - канал, через который возможна одновременная передача только одного сигнала. Физический моноканал строится на основе коаксиального либо оптического кабеля, скрученной пары проводов, плоского кабеля, через который одновременно направляется только один сигнал. Последний использует физическую среду полностью.

В ***частотном канале*** за счет создания частотных полос одновременно передается группа сигналов (по каждой полосе по сигналу). Частотный моноканал, напротив, занимает только одну полосу, в используемой физической среде. Так, на рис. 7.4 показана группа частотных каналов, построенных на основе широкополосного коаксиального кабеля. Для упрощения изображены лишь две используемые полосы, в действительности же в кабеле создается значительное число частотных полос, на основе которых строится большое число частотных моноканалов. На основе двух частотных моноканалов, образованы две не связанные друг с другом информационные сети. Сигналы по общему каналу передаются только в одну сторону. Вследствие этого приходится принимать специальные меры.

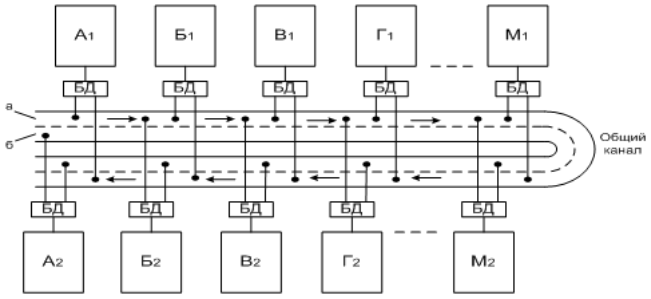


Рис. 6.4. Частотный моноканал

В коммуникационных подсетях все шире начинают применяться ***оптические моноканалы***. Это связано с тем, что оптическое волокно по сравнению с металлом имеет ряд важных преимуществ. К ним, прежде всего, следует отнести высокую защищенность от электромагнитных помех, малую массу и отсутствие все более дефицитной меди. Кроме того, если затухание сигнала, передаваемого по коаксиальному кабелю, составляет 50—200 дБ/км, то в качественном оптическом волокне оно равно всего 2—5 дБ/км. Это позволяет резко повысить частоту передаваемых в моноканале сигналов и увеличить длину кабеля без повторителей и усилителей. Современные оптические кабели обеспечивают передачу данных со скоростями, >500 Мбит/с, при расстоянии между повторителями до 5 км.

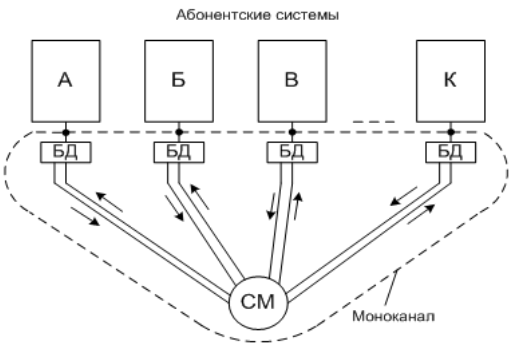


Рис. 6.5. Оптический моноканал со смесителем сигналов

Моноканал, в котором сигналы по оптическим волокнам передаются только в одном направлении, показан на рис.10. 5. Моноканал имеет форму звезды, исходящей из специального устройства, именуемого смесителем (СМ) сигналов. К нему от каждого блока доступа (БД) подходит два оптических волокна. Каждое из них передает сигналы в одном направлении. Задачей смесителя является передача пришедшего по одному из волокон сигнала параллельно всем волокнам, направленным к абонентским системам сети. В большом оптическом моноканале используется группа активных смесителей, располагаемых в несколько ярусов. Большое число абонентских систем, включаемых в моноканальную сеть, все возрастающие объемы информации требуют увеличения скоростей передачи блоков данных. Эта задача может быть решена созданием многоканальных моноканалов.

Первый способ повышения скорости передачи данных заключается в создании не одного, а нескольких общих каналов. Несмотря на наличие нескольких каналов, здесь не возникает, как в узловой подсети, проблема маршрутизации информации. В рассматриваемом моноканале выбирается не маршрут передачи, а номер общего канала. И, несмотря на наличие нескольких каналов осуществляется, как обычно, селекция (выбор по адресам назначения) принимаемых блоков информации.

Второй способ повышения скорости — заключается в создании моноканальной иерархии. В сети функционирует 18 абонентских систем (А - Т). Однако они подключены не к одному, а к шести моноканалам (1—6).

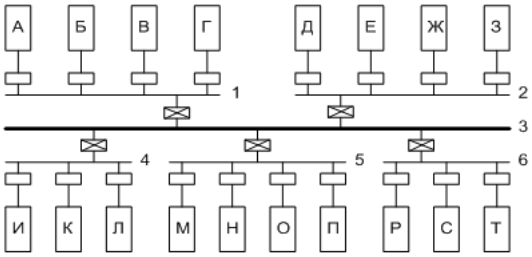


Рис. 6.6. Иерархия моноканалов

В рассматриваемой сети в большинстве случаев взаимодействующие системы передают данные соответственно через свои моноканалы 1, 2, 4, 5, 6. Что касается моноканала 3, то он используется только тогда, когда необходимо взаимодействие систем, подключенных к разным моноканалам. В результате использования иерархии моноканалов можно резко повысить скорость передачи информации.

6.4. Множественный доступ.

К общему звену моноканала подключается значительное число абонентских систем. Поэтому возникает проблема множественного доступа. Ее решение обеспечивает принцип функционирования моноканала.

Доступом называют операцию, обеспечивающую запись, модификацию, чтение или передачу данных. Ситуация, в которой несколько объектов хотят одновременно использовать ресурс, называют состязанием. Упорядочение этой ситуации осуществляется недопущением либо прекращением состязаний. **Метод доступа –** это способ определения того, какая из рабочих станций сможет следующей использовать ИС. Метод доступа — набор правил, которые определяют, как компьютер должен отправлять и принимать данные по сетевому кабелю. То, как сеть управляет доступом к каналу связи (кабелю), существенно влияет на ее характеристики. Примерами методов доступа являются:

6.4.1. Множественный доступ с разделением времени (TDMA)

Множественный доступ с разделением времени (Time Division Multiple Access (TDMA) — это множественный доступ, основанный на распределении времени работы канала между информационными системами.

Доступ TDMA основан на использовании специального устройства, именуемого тактовым генератором. Этот генератор делит время работы канала на повторяющиеся циклы. Каждый из циклов начинается сигналом - разграничителем. Цикл включает n пронумерованных временных интервалов, именуемых ячейками. Интервалы предоставляются для загрузки в них блоков данных.

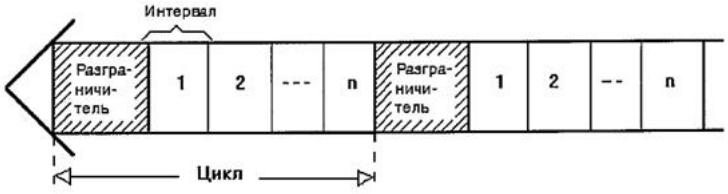


Рис. 6.7. Структура разделения времени

6.4.2. Множественный доступ с передачей полномочия (TPMA)

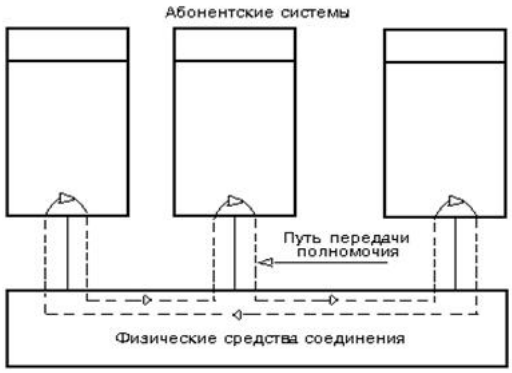


Рис. 6.8. Цикл движения полномочия

Множественный доступ с передачей полномочия (Token Passing Multiple Access (TPMA)) — это множественный доступ в моноканал либо циклическое кольцо при помощи полномочия. Сущность TPMA заключается в том, что абонентские системы передают по логическому кольцу (пунктир на рис.) друг другу особый блок данных, называемый полномочием либо жезлом. В передаче полномочия участвуют не все абонентские системы локальной сети, а только те, которые являются активными (желают начать передачу либо прием данных). Метод TPMA характеризуется двумя важными особенностями. Во-первых, он гарантирует определенное время доставки блоков данных абонентским системам. Во-вторых, он дает возможность предоставления различных приоритетов передачи данных. Вместе с этим, метод имеет немаловажный недостаток. Здесь, всегда есть возможность потери полномочия либо появления в сети нескольких полномочий. В обоих случаях сеть прекращает свою работу. В этой связи в сети создаются централизованный либо распределенный комплекс средств, задачей которого является восстановление потерянного полномочия и уничтожение всех, кроме одного из полномочий. Это значительно усложняет структуру сети.

6.4.3. Множественный доступ с контролем передачи и обнаружением столкновений (CSMA/CD и CSMA/CA)

Множественный доступ (*Carrier Sense Multiple Access with Collision Detection-* ***CSMA/CD)*** — это случайный метод множественного доступа в моноканал. Основан метод доступа на допущении состязаний абонентских систем за право вести передачу данных и организации выхода из этих состязаний. Сущность метода заключается в том, что каждая абонентская система следит за тем, какие сигналы появляются в моноканале. Данный метод характерен тем, что позволяет включать в локальную сеть новые абонентские системы и отключать из нее системы без изменения адресов и извещения остальных систем.

Рассматриваемый метод достаточно прост и надежен. Однако он не гарантирует времени доставки блоков данных. Поэтому, в последние годы появилась его модификация. CSMA/CA отличается от CSMA/CD тем, что коллизиям подвержены не пакеты данных, а только jam-сигналы. Отсюда и название «Collision Avoidance» — предотвращение коллизий (именно пакетов данных).

6.4.4. Множественный доступ с разделением частоты (FDMA)

Множественный доступ с разделением частоты (Frequency Division Multiple Access (FDMA)) — это множественный доступ, основанный на использовании в канале группы полос частот, образующих логические каналы. При использовании FDMA широкая полоса пропускания канала делится на ряд узких полос, разделенных защитными полосами. В каждой узкой полосе создается логический канал. Размеры узких полос могут быть различными. Передаваемые по этим каналам сигналы накладываются на разные несущие и поэтому в частотной области не должны пересекаться. Вместе с этим, иногда, несмотря на наличие защитных полос, спектральные составляющие сигнала могут выходить за границы логического канала и вызывать шум в соседнем логическом канале. Метод доступа FDMA относительно прост, но для его реализации необходимы передатчики и приемники, работающие на различных частотах.

6.4.5. Множественным доступом с разделением волны (WDMA)

Данный метод широко используется в оптических каналах. В нем разделение частоты осуществляется направлением в каждый из них лучей света с различными частотами. Благодаря этому пропускная способность физического канала увеличивается в несколько раз, и уже превысила 1 Тбит/с.

6.4.6. Сравнение методов доступа

Свойство или функция	**CSMA/CD**	**CSMA/CA**	**Доступ с передачей маркера**	**Доступ по приоритету запроса**
Тип связи	Широковещательный	Широковещательный	Передача маркера	Через концентратор
Тип доступа	Состязательный	Состязательный	Не состязательный	Состязательный
Тип сети	Ethernet	Local Talk®	Token Ring, ArcNet	100VG-AnyLAN

Контрольные вопросы:

1. Что такое аналоговая, коммуникационная и дискретная сеть?

2 Дайте классификацию коммуникационных подсетей.
3. Что такое моноканал?
4. Какие существуют методы доступа?
5. Назовите какие узлы существуют в ретрансляционных системах?
6. При каком методе доступа обе станции могут одновременно начать передачу и войти в конфликт?
7. В каких сетевых технологиях используется метод CSMA/CD?
8. Охарактеризовать метод доступа с передачей полномочия.
9. Охарактеризовать метод множественного доступа с разделением частоты.
10. Что такое метод доступа и как влияет метод доступа на передачу данных в сети?

Практические задания:

ЗАДАНИЕ № 6.1. Проверка проходимости сети в зависимости от загрузки канала и кол-ва абонентов сети.

Цели работы:
· закрепление основных показателей работы современной компьютерной сети;
· изучение влияния факторов загрузки и объёмов передаваемых пакетов на пропускную способность сети;
· закрепление принципов устранения коллизий и влияния коллизий на пропускную способность сети.

Задание на выполнение работы:

В ходе работы необходимо получить значения характеристик и объяснить некоторые особенности функционирования сети со случайным методом доступа.

Эти особенности хорошо иллюстрируются зависимостями эффективности работы сети от исходных данных. Вам необходимо получить по 10-15 значений исследуемого параметра и занести их в таблицу для дальнейшего построения графиков зависимостей. При этом значения величины влияющий на исследуемый параметр необходимо брать таким образом, чтобы он изменялся от своего минимально возможного значения до максимума. После этого необходимо объяснить полученные результаты. Используя значения указанные в вашем варианте необходимо исследовать следующие зависимости:

1. Зависимость эффективной загрузки моноканала $\rho_{эфф}$ от общей загрузки ρ. Общая загрузка определяется как сумма загрузок данными, служебной информацией и конфликтами.
2. Зависимость загрузки моноканала конфликтами от общей загрузки моноканала.
3. Зависимость загрузки моноканала от интенсивности абонентов.
4. Зависимость загрузки моноканала конфликтами от общей загрузки моноканала.
5. Зависимость загрузки моноканала от количества абонентов.
6. Зависимость загрузки моноканала от его пропускной способности.
7. Зависимость времени доставки сообщения от загрузки моноканала.
8. Зависимость времени доставки сообщения от вероятности конфликта.
9. Зависимость времени доставки от размера пакета информации.
10. Зависимость времени доставки от суммарной интенсивности абонентов.
11. Зависимость времени доставки от пропускной способности моноканала.
12. Зависимость вероятности возникновения конфликта от числа абонентов.
13. Зависимость вероятности возникновения конфликта от интенсивности абонентов.
14. Зависимость вероятности возникновения конфликта от времени восстановления.
15. Зависимость вероятности возникновения конфликта от общей загрузки.
16. Зависимость вероятности возникновения конфликта от длины информационной части пакета.

Отчет по проделанной работе.

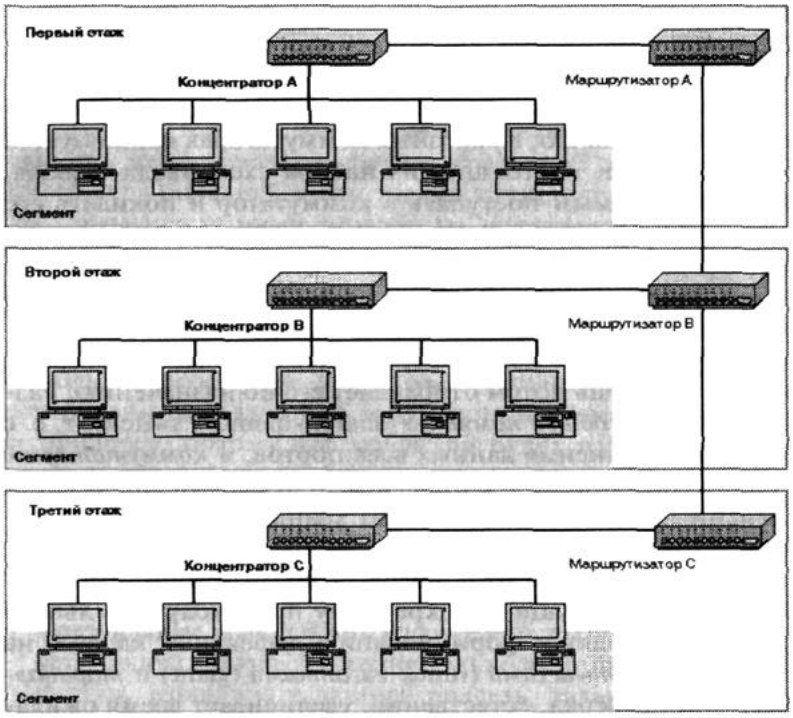
В данной работе исходные данные взяты произвольно. Далее по средствам программы «ЛВС» данные были обработаны и классифицированы в таблице excel, исходя из параметра зависимых элементов.

Таким образом были получены таблицы представленные в файле с практическим заданием. В дальнейшем для наглядности были созданы графики на основе данных таблиц.

ЗАДАНИЕ № 6.2. Механизм CSMA/CD/ Расположите следующие шаги процесса передачи данных CSMA/CD в правильном порядке.

1. Система начинает передачу данных.
2. Система повторяет передачу данных.
3. Система фиксирует признак коллизии.
4. Система делает паузу в передаче данных.
5. Система проверяет, свободна ли сеть.
6. Система прерывает передачу данных.
7. Система передает сигнал затора.
8. Система обнаруживает, что сеть свободна.

ЗАДАНИЕ № 6.3. Функции коммутатора. Изучите приведенную схему сети и укажите, какое устройство (или устройства) нужно заменить коммутаторами, чтобы с минимумом расходов добиться перечисленных результатов.



1. Какие устройства нужно заменить коммутаторами, чтобы сократить число коллизий в магистрали?
a. Концентратор А;
b. Маршрутизаторы А, В и С и Концентраторы А, В и С;
c. Концентраторы А, В и С;
d. Маршрутизаторы А, В и С.

2. Какие устройства нужно заменить коммутаторами, чтобы сократить трафик в сегменте на первом этаже?
a. Концентратор А;
b. Маршрутизатор А;
c. Маршрутизатор А и Концентратор А;
d. Маршрутизаторы А, В и С.

3. Какие устройства нужно заменить коммутаторами, чтобы объединить всю сеть в единый широковещательный домен?
a. Маршрутизатор В и Концентратор В;
b. Маршрутизаторы А, В и С;
c. Концентраторы А, В и С;
d. Маршрутизаторы А, В и С и Концентраторы А, В и С.

ЗАДАНИЕ № 6.4. Сегментирование сети. Представьте себе ЛВС Ethernet со скоростью передачи 10 Мбит/сек, которая объединяет 45 компьютеров с помощью 3 обычных концентраторов-повторителей. Трафик в сети слишком велик, что приводит к частым коллизиям и общему снижению производительности. Ответьте на следующие вопросы.

1. Что нужно сделать с сетью, чтобы снизить в ней трафик с минимальными затратами?
a. Разделить сеть на три ЛВС и соединить их аппаратно реализованными маршрутизаторами;
b. Заменить концентраторы коммутаторами;
c. Установить между двумя концентраторами прозрачный мост;
d. Повысить скорость сети до 100 Мбит/сек, установив сетевые платы и концентраторы Fast Ethernet.

2. Какое решение не увеличит полосу пропускания, доступную каждой рабочей станции?
a. Разделить сеть на три ЛВС и соединить их аппаратно реализованными маршрутизаторами;
b. Заменить концентраторы коммутаторами;
c. Установить между двумя концентраторами прозрачный мост;
d. Повысить скорость сети до 100 Мбит/сек, установив сетевые платы и концентраторы Fast Ethernet.

3. Что нужно сделать, чтобы в сети совершенно не использовалась общая сетевая среда?
a. Разделить сеть на три ЛВС и соединить их аппаратно реализованными маршрутизаторами;
b. Заменить концентраторы коммутаторами;
c. Установить между двумя концентраторами прозрачный мост;
d. Повысить скорость сети до 100 Мбит/сек, установив сетевы платы и концентраторы Fast Ethernet.

4. Как повысить производительность сети, не уменьшив количество коллизий?
a. Разделить сеть на три ЛВС и соединить их аппаратно реализованными маршрутизаторами;
b. Заменить концентраторы коммутаторами;
c. Установить между двумя концентраторами прозрачный мост;
d. Повысить скорость сети до 100 Мбит/сек, установив сетевые платы и концентраторы Fast Ethernet.

Перечень литературы и Интернет-ресурсов:

1. Автоматическая коммутация: Учебник для вузов / О.Н.Иванова, М.Ф.Копп, З.С.Коханова, Г.Б.Метельский; Под ред. О.Н.Ивановой. - М.: Радио и связь, 1988. - 624 с.: ил.

2. Вишневский В.М., Ляхов А.И., Портной С., Шахнович И.В. Широкополосные беспроводные сети передачи информации, М.: Техносфера, серия: Мир связи, 2005.

3. В.Г. Олифер, Н.А. Олифер. Компьютерные сети. Принципы, технологии, протоколы. (рекомендовано Мин. образования РФ). СПб: Питер, 2001,668 с.

4. Гоноровский И.С. Радиотехнические цепи и сигналы. Ч. I. – М.: Советское радио, 1966. – 440 с.

5. Дымарский Я.С., Крутякова Н.П., Яновский Г.Г. Управление сетями связи: принципы, протоколы, прикладные задачи. – М.: Мобильные коммуникации, 2003. – 384 с.

6. Зингеренко А.М., Баева Н.Н., Тверецкий М.С. Системы многоканальной связи. - М.: Связь, 1980. - 439 с.

7. Иммореев И.Я., Судаков А.А., Сверхширокополосная помехоустойчивая система скрытной связи с высокой скоростью передачи данных. - Труды Всероссийской научной конференции-семинара «Сверхширокополосные сигналы в радиолокации, связи и акустике» (СРСА`2003), Россия, Муром, Июль 2003.

8. Локальные сети на основе коммутаторов — http://www.citforum.ru/nets/lsok/contents.shtml

9. Многоканальная связь и РРЛ / Баева Н.Н., Бобровская И.К., Брескин В.А., Федорова Е.Л.: Учебник для вузов связи. - М.: Радио и связь, 1984. - 216 с., ил.

10. Основные сетевые приложения — http://www.citforum.ru/nets/articles/atm_2_000.shtml

11. Основы технологии ATM — http://www.citforum.ru/nets/articles/atm_base.shtml

12. Подсистема изучения циклических кодов — http://uiits.ruweb.net/systems/cod/lec_main.php

13. Пятибратов А.П., Гудыно Л.П. Вычислительные системы, сети и телекоммуникации. – М.: Финансы и статистика, 2001. – 512 с.

14. Роль коммуникационных протоколов и функциональное назначение основных типов оборудования корпоративных сетей. Н. Олифер, В. Олифер, ЦИТ — http://www.citforum.ru/nets/protocols/index.shtml

15. Справочник Novell Netware 4 С.Б. Орлов, по заказу ИИЦ "Попурри", 1994. — http://www.citforum.ru/operating_systems/nw4/index.shtml

16. Статическая IP-маршрутизация, Дмитрий Карпов — http://www.citforum.ru/nets/tcp/iproutng.shtml

17. Столлингс В. Современные компьютерные сети. – СПб.: Питер, 2003. – 783 с.

18. Шахнович И. В., Стандарт широкополосного доступа IEEE 802.16 для диапазона ниже 11 ГГц. ЭЛЕКТРОНИКА: наука, технология, бизнес, Россия, Москва, 2005, №1.

Тема 7. Циклические и узловые подсети

Цели:

- Изучить особенности передачи информации по циклической подсети.
- Рассмотреть особенности передачи информации по узловой подсети.
- Проанализировать типы локальных сетей по методам передачи информации.

7.1. Циклическое кольцо.

Циклическое кольцо – это кольцевой физический канал, обеспечивающий последовательную передачу сигналов группе систем. Циклическое кольцо является одним из типов сети с селекцией данных. Эта локальная сеть состоит из общего звена, блоков доступа и абонентских звеньев.

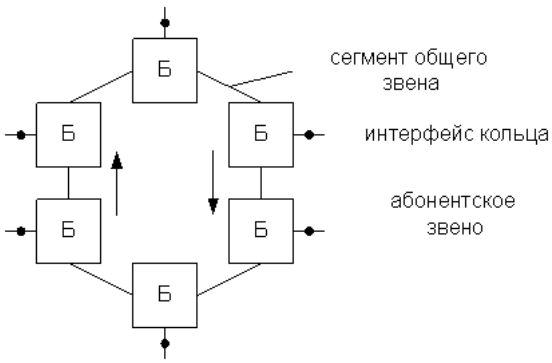


Рис. 7.1. Состав циклической сети

Общее звено блоками доступа делится на сегменты, создаваемые на основе витой пары, плоского коаксиального кабеля либо оптического канала. Блоки доступа (Б) при помощи абонентских звеньев соединяются с абонентскими системами. В базовой эталонной модели взаимодействия открытых систем кольцевой канал представляется физическими средствами соединения. Передача сигналов осуществляется в кольце в одном направлении: от одного блока доступа к другому. При этом, блок, передавший кадр, после того, как последний пройдет по всему кольцу, должен его уничтожить. Остальные блоки доступа транслируют передаваемый кадр. Блоки доступа анализируют проходящие через них кадры и принимают решение о необходимых формах взаимодействия с кольцом: снять копию кадра, передать его далее и т. д. Для этого, прежде всего, блок доступа читает адрес назначения кадра. Если он адресован данной системе, то она снимает для себя его копию и направляет ее своим прикладным процессам для обработки. В оригинале кадра, остающемся в кольце, блок доступа делает отметку о том, что кадр принят. Принятый адресатом кадр с отметкой должен по кольцу быть доставлен его отправителю. В противном случае отправитель пошлет кадр вторично. Вследствие этого, в кольце посланный кадр может быть передан только одному адресату. В кольце должна быть обеспечена синхронизация работы всех блоков доступа. Для этого осуществляется тактирование движения кадров. Один из блоков доступа объявляется главным. Взаимодействие систем в кольце обеспечивается множественным доступом с передачей полномочия. Благодаря этому, не допускается возможность того, что две либо более систем будут вести передачу данных, мешая друг другу. Общее звено кольца может состоять из одного кольцевого канала, с низкой надежностью. В случае обрыва канала либо его неисправности в любой точке звена прекращает работу вся сеть. Чтобы избежать этого применяют различные модификации циклического кольца.

1. Кольцо с переключающими концентраторами – кольцевая сеть, представленное в форме одной либо группы взаимосвязанных звезд.

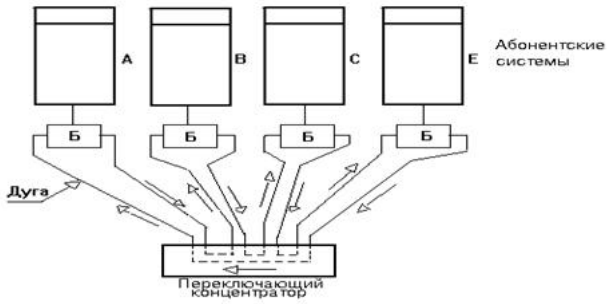


Рис. 7.2. Кольцо с переключающими концентраторами

Задачей переключающего концентратора является обеспечение надежности работы циклического кольца. Для этого концентратор соединяет дуги друг с другом таким образом, чтобы было создана в смысле топологии звездообразная сеть. В результате образуется единое кольцо, проходящее через все блоки доступа (Б). При появлении неисправности в дуге либо в абонентской системе концентратор отключает из кольца соответствующую дугу. Благодаря этому, остальная часть кольца продолжает нормальную работу. В зависимости от надобности в сети устанавливается один либо несколько концентраторов. Сложное кольцо может иметь не только несколько переключающих концентраторов, но также содержать ретрансляционные системы. Последние соединяют кольцо с другими коммуникационными сетями. Переключающий концентратор может быть как пассивным, так и активным. В первом случае концентратор содержит лишь электронные реле, выводящие дуги из кольца.

Активный концентратор, кроме этого, имеет логические элементы, способные обнаруживать и обходить возникающие неисправности.

2. Двойное кольцо – кольцевая сеть, образованная двумя кольцевыми каналами.

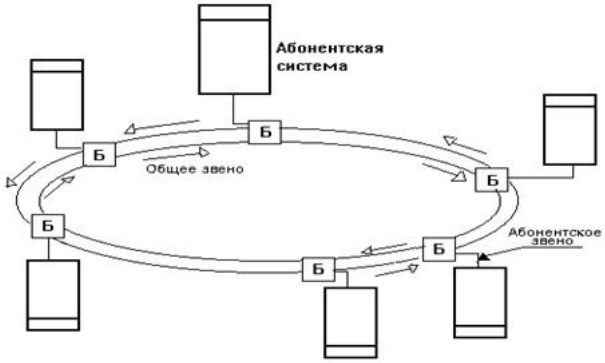


Рис. 7.3. Работа двойного кольца в нормальном режиме

Двойное кольцо состоит из двух общих звеньев, блоков доступа (Б) и абонентских звеньев. Оба общих звена проходят сквозь блоки доступа и в нормальном режиме работы работают параллельно, передавая сигналы в разные стороны. Абонентские системы и административные системы подключаются к обоим общим звеньям. При разрыве одного из общих звеньев, сигналы продолжают передаваться по другому общему звену. В тех случаях, когда происходит разрыв обоих общих звеньев, соответствующий их сегмент выходит из строя. В этом случае два общих звена превращаются в одно кольцо, а блоки доступа, примыкающие к сегменту разрыва, обеспечивают разворот сигналов и передачу их из одного разорванного общего звена в другое.

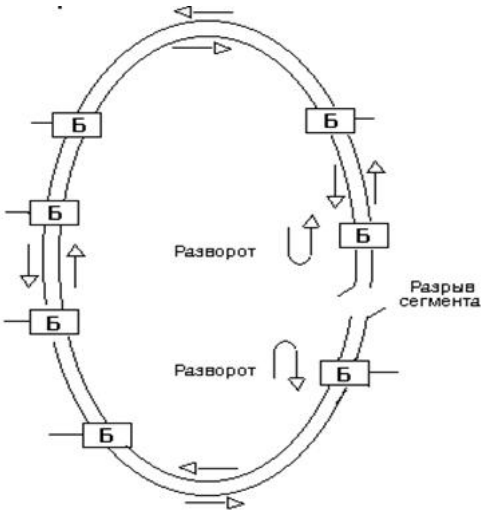


Рис. 7.4. Работа двойного кольца в случае разрыва обоих общих звеньев

Предложено несколько схем создания комплексных ассоциаций, в которых группы различных по типу подсетей соединяются между собой ассоциативными системами. На следующем рисунке показана схема, в которой четыре кольца и группа абонентских систем (А—З) соединены тремя моноканалами. Кроме того, кольца 1, 2 могут взаимодействовать друг с другом напрямую. В результате создается информационная сеть, опирающаяся на семь коммуникационных подсетей.

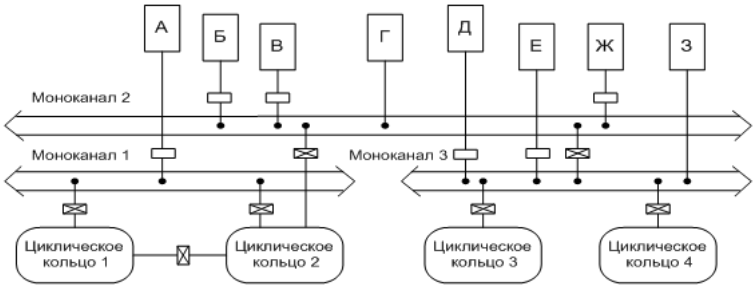


Рис. 7.5. Циклические кольца, соединенные группой моноканалов

7.2. Узловые коммуникационные подсети.

Узловые подсети коренным образом отличаются моноканальных и циклических. Последние имеют общие каналы, к которым подключаются все абонентские системы сети. Узловая подсеть содержит множество различных каналов, соединяемых узлами коммутации. На рис.8.6, где показана ее типовая структура, изображены четыре узла (1-4) коммутации, к которым походит большое число каналов. В зависимости от размера узла это число может изменяться от 3 до 10000. Все используемые каналы делятся на две группы: магистральные и абонентские. *Магистральным* является канал, соединяющий два узла. *Абонентский* канал связывает узел с абонентской системой. Кроме того, каналы, используемые в узловой подсети, подразделяются на аналоговые и дискретные. Аналоговые методы обработки и передачи данных уступают более надежным и экономичным дискретным, поэтому в новых узловых подсетях предпочтение отдается дискретным каналам. Обычно пользователи «не видят» магистральных каналов и даже не знают о их существовании. Пользователей интересуют абонентские каналы, поэтому пользователям предоставляются абонентские интерфейсы. Характеристики абонентских систем, подключаемых к узловой подсети, многообразны. Поэтому в точках их соединения с подсетью предусматривается не один, а несколько абонентских интерфейсов. Их число определяет «интеллектуальность» подсети. Практически подсеть имеет один интерфейс, поэтому в узлах несколько абонентских интерфейсов преобразуются в один главный. Основные функции узлов заключатся в коммутации передаваемых блоков информации и создании маршрутов между взаимодействующими абонентскими системами. Например, одним из маршрутов, связывающих на рис.8.6 абонентские системы *И, Г,* является тот, который показан стрелками. Чем больше различных маршрутов, связывающих пару систем, можно проложить в подсети, тем надежнее она работает. Каждый маршрут состоит из последовательности каналов узловой подсети. Кроме основных функций в узле коммутации осуществляется диагностика неисправностей части подсети и ведется статистика потоков блоков данных в окрестностях узла.

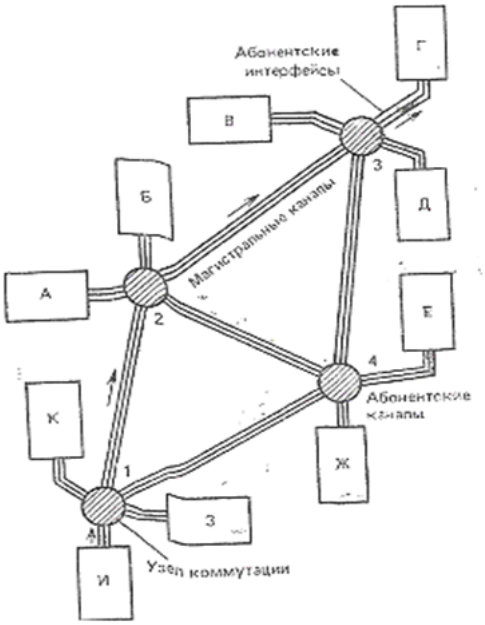


Рис. 7.6. Четырехузловая подсеть

Узловые коммуникационные подсети могут быть не только территориальными, но и локальными. Однако использование в локальной информационной сети большого числа узлов является непозволительной роскошью. Кроме того, здесь узлы должны быть в основном необслуживаемыми, т. е. работать без персонала, ибо в противном случае информационная сеть становится слишком дорогой. Чаще всего в узловой локальной сети устанавливается только один узел. В этом случае в коммуникационной подсети имеются только такие магистральные каналы, которые связывают рассматриваемую локальную сеть с другими локальными либо территориальными сетями. В одноузловой коммуникационной подсети абонентские каналы (1-8) располагают в виде звезды, лучи которой расходятся из точки, где установлен узел. По концам этих лучей устанавливаются абонентские системы и центр управления сетью. Напомним, что такую же форму имеет и учрежденческая телефонная сеть. В центре сети располагается телефонная станция, а по концам лучей звезды устанавливаются телефоны. Телефонная сеть обеспечивает телефонные разговоры, т. е. передачу речи. Если в этой сети заменить телефонную станцию узлом, а телефоны - информационными системами, то на базе тех же каналов можно создать одноузловую локальную информационную сеть. В этой сети будет возможна передача не только речи, но также данных и изображений (чертежей, рисунков, схем, фотографий и т. д.). Рассмотренная реконструкция сети обеспечивает перевод учреждения на современные формы обработки информации. Одноузловая информационная сеть имеет ряд положительных преимуществ. К ним относятся: низкая стоимость включения в сеть абонентских систем; возможность использования имеющихся каналов учрежденческой телефонной сети; применение необслуживаемых узлов; одновременная передача в сети данных, речи и изображений.

Наряду с этим **узловая сеть** имеет по сравнению с другими локальными сетями и ряд недостатков. К ним прежде всего относятся относительно небольшая скорость передачи информации и необходимость иметь значительное число каналов.

7.3. Типы локальных сетей по методам передачи информации.

7.3.1. Ethernet

Это метод доступа, разработанный фирмой Xerox в 1975 году, пользуется наибольшей популярностью. Он обеспечивает высокую скорость передачи данных и надежность.Для данного метода доступа используется топология "общая шина". Поэтому сообщение, отправляемое одной рабочей станцией, принимается одновременно всеми остальными, подключенными к общей шине. Та станция, которой предназначено сообщение, принимает его, остальные игнорируют.

Метод доступа Ethernet является методом множественного доступа с прослушиванием несущей и разрешением коллизий (конфликтов) (CSMA/CD - Carier Sense Multiple Access with Collision Detection).

Перед началом передачи рабочая станция определяет, свободен канал или занят. Если канал свободен, станция начинает передачу.

Ethernet не исключает возможности одновременной передачи сообщений двумя или несколькими станциями. Аппаратура автоматически распознает такие конфликты, называемые коллизиями. После обнаружения конфликта станции задерживают передачу на некоторое время. Это время небольшое и для каждой станции свое. После задержки передача возобновляется. Реально конфликты приводят к уменьшению быстродействия сети только в том случае, если работает порядка 80-100 станций.

7.3.2. Token Ring

Важнейшими стандартами, определяющими протоколы канального и физического уровня в сетях с кольцевой структурой с маркерным доступом, являются стандарты Token Ring фирмы IBM (наряду со стандартами IEEE 802.5, ISO 8802-5, ECMA-89). Все эти стандарты определяют физическую среду и уровень доступа к среде MAC. Стандарты Token Ring допускают использование в качестве среды экранированную витую пару и оптоволоконный кабель со скоростями передачи по ней от 1 до 4 Мб/с. Имеется модификация стандарта Token Ring со скоростью передачи данных 16 Мб/с на тех же средах. В качестве метода управления доступом станций к передающей среде используется метод - маркерное кольцо (англ. Token Ring). Основные положения этого метода:

- устройства подключаются к сети по топологии кольцо;
- все устройства, подключенные к сети, могут передавать данные, только получив разрешение на передачу (маркер);
- в любой момент времени только одна станция в сети обладает таким правом.

Типы пакетов.

В Token Ring существует три различных формата кадров, (основных типа пакетов):

- маркер, пакет «маркер» (англ. Token);
- кадр данных, пакет «управление/данные» (англ. Data/Command Frame);
- прерывающая последовательность, пакет «сброса» (англ. Abort).

7.3.3. Маркер

Кадр маркера состоит из трех полей, каждое длиной в один байт: поля начального ограничителя; поля контроля доступа; поля конечного ограничителя.

Поле начального ограничителя появляется в начале маркера, а также в начале любого кадра, проходящего по сети. Поле состоит из уникальной серии электрических импульсов, которые отличаются от тех импульсов, которыми кодируются единицы и нули в байтах данных. Поэтому начальный ограничитель нельзя спутать ни с какой битовой последовательностью.

Поле контроля доступа разделяется на четыре элемента данных:

PPP T M RRR,

где PPP - биты приоритета, T - бит маркера, M - бит монитора, RRR - резервные биты.

Каждый кадр или маркер имеет приоритет, устанавливаемый битами приоритета в значении от 0 до 7 (7 - наивысший приоритет). Станция может воспользоваться маркером, если только она получила маркер с приоритетом меньшим или равным, чем ее собственный. Сетевой адаптер станции, если ему не удалось захватить маркер, помещает свой приоритет в резервные биты маркера, но только в том случае, если записанный в резервных битах приоритет ниже его собственного. Эта станция будет иметь преимущественный доступ при последующем поступлении к ней маркера. Бит маркера имеет значение 0 для маркера и 1 для кадра. Бит монитора устанавливается в 1 активным монитором и в 0 любой другой станцией, передающей маркер или кадр. Если активный монитор видит маркер или кадр, содержащий бит монитора в 1, то активный монитор знает, что этот кадр или маркер уже однажды обошел кольцо и не был обработан станциями. Если это кадр, то он удаляется из кольца. Если это маркер, то активный монитор переписывает приоритет из резервных битов полученного маркера в поле приоритета. Поэтому при следующем проходе маркера по кольцу его захватит станция, имеющая наивысший приоритет.

Поле конечного ограничителя - последнее поле маркера. Так же, как и поле начального ограничителя, это поле содержит уникальную серию электрических импульсов, которые нельзя спутать с данными. Кроме отметки конца маркера это поле также содержит два подполя: бит промежуточного кадра и бит ошибки. Эти поля относятся больше к кадру данных, который мы и рассмотрим.

7.3.4. Кадр данных

Кадр данных состоит из нескольких групп полей: последовательность начала кадра; адрес получателя; адрес отправителя; данные; последовательность контроля кадра; последовательность конца кадра. Кадр данных может переносить данные либо для управления кольцом (данные MAC-уровня), либо пользовательские данные (LLC-уровня). Стандарт Token Ring определяет 6 типов управляющих кадров MAC-уровня. Поле "*последовательность контроля кадра*" определяет тип кадра (MAC или LLC) и, если он определен как MAC, то поле также указывает, какой из шести типов кадров представлен данным кадром. Назначение этих шести типов кадров следующее.

1. Чтобы удостовериться, что ее адрес уникальный, станция посылает кадр "Тест дублирования адреса", когда впервые присоединяется к кольцу.

2. Чтобы сообщить другим станциям, что он еще жив, активный монитор запускает кадр "Активный монитор существует" так часто, как только может.

3. Кадр "Существует резервный монитор" отправляется любой станцией, не являющейся активным монитором.

4. Резервный монитор отправляет "Маркеры заявки", когда подозревает, что активный монитор отказал. Резервные мониторы затем договариваются между собой, какой из них станет новым активным монитором.

5. Станция отправляет кадр "Сигнал" в случае возникновения серьезных сетевых проблем, таких как оборванный кабель, или при обнаружении станции, передающей кадры без ожидания маркера. Определяя, какая станция отправляет кадр сигнала, диагностирующая программа может локализовать проблему.

6. Кадр "Очистка" отправляется после того, как произошла инициализация кольца, и новый активный монитор заявляет о себе.

7.3.5. Прерывающая последовательность

Состоит из двух байтов, содержащих начальный ограничитель и конечный ограничитель. Прерывающая последовательность может появиться в любом месте потока битов и сигнализирует о том, что текущая передача кадра или маркера отменяется. Как видно из описания процедур обмена данными, в сети Token Ring на уровнях MAC и LLC применяются процедуры без установления связи, но с подтверждением получения кадров.

Стандарт Token Ring фирмы IBM предусматривает построение связей в сети с помощью концентраторов, называемых MAU, и мостов, упрощающих реконфигурацию сети и ее обслуживание. Сеть имеет комбинированную звездно-кольцевую конфигурацию, объединяющую несколько колец, работающих на скорости как 4 Мб/с, так и 16 Мб/с. Отдельные кольца взаимодействуют через высокоскоростные мосты (Рис.8.7). Адрес состоит из двух частей: первые два байта определяют адрес кольца, а следующие - станцию в кольце. Для обеспечения надежности связей в сети каждый сетевой адаптер и концентратор должен иметь обходные пути передачи сигналов, которые замыкаются при исчезновении питания сетевого адаптера или концентратора. Использование концентраторов приводит к топологии сети, аналогичной топологии стандартов 10BaseT и 10BaseF.

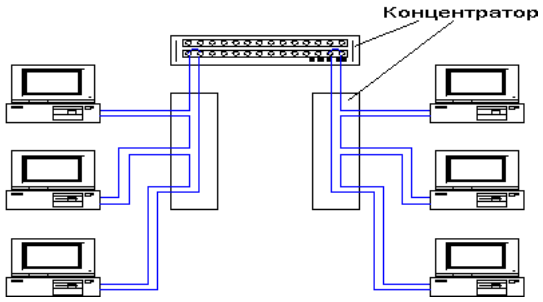


Рис. 7.7. Сеть Token Ring

7.3.6. FDDI

Высокоскоростной протокол FDDI (Fiber Distributed Data Interface) - оптоволоконный интерфейс распределенных данных - появился значительно позже, чем Ethernet и Token Ring. Проблемная группа X3T9.5 института ANSI разработала стандарт FDDI, который обеспечивает передачу кадров по двойному волоконно-оптическому кольцу со скоростью 100 Мб/с. Протокол специально разрабатывался, чтобы быть как можно больше похожим на стандарты Token Ring и IEEE 802.5 и отличаться от них только теми особенностями, которые необходимы для поддержки большей скорости и больших расстояний. В качестве передающей среды в FDDI используются:

- многомодовый оптоволоконный кабель, обеспечивающий расстояние до 2 км,
- одномодовый оптоволоконный кабель, расстояние между станциями зависит от марки кабеля и приемопередатчиков и равно 20-60 км,
- витая пара (подстандарт CDDI), расстояние между станциями - до 100 м.

Максимальная общая длина кольца FDDI составляет 100 километров, максимальное число станций в кольце - 500. Базовая топология FDDI - двойное кольцо, вторичное кольцо используется как резервное. Для обеспечения отказоустойчивости в стандарте FDDI предусмотрено создание двух оптоволоконных колец. При разрыве связей между двумя станциями в первичном кольце происходит использование связей вторичного кольца, причем передача информации во вторичном кольце происходит в обратном направлении. При отказе или отключении какой-либо станции, ее сетевой адаптер должен обеспечить обходной путь. В стандарте FDDI допускается использование двух видов подсоединения станций к кольцу. Станции класса A подключаются к первичному и вторичному кольцам и называются DAS - dual attached station. Станции класса B подключаются только к первичному, основному кольцу и называются SAS - single attached station. Обычно рабочая станция является узлом с одиночными связями, а концентратор - узлом с дуальными связями. В случае однократного обрыва кабеля можно предусмотреть автоматическую реконфигурацию кольца за счет переключения связей в концентраторе. Если вышла из строя или была выключена станция класса A, то кольцо FDDI может сохранить работоспособность путем использования обходных оптических переключателей. И, наконец, станции класса B можно подключать сразу к двум концентраторам, в результате чего образуется основная и резервная связи.

7.3.7. Отличия в управлении маркером

Существует два основных различия в том, как происходит управление маркером в протоколах FDDI и Token Ring:

- В Token Ring новый маркер начинает циркулировать только после возвращения отправленного кадра. В FDDI новый маркер начинает циркулировать непосредственно после передачи кадра отправляющей станцией. Таким образом, в кольце Token Ring в один момент времени присутствуют кадры только одной станции. В кольце FDDI в один и тот же момент времени передаются кадры различных станций, что повышает производительность кольца;
- Стандарт FDDI не использует приоритет кадра. Вместо этого FDDI использует сложный алгоритм для управления доступом к сети, основанный на таймерных интервалах.

В стандарте FDDI различаются асинхронные (обычные) пакеты и синхронные - пакеты multimedia, например, пакеты с кодами изображений, которые должны передаваться через строго фиксированные интервалы времени. Каждая станция кольца FDDI учитывает три различных таймерных интервала:

- TRT - интервал между двумя последовательными приходами маркера;
- T - фиксированный интервал, о котором станции договорились при инсталляции;
- THT - время удержания маркера - время, в течение которого станция может удерживать маркер и передавать свои пакеты.

Интервал THT вычисляется по формуле: THT = T - TRT, из которой видно, что чем дольше маркер совершает оборот, тем меньше станции остается времени на передачу своих пакетов. Если THT становится отрицательным, то станция не передает свои пакеты, а передает только маркер. Условие передачи пакета относится только к асинхронным пакетам. Синхронный пакет передается всегда. Структура кадра данных сети FDDI соответствует структуре кадра данных сети Token Ring, а структура маркера FDDI значительно отличается.

7.3.8. Особенности кодирования в FDDI

Для самосинхронизации приемника и передатчика в сетях передачи данных используются так называемые самосинхронизирующиеся коды, которые часто изменяют уровень сигнала. Это изменение уровня и синхронизирует приемник с передатчиком. Наиболее популярна так называемая манчестерская схема кодирования, при которой перепад потенциала происходит в каждом такте, единица кодируется перепадом от низкого уровня к высокому, а нуль - наоборот. Использование манчестерского кода приводит к удвоению частоты передаваемого сигнала, то есть для передачи данных со скоростью 10 Мб/с нужно менять потенциал со средней скоростью 20 Мгц. Если бы FDDI использовал ту же манчестерскую схему кодирования битов, что и применяемая в Token Ring, то каждый бит потребовал бы двух оптических сигналов: импульс света, а затем пауза темноты. Это означает, что FDDI потребовалось бы посылать 200 миллионов сигналов в секунду, чтобы передавать данные со скоростью 100 Мб/с. Вместо этого, схема 4B/5B, используемая в FDDI, кодирует 4 бита данных в 5 битов для передачи так, чтобы на каждые четыре единицы в последовательности передаваемых бит всегда приходился один ноль, который и обеспечивает самосинхронизацию. При скорости передачи 100 Мб/с, схема 4B/5B в действительности отправляет 125 миллионов сигналов в секунду. Кроме того, так как каждый тщательно подобранный символ светового представления представляет 4 бита (полубайт), то оборудование FDDI может оперировать на уровне байтов и полубайтов, а не на уровне битов, что несколько упрощает достижение высокой скорости передачи данных.

7.3.9. 100 VG-Any-LAN

В качестве альтернативы 100Base-T фирмы AT&T и HP выдвинули проект 100BaseVG, изменяющий уровень MAC, но сохраняющий размер пакета. В сентябре 1993 года фирмы IBM и HP образовали комитет IEEE 802.12 и предложили использовать эту технологию для повышения скорости в сети Token Ring. Эта технология была названа 100VG-AnyLAN. В ней определены новый метод доступа Demand Priority и новая схема квартетного кодирования Quartet Coding - самосинхронизирующийся код 5B6B. 100VG-AnyLAN поддерживает передачу данных по четырем неэкранированным витым парам категорий 3, 4, 5. Данные передаются одновременно по четырем парам со скоростью 25 Мб/с, что в сумме дает 100 Мб/с. Сеть 100VG-AnyLAN состоит из центрального коммутирующего концентратора, называемого также корневым, и соединенных с ним конечных узлов и других концентраторов. Допускаются три уровня каскадирования. Каждый концентратор 100VG-AnyLAN должен быть настроен либо на работу с кадрами Ethernet, либо Token Ring, причем все концентраторы в сети должны быть настроены на один и тот же тип кадра. Специальное программное обеспечение концентратора 100VGAnyLAN позволяет установить мост с низкоскоростной сетью Ethernet или Token Ring в зависимости от типа высокоскоростной сети. Фирмы IBM и HP объявили, что идет разработка метода, позволяющего обрабатывать в одном устройстве кадры обоих типов одновременно. Рисунок 8.11 иллюстрирует работу протокола Demand Priority. Согласно этому методу, концентратор циклически выполняет опрос портов. Станция, желающая передать пакет, посылает низкочастотный сигнал концентратору, запрашивая низкий приоритет для обычных данных и высокий приоритет для данных, чувствительных к временным задержкам (например, мультимедиа). Приоритеты запросов имеют статическую и динамическую составляющие. Если сеть свободна, концентратор разрешает передачу пакета. После анализа адреса получателя в принятом пакете концентратор автоматически отправляет пакет станции назначения. Если сеть занята, концентратор ставит полученный запрос в очередь, которая обрабатывается в соответствии с порядком поступления запросов и с учетом приоритетов. Если к порту подключен другой концентратор, то опрос приостанавливается до завершения опроса концентратором нижнего уровня.

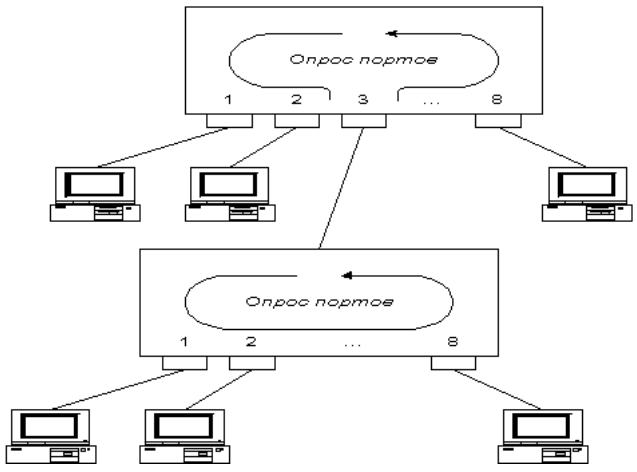


Рис. 7.8. Протокол Demand Priority стандарта 100VG-AnyLAN

Важная особенность метода Demand Priority - сохранение форматов кадров Ethernet и Token Ring. Сторонники 100VG-AnyLAN утверждают, что этот подход облегчит межсетевое взаимодействие через мосты и маршрутизаторы, а также обеспечит совместимость с существующими средствами сетевого управления, в частности с анализаторами протоколов. Основное применение технология 100VG-AnyLAN скорее всего найдет в сетях Token Ring, пользователям которых она позволит в 6-25 раз увеличить производительность сети, а также в сетях, активно использующих приложения мультимедиа.

7.3.10. ArcNet

ArcNet (англ. Attached Resource Computer Network) - простая, недорогая, надежная и достаточно гибкая архитектура локальной сети. Разработана корпорацией Datapoint в 1977 году. Впоследствии лицензию на ArcNet приобрела корпорация SMC (англ. Standard Microsystems Corporation), которая стала основным разработчиком и производителем оборудования для сетей ArcNet. В качестве передающей среды используются витая пара, коаксиальный кабель (RG-62) с волновым сопротивлением 93 Ом и оптоволоконный кабель. Скорость передачи данных - 2,5 Мбит/с, существует также расширенная версия - ArcNetplus - поддерживает передачу данных со скоростью 20 Мбит/с. При подключении устройств в ArcNet применяют топологии шина и звезда. Метод управления доступом станций к передающей среде - маркерная шина (англ. Token Bus). Этот метод предусматривает следующие правила:

- Все устройства, подключенные к сети, могут передавать данные только получив разрешение на передачу (маркер);
- В любой момент времени только одна станция в сети обладает таким правом;
- Данные, передаваемые одной станцией, доступны всем станциям сети.

Контрольные вопросы:

1. Какую топологию имеют сети: Token Ring, FDDI, состоящие из станций двойного подключения, FDDI, состоящие из станций одинарного подключения, сети 100VGanyLAN, ArcNet, Ethernet с точки зрения соединения узлов сети?
2. Какую топологию имеют сети: Token Ring, FDDI, состоящие из станций двойного подключения, FDDI, состоящие из станций одинарного подключения, сети 100VGanyLAN, ArcNet, Ethernet с точки зрения передачи сигналов?
3. Какую топологию имеют сети Token Ring, FDDI, 100VGanyLAN, ArcNet, Ethernet с точки зрения управления доступом к моноканалу?
4. Какой вид кабеля является типичным для построения сети Token Ring, FDDI, 100VGanyLAN, ArcNet?
5. Сколько уровней приоритета предусмотрено в сети: Token Ring, 100VGanyLAN, ArcNet, Ethernet?
6. Что такое маркер? Назовите отличия в управлении маркером. Какие сети используют маркер?
7. Что такое узловые коммуникационные подсети?
8. Что такое циклическое кольцо?
9. Назовите особенности работы циклических подсетей.
10. Перечислите типы локальных сетей по методам передачи информации.

Практические задания:

ЗАДАНИЕ № 7.1. Основы FDDI.

Подберите для сокращения в левой колонке соответствующее описание в правой.

Сокращение	Описание
1. DAS	a. Вариант FDDI для медного кабеля.
2. DAC	b. Компьютер, подключенный к сети FDDI с помощью топологии ≪звезда ≫.
3. SAS	c. Кадр FDDI, отвечающий за организацию работы кольца.
4. CDDI	d. Концентратор в сети FDDI с топологией ≪звезда≫.
5. SMT	e. Компьютер, подключенный к обоим кольцам двойного кольца.

ЗАДАНИЕ № 7.2. Выбор протокола канального уровня.

Для каждого из описанных случаев укажите наиболее подходящий протокол канального уровня (Ethernet или Token Ring) и объясните свой выбор. Поскольку в некоторых ситуациях приемлемы оба протокола, на Вашу оценку повлияет не столько выбранный протокол, сколько приведенные в его пользу доводы.

1. Два домашних компьютера нужно соединить в сеть для совместного использования принтера и подключения к Интернету.
2. Небольшая дизайнерская фирма хочет объединить 10 компьютеров в сеть, чтобы передавать с компьютера на компьютер и на сервер печати очень большие графические файлы.
3. В компании для ввода информации о заказах используется ЛВС из 50 компьютеров. Компания собирается выходить на внешний рынок и ожидает значительного роста в ближайшие несколько лет.

ЗАДАНИЕ № 7.3. Стандарты и технологии IEEE.

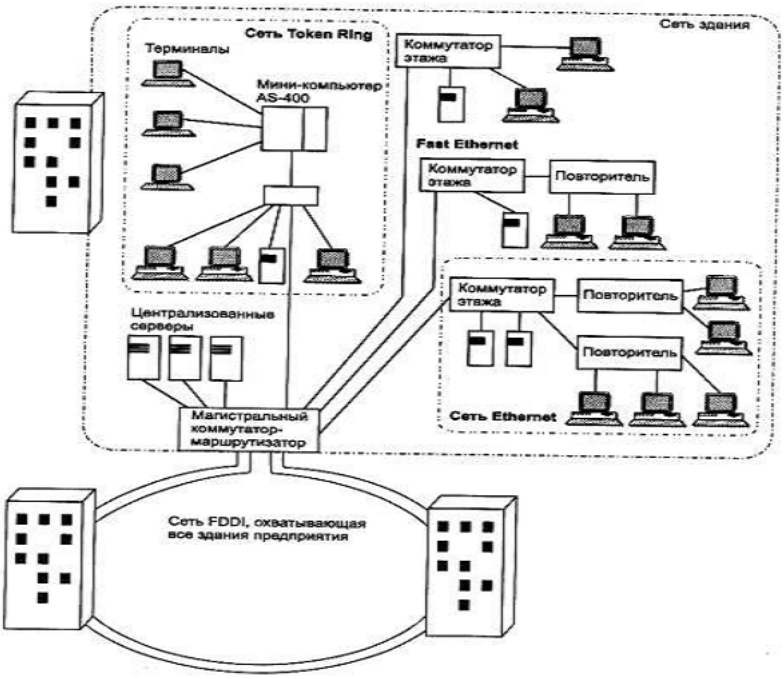
Для стандарта в левой колонке найдите наиболее подходящую технологию в правой.

Стандарт	Технология
1. IEEE 802.2	a. Gigabit Ethernet
2. IEEE 802.3	b. Fast Ethernet
3. IEEE 802.3u	c. Thick Ethernet

4. IEEE 802.3z .	d. Logical Link Control
5. IEEE 802.3ab .	e. lOBaseT
6. IEEE 802.5	f. Thin Ethernet
7. DIX Ethernet	g. lOOOBaseT
8. DIX Ethernet II	h. Token Ring

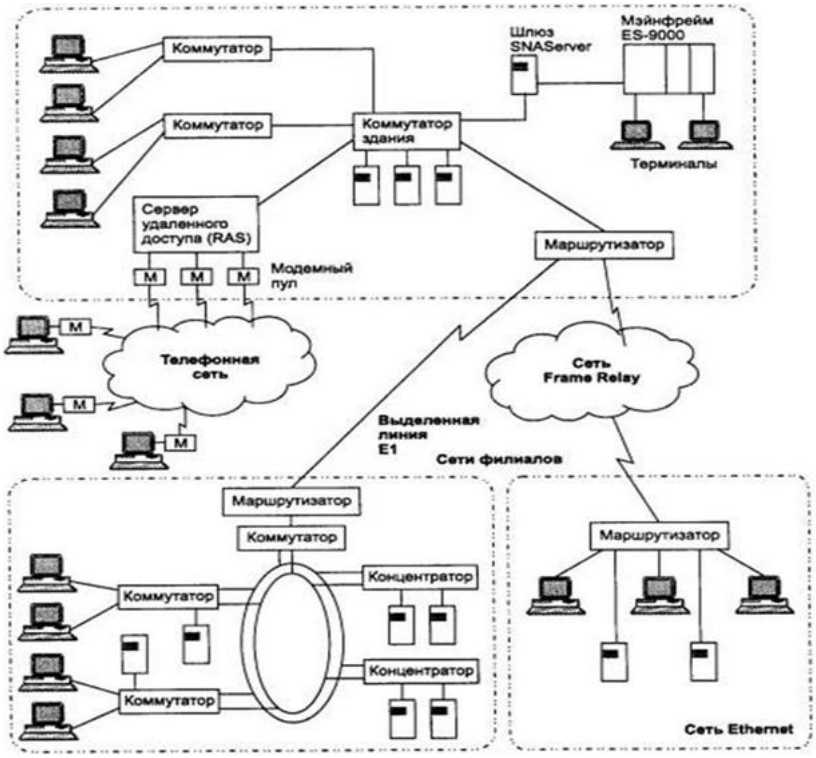
ЗАДАНИЕ № 7.4. Разработка разнородных сетей.

Разработать информационную сеть кампуса состоящую из разнородных сетей: FDDI, Token Ring, сеть здания построенная на сети Ethernet и Fast Ethernet.



ЗАДАНИЕ № 7.5. Разработка ретрансляционной сети.

Разработать структурную схему ретрансляционной системы (на коммутаторах, маршрутизаторах, концентраторах) состоящую из разнородных сетей: Ethernet и Frame Raley.



Перечень литературы и Интернет-ресурсов:

1. Бройдо В.Л. Вычислительные системы, сети и телекоммуникации: Учебник для вузов. 2-е изд. – СПб.: Питер, 2005. – 703 с.: ил.

2. Кульгин М. Практика построения компьютерных сетей. Для профессионалов. – СПб.: Питер, 2001. – 320 с.
3. Кульгин М. Технологии корпоративных сетей. Энциклопедия. — СПб.: Изд-во «Питер», 1999.
4. Учебник по компьютерным сетям. Сетям — http://kompset.narod.ru/siteunior.html
5. Олифер В.Г., Олифер Н.А. "Введение в IP-сети" — http://lemoi-www.dvgu.ru/lect/protoc/tcpip/networks/contents.htm
6. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. - СПб.: Издательство "Питер", 2000. - 672 с.
7. Олифер В.Г., Олифер Н.А. Новые технологии и оборудование IP-сетей. - СПб.: БХВ - Санкт-Петербург, 2000. - 512 с.
8. Основы построения объединенных сетей — http://www.citforum.ru/nets/ito/index.shtml
9. Пятибратов А.П. и др. Вычислительные системы, сети и телекоммуникации: Учебник/ Под редакцией А.П. Пятибратова. – М.: Финансы и статистика, 2001. – 512 с.
10. Telecommunication technologies - телекоммуникационные технологии — http://www.opennet.ru/docs/RUS/inet_book/
11. Технология LAN Emulation для согласования сетей ATM и традиционных сетевых технологий — http://www.citforum.ru/nets/tpns/glava_8.shtml

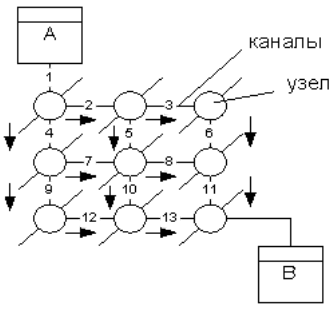
Тема 8. Методы маршрутизации и коммутации информационных потоков

Цели:

· Изучить различные методы маршрутизации и коммутации.
· Сравнить преимущества и недостатки коммутации: каналов, сообщений, пакетов.
· Получить представление о матричном коммутаторе и баньяновой сети систем.

8.1. Методы маршрутизации.

Маршрутизация – это процесс определения в коммуникационной сети пути, по которому вызов либо блок данных может достигнуть адресата. Маршрутом в информационной сети именуют путь, по которому осуществляется передача данных из одного порта в другой. Наиболее удобной формой представления маршрута является граф. Маршрутизация обеспечивает преобразование адреса объекта назначения в перечень каналов, по которым этот блок следует к адресату. Маршрутизация является распределенным процессом и выполняется всеми узлами коммутации сети с маршрутизацией данных. Для этого каждый узел определяет канал, по которому необходимо направить вызов либо блок данных. Выполняя такие действия, в каждом узле обеспечивается передача вызова либо блока данных от системы-отправителя к системе-адресату, по оптимальному маршруту. Последний изменяется в зависимости от выхода из строя отдельных каналов, их загрузки и протяженности.



На рисунке стрелками показаны возможные направления передачи данных через коммуникационную сеть от абонентской системы А до абонентской системы В. При коммутации каналов прокладка маршрута через коммуникационную сеть осуществляется только в момент начала сеанса взаимодействия абонентских систем. Для этой цели система-инициатор сеанса передает через сеть вызов. Он проходит через узлы коммутации, каждый из которых вносит свою лепту в маршрутизацию. В результате создается последовательность каналов, соединяющих две взаимодействующие в течении сеанса системы. При осуществлении коммутации пакетов маршрутизация происходит в течение всего сеанса взаимодействия. Через сеть не передается сигнальная информация и не создается постоянная (на все время сеанса) последовательность каналов. Здесь узлы коммутации осуществляют маршрутизацию блоков данных по адресам их назначения.

В сетях используются различные методы маршрутизации: ***Селективная маршрутизация*** характеризуется тем, что блоки данных посылаются сразу по нескольким направлениям, исходя из того, что они достигнут адресата. Пример — лавинный алгоритм: основан на рассылке копий пакета по всем направлениям. Пакеты сбрасываются, если в данном узле копия уже проходила. Лавинный алгоритм обеспечивает надёжную доставку, но порождает значительный трафик, поэтому используется для передачи пакетов большой ценности. ***Вероятностная маршрутизация*** предполагает случайный выбор пути блоков данных, при этом считается, что они обязательно достигнут адресата. ***Фиксированная (статическая) маршрутизация*** предусматривает составление таблиц маршрутов, указывающих наиболее эффективные пути предполагаемого трафика сети. Здесь маршрут выбирается заранее и не зависит от состояния сети. ***Адаптивная маршрутизация*** отличается от фиксированной тем, что таблицы маршрутов обновляются в зависимости от колебаний трафика. Пример — алгоритм «кратчайшей очереди»: пакет посылается по направлению, в котором наименьшая очередь в данном узле.

Блоки данных не всегда прибывают в пункты назначения в том же порядке, в котором отправляются. Это происходит по следующим причинам: различные время и расстояние при передаче блоков, связанное с использованием разных маршрутов коммуникационной сети; потеря блоков в сети и повторная их передача; блуждание блоков по сети, в результате чего блоки передаются повторно. В результате для того, чтобы восстанавливать сообщение, передаваемое последовательностями блоков, последнее необходимо обрабатывать в пунктах назначения. Составление таблицы маршрутов для фиксированной (статической) маршрутизации осуществляется администрацией сети при проектировании или модификации сети. Такой принцип маршрутизации во многих случаях может оказаться неэффективным, т.к. на сети могут оказаться повреждения или перегрузки. Целесообразно корректировать план распределения информации в зависимости от текущей топологии сети, длин очередей в узлах коммутации, интенсивности входных потоков и т.д. Цель маршрутизации – доставка пакетов по назначению с максимальной эффективностью. Эффективность выражена взвешенной суммой времени доставки сообщений при ограничении снизу на вероятность доставки. Алгоритмы маршрутизации включают процедуры: измерение и оценивание параметров сети; принятие решения о рассылке служебной информации; расчёт таблиц маршрутизации; реализация принятых маршрутных решений. В зависимости от того, используется при выборе направления информация о состоянии только данного узла или всей сети, различают алгоритмы изолированные и глобальные. Простейший алгоритм – это изолированный статический. В алгоритмах маршрутизации используется много различных показателей. Сложные алгоритмы маршрутизации при выборе маршрута
могут базироваться на множестве показателей, комбинируя их таким образом, что в результате получается один отдельный (гибридный) показатель. Показатели, которые используются в алгоритмах маршрутизации: длина маршрута; надежность; задержка; ширина полосы пропускания; нагрузка; стоимость связи

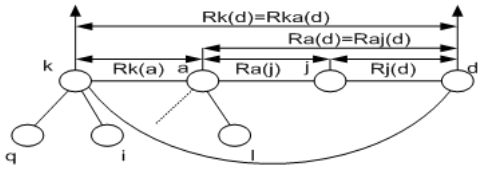
Алгоритм Дийкстры и протокол OSPF (Open Shortest Path First – "первоочередность наикратчайшего маршрута") направляет потоки маршрутной информации во все узлы объединенной сети. Однако каждый маршрутизатор посылает только ту часть таблицы маршрутизации, которая описывает состояние его собственных каналов.

Алгоритм Беллмана-Форда и протокол RIP (Routing Information Protocol) требует от каждого маршрутизатора посылки всей или части своей таблицы маршрутизации, но только своим соседям. По сравнению с алгоритмами состояния канала, которые

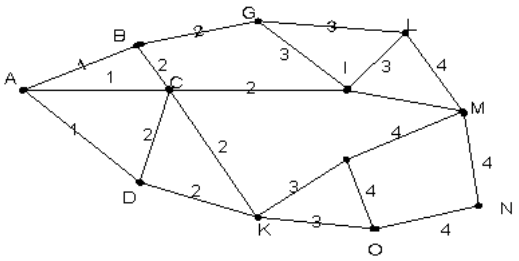
направляют небольшие корректировки по всем направлениям, алгоритмы вектора расстояний отсылают более крупные корректировки только в соседние маршрутизаторы.

8.1.1. RIP (Метод рельефов)

Рельеф – это оценка кратчайшего пути от узла A до узла B. Оценка (расстояние) может выражаться временем доставки, надёжностью доставки или числом узлов коммутации на данном маршруте. В таблице маршрутизации узла A каждому из основных узлов отводится одна строка со следующей информацией: узел назначения, длина кратчайшего пути, номер N ближайшего узла, соответствующего кратчайшему пути, список рельефов от A до B через каждый из смежных узлов. Например, для узла a строка для d выглядит так (зная, что из узла a можно попасть в узел d через узлы j и k): пункт назначения – d; длина кратчайшего пути Ra(d); номер ближайшего узла N(d)=j; список рельефов: Raj(d), Rak(d). Пусть изменилась задержка Rak(d) так, что она стала меньше, чем Raj(d). Тогда в строке d таблицы маршрутизации узла a корректируется Ra(d), N(d) изменяется на k, и кроме того всем соседям узла a посылается сообщение об изменённом Ra(d). Например, в некотором соседнем узле *l* при этом будет изменено значение R*l*a(d)=Ra(d)+R*l*(a). Мы видим, что возникает итерационный процесс корректировки маршрута информации в узлах коммутации. Хотя данный алгоритм сходится медленно, для относительно небольших сетей он вполне приемлем.



Возможен упрощенный вариант формирования рельефов. Он заключается в следующем: пусть i – это произвольный узел коммутации сети связи. i-рельефом называется процедура присвоения значений числовой функции каждой линии связи. Он строится следующим образом: из i-ого узла коммутации по всем исходящим линиям связи передается число «1». Все узлы коммутации, в которые поступило число 1, передают по всем исходящим линиям связи, кроме тех, по которым поступила 1, число 2. Далее узлы коммутации, по которым поступило число 2, передают 3, и т.д. до тех пор, пока все линии связи не будут пронумерованы. Говорят, что линия связи имеет n высоту, если она обозначена числом n в i-рельефе. Указанным способом формируется рельеф из каждого узла коммутации сети связи. В результате линия связи с минимальной высотой является исходящей линией связи первого выбора. Линии связи с большими высотами соответственно являются линиями связи 2, 3, и т.д. выбора.



Чтобы найти кратчайший маршрут коммутации к узлу A, достаточно в каждом узле коммутации выбирать линию связи с меньшим весом. Например, кратчайший маршрут от N до A будет следующий:

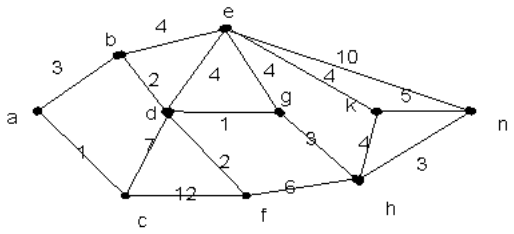
$$\mu^1_{NA} = \{NO;OK;KD;DA\}$$
$$\mu^2_{NA} = \{NM;MI;IC;CA\}$$
$$\mu^3_{NA} = \{NO;OK;KC;CA\}$$

Протокол RIP (Routing Information Protocol, RFC 1058, 1581, 1582, 1724) часто используется для класса протоколов маршрутизации, базирующихся на протоколах XNS (Xerox Network System — сетевая система Xerox) фирмы Xerox. Реализация протокола RIP для семейства протоколов TCP/IP широко доступна, поскольку входит в состав программного обеспечения ОС UNIX, например, FreeBSD или Linux. В силу своей простоты протокол RIP имеет наибольшие шансы превратиться в **«открытый»** протокол IGP, т.е. протокол, который может использоваться для совместной работы шлюзов, поставляемых разными фирмами. В качестве метрики маршрутизации RIP использует число скачков (шагов) до цели. Такой вид метрики не учитывает различий в пропускной способности или загруженности отдельных сегментов сети. Каждому маршруту ставится в соответствие таймер **тайм-аута** и **«сборщик мусора».** Таймер тайм-аута сбрасывается каждый раз, когда маршрут инициализируется или корректируется. Если со времени последней коррекции прошло 3 минуты или получено сообщение в том, что вектор расстояния равен 16, маршрут считается закрытым, но запись о нём не стирается, пока не истечёт время «уборки мусора» (2 минуты). При появлении эквивалентного маршрута переключение на него не происходит.

Протокол RIP достаточно простой, но не лишённый недостатков: требуется много времени для восстановления связи после сбоя в маршрутизаторе (минуты); в процессе установления режима возможны циклы; число шагов — важный, но не единственный параметр маршрута, да и 15 шагов — не предел для современных сетей.

8.1.2. Метод OSPF

Он основан на использовании в каждом маршрутизаторе информации о состоянии всей сети. Рассмотрим алгоритм применительно к формированию маршрутной таблицы узла A графа, изображенного на рисунке:



Обозначим кратчайшее расстояние от а к i через Ri. Разделим узлы на 3 группы: перманентные, для которых Ri уже рассчитано; пробные, для которых получена некоторая промежуточная оценка, возможно, неокончательная; пассивные, еще не вовлеченные в итерационный процесс. Итерационный процесс начинается с отнесения узла а к группе перманентных. Далее определяются узлы, смежные с узлом а. Это узлы b и c, которые включаются в группу пробных. Включение в группу пробных отмечается указанием в клетке таблицы, рядом с оценкой, расстояния также имени узла, включаемого в этом шаге в число перманентных. На следующем шаге узел с минимальной оценкой (c) включается в группу перманентных, а узлы, смежные с ним, в группу пробных, и для них оцениваются расстояния Rd=8 и Rf=13. Теперь среди пробных узлов минимальную оценку имеет узел b. Он включается в группу перманентных узлов, узел e в группу пробных, и для всех пробных узлов, смежных с b, рассчитываются оценки. Это, в частности, приводит к уменьшению оценки узла d с 8 на 5. В таблице это отражено, во-первых подчеркиванием, а во-вторых заменой у узла d метки с на b.Если же новая оценка оказывается больше прежней, то она игнорируется. Этот процесс продолжается пока все узлы не окажутся в группе перманентных. Теперь виден кратчайший путь от а к любому другому узлу x, или что тоже самое – от x к a. Это последовательность конечных отметок в строках таблицы, начиная с последнего узла x. Так для узла x=n, имея в строке n отметку h, в строке h отметку g, и окончательно кратчайший путь есть: a-b-d-g-h-n.

№ итерации	1	2	3	4	5	6	7	8	9
b	3,a	3							
c	1,a								
d		8,c	**5,b**						
e			7,b	7	7				
f		13,c	13	**7,d**	7	7			
g				6,d					
h					9,g	9	9		
k						11,e	11	11	
n						17,e	17	**12,h**	12

Протокол OSPF (Open Shortest Path First, RFC 1850, 1583, 1584, 1587) представляет собой протокол состояния маршрута, причём в качестве метрики используется коэффициент качества обслуживания. Каждый маршрутизатор обладает полной информацией о состоянии всех интерфейсов шлюзов автономной системы. Определяющими являются три характеристики: задержка, пропускная способность и надёжность.

Преимущества OSPF: для каждого адреса может быть несколько маршрутных таблиц, по одной на каждый вид IP-операции; каждому интерфейсу присваивается безразмерная цена, учитывающая пропускную способность, время транспортировки сообщения; каждой IP-операции может быть присвоена своя цена; при существовании эквивалентных маршрутов OSFP распределяет поток равномерно по этим маршрутам; при связи «точка–точка» не требуется IP-адрес для каждого из концов; применяется мультикастинг вместо широковещательной адресации, что снижает загрузку не вовлечённых в обмен сегментов.

Недостатки OSPF — трудно получить информацию о предпочтительности каналов для узлов, поддерживающих другие протоколы или имеющих статическую маршрутизацию.

8.2. Методы коммутации информации.

Под коммутацией данных понимается их передача, при которой канал передачи данных может использоваться попеременно для обмена информацией между различными пунктами информационной сети. Коммутация основана на использовании маршрутизации, определяющей путь, по которому в соответствии с адресом назначения передаются данные. Коммутация является основой технологии сети с маршрутизацией данных. В зависимости от задач, поставленных перед коммуникационной сетью, используют несколько методов коммутации (рис.9.1). Каждый из них определяется различными штабелями уровней области Взаимодействия Открытых Систем (ВОС). Осуществляется коммутация функциональными блоками всех систем информационной сети. У каждого из методов коммутации имеется своя область применения, обусловленная его особенностями. Выбор методов коммутации - достаточно сложная оптимизационная задача.

8.1.3. Коммутация Блоков (КБ), Каналов (КК), Пакетов (КП), сообщений

Коммутация сообщений **—** обеспечивает передачу через сеть сообщений с промежуточной их сборкой, хранением и разборкой в узлах коммутации. Здесь N=7 и каждый узел принимает по частям сообщение, собирает его, записывает в память, проверяет наличие ошибок в сообщении и лишь затем передает его (разбирая на части) следующему узлу. Необходимость в большой памяти и относительно медленная передача данных привели к тому, что коммутация сообщений в большинстве сетей заменена другими видами коммутации. Коммутация пакетов и сообщений, в отличие от коммутации каналов, являются коммутацией с запоминанием. В ***коммутации блоков данных*** участвуют N нижних уровней взаимодействующих друг с другом абонентских или административных систем, а также расположенных между ними ретрансляционных систем. В зависимости от метода коммутации, число уровней N изменяется от одного до семи. ***Коммутация Пакетов (КП)*** **—** коммутация, обеспечивающая передачу через сеть пакетов без монопольного использования каналов. Пары каналов на время сеанса в единое целое не соединяются. Здесь сообщения не собираются и не разбираются, N = 3, а коммутация осуществляется сетевыми процессами, опирающимися на функции физического, канального уровня и сетевого уровня. Характерной особенностью, отличающей коммутацию пакетов от коммутации каналов, являются коммутация с запоминанием и коллективное использование каналов коммуникационной сети. Пакеты по одному и тому же каналу идут, по мере их поступления, не зависимо от их источников и адресатов. Для повышения надежности работы коммуникационной сети в ней топология размещения узлов коммутации пакетов и соединяющих их каналов строится исходя из того, что между парами взаимодействующих систем создается несколько путей передачи пакетов. Пакеты узлами коммутации направляются по тем последовательностям каналов, которые, в конце концов, позволят достичь абонентской системы-адресата. Здесь, в отличие от коммутации каналов, коммутация пакетов происходит в течение всего сеанса взаимодействия систем (а не только в начале этого сеанса). В результате того, что пакеты идут по различным направлениям (последовательностям каналов), они могут приходить в пункт назначения с разным запаздыванием. Кроме этого, после прохождения через какие-нибудь каналы в пакетах могут возникнуть ошибки, из-за чего пакеты уничтожаются и передаются вновь. Все это приводит к тому, что все пакеты, посланные системой, не могут быть доставлены с одинаковым временем прохождения через коммуникационную сеть. Различают два способа (режима) передачи пакетов: режим виртуальных соединений и дейтаграммный. ***Коммутация Каналов*** **—** обеспечивающая предоставление каждой паре абонентов последовательности каналов сети для монопольного использования. Коммутация Каналов, связана с предоставлением на время сеанса последовательностей каналов, соединяющих пары абонентских систем или административных систем друг с другом. Положительными особенностями коммутации каналов, по сравнению с коммутацией пакетов, является относительная дешевизна используемых для этой цели узлов. Кроме этого, все передаваемые во время сеанса блоки данных доставляются адресату с одинаковой задержкой во времени, определяемой скоростными характеристиками узлов и каналов. Это упрощает передачу через коммуникационную сеть речи. Однако коммутация каналов имеет и ряд существенных недостатков. Во время сеанса последовательность используемых каналов загружена потоками битов относительно небольшое время. Остальное время каналы простаивают. Вторым недостатком метода коммутации каналов является относительно длительное время создания последовательности каналов. При коротких сеансах время создания последовательности может превышать продолжительность сеанса.

8.1.4. Смешанная, сквозная коммутация и коммутация с запоминанием

Смешанная коммутация **—** комплексный транспортный сервис, обеспечивающий коммутацию каналов (при N=1) и коммутацию пакетов (при N=3). Смешанная коммутация, именуемая также гибридной коммутацией, осуществляется Цифровой Сетью с Интегральным Обслуживанием (ЦСИО). Для этой цели в ней используются узлы смешанной коммутации, способные выполнять оба вида коммутации. При смешанной коммутации имеющиеся в коммуникационной сети логические каналы, в первую очередь, используются для коммутации каналов и создания последовательностей, соединяющих пары административных систем или абонентских систем. По свободным каналам осуществляется передача блоков данных в режиме коммутации пакетов. Естественно, что в соответствии с запросами систем соотношение числа каналов, входящих в оба множества все время меняется. Рассматриваемая коммутация выполняет коммутацию каналов и пакетов на базе одного и того же оборудования. Его ПО позволяет при использовании только физического уровня и физических процессов ретрансляционной системы обеспечить коммутацию каналов. При функционировании физического, канального уровня, сетевого уровня и сетевых процессов ретрансляционная система осуществляет коммутацию пакетов.

Сквозная коммутация **—** способ коммутации, при котором блок данных начинает передаваться ретрансляционной системой до того, как его содержимое ею получено полностью. Важным преимуществом сквозной коммутации является очень небольшая задержка блока в ретрансляционной системе. Поэтому рассматриваемая коммутация, обеспечивая коммутацию каналов, ретрансляцию кадров либо ретрансляцию ячеек, используется в сетях скоростной коммутации данных, а также в коммутируемых локальных сетях. Метод сквозной коммутации основан на том, что выбор канала, по которому далее передается блок данных, происходит тотчас, как только прочитан адрес его назначения. Адрес располагается в начальной части блока. Между тем, сквозная коммутация имеет и ряд недостатков. Первый из них заключается в том, что в этом режиме не обеспечивается выявления ошибок с помощью Контроля циклической избыточности CRC. Второй недостаток сквозной коммутации связан с тем, что блок данных не может быть передан из канала с низкой в канал, работающий с более высокой скоростью. Альтернативой рассматриваемой является коммутация с запоминанием. ***Коммутация с запоминанием*** **—** способ коммутации, при котором блок данных передается ретрансляционной системой после того, как его содержимое получено ею полностью. Коммутация с запоминанием является классической технологией, используемой при коммутации пакетов и коммутации сообщений. Она заключается в том, что из принятого ретрансляционной системой пакета либо сообщения извлекаются заголовок, концевик и содержащаяся в нем передаваемая информация. Затем, осуществляется проверка ошибок с помощью Контроля циклической избыточности CRC. Рассматриваемая коммутация проста, но характеризуется относительно большими задержками, происходящими в ретрансляционных системах. Поэтому в скоростных сетях она заменяется сквозной коммутацией. Дальнейшее развитие методов коммутации привело к созданию интегральной коммутации. Это универсальный пакетно-ориентированный метод коммутации. В этой технологии коммутация пакетов, коммутация каналов, ретрансляция кадров и ретрансляция ячеек слились в единый способ передачи блоков данных. Связанные с этим операции осуществляются аппаратно и через каждый узел интегральной коммутации одновременно может проходить не один, а группа блоков данных. Благодаря

этому выполняется методология скоростной коммутации данных, реализующая сквозную коммутацию быстрых пакетов, что позволяет эффективно загружать широкополосные каналы и скоростные базовые сети. Наиболее перспективной базой для интегральной коммутации является асинхронный способ передачи. Высокая надежность современных коммуникационных сетей позволяет отказаться от проверки блоков данных во всех промежуточных узлах. Она может происходить только в конечных узлах либо уже в абонентских системах. По существу, коммутация на сетевом уровне заменяется ретрансляцией кадров либо ретрансляцией ячеек, выполняемыми на канальном уровне.

8.1.5. Ретрансляция кадров и ячеек

Ретрансляция кадров и ретрансляция ячеек являются новыми методами передачи данных. Здесь каждая ретрансляционная система выполняет интегральную коммутацию и с высокой скоростью распределяет потоки кадров либо ячеек в соответствии с их адресацией по каналам передачи данных. В промежуточных узлах коммутации кадры и ячейки не обрабатываются. Ретрансляция кадров и ячеек являются сквозной коммутацией. Напомним, что ***пакет*** — это блок данных, передаваемый на сетевом уровне. В отличие от него, ***кадр*** - это блок данных, передаваемый на канальном уровне. В сетях со сквозной коммутацией кадр принято называть быстрым пакетом, а в тех случаях, когда он имеет постоянную длину - ячейкой. ***Ретрансляция кадров (frame relay)*** — технология аппаратной скоростной коммутации данных. Передача больших потоков информации через коммуникационную сеть потребовала резкого увеличения скоростей передачи данных. В результате появились сети ретрансляции кадров. Технология ретрансляции заключается в сквозной коммутации быстрых пакетов, обеспечивающей аппаратную самомаршрутизацию (распределение в каждом узле интегральной коммутации проходящих кадров по адресам их назначения). Кадры, в которых появились ошибки, уничтожаются. В промежуточных узлах коммутации ради получения высоких скоростей, не осуществляется контроль достоверности и целостности данных. Он возлагается на оконечные узлы коммутации. Последние создают на канальном уровне соединения, осуществляют управление потоками данных через виртуальные каналы, выявляют и исправляют ошибки. Ретрансляция используется в коммуникационных сетях, работающих с малым числом ошибок. При возникающих ошибках и перегрузках узлы выбрасывают мешающие им кадры. Сетевого уровня здесь нет. В сети передаются кадры переменной длины размером до 1024 байт. Скорость передачи до 1,5 Мбит/с. Ретрансляция кадров отличается от коммутации пакетов тем, что в рассматриваемом случае в коммуникационной сети отсутствуют пакеты. Фрагменты данных, передаваемые прикладным процессом, помещаются непосредственно в кадры, которые передаются не только между смежными системами, но и ретранслируются через всю коммуникационную сеть. ***Ретрансляция ячеек (cell relay)*** — сетевая технология, обеспечивающая аппаратную скоростную коммутацию данных, упакованных в ячейки. Ретрансляция ячеек выполняет сквозную коммутацию и используется, в первую очередь, в базовых сетях. Она отличается от ретрансляции кадров тем, что обеспечивает передачу через эти сети блоков данных постоянной длины, именуемых ячейками. Это происходит в режиме реального времени. Ретрансляция ячеек выполняется узлами интегральной коммутации.

8.1.6. Матричный коммутатор и баньяновая сеть (интегральная коммутация)

Матричный коммутатор состоит из множества одинаковых коммутирующих элементов. В узлах сетки имеются коммутирующие элементы, причем в каждом столбце сетки может быть открыто не более чем по одному элементу. Если N?M, то коммутатор может обеспечить соединение каждого входа с не менее чем одним выходом; в противном случае коммутатор называется блокирующим, т.е. не обеспечивающим соединения любого входа с одним из выходов. Обычно применяются коммутаторы с равным числом входов и выходов N*N. Недостаток рассмотренной схемы - большое число коммутирующих элементов в квадратной матрице, равное N^2. Для устранения этого недостатка применяют многоступенные коммутаторы. ***Баньяновая сеть*** — скоростная распределительная сеть, с каскадной адресацией. Технология скоростной коммутации данных требует максимального использования параллелизма при ретрансляции кадров и ретрансляции ячеек. Важной базой этой технологии являются баньяновые (banyan-управляющий) сети. Структура баньяновой сети, выполненная в виде узла на 16 входов и выходов состоит из простых коммутирующих элементов, соединенных друг с другом. Через последовательности этих элементов передаются блоки данных. Изображенная структура имеет четыре каскада (1-4) коммутирующих элементов. Каждый передаваемый блок данных имеет в заголовке адрес, разрядность которого равна числу элементов баньяновой сети. Блок, поданный на вход i-того каскада попадает на один из его выходов, если в i-том разряде адреса записан "0". Если в этом разряде находится "1", то блок передается на другой выход элемента. Так, по каскадам, происходит ретрансляция блоков данных, определяемая деревом выбора путей передачи. Таким образом, осуществляется самомаршрутизация блоков, определяемая их адресами. В результате, баньяновые сети обеспечивают большую пропускную способность, ибо блоки данных через них проходят параллельно, а функции маршрутизации выполняются аппаратно. Однако нужно иметь в виду, что в баньяновых сетях могут происходить взаимные блокировки и возникать тупиковые ситуации. Поэтому в рассматриваемых сетях должны быть приняты специальные меры, предотвращающие появление этих тупиков. Баньяновые сети используются в узлах интегральной коммутации.

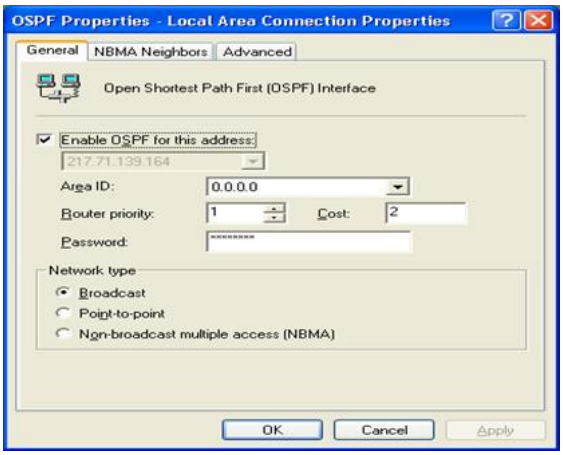
Контрольные вопросы:

1. Сколько уровней модели OSI/ISO обеспечивают сети frame relay?
2. Сколько уровней модели OSI/ISO обеспечивают сети X.25?
3. Какие выделенные каналы являются наиболее перспективными?
4. Что используются для передачи данных по аналоговым выделенным каналам?
5. Какие типы цифровых каналов иерархии PDH используются в России?
6. Что такое маршрутизация?
7. Что такое алгоритм Дейкстры?
8. Что такое алгоритм Беллмана-Форда?
9. В чём разница коммутации блоков, каналов, сообщений?
10. В чём разница смешанной и сквозной коммутации?

Практические задания:

ЗАДАНИЕ № 8.1. Развёртывание протокола маршрутизации OSPF.

Маршрутизируемая межсетевая OSPF-среда использует протокол маршрутизации OSPF, чтобы динамически пересылать информацию о маршрутизации между маршрутизаторами. Правильно развернутая OSPF-среда автоматически добавляет и удаляет маршруты, когда из межсетевой среды добавляются или удаляются сети. OSPF-объявления маршрутов должны распространяться между OSPF-маршрутизаторами в межсетевой среде. Для установки на маршрутизаторе протокола OSPF следует в контекстном меню объектаGeneral (Общие) выбрать пункт New Routing Protocol (Новый протокол маршрутизации). В открывшемся окне необходимо выбрать из списка элементOpen Shortest Path First (OSPF). Система выполнит установку всех необходимых компонентов. В пространстве имен оснастки появится новый контейнер — OSPF. После того как протокол установлен на маршрутизаторе, нужно определить сетевые интерфейсы, для которых он будет активизирован. В процессе добавления интерфейса система предложит определить конфигурацию протокола OSPF для этого интерфейса. В поле Area ID администратору необходимо выбрать область OSPF, к которой будет отнесен данный маршрутизатор.



ЗАДАНИЕ № 8.2. Расчет параметров сети.

В условиях информационного обмена возникает необходимость в применении научно обоснованных методов определения возможностей физической среды, последствий изменений в сети, смены топологии сети и т.д., что влияет на производительность, время ответа, доступность тех или иных сервисов.

Расчет параметров сети Ethernet.

Важным явлением в сетях Ethernet является коллизия – ситуация, когда две станции одновременно пытаются передать кадр данных по общей среде (следствие случайного метода доступа к среде). Для четкого распознавания коллизий необходимо правильно рассчитывать параметры такой сети. Соблюдение ограничений для сетей Ethernet, гарантирует корректную работу сети (при условии исправности всех элементов). В таблице9.1 приведены общие ограничения для всех стандартов Ethernet. Для неоднородной сети проводится дополнительный расчет параметров PDV (Path Delay Value) и PVV (Path Variability Value).

Таблица 8.1.

Общие ограничения стандартов Ethernet

Номинальная пропускная способность	10 Мбит/ с
Максимальное число станций в сети	1024
Максимальное расстояние между узлами	2500 м (в 10 Base- FB 2750 м)
Максимальное число коаксиальных сегментов в сети	4

Расчет PDV.

Для расчетов используются справочные данные IEEE, содержащие значения задержек распространения сигналов в повторителях, приемопередатчиках и различных физических средах. В таблице 8.2 приведены данные, необходимые для расчета значения PDV для всех физических стандартов сетей Ethernet (битовый интервал обозначен как bt).

Таблица 8.2.

Данные для расчета PDV

Сегмент	База левого сегмента, bt	База промежуточного сегмента, bt	База правого сегмента, bt	Задержка среды на 1 м, bt	Максимальная длина сегмента, м
10Base-5	11,8	46,5	169,5	0,0866	500
10Base-2	11,8	46,5	169,5	0,1026	185
10Base-T	15,3	42,0	165,0	0,113	100
10Base-FB	-	24,0	-	0,1	2000
10Base-FL	12,3	33,5	156,5	0,1	1000

Данные, приведенные в таблице, включают сразу несколько этапов прохождения сигнала. Например, задержки, вносимые повторителем, состоят из задержки блока повторения и задержки выходного трансивера. Чтобы не нужно было два раза складывать задержки, вносимые кабелем, в таблице даются удвоенные величины задержек для каждого типа кабеля. Также используются понятия, левый сегмент, правый сегмент и промежуточный сегмент. С каждым сегментом связана постоянная задержка, названная базой, которая зависит только от типа сегмента и от положения сегмента на пути сигнала. С каждым сегментом связана задержка распространения сигнала вдоль кабеля сегмента, которая зависит от длины сегмента и вычисляется путем умножения времени распространения сигнала по одному метру кабеля на длину кабеля в метрах.

Расчет заключается в вычислении задержек, вносимых каждым отрезком кабеля, а затем суммировании этих задержек с базами левого промежуточных и правого сегментов. Общее значение PDV не должно превышать 575.

Расчет PVV.

Чтобы признать конфигурацию сети корректной, нужно рассчитывать также, уменьшение меж кадрового интервала повторителями, то есть величину PVV. Для расчета PVV также можно воспользоваться значениями максимальных величин уменьшения меж кадрового интервала при прохождении повторителей различных физических сред, рекомендованными IEEE и приведенными в таблице 8.3.

Таблица 8.3.

Сокращение межкадрового интервала повторителями

Тип сегмента	Передающий сегмент, bt	Промежуточный сегмент, bt
10Base-5	16	11
10Base-2	16	11
10Base-T	10,5	8
10Base-FB	-	2
10Base-FL	10,5	8

Расчет параметров сети Fast Ethernet.

Правила корректного построения сетей Fast Ethernet включает:

· ограничения на максимальные длины сегментов, от источника кадров к источнику кадров;
· ограничения на максимальные длины сегментов, соединяющих источник данных с портом повторителя;
· ограничения на максимальный диаметр сети;
· ограничения на максимальное число повторителей и максимальную длину;
· ограничения длин между сегментами, от источника кадров к источнику кадров.

В качестве источника кадров может выступать: сетевой адаптер, порт маршрутизатора, модуль управления сетью. Отличительная особенность источника кадров – вырабатывается новый кадр для разделяемого сегмента. Порт повторителя не является источником кадров, так как он побитно повторяет уже появившийся в сегменте кадр. Спецификация IEEE определяет следующие максимальные длины сегментов, приведенные в таблице 8.4. Ограничения сетей Fast Ethernet, построенных на повторителях. Они делятся на два класса. Повторители класса I позволяют выполнять трансляцию логических кодов с битовой скоростью 100Мбит/с, повторители класса II позволяют выполнять трансляцию логических кодов с битовой скоростью 10Мбит/с и 100Мбит/с. В одном домене коллизий допускается наличие только одного повторителя класса I. Это связано с тем, что такой повторитель вносит большую задержку при распространении сигналов из-за необходимости различных систем сигнализации-70bt (удвоенная задержка 140 bt).

Таблица 8.4.

Максимальные длины сегментов

Стандарт	Тип кабеля	Максимальная длина сегмента
10 Base-TX	Категория 5 UTP	100 м
10 Base- FX	Многомодовое оптоволокно 62,5/ 125 мкм	412 м (полудуплекс) 2 км (полный дуплекс)
10 Base-T4	Категория 3,4 или 5 UTP	100 м

Повторители класса II вносят меньшую задержку при передаче сигналов: 46bt для портов TX(или FX) и 33,5bt для портов T4. Поэтому максимальное число повторителей класса II в домене коллизий - 2, причем они должны быть соединены между собой кабелем не длиннее 5 метров. Небольшое количество повторителей Fast Ethernet не является серьезным препятствием при построении больших сетей, так как применение коммутаторов и маршрутизаторов делит сеть на несколько доменов коллизий, каждый из которых будет строиться на одном или двух повторителях. Общая длина сети не будет иметь в этом случае ограничений.

Таблица 8.5.

Параметры сетей на основе повторителей класса I

Тип кабеля	Максимальный диаметр сети, м	Максимальная длина сегмента, м

Только витая пара (TX)	200	100
Только оптоволокно (FX)	272	136
Несколько сегментов на витой паре и один на оптоволокне	260	100 (TX) 160 (FX)
Несколько сегментов на витой паре и несколько сегментов на оптоволокне	272	100 (TX) 136 (FX)

Задержки, вносимые прохождением сигналов по кабелю, можно рассчитать на основании данных таблицы 8.6. Задержки, которые вносят два взаимодействующих через повторитель сетевых адаптера можно рассчитать, используя таблицу 8.7.

Таблица 8.6.

Задержки, вносимые кабелем

Тип кабеля	Удвоенная задержка в bt на 1 м	Удвоенная задержка на кабеле максимальной длины
UTP-3	1,14 bt	114 bt (100 м)
UTP-4	1,14 bt	114 bt (100 м)
UTP-5	1,112 bt	111,2 bt (100 м)
STP	1,112 bt	111,2 bt (100 м)
Оптоволокно	1,0 bt	412 bt (412 м)

Учитывая, что удвоенная задержка, вносимая повторителем класса I, равна 140bt, можно рассчитать время двойного оборота для произвольной конфигурации сети, учитывая также максимально возможные длины непрерывных сегментов кабелей. Если получившееся значение меньше 512, значит, по критерию распознавания коллизий сеть является корректной. Разрешается оставлять запас из диапазона от 0 до 5bt для устойчивой работы сети.

Таблица 8.7.

Задержки, вносимые сетевым адаптером

Тип сетевых адаптеров	Максимальные задержки при двойном обороте
Два адаптера TX/ FX	100 bt
Два адаптера T4	38 bt
Один адаптер TX/ FX и один T4	127 bt

Например. Рассчитать сеть, состоящую из одного повторителя и двух оптоволоконных сегментов длиной по 136 метров, используя предложенную в таблице конфигурацию. Каждый сегмент вносит задержку по 136bt, пара сетевых адаптеров FX дает задержку в 100bt, а сам повторитель вносит задержку в 140bt. Сумма задержек равна 512bt, что говорит о том, что сеть корректна, но запас принят равным 0.

ЗАДАНИЕ № 8.2. Расчет информационных параметров неодноранговых сетей.

Для эффективной работы сети необходимо учитывать неоднородность информационных потоков. При проектировании неоднорангговых сетей используют модели основанные на теории очередей. Для вычислений параметров системы с очередью, необходимо определить условия работы этой системы и выявить диапазон изменений параметров. Исходные данные: средняя скорость поступления запросов равна одному запросу в миллисекунду. Из-за нерегулярности поступления запросов используется буферная память (для невыполненных запросов), т.е. сервер помещает эти запросы в очередь.

Условия системы с очередями: определение количества элементов данных; очередь может неограниченно расти; определенный порядок обслуживания элементов данных.

λ	Средняя скорость поступления элементов данных в систему (число элементов в секунду)
T_S	Среднее время обслуживания элементов (сек)
σ_{TS}	Стандартное отклонение во времени обслуживания элементов (сек)
ρ	Утилизация сервера при обслуживании (доля времени, когда сервер занят)
u	Интенсивность трафика
Q	Общее количество элементов данных в системе
q	Среднее количество элементов данных в системе
T_Q	Время, которое элементы данных проводят в системе (сек)
T_q	Среднее время, которое элементы данных проводят в системе (сек)
σ_q	Стандартное отклонение q
σ_{Tq}	Стандартное отклонение T_q (сек)
ω	Среднее количество элементов данных ожидающих обслуживания в очереди (размер очереди)
$T\omega$	Среднее время, которое элементы данных ожидают обслуживания (сек)
Td	Среднее время ожидания обслуживания для элементов данных, находившихся в

	очереди (т.е. не включая элементы, для которых время обслуживания равно 0)
σ_ω	Стандартное отклонение ω
N	Число серверов
$m_x(r)$	X меньше или равно $m_x(r)$ в r процентах случаев

Используемые в расчетах параметры:
u скорость поступления элементов данных в очередь;
u время обслуживания этих элементов на сервере на входе в систему;
u общее количество ожидающих элементов; время ожидания элементов в системе.

Теоретическая максимальная скорость поступления элементов данных равна $\lambda_{max} = \frac{1}{T_s}$. Следовательно, для системы с N серверами: $\lambda_{max} = \frac{N}{T_s}$, т.е. $N \cdot \rho$ это утилизация всей системы серверов.

Вид структуры с организацией N серверов дан на рисунке 8.2.

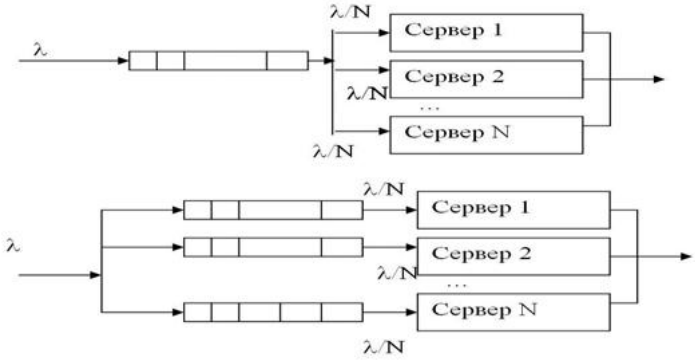


Рис. 8.2. Структура с организацией N серверов

Таблица 8.8.

Формулы для вычислений структуры системы

Основные	Один сервер	Множество серверов
$q = \lambda \cdot T_q$	$\rho = \lambda \cdot T_s$	$\rho = \frac{\lambda \cdot T_s}{N}$
$\omega = \lambda \cdot T_\omega$	$q = \omega + \rho$	$q = \omega + N_q$
$T_q = T_\omega + T_s$		$u = \lambda \cdot T_s = \rho \cdot N$

Формулы таблицы 10 могут быть использованы для вычислений некоторых параметров при “интуитивном” выборе структуры системы. Для получения формулы $\rho = \lambda \cdot T_s$ достаточно заметить, что для скорости поступления элементов данных, среднее время между поступлениями элементов будет определяться выражением $T = 1/\lambda$. Если интервал времени T меньше интервала времени T_S, то можно будет записать $T_s/T = \lambda \cdot T_s$. Аналогично в случае с множеством серверов $\rho = (\lambda \cdot T_s) / N$.

При поступлении очередного элемента данных в систему в очереди находится в среднем ω элементов данных, которые ожидают обслуживания. Среднее время, которое элемент ждет своей очереди до обслуживания, равно T_S. За промежуток T_ω должно поступить $\lambda \cdot T_\omega$ элементов данных. Следовательно, $\omega = \lambda \cdot T_\omega$. Рассуждая аналогично $q = \lambda \cdot T_q$.

Время, которое элемент данных находится в системе равно сумме времени ожидания обслуживания и времени самого обслуживания. Для одного сервера среднее число элементов, которое обслуживается в данный момент, равно ρ, $q = \omega + N \cdot \rho$, если брать N серверов. Большое значение имеют стандартные (среднеквадратичные) отклонения от средних величин. Необходимо знать закон изменения скорости поступления элементов данных в систему и закон распределения времени обслуживания элементов данным сервером. Например, скорость поступления элементов данных подчиняется закону Пуассона.

$P_n(t) = \frac{e^{-\lambda t}(\lambda t)^n}{n!}$, где λ - скорость поступления элементов, n - количество элементов, поступивших за время t

Для применимости закона Пуассона необходимо выполнение следующих гипотез: поступление одного элемента данных не зависит от поступления другого элемента, т.е. события происходят независимо; никогда не поступают сразу два или более элементов данных; среднее количество поступлений не изменяется со временем (распределено статично).

Для обобщения всех возможных случаев организации системы с очередями была использована система: X/Y/N, где X – закон распределения времени поступления элементов данных в систему, Y - закон распределения времени обслуживания элементов данных в сервером, N – количество серверов. Характерны следующие возможные законы:

G – нормальное распределение времени поступления или времени обслуживания;
M – пуассоновское распределение времени поступления или пуассоновское (экспоненциальное) времени обслуживания;
D – детерминированное время поступления или время обслуживания элементов данных.

ЗАДАНИЕ № 8.3. Расчет системы с несколькими серверами.

Для N серверов используется функция Эрланга (C), которая, во-первых, определяет вероятность того, что все сервера заняты в определенный момент времени или, во вторых, определяет вероятность того, что количество элементов данных, находящихся в данной системе, будет больше или равно количеству серверов.

$C(N,u) = \frac{10k}{1 - k \cdot p}$, где к – коэффициент пуассоновского распределения. Для системы с одним сервером $C(1,u) = p$

Таблица 8.9.

Формулы для определения параметров системы с одним сервером

Модель с нормальным распределением времени обслуживания (M/G/1)	Модель с экспоненциальным распределением времени обслуживания (M/M/1)	Модель с постоянным времени обслуживания (M/D/1)
$A = \frac{1}{2}\left[1 + \left(\frac{\sigma_{T_s}}{T_s}\right)^2\right]$	$q = \frac{\rho}{1-\rho}; \quad \omega = \frac{\rho^2}{1-\rho}$	$q = \frac{\rho^2}{2(1-\rho)} + \rho$
$q = \rho + \frac{\rho^2 \cdot A}{1-\rho}$	$T_q = \frac{T_s}{1-p}, T_\omega = \frac{p \cdot T_s}{1-p}$	$\omega = \frac{p^2}{2 \cdot (1-p)}$
$\omega = \frac{\rho^2 \cdot A}{1-\rho}$	$\sigma_q = \frac{\sqrt{p}}{1-p}, \sigma_{T_q} = \frac{T_q}{1-p}$	$T_q = \frac{T_s \cdot (2-p)}{2 \cdot (1-p)}$
$T_q = T_s + \frac{\rho \cdot T_s \cdot A}{1-\rho}$	$P_r[Q = N] = (1-p) \cdot p^N$	$T_\omega = \frac{p \cdot T_s}{2 \cdot (1-p)}$
$T_\omega = \frac{\rho \cdot T_s \cdot A}{1-\rho}$	$P_r[Q \le N] = \sum_{I=0}^{N} (1-p) \cdot p$	$\sigma_q = \frac{1}{1-p} \cdot \sqrt{p + \frac{3 \cdot p^2}{2} + \frac{5 \cdot p^3}{6}}$
	$P_r[T_Q \le t] = 1 - e^{-(1-p) \cdot t/T}$	$\sigma_{T_q} = \frac{T_s}{1-p} \cdot \sqrt{\frac{p}{3} - \frac{p^2}{12}}$
	$m_{T_q}(r) = T_q \cdot \ln\frac{100}{100-r}$	

Таблица 8.10.

Формулы для определения параметров системы с множеством серверов

$k = \sum_{I=0}^{N} \frac{(N \cdot p)^I}{I!} \Big/ \sum_{I=0}^{N} \frac{(N \cdot p)^I}{I!}$	$\sigma_\omega = \frac{1}{1-p} \cdot \sqrt{C \cdot p \cdot (1 + p - C \cdot p)}$
$q = C \cdot \frac{p}{1-p} + N \cdot p$	$P_r[T_\omega = t] C \cdot e^{-N \cdot (1-p) \cdot t / T_q}$
$T_q = \frac{C}{N} \cdot \frac{T_s}{1-p} + T_s$	$T_d = \frac{T_s}{N \cdot (1-p)}$
$T_\omega = \frac{C}{N} \cdot \frac{T_s}{1-p}$	$\omega = C \cdot \frac{p}{1-p}$
$\sigma_{T_q} = \frac{T_s}{N \cdot (1-p)} \cdot \sqrt{C \cdot (2-C) + N^2 \cdot (1-p)}$	$m_{T_\omega} = \frac{T_s}{N \cdot (1-p)} \cdot \ln\frac{100 \cdot C}{100-r}$

ЗАДАНИЕ № 8.4. Распределение адресного пространства.

Важной проблемой при объединении компьютеров в сеть, является проблема их адресации:
- адрес должен уникально идентифицировать компьютер в сети любого масштаба;
- схема назначения адресов должна сводить к минимуму ручной труд администратора и вероятность дублирования адресов;
- адрес должен иметь иерархическую структуру, удобную для построения больших сетей;
- адрес должен быть удобен, для пользователя сети и иметь символьное представление;
- адрес должен иметь компактное представление, чтобы не перегружать память коммуникационной аппаратуры.

Для автоматизации процедуры используются специальные протоколы.

Протокол RIP - сетевой маршрут определяются по нулевой хост-части; адрес, у которого в хост-части есть хоть один единичный бит, определяет маршрут узла. При переходе на подсети принято соглашение о том, что адресация внешних сетей выполняется по классовому признаку, а локальные маршрутизаторы, работающие с подсетями, получают значение масок при ручной настройке (подсетевой маршрут). Протоколы маршрутизации RIP использую только классовую адресацию.

Протокол OSPF (протокол обмена маршрутной информацией) поддерживает префиксы произвольного размера и обменивается информацией, включающий 32- битный адрес и длину префикса. Распространена форма задания префикса в виде маски (под) сети. Маска представляет собой 32 - битное число. По общим правилам записи IP- адреса, у которого старшие биты,

соответствующие префиксу, имеют единичное значение, младшие (локальная хост-часть)- нулевые. Маски могут принимать значения из ограниченного списка.

Таблица 8.11.

Длина префикса, значение маски и количество узлов подсети

Длина префикса	Маска подсети	Число узлов
32	255.255.255.255	-
31	255.255.255.254	-
30	255.255.255.252	2
29	255.255.255.248	6
28	255.255.255.240	14
27	255.255.255.224	30
26	255.255.255.192	62
…	…	…

Образование байт маски поясняет таблица 8.12.

Количество допустимых адресов хостов в (под)сети (с учетом резервирования крайних значений адреса) определяется по формуле $N = 2^{(32 - p)} - 2$, где P - длина префикса. Префиксы длиной 31 или 32 бит, непригодны для употребления, префикс длиной 30 бит позволяет адресовать только два узла.

Таблица 8.12.

Возможные значения элементов масок

Двоичное	Десятичное	Двоичное	Десятичное	Двоичное	Десятичное
11111111	255	11111000	248	11000000	192
11111110	254	11110000	240	10000000	128
11111100	252	11100000	224	00000000	0

Адресом сети можно считать адрес любого ее узла с обнуленными битами хост части. В десятичном представлении диапазоны адресов и маски сетей стандартных классов имеют следующие значения:

Класс A: 1.0.0.0- 126.0.0.0, маска 255.0.0.0.

Класс B: 128.0.0.0- 191.255.0.0, маска 255.255.0.0.

Класс C: 192.0.0.0- 233.255.255.0, маска 255.255.255.0.

Класс D: 224.0.0.0- 239.255.255.255, маска 255.255.255.255.

Класс E: 240.0.0.0- 247.255.255.255, маска 255.255.255.255.

Протоколы DHCP. IP-адреса и маски назначаются узлам при их конфигурировании вручную или автоматически с использованием DHCP или BootP серверов. Ручное назначение адресов требует внимания, т.к. некорректное назначение адресов и масок приводит к невозможности связи по IP, однако с точки зрения надежности и безопасности (защиты несанкционированного доступа) оно имеет свои преимущества. DHCP-протокол, обеспечивает автоматическое динамическое назначение IP- адресов и масок подсетей для узлов-клиентов DHCP-сервера. Адреса назначаются автоматически из области пула адресов, выделенных DHCP-серверу. По окончании работы узла его адрес возвращается в пул и в дальнейшем может назначаться для другого узла. Применение DHCP облегчает инсталляцию и диагностику для узлов, а также снимает проблему дефицита IP-адресов. Протокол BootP - выполняет аналогичные функции, но использует статическое распределение ресурсов. При инициализации узел посылает широковещательный запрос, на который BootP-сервер ответит пакетом с IP- адресом, маской, а также адресами шлюзов и серверов службы имен. Эти данные хранятся в списке, составленном по MAC-адресам клиентов BootP, хранящимся на сервере. По отключении узла его IP-адрес не может быть использован другими узлами.

ЗАДАНИЕ № 8.5. Виды коммутации.

Подобрать правильно каждому уровню коммутации свой метод и устройства.

Уровни коммутации	Метод	Устройство
Одноуровневая	Коммутация сообщений	Узел коммутации каналов
Двухуровневая	Коммутация пакетов	Узел интегральной коммутации
Трехуровневая	Интегральная коммутация	Узел коммутации пакетов
Семиуровневая	Коммутация каналов	Узел коммутации сообщений

Перечень литературы и Интернет-ресурсов:

1. Андерсон К. с Минаси М. Локальные сети. Полное руководство. К.: ВЕК+, М.:ЭНТРОП, СПб.:КОРОНА 1999, 624 с.

2. Бертсекас Д., Галлагер Р. Сети передачи данных / Пер с англ. – М.: Мир, 1989. – 562 с.
3. Внутренний протокол маршрутизации RIP - http://www.opennet.ru/docs/RUS/inet_book/4/44/rip44111.html
4. МЕТОДЫ МАРШРУТИЗАЦИИ В ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ — http://www.ict.edu.ru/ft/005595/Krylov2.pdf
5. Олифер В.Г., Олифер. Н.А. Компьютерные сети. Принципы, технологии, протоколы. (рекомендовано Мин. образования РФ). СПб: Питер, 2001,668 с.
6. Основы построения объединенных сетей — http://www.citforum.ru/nets/ito/index.shtml
7. Протокол OSPF (алгоритм Дикстры)) — http://www.opennet.ru/docs/RUS/inet_book/4/44/osp44112.html
8. Протоколы маршрутизации (обзор, таблицы маршрутизации, вектор расстояния — http://www.opennet.ru/docs/RUS/inet_book/4/44/rut_4411.html
9. Титтел Эд, Хадсон Курт, Дж. Майкл Стюард TCP/IP – СПб ПИТЕР, 1999.
10. Учебник по компьютерным сетям. Сетям — http://kompset.narod.ru/siteunior.html
11. Якубайтис Э.А. Информационные сети и системы: Справочная книга. – М.: Финансы и статистика, 1996.
12. Telecommunication technologies - телекоммуникационные технологии — http://www.opennet.ru/docs/RUS/inet_book/

Тема 9. Протокольные реализации

Цели:

· Понять принципы работы протоколов и стека протоколов.
· Разобраться в стандартах протокола разного уровня.
· Получить представление о протоколе IPX/SPX и межсетевом протоколе TCP/IP.

9.1. Протокол.

Протокол— стандарт, определяющий поведение функциональных блоков при передаче данных. Протокол является набором правил взаимодействия функциональных блоков, расположенных на одном уровне. Обычно протокол описывает: синтаксис сообщения, являющийся способом идентификации данных при их передаче. Например, порядок, в котором отображаются адрес назначения и элементы данных; имена элементов данных, что позволяет обеспечивать интерпретацию передаваемой информации; операции управления и состояния. Они сводятся к динамичному согласованию фаз функционирования, связанного с передачей данных. Для случаев появления отказов в сети предусматривается порядок выхода из этих состояний.

Базовая эталонная модель взаимодействия открытых систем определяет семь уровней области Взаимодействия Открытых Систем (ВОС). Соответственно этому вводится в рассмотрение семь групп протоколов. Они именуются так же, как и уровни. Протоколы, располагаясь друг над другом, образуют штабель. В зависимости от задачи, поставленной перед системой, ее штабель может содержать все уровни области взаимодействия либо только часть из них. Так абонентская система определяется штабелем из семи уровней, а ретрансляционная система для целей коммутации чаще всего имеет штабель из двух-трех уровней. На каждом уровне в сети может работать один либо несколько различных независимых друг от друга протоколов. Каждый протокол N-уровня обеспечивает взаимодействие объектов того же уровня, расположенных в различных системах сети. Любой протокол не знает о существовании других протоколов. Но он получает сервис от протоколов, расположенных на соседнем снизу уровне. Абстрактное описание взаимодействия через точку доступа к сервису называется примитивом. В базовой эталонной модели определены четыре типа примитивов: запрос, признак, ответ и подтверждение. В информационной сети выделяют два типа протоколов, определяемых точками их приложения . Протоколы Р-типа обеспечивают непосредственное взаимодействие объектов абонентских систем либо административных систем на соответствующем уровне. Что же касается протоколов К-типа, то они описывают взаимодействие пар смежных систем. Эти протоколы описывают характеристики коммуникационной сети. В зависимости от наборов уровней, на которых располагаются протоколы, выделяются четыре класса сети:

No	Класс сети	Уровни, на которых функционируют протоколы		Х-процессы, обеспечивающие взаимодействие частей
		Р-типы	К-типы	
1.	Сеть с селекцией данных	1, 2, 3, 4, 5, 6, 7	-	-
2.	Сеть коммутации каналов	2, 3, 4, 5, 6	1	Физический
3.	Сеть скоростной коммутации данных	3, 4, 5, 6	1, 2	Канальный
4.	Сеть коммутации пакетов	4, 5, 6	1, 2, 3	Сетевой

Рис. 9.1. Классы сетей

Три последние класса сетей образуют сети с маршрутизацией данных. В соответствии со сказанным, например, в сети коммутации пакетов к К-типу относятся протоколы уровней 1-3, а к Р-типу - протоколы уровней 4-7. Здесь в роли ретрансляционной системы выступает трехуровневый узел коммутации пакетов.

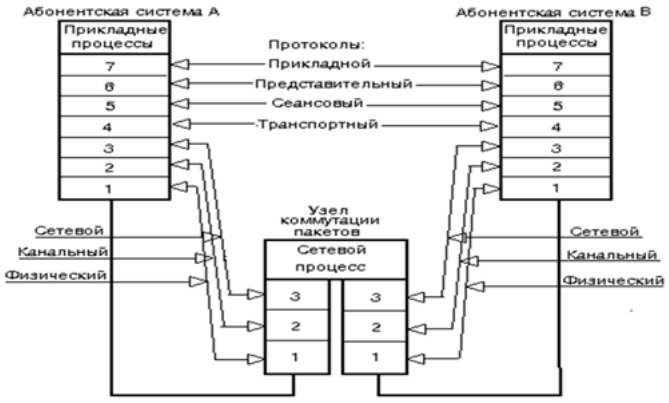


Рис. 9.2.

Пользовательский протокол дейтаграмм (UDP) предназначен для отправки небольших объемов данных без установки соединения и используется приложениями, которые не нуждаются в подтверждении адресатом их получения. UDP также использует номера портов для определения конкретного процесса по указанному IP адресу. Однако UDP порты отличаются от TCP портов и, следовательно, могут использовать те же номера портов, что и TCP, без конфликта между службами. В отличие от TCP UDP не устанавливает соединения. ***Межсетевой уровень*** отвечает за маршрутизацию данных внутри сети и между

различными сетями. На этом уровне работают маршрутизаторы, которые зависят от используемого протокола и используются для отправки пакетов из одной сети (или ее сегмента) в другую (или другой сегмент сети).

Протокол управления сообщениями Интернета (ICMP – Internet Control Message Protocol) используется IP и другими протоколами высокого уровня для отправки и получения отчетов о состоянии переданной информации. Этот протокол используется для контроля скорости передачи информации между двумя системами. Если маршрутизатор, соединяющий две системы, перегружен трафиком, он может отправить специальное сообщение ICMP – ошибку для уменьшения скорости отправления сообщений. Узлы локальной сети используют ***протокол управления группами Интернета (IGMP – Internet Group Management Protocol)***, чтобы зарегистрировать себя в группе. Информация о группах содержится на маршрутизаторах локальной сети. Маршрутизаторы используют эту информацию для передачи групповых сообщений. Групповое сообщение, как и широковещательное, используется для отправки данных сразу нескольким узлам.

Протоколы сопоставления адреса ARP и RARP. Для определения локального адреса по IP-адресу используется протокол разрешения адреса *Address Resolution Protocol (ARP)*. ARP работает различным образом в зависимости от того, какой протокол канального уровня работает в данной сети – протокол локальной сети (Ethernet, Token Ring, FDDI) с возможностью широковещательного доступа одновременно ко всем узлам сети, или же протокол глобальной сети (X.25, frame relay), как правило, не поддерживающий широковещательный доступ. Существует также протокол, решающий обратную задачу – нахождение IP-адреса по известному локальному адресу. Он называется реверсивный ARP – *RARP (Reverse Address Resolution Protocol)* и используется при старте бездисковых станций, не знающих в начальный момент своего IP-адреса, но знающих адрес своего сетевого адаптера. В локальных сетях ARP использует широковещательные кадры протокола канального уровня для поиска в сети узла с заданным IP-адресом. Узел, которому нужно выполнить отображение IP-адреса на локальный адрес, формирует ARP-запрос, вкладывает его в кадр протокола канального уровня, указывая в нем известный IP-адрес, и рассылает запрос широковещательно. Все узлы локальной сети получают ARP-запрос и сравнивают указанный там IP-адрес с собственным адресом. В случае их совпадения узел формирует ARP-ответ, в котором указывает свой IP-адрес и свой локальный адрес и отправляет его уже направленно, так как в ARP-запросе отправитель указывает свой локальный адрес. ARP-запросы и ответы используют один и тот же формат пакета.

Network Device Interface Specification (NDIS) – спецификация интерфейса сетевого устройства, программный интерфейс, обеспечивающий взаимодействие между драйверами транспортных протоколов, и соответствующими драйверами сетевых интерфейсов. Позволяет использовать несколько протоколов, даже если установлена только одна сетевая карта. ***Уровень сетевого интерфейса.*** Этот уровень модели TCP/IP отвечает за распределение IP-дейтаграмм. Он работает с ARP для определения информации, которая должна быть помещена в заголовок каждого кадра. Затем на этом уровне создается кадр, подходящий для используемого типа сети, такого как Ethernet, Token Ring или ATM, затем IP-дейтаграмма помещается в область данных этого кадра, и он отправляется в сеть.

9.2. Протоколы и стеки протоколов.

Согласованный набор протоколов разных уровней, достаточный для организации межсетевого взаимодействия, называется *стеком протоколов*. Для каждого уровня определяется набор функций–запросов для взаимодействия с выше лежащим уровнем, который называется *интерфейсом*. Правила взаимодействия двух машин могут быть описаны в виде набора процедур для каждого из уровней, которые называются *протоколами*.

Стек OSI. Следует различать стек протоколов OSI и модель OSI рис.9.3. Стек OSI – это набор вполне конкретных спецификаций протоколов, образующих согласованный стек протоколов. Этот стек протоколов поддерживает правительство США в своей программе GOSIP. Стек OSI в отличие от других стандартных стеков полностью соответствует модели взаимодействия OSI и включает спецификации для всех семи уровней модели взаимодействия открытых систем.

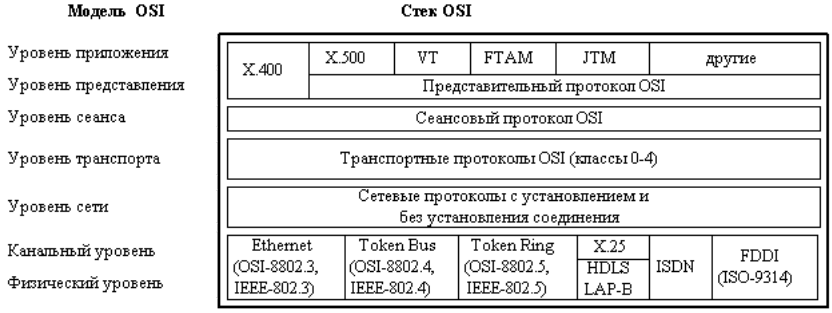


Рис. 9.3. Стек OSI

На *физическом и канальном уровнях* стек OSI поддерживает спецификации Ethernet, Token Ring, FDDI, а также протоколы LLC, X.25 и ISDN. На *сетевом* уровне реализованы протоколы, как без установления соединений, так и с установлением соединений. *Транспортный* протокол стека OSI скрывает различия между сетевыми сервисами с установлением соединения и без установления соединения, так что пользователи получают нужное качество обслуживания независимо от нижележащего сетевого уровня. Чтобы обеспечить это, транспортный уровень требует, чтобы пользователь задал нужное качество обслуживания. Определены 5 классов транспортного сервиса, от низшего класса 0 до высшего класса 4, которые отличаются степенью устойчивости к ошибкам и требованиями к восстановлению данных после ошибок. Сервисы *прикладного уровня* включают передачу файлов, эмуляцию терминала, службу каталогов и почту. Из них наиболее перспективными являются служба каталогов (стандарт X.500), электронная почта (X.400), протокол виртуального терминала (VT), протокол передачи, доступа и управления файлами (FTAM), протокол пересылки и управления работами (JTM). В последнее время ISO сконцентрировала свои усилия именно на сервисах верхнего уровня. Стеки протоколов разбиваются на три уровня:

9.2.1. Стеки сетевых протоколов

Сетевые протоколы предоставляют следующие услуги: адресацию и маршрутизацию информации, проверку на наличие ошибок, запрос повторной передачи и установление правил взаимодействия в конкретной сетевой среде.

· **DDP** (Datagram Delivery Protocol – Протокол доставки дейтаграмм). Протокол передачи данных Apple, используемый в Apple Talk.

· **IP** (Internet Protocol – Протокол Internet). Протокол стека TCP/IP, обеспечивающий адресную информацию и информацию о маршрутизации.

· **IPX** (Internetwork Packet eXchange – Межсетевой обмен пакетами) в NWLink. Протокол Novel NetWare, используемый для маршрутизации и направления пакетов.

· **Протокол NWLink.** Это Microsoft-совместимый IPX/SPX протокол для Windows. Необходим для доступа к сетям под управлением серверов с ОС Nowell NetWare. Сам протокол NWLink реализует сетевой и транспортный уровень взаимодействия. Для доступа к файлам или принтерам сервера NetWare надо задействовать специальный редиректор, представленный в Windows XP Professional службой CSNW (клиент для сетей NetWare), а в Windows Server 2003 - службой GSNW (шлюз для сетей NetWare). Протокол NWLink включен в состав обеих ОС Windows и устанавливается автоматически вместе с клиентом и службой шлюза для NetWare.

· **NetBEUI** (NetBIOS Extended User Interface – расширенный пользовательский интерфейс базовой сетевой системы ввода вывода)**.** Разработанный совместно IBM и Microsoft, этот протокол обеспечивает транспортные услуги для **NetBIOS.** Разрабатывался как протокол для небольших локальных сетей, содержащих 20-200 компьютеров. NetBEUI - немаршрутизируемый протокол, поскольку в нем не реализован сетевой уровень. Данный протокол поддерживается всеми операционными системами Microsoft, однако в современных версиях Windows он выключен по умолчанию и используется, в основном, для поддержки рабочих станций Windows 9x.

· **Протокол Apple Talk.** Это набор протоколов, разработанный Apple Computer, Inc. для связи компьютеров Apple Macintosh. Windows поддерживает все протоколы AppleTalk, что позволяет этой операционной системе выступать в роли маршрутизатора и сервера удаленного доступа сетей Macintosh. Для работы с протоколом AppleTalk предоставляется соответствующая служба доступа к файлам и принтерам.

· **Протокол DLC.** Протокол DLC (Data Link Control) был разработан для объединения мэйнфрэймов IBM. Он не проектировался как основной протокол персональных компьютеров в сети. Зачастую его используют для печати на сетевых принтерах Hewlett-Packard.

· **Стандарт IrDA.** Ассоциация Infrared Data Association (IrDA) определила группу двусторонних высокоскоростных беспроводных протоколов для обмена информацией в инфракрасном диапазоне, обычно называемых IrDA. Протоколы IrDA обеспечивают взаимодействие компьютеров со множеством устройств: цифровыми камерами, принтерами, карманными компьютерами типа PocketPC и др. В Windows XP и Windows Server 2003 включена поддержка IrDA.

· **Порядок привязки протоколов.** Протоколы можно добавлять, удалять и выборочно привязывать ко всем сетевым интерфейсам сервера. По умолчанию порядок привязки протоколов определяется последовательностью, в которой они были установлены. Но при этом администратор всегда может изменить этот порядок для отдельных интерфейсов, что делает процесс управления более гибким. Например, к одному интерфейсу могут быть привязаны протоколы TCP/IP и IPX/SPX с приоритетом протокола TCP/IP, а к другому - те же протоколы, но с приоритетом IPX/SPX.

9.2.2. Стеки прикладных протоколов

Прикладные протоколы отвечают за взаимодействие приложений.

· **AFP** (Apple Talk File Protocol – Файловый протокол Apple Talk). Протокол удаленного управления файлами Macintosh.

· **FTP** (File Transfer Protocol – Протокол передачи файлов). Протокол стека TCP/IP, используемый для обеспечения услуг по передачи файлов.

· **NCP** (NetWare Core Protocol – Базовый протокол NetWare). Оболочка и редиректоры клиента Novel NetWare.

· **протокол Telnet** - протокол эмуляции терминала, применяемый для подключения к удаленным узлам сети. Telnet позволяет клиентам удалено запускать приложения; кроме того, он упрощает удаленное администрирование. Реализации Telnet, доступные практически для всех ОС, облегчают интеграцию в разнородных сетевых средах. В Windows XP и Windows Server 2003 включены клиент и сервер Telnet.

· **SNMP** (Simple Network Management Protocol – Простой протокол управления сетью). Позволяет централизованно управлять узлами сети, например серверами, рабочими станциями, маршрутизаторами, мостами и концентраторами. Кроме того, SNMP можно использовать для конфигурирования удаленных устройств, мониторинга производительности сети, выявления ошибок сети и попыток несанкционированного доступа, а также для аудита использования сети.

· **HTTP** (Hyper Text Transfer Protocol) **–** протокол передачи гипертекста и другие протоколы, используется для организации доступа к общим данным, расположенным на веб-серверах, с целью публикации и чтения общедоступной информации. Протокол HTTP описывает взаимодействие между HTTP-серверами (веб-серверами) и HTTP-клиентами (веб-браузерами). В состав Windows XP и Windows Server 2003 входит как клиентская часть (веб-браузер Internet Explorer v6.0), так и серверная (веб-сервер Internet Information Server, IIS).

· **протокол SMTP** - применяется почтовыми серверами для передачи электронной почты. Сервер IIS поддерживает работу с протоколом SMTP для обработки почтовых сообщений.

· **службы имен** - набор протоколов и служб позволяющий управлять именованием компьютеров в сети.

9.2.3. Стеки транспортных протоколов

Транспортные протоколы предоставляют следующие услуги надежной транспортировки данных между компьютерами.

· **ATP** (Apple Talk Protocol – Транзакционный протокол Apple Talk) и **NBP** (Name Binding Protocol – Протокол связывания имен). Сеансовый и транспортный протоколы Apple Talk.

· **NetBIOS (**Базовая сетевая система ввода вывода)**.** NetBIOS Устанавливает соединение между компьютерами, а **NetBEUI** предоставляет услуги передачи данных для этого соединения.

· **SPX** (Sequenced Packet eXchange – Последовательный обмен пакетами) в NWLink. Протокол Novel NetWare, используемый для обеспечения доставки данных.

· **TCP** (Transmission Control Protocol – Протокол управления передачей). Протокол стека TCP/IP, отвечающий за надежную доставку данных.

9.3. Стандарты протоколов разных уровней.

9.2.4. Физического уровня

Функции протоколов физического уровня (уровень 1) обеспечивают взаимодействие процедур канального уровня с физической средой передачи, по которой передается сигнал. В этих стандартах, как правило, описываются принципы построения устройств преобразования сигналов (модемов) и межуровневых интерфейсов, описывающих как уровень 1 связывается с уровнем 2, предоставляя ему свои услуги. Наибольшее количество стандартов физического уровня и интерфейсов между физическим и канальным уровнем опубликовано МККТТ (МСЭ-Т). Среди них, например, протоколы V.21-V.27 Кроме МСЭ-Т, стандарты физического уровня разрабатывались и другими организациями. Например, всемирно-известный стандарт RS-232C, разработанный EIA и используемый в устройствах подключения к персональным компьютерам периферийных устройств.

9.2.5. Канального уровня

В качестве основных функций канального уровня можно перечислить следующие: синхронизация по кодовым комбинациям (по байтам); разбиение потока информации, поступающего из физического уровня, на сегменты (блоки информации), которые называются кадрами канального уровня, и формирование кадров канального уровня из протокольных единиц (для сетей с коммутацией пакетов - это пакеты), поступающих на канальный уровень с вышележащего сетевого уровня; распознавание кадров, передаваемых между станциями компьютерных сетей (каждый кадр имеет адрес станции его передавшей); обеспечение возможности передачи информации любым кодом (прозрачности по кодам); обеспечение коррекции ошибок, возникающих при передаче информации. Протоколы канального уровня можно разделить на две группы: байт- и бит-ориентированные протоколы. Информация, передаваемая с их помощью, рассматривается соответственно на уровне одного байта или бита, и наименьшей обрабатываемой единицей информации является байт или бит. *Байт-ориентированные протоколы* - это процедуры управления каналом передачи данных, в которых для функции управления применяются структуры определенных знаков первичного кода, например, стандартного американского национального кода ASCII. В *бит-ориентированных протоколах* управление каналом производится посредством анализа битовых последовательностей, представляющих собой поля кадра канального уровня.

9.2.6. Сетевого уровня

Широко используемыми стандартами сетевого уровня являются протоколы:

· X.25, разработанный МСЭ-Т для сетей с коммутацией пакетов;

· Стандарты IPX/SPX, разработанные фирмой "Novell";

· TCP/IP (Transmission Control Protocol/Internet Protocol), разработанный в конце 60-х годов XX в. для глобальной сети Агентства по передовым исследовательским проектам министерства обороны США.

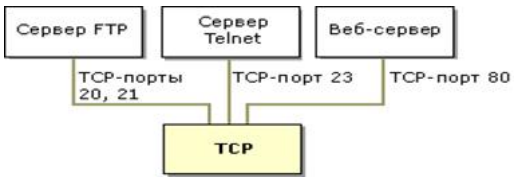
9.2.7. Транспортного уровня.

Сетевой уровень предоставляет услуги транспортному, который требует от пользователей запроса на качество обслуживания сетью. После получения от пользователя запроса на качество обслуживания транспортный уровень выбирает класс протокола, который обеспечивает требуемое качество обслуживания. *Качество обслуживания* сети зависит от ее типа, доступного конечному пользователю, а также от транспортного уровня. МСЭ-Т, ISO, ECMA определяют три типа сетей: сети, обеспечивающие приемлемые уровни ошибок и сигнализации об ошибках (приемлемое качество); сети, обеспечивающие приемлемый уровень ошибок и неприемлемо слабую сигнализацию об ошибках; сетевые соединения, представляющие неприемлемый уровень ошибок для пользователя (ненадежные сети). При существовании разных типов сетей транспортный уровень позволяет установить следующие параметры качества обслуживания: пропускная способность; надежность сети; задержка передачи информации через сеть; приоритеты; защита от ошибок; мультиплексирование; управление потоком; обнаружение ошибок. Транспортный уровень отвечает за выбор соответствующего протокола, обеспечивающего требуемое качество обслуживания на сети. Примером протоколов транспортного уровня могут служить протокол МСЭ-Т (МККТТ) X.224 – "Спецификация протокола транспортного уровня взаимосвязи открытых систем для применения МККТТ" и стандарт ISO 8073.

Протокол TCP (Transmission Control Protocol) - протокол, обеспечивающий гарантированную доставку данных с установлением виртуального соединения между программами, которым требуется использовать сетевые услуги. Установление виртуального соединения предполагает, что получатель готов к приему данных от конкретного отправителя. Это означает, что все параметры взаимодействия согласованы, и компьютер-получатель выделил соответствующие ресурсы для обеспечения приема.

Протокол UDP (User Datagram Protocol) - протокол, обеспечивающий негарантированную доставку данных без установления виртуального соединения между программами, которым требуется использовать сетевые услуги. Протокол IP обеспечивает доставку данных между двумя (или более) компьютерами. Однако на одном узле может функционировать параллельно несколько программ, которым требуется доступ к сети. Следовательно, данные внутри компьютерной системы должны распределяться между программами. Поэтому, при передаче данных по сети недостаточно просто адресовать конкретный узел. Необходимо также идентифицировать программу-получателя, что невозможно осуществить средствами сетевого уровня. Другой серьезной проблемой IP является невозможность передачи больших массивов данных. Протокол IP разбивает передаваемые данные на пакеты, каждый из которых передается в сеть независимо от других. В случае если какие-либо пакеты потерялись, то модуль IP на принимающей стороне не сможет обнаружить потерю, т.е. нарушение целостности общего массива данных. Для решения этих проблем разработаны протоколы транспортного уровня TCP и UDP. Идентификация программ в протоколах TCP и UDP обеспечивается уникальными числовыми значениями, так называемыми **номерами портов.** Номера портов назначаются программам в соответствии с ее функциональным назначением на основе определенных стандартов.

Для каждого протокола существуют стандартные списки соответствия номеров портов и программ. Так, например, программное обеспечение WWW, работающее через транспортный протокол TCP, использует TCP-порт 80, а служба DNS взаимодействует с транспортными протоколами TCP и UDP через TCP-порт 53 и UDP-порт 53 соответственно. Таким образом, протокол сетевого уровня IP и транспортные протоколы TCP и UDP реализуют двухуровневую схему адресации: номера TCP- и UDP-портов позволяют однозначно идентифицировать программу в рамках узла, однозначно определяемого IP-адресом. Следовательно, комбинация IP-адреса и номера порта позволяет однозначно идентифицировать программу в сети Интернет. Такой комбинированный адрес называется **сокетом** (socket).



9.2.8. Протоколы верхних уровней

К верхним уровням относят протоколы сеансового, представительного и прикладного уровней. *Сеансовый уровень*. Здесь производится организация способов взаимодействия между прикладными процессами пользователей, т.е. управление взаимодействием между открытыми системами. В качестве примеров протоколов сеансового уровня можно рассматривать стандарт X.225 – "Спецификация протокола сеансового уровня взаимосвязи открытых систем для применений МККТТ", разработанный МСЭ-Т и стандарт ISO 8327 "Системы обработки информации. Взаимосвязь открытых систем. Базовая спецификация протокола сеансового уровня, ориентированная на соединение". *Представительный уровень*. Определяет синтаксис передаваемой информации, т.е. набор знаков и способы их представления, которые являются понятными для всех взаимодействующих систем. Это процесс согласования различных кодов, согласно ему взаимодействующие системы договариваются о той форме, в которой будет передаваться информация. Примером протоколов представительного уровня являются: X.226 "Спецификация протокола уровня представления взаимосвязи открытых систем для применения МККТТ" и стандарт ISO 8823 "Системы обработки информации. Взаимосвязь открытых систем. Спецификация протоколов уровня представления в режиме управления соединением". *Прикладной уровень*. Определяет семантику, т.е. смысловое содержание информации, которой обмениваются открытые системы. Примером стандарта прикладного уровня может служить стандарт МСЭ-Т X.400.

9.4. Протокол IPX/SPX.

Протокол IPX/SPX (IPX/SPX protocol) **—** пара протоколов, обеспечивающая передачу данных в сети NetWare. Протоколы в базовой эталонной модели взаимодействия открытых систем соответствуют сетевому уровню и транспортному уровню. Задачей протокола Межсетевого пакетного обмена IPX является установление структуры и процедур передачи пакетов между абонентскими системами сети NetWare. Протокол определяет передачу отдельных пакетов - датаграмм. Доставка каждой из них не гарантируется. Поэтому при использовании IPX системы должны иметь Программное Обеспечение (ПО), которое обеспечивает управление передачей и запрашивает потерянные пакеты. Функцию управления передачей выполняет протокол Последовательный пакетный обмен SPX. Он осуществляет передачу последовательностей пакетов. При использовании протокола SPX в начале каждого сеанса между взаимодействующими системами выполняются процедуры, связанные с созданием соединения. По нему осуществляется управление передачей последовательности пакетов, их проверка и повторная передача пропавших пакетов либо пакетов, в которых появились ошибки. В протоколе IPX/SPX заложены те же идеи, что в протоколе управления передачей/межсетевом протоколе.

9.5. Протокол управления передачей/межсетевой протокол.

Протокол управления передачей/межсетевой протокол (Transmission Control Protocol/Internet Protocol (TCP/IP)) **—** пара взаимосвязанных протоколов транспортного уровня и сетевого уровня. Агентство DARPA в начале семидесятых годов разработало сеть ARPANET, в основу которой была положена пара протоколов TCP/IP. Затем, эти протоколы были приняты в качестве стандарта в коммуникационных сетях Министерства обороны США. Глобальная сетевая среда, определяемая TCP/IP и состоящая из соединенных сетей, получила название сети Internet. Протоколы TCP/IP располагаются между протоколами верхних уровней и канальным уровнем. Протокол TCP организует создание виртуальных каналов, проходящих через коммуникационную сеть. В соответствии с этим, TCP относят к транспортному уровню области Взаимодействия Открытых Систем (ВОС). Протокол IP ориентирован на использование одиночных пакетов, именуемых дейтаграммами. Его задачей является обеспечение взаимодействия сетей друг с другом и выполнение процессов, связанных с коммутацией и маршрутизацией. Для этого IP передает дейтаграммы из одной сети в другую. IP относят к сетевому уровню. Задачей TCP является предоставление сервиса передачи дейтаграмм, гарантируя упорядоченную доставку последовательностей блоков данных несмотря на возможные их повреждения, потери, дублирование, нарушение последовательности. TCP имеет три фазы работы: установление соединения, передача по нему дейтаграмм, разъединение соединения. Так как межсетевой протокол IP ненадежен, то TCP является сложным протоколом, обеспечивающим высокую степень надежности передачи данных.

Протокол IP, осуществляет реализацию коммуникационных аспектов:

- присвоение, контроль и преобразование имен объектов сетей;
- сообщения о состояниях: недостижимость адресатов, ошибки и запросы повторных вызовов;
- обеспечение обмена данными через шлюзы;
- управление передачей и сбор данных о работе сетей;
- изменение размеров передаваемых дейтаграмм (их фрагментация).

Успех продуктов TCP/IP связан с тем, что благодаря современному техническому развитию микропроцессоров стала возможной их эффективная реализация.

Контрольные вопросы:

1. Дать определение стека протоколов.
2. На какие уровни разбиваются стеки протоколов?
3. Назвать наиболее популярные сетевые протоколы.
4. Назвать наиболее популярные транспортные протоколы.
5. Назвать наиболее популярные прикладные протоколы.
6. Перечислить наиболее популярные стеки протоколов.
7. Чем отличается протокол TCP от UDP?
8. Какие существуют виды адресации в IP-сетях?
9. Какой протокол используется для управления сообщениями Интернета?
10. Назначение уровня сетевого интерфейса стека TCP/IP.

Практические задания:

ЗАДАНИЕ № 9.1. ***Установка протокола NetBEUI.***

*Операционные системы Windows XP и Windows Server 2003 не поддерживают сетевой протокол NetBEUI. Данный протокол не включен в список сетевых протоколов устанавливаемых при инсталляции Windows.*При обновлении предыдущей версии Microsoft Windows с установленным протоколом NetBEUI мастер проверки совместимости выводит сообщение о том, что протокол NetBEUI будет удален при обновлении операционной системы, т.к. является несовместимым с Windows XP.

Однако, возможность установки протокола NetBEUI в Windows XP существует. На установочном компакт-диске присутствуют файлы Netnbf.inf и Nbf.sys, необходимые для его установки. Чтобы установить протокол NetBEUI выполните следующие действия:

1. Нажмите кнопку Пуск, откройте Панель управления и выберите элемент панели управления Сетевые подключения.
2. Щелкните правой кнопкой мыши по значку сетевой платы, для которой необходимо добавить протокол NetBEUI, и в контекстном меню выберите пункт Свойства.
3. Перейдите на вкладку Главная и нажмите кнопку Установить.
4. В списке сетевых компонентов выберите Протокол и нажмите кнопку Добавить.
5. Нажмите кнопку Установить с диска, вставьте установочный компакт-диск Windows XP, в окне обзора откройте папку Valueadd\msft\net\netbeui, выберите файл Netnbf.inf и нажмите кнопку Открыть.
6. Нажмите кнопку ОК. В окне «Выбор сетевого протокола» нажмите кнопку ОК для завершения установки.

ЗАДАНИЕ № 9.2. Схемы адресации ресурсов Internet. Схема HTTP.

Существует 8 схем адресации ресурсов Internet. В схеме указывается ее идентификатор, адрес машины, TCP-порт, путь в директории сервера, переменные и их значения, метка. Изучить предложенные ниже схемы

Схема HTTP. Это основная схема для WWW. В схеме указывается ее идентификатор, адрес машины, TCP-порт, путь в директории сервера, поисковый критерий и метка.

Синтаксис:

http://[<user>[:<password]>@]<host>[:<port>][/[<url-path>][?<query>]]

http - название схемы

user - имя пользователя

password - пароль пользователя

host - имя хоста

port - номер порта

url-path - путь к файлу и сам файл

query (<имя-поля>=<значение>{&<имя-поля>=<значение>) - строка запроса

По умолчанию, port=80.

Приведем несколько примеров URI для схемы HTTP:

http://polyn.net.kiae.su/polyn/manifest.html

Это наиболее распространенный вид URI, применяемый в документах WWW. Вслед за именем схемы (http) следует путь, состоящий из доменного адреса машины и полного адреса HTML-документа в дереве сервера HTTP.

В качестве адреса машины допустимо использование и IP-адреса:

http://144.206.160.40/risk/risk.html Если сервер протокола HTTP запущен на другой, отличный от 80 порт TCP, то это отражается в адресе:

http://144.206.130.137:8080/altai/index.html

При указании адреса ресурса возможна ссылка на точку внутри файла HTML. Для этого вслед за именем документа может быть указана метка внутри документа:

http://polyn.net.kiae.su/altai/volume4.html#first

ЗАДАНИЕ № 9.3. Схемы адресации ресурсов Internet. Схема FTP.

Схема FTP. Данная схема позволяет адресовать файловые архивы FTP из программ-клиентов World Wide Web. При этом программа должна поддерживать протокол FTP. В данной схеме возможно указание не только имени схемы, адреса FTP-архива, но и идентификатора пользователя и даже его пароля.

Синтаксис:

ftp://[<user>[:<password]>@]<host>[:<port>][/<url-path>]

ftp - название схемы

user - имя пользователя

password - пароль пользователя
host - имя хоста
port - номер порта
url-path - путь к файлу и сам файл
По умолчанию, port=21, user=anonymous, password=email-адрес.
Наиболее часто данная схема используется для доступа к публичным архивам FTP:
ftp://polyn.net.kiae.su/pub/0index.txt
В данном случае записана ссылка на архив "polyn.net.kiae.su" с идентификатором "anonymous" или "ftp" (анонимный доступ). Если есть необходимость указать идентификатор пользователя и его пароль, то можно это сделать перед адресом машины:
ftp://nobody:password@polyn.net.kiae.su/users/local/pub
В данном случае эти параметры отделены от адреса машины символом "@", а друг от друга двоеточием.

ЗАДАНИЕ № 9.4. Схемы адресации ресурсов Internet. Схема TELNET.

Схема TELNET. По этой схеме осуществляется доступ к ресурсу в режиме удаленного терминала. Обычно клиент вызывает дополнительную программу для работы по протоколу telnet. При использовании этой схемы необходимо указывать идентификатор пользователя, допускается использование пароля.
Синтаксис:
telnet://[<user>[:<password]>@]<host>[:<port>]/
telnet - название схемы
user - имя пользователя
password - пароль пользователя
host - имя хоста
port - номер порта
По умолчанию, port=23.
Пример: telnet://name:password@ipm.kstu.ru
Реально, доступ осуществляется к публичным ресурсам, и идентификатор и пароль являются общеизвестными, например, их можно узнать в базах данных Hytelnet.
telnet://guest:password@apollo.polyn.kiae.su
Из приведенных выше примеров видно, что спецификация адресов ресурсов URI является довольно общей и позволяет проидентифицировать практически любой ресурс Internet. При этом число ресурсов может расширяться за счет создания новых схем.

ЗАДАНИЕ № 9.5. Схемы адресации ресурсов Internet. Схема работы WWW сервера.

Схема работы WWW сервера. WWW сервер - это такая часть глобальной или внутрикорпоративной сети, которая дает возможность пользователям сети получать доступ к гипертекстовым документам, расположенным на данном сервере. Для взаимодействия с WWW сервером пользователь сети должен использовать специализированное программное обеспечение - броузер (от англ. browser) - программа просмотра.
Рассмотрим более схему работы WWW-сервера:
1. Пользователь сети запускает броузер**,** в функции которого входит:
- установление связи с сервером;
- получение требуемого документа;
- отображение полученного документа;
- реагирование на действия пользователя - доступ к новому документу.

После запуска броузер по команде пользователя или автоматически устанавливает связь с заданным WWW - сервером и передает ему запросполучение заданного документа.

2. WWW сервер ищет запрашиваемый документ и возвращает результаты броузеру.
3. Броузер, получив документ, отображает его пользователю и ожидает его реакции. Возможные варианты:
- ввод адреса нового документа;
- печать, поиск, другие операции над текущим документом;
- активизация (нажатие) специальных зон полученного документа, называемых связями (link) и ассоциированными с адресом нового документа. В первом и третьем случае происходит обращение за новым документом.

Перечень литературы и Интернет-ресурсов:
1. Блэк Ю. Сети ЭВМ: протоколы, стандарты, интерфейсы.- М.: Мир, 1990.
2. Документация по TCP|IP — http://lemoi-www.dvgu.ru/lect/protoc/tcpip/main.htm
3. Комер Д. "Межсетевой обмен с помощью TCP/IP" — http://lemoi-www.dvgu.ru/lect/protoc/tcpip/comer/pref.htm
4. Олифер В.Г., Олифер Н.А. Новые технологии и оборудование IP-сетей. - СПб.: БХВ - Санкт-Петербург, 2000. - 512 с.
5. Основы построения объединенных сетей — http://www.citforum.ru/nets/ito/index.shtml
6. Протокол TCP — http://lemoi-www.dvgu.ru/lect/protoc/tcpip/tcp/tcp.htm
7. Семенов Юрий Алексеевич. Протоколы и ресурсы Internet . -М.: Радио и связь,1996-320с.: ил.
8. Telecommunication technologies - телекоммуникационные технологии — http://www.opennet.ru/docs/RUS/inet_book/
9. Уолрэнд Дж. Телекоммуникационные и компьютерные сети: Вводный курс / Пер. с англ.- М.: Постмаркет, 2001.- 480с.
10. Учебник по компьютерным сетям. Сетям — http://kompset.narod.ru/siteunior.html

Тема 10. Сетевые службы

Цели:

· Получить представление о сетевых службах и сервисах.
· Научиться идентифицировать информационные сети.
· Научиться классифицировать сетевые службы, согласно МОС.
· Получить представление об открытых информационных систем.
· Научиться определять тип сети, подходящий для решения конкретной задачи.

Сетевая служба Network service.

Сетевая служба - прикладная программа, которая:
- взаимодействует в сети с клиентами, серверами и данными;
- управляет процедурами распределенной обработки данных;
- информирует пользователей о происходящих в сети изменениях.

Сетевая служба:
- использует сервис, предоставляемый областью взаимодействия; и
- обеспечивает связь прикладных процессов, расположенных в различных абонентских системах сети.

Сетевые протоколы фактически управляют сетью, указывая сетевым устройствам, что они должны делать. Сетевые протоколы - это набор правил по которым работает сеть. Для передачи информации по сети, компьютеры должны использовать один и тот же набор правил, т.е. единый сетевой протокол.

Сетевые службы предназначены для выполнения определенных функций, в рамках действующего протокола, например служба разрешения имен, служба автоматического выделения адресов и т.д.

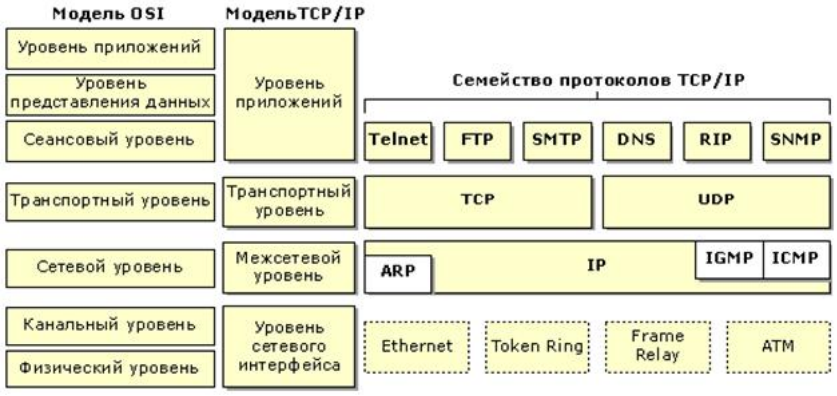
Существует множество типов сетевых протоколов, работающих в разных сетях и на разных уровнях модели OSI. Вот некоторые из них:

· TCP/IP;
· NetBEUI;
· IPX/SPX;
· NWLink;
· Apple Talk;
· DLC.

Протоколы удаленного доступа В состав операционных систем Windows входит служба Routing and Remote Access Service (RRAS), которая позволяет удаленным клиентам прозрачно подключаться к удаленному серверу. Служба RRAS поддерживает три протокола удаленного доступа:

· **Point-to-Point Protocol** (PPP) - стандартизованный набор протоколов обеспечивающий:
o механизм согласования параметров устройств передачи данных;
o механизм сжатия передаваемой информации с целью повышения эффективности и надежности передачи;
o механизм обнаружения и исправления ошибок;
o механизмы защиты, предотвращающие несанкционированные подключения.
· **Serial Line Internet Protocol** (SLIP) - простой протокол, не располагающий средствами обнаружения ошибок, возникающих при передаче данных, и позволяющий использовать только один протокол сетевого уровня - IP, что делает его малоэффективным.
· **Asynchronous NetBEUI** (AsyBEUI) - протокол службы удаленного доступа Microsoft, известный также как асинхронный NetBEUI; применяется устаревшими клиентами удаленного доступа под управлением Windows NT, Windows 3.1, Windows for Workgroups, MSDOS и LAN Manager.

Стек протоколов TCP/IP. Стек TCP/IP - набор протоколов, разработанных для обеспечения взаимосвязи различных устройств в сети Интернет. Стек включает следующие протоколы:



Протокол реализуется устройствами, или программами. В обоих случаях говорят о протокольных реализациях. Естественно, что различные производители и программисты создают разные протокольные реализации одного и того же протокола. Поэтому возникает проблема корректной конформности — отображения языка стандарта в язык программирования. Корректность работы реализации определяется ее тестированием на предмет соответствия протоколу. Тестирование должно проводиться независимой организацией, не участвовавшей в создании устройства либо программы. Для обеспечения гарантии

того, что данный протокол выполняет указанные требования, он подвергается верификации и сертификации. Стандарт по взаимодействию вычислительных систем принят международной организацией по стандартизации (МОС, английская аббревиатура ISO), а позднее - Международным консультативным комитетом по телефонии и телеграфии (МККТТ, современное название этой организации - Международный союз электросвязи МСЭ-Т), под номером X.200. Помимо вышеупомянутых МОС и МСЭ-Т, стандартизацией в области электросвязи занимаются также:

1) ANSI— American National Standards Institute (Американский национальный институт стандартов);
2) EIA— Electronic Industries Association (Ассоциация электронной индустрии);
3) ECMA— European Computer Manufactories Association (Европейская ассоциация производителей ЭВМ);
4) IEEE— Institute of Electronic and Electrical Engineers (Институт инженеров по электронике и электротехнике);
5) Госстандарт Российской Федерации.

Сетевая служба — вид сервиса, предоставляемого сетью. Сетевая служба – это совокупность серверной и клиентской частей ОС, предоставляющая доступ к конкретному типу ресурса через сеть, например файловой службе, службе печати, службе удаленного доступа и т. д. Каждая служба предоставляет пользователю набор услуг (сетевых сервисов).

Сервис — процесс обслуживания объектов. Сервис – это интерфейс между потребителем услуг и поставщиком услуг (службой). Сервис предоставляется пользователям, программам, системам, уровням, функциональным блокам и другим объектам сети. Наиболее распространенными видами сервиса являются:

- хранение данных и поиск информации;
- передача сообщений и блоков данных;
- электронная почта и речевая почта;
- организация и управление диалогом партнеров;
- предоставление соединений;
- проведение сеансов взаимодействия прикладных процессов.

Сервис осуществляют сетевые службы. В последние годы особенно быстро развивается видеосервис: видеодиалог, видеоконференции, видеобиблиотеки, видеопочта, телевидение. В телефонии предоставляется так называемый дополнительный сервис.

В базовой эталонной модели взаимодействия открытых систем объекты N-уровня предоставляют сервис объектам N+1 уровня. Он осуществляется благодаря передаче между уровнями специальных блоков данных, именуемых сервисными примитивами. Благодаря этому, прикладные процессы в своем взаимодействии используют суммарный сервис, предоставляемый всеми семью уровнями области взаимодействия.

Сетевая служба может располагаться на сеансовом уровне, представительном уровне, прикладном уровне и предоставлять сервис пользователям и прикладным процессам. Современная сетевая служба, как правило, располагается на прикладном уровне. Вместе с этим, нередко она охватывает также представительный уровень. Во всех случаях сетевая служба не зависит от типа используемой коммуникационной сети.

Одной из первых сетевых служб явилась телефония. Первоначально для ее работы создавалась специальная телефонная сеть. Аналогично этому, для телевидения использовалась телевизионная сеть. Протоколы обеих сетей были предназначены для одного вида сервиса. Позже к этим сетям стали подключать и компьютеры. Однако, между компьютерами и сетью ставились модемы, чтобы сигналы первых соответствовали стандартам последних. С созданием современных многоцелевых коммуникационных сетей ситуация резко изменилась. Различные сетевые службы стали опираться на общие этажерки протоколов.

Любая сетевая служба, используя сервис, предоставляемый областью взаимодействия, обеспечивает связь прикладных процессов, расположенных в различных абонентских системах сети. В свою очередь, служба выполняет сервис, который необходим для прикладных процессов. Например управление файлами, сообщениями. Поэтому сетевые службы являются платформами, на которых располагаются прикладные процессы. Это позволяет создавать Базы Данных (БД), Базы Знаний (БЗ), другие разнообразные службы, например, службы коммерческой информации. Последние определяются стандартами ISO, ITU, а также крупных фирм - производителей систем.

В сети работает значительное число различных служб. Все большее их число определяется стандартами Международной Организации Стандартов (МОС):

- сетевая служба справочной информации DS*;
- сетевая служба обмена электронными данными EDI;
- сетевая служба управления файлами и доступа к ним FTAM;
- сетевая служба передачи заданий и управления их выполнением JTM;
- сетевая служба электронной почты MHS/MOTIS;
- сетевая служба обработки и передачи документов ODA;
- сетевая служба управления сетью NMS;
- сетевая служба обеспечения стандартных форм работы терминалов VT.

Целям распределенной обработки данных служит прикладная служба. Появились также сетевые службы, определяемые фирменными стандартами, например, сетевая служба MMS, служба глобального соединения, сетевая служба ENS.

Особыми видами служб являются электронная библиотека, телетекст, видеотекст, факсимильная связь.

10.1. Сетевая служба DS.*

Сетевая служба DS* - сетевая служба справочной информации.

Сетевая служба DS* располагается на прикладном уровне и является вспомогательной, ибо предназначена для создания сетевой службы каталогов, выдачи справок и отображения адресов сетевых объектов (служб, Баз Данных (БД), прикладных процессов, ...) в физические.

Она имеет базу данных, которая расположена в одной либо нескольких абонентских системах. В последнем случае информационная база состоит из группы агентов сервиса (АС), расположенных в различных системах и взаимодействующих друг с другом в соответствии со специальным протоколом.

10.2. Сетевая служба EDI.

Сетевая служба EDI — сетевая служба обмена электронными данными.

Технология EDI, именуемая также Сервисом электронных писем ELS, представляет собой стандартный и не зависимый от платформ способ обмена деловыми документами (письмами, предложениями на поставку, заказами, счетами, накладными и т.д.) между предприятиями, фирмами, учреждениями. Она является важным направлением в электронном маркетинге, ибо обеспечивает возможность заключения сделок с помощью компьютеров и отслеживания поставок товаров.

Располагается EDI на прикладном уровне.

Средой, в которой используется EDI, часто является сетевая служба MHS/MOTIS. Между тем, EDI не зависит от MHS/MOTIS и может использовать любую другую среду передачи сообщений. EDI работает не только с текстами, но и с неподвижными изображениями, видеофильмами и фрагментами звука.

Предприятия, фирмы, корпорации часто используют свои стандарты на электронный обмен данными. В этих случаях Программное Обеспечение (ПО) EDI осуществляет преобразование фирменных форматов и синтаксис в стандартные и, наоборот, стандартные в фирменные. Ядром такого программного обеспечения является Электронная Таблица (ЭТ). Она отображает фирменные деловые документы в стандартные наборы трансакций.

Первоначально EDI использовалась в территориальных сетях. Теперь же эта технология применяется и в локальных сетях Из технологии обработки заказов EDI превратилась в комплексный универсальный элемент управления бизнесом. На основе EDI создаются даже автоматизированные электронные биржи.

10.3. Сетевая служба FTAM.

Сетевая служба FTAM - сетевая служба, обеспечивающая управление файлами и доступ к ним.

FTAM расположена на прикладном уровне, определена Международной Организацией Стандартов (МОС) и опирается на базовую эталонную модель взаимодействия открытых систем.

Располагается FTAM на верхнем подуровне прикладного уровня. FTAM обеспечивает взаимодействие в информационной сети разнотипных абонентских систем, которые имеют различные виды файлов, их форматы и состав операций с ними. Протокол FTAM основан на модели виртуальной Базы Данных (БД), определяемой стандартными процедурами и характеристиками.

FTAM предназначена для организации взаимодействия прикладных процессов, один из которых управляет базой данных, а другой работает с ее файлами. Первый процесс пассивен и отвечает на запросы второго. Второй же активен и является инициатором взаимодействия. В течении этого взаимодействия второй процесс получает доступ к файлам и осуществляет нужные действия над ними. Используемые во FTAM файлы являются стандартными. В каждой базе данных хранятся атрибуты и содержимое файлов, а также атрибуты режимов работы с файлами. Например, пароль доступа, метод обработки, форма управления соперничеством пользователей.

Пользователю виртуального файлохранилища FTAM предоставляет четыре вида сервиса:

- создание ассоциации взаимодействующих прикладных процессов;
- поиск и выбор файла;
- доступ к содержимому файла;
- пересылка файла из одной системы в другую.

10.4. Сетевая служба JTM.

Сетевая служба JTM — сетевая служба передачи заданий и управления их выполнением.

JTM работает в соответствии со стандартами ISO и оперирует с так называемыми виртуальными заданиями. Виртуальные задания, т.е. задания, удовлетворяющие принятыми в JTM требованиям, выполняются во всех, работающих со службой абонентских системах. В этом смысле служба выступает в роли компонента Сетевой Операционной Системы (СОС), выполняющего задания пользователей.

При работе с заданиями могут происходить различные отказы: прекращение взаимодействия, перегрузки, тупиковые ситуации. Служба следит за выполняемой работой и ликвидирует возникающие отказы. Эти действия осуществляются специальной подслужбой, называемой "Целостность, одновременность, восстановление" CCR. Подслужба CCR разработана не специально для JTM и используется в других службах, определяемых стандартами ISO. CCR начинает цикл действий, контролирует ход его выполнения, завершает работу либо возвращается, в случае отказа, к исходной точке.

Выполняемое задание делится на части. Задание может ветвиться и распространяться по информационной сети. Благодаря этому, JTM обеспечивает выполнение в сети любых прикладных процессов. Задания, в случае необходимости, могут передаваться из одной абонентской системы в другую. Для этого программы и файлы, необходимые для работы, должны находиться в выделенных для этой цели системах. Данные, полученные в результате выполнения задания, направляются в указанную пользователем абонентскую систему.

Сетевая служба JTM располагается в прикладной платформе на верхнем подуровне прикладного уровня.

10.5. Сетевая служба MHS/MOTIS.

Сетевая служба MHS/MOTIS — сетевая служба, обеспечивающая работу электронной почты.

Задачей Системы управления сообщениями MHS, определенной стандартом ITU-T, является хранение, копирование, передача и выдача адресатам самых разнообразных сообщений. При этом пользователь имеет возможность не только формировать и отправлять по необходимому ему адресу сообщение, но также выбирать вариант его доставки, устанавливать уровень защиты данных. О доставке сообщения пользователь получает подтверждение. Благодаря гибкой структуре MHS/MOTIS может размещаться в одной либо группе абонентских систем.

Важнейшими характеристиками сетевой службы являются межпользовательский обмен сообщениями, который, строго говоря, осуществляется не между системами, а между конкретными пользователями. Роль пользователей могут выполнять не только определенные лица, но и прикладные программы, находящиеся в системах, работающих с сетевой службой.

MHS/MOTIS выполняет для пользователей различные виды сервиса:

· редактирование сообщений;
· передача сообщений одному либо группе адресатов;
· вручение адресату сообщения в заранее указанное отправителем время;
· регистрация времени представления отправителем и получения адресатом сообщения;
· оповещение отправителя о доставке либо невозможности доставки сообщения;
· создание копий сообщения;
· обеспечение секретности содержимого сообщения;
· информация об изменении адресов, о появлении новых абонентов;
· ведение справочника пользователей (абонентов), их почтовых ящиков.

Непосредственно с электронной почтой связана сетевая служба DS* и служба электронного перевода денег EFT. Она предоставляет справочную информацию о пользователях службы MHS/MOTIS.

10.6. Сетевая служба NMS.

Сетевая служба NMS — сетевая служба, выполняющая процессы управления сетью.

NMS разработана Международной Организацией Стандартов (МОС) и располагается на прикладном уровне. Обеспечивая управление информационной сетью, эта служба определяет:

· функции управления;
· виды сервиса, предоставляемые для управления;
· структуру управляющей информации (термины и категории);
· протоколы, определяющие транспортировку управляющей информации.

Основная работа, связанная с управлением сетью, осуществляется Объектами административного управления (ОАУ), расположенными на всех уровнях области Взаимодействия Открытых Систем (ВОС).

Каждый уровень осуществляет собственное управление. Для этого объект административного управления получает всю необходимую ему информацию о работе своего уровня. Она содержит сведения о функционировании протоколов уровня, передаче сообщений, появляющихся ошибках, изменениях состояний, потоках данных. Объект административного управления осуществляет загрузку программ уровня, управляёт изменением протокольных параметров и ресурсов. NMS требует предоставления информации о работе всех уровней. Поэтому в системе создается группа взаимосвязанных Баз Данных (БД), состоящая из основной базы и баз (Б), находящихся на всех уровнях. Последние собирают сведения о работе уровней.

Прикладной сервисный объект системного управления SMASE является функциональным блоком, обеспечивающим обработку сведений, необходимых для работы управляющих прикладных процессов. Для этого прикладные объекты системного управления, расположенные во всех системах сети, обмениваются друг с другом необходимыми сообщениями. Эти объекты располагаются на верхнем подуровне (7Б) прикладного уровня и работают совместно с Сервисными объектами общей управляющей информации CMISE и Протоколом общей управляющей информации CMIP.

NMS обеспечивает работу Управляющих прикладных процессов, которые получают сведения от Прикладного сервисного объекта системного управления SMASE и Объектов Административного Управления (ОАУ) всех уровней системы. Управляющие прикладные процессы выполняют пять функций: определение неисправностей и ликвидация ошибок, поддержание высокой производительности, обеспечение безопасности данных, управление конфигурацией сети, учет работы сети и составление отчетов.

NMS обеспечивает управление не только сетью, но и входящими в нее системами. Для этого выполняются функции:

· формирование и модификация логической структуры систем, включая удаленную загрузку программ и установление изменяемых параметров;
· контроль за работой систем;
· сбор, обработка и регистрация сообщений о происходящих ошибках;
· анализ и локализация неисправностей;
· подключение при неисправностях альтернативных компонентов сети: каналов, процессоров,...;
· регистрация сведений, характеризующих работу систем;
· передача сведений персоналу сети.

Сетевая служба NMS может быть предназначена не только для управления одной сетью, но и обеспечения интегрального сетевого управления смешанными сетями. Служба располагается в административной системе, предназначенной для управления сетью. Агенты управления находятся во всех абонентских системах.

10.7. Сетевая служба ODA.

Сетевая служба ODA — сетевая служба, обеспечивающая обработку и передачу документов.

ODA располагается на прикладном уровне и определяет обмен документами (письмами, служебными записками, отчетами), которые могут содержать тексты, таблицы, изображения, речь. Документы могут редактироваться и их формат изменяться.

Архитектура документа определяет:

· взаимоотношение различных видов данных;
· информационную структуру документа (редактирование, форматирование, размещение в файле, ключевые слова, расположение столбцом,...);
· взаимосвязь документов: их группировка в зависимости от темы, адреса отправления либо назначения и т.д.

Содержание документа может быть представлено в следующих формах:

· символьный текст;
· растровые изображения;
· диаграммы (геометрическая графика);

· вычисляемые таблицы;
· звук (речевые аннотации).
· Распределение документов включает:
· кодирование документов и их частей;
· синтаксис передачи документов;
· методика передачи частей документов (например, только данных, необходимых для заполнения таблицы);
· удаленный интерактивный доступ к документам.

Сетевая служба ODA достаточно сложна. Поэтому в ней определяются подмножества, именуемые прикладными профилями документов. Важное значение для ODA имеют цветное изображение документов и их аудио-содержание (речевые аннотации). Новые возможности предоставляет динамическая графика, которая обеспечивает создание и обработку видеофильмов.

В прикладной платформе сетевая служба ODA расположена на верхнем подуровне прикладного уровня.

10.8. Сетевая служба VT.

Сетевая служба VT - сетевая служба, обеспечивающая стандартные формы работы терминалов в информационной сети.

Сетевая служба VT, определяемая стандартами ISO, располагается на прикладном уровне и заменяет собой большое множество программ эмуляции многочисленных терминалов, выпускаемых различными производителями.

В службе используется понятие виртуального терминала.

В соответствии с этим, реальные терминалы, используемые в информационной сети, должны быть отображены в виртуальный терминал. Естественно, что реальные терминалы имеют различные характеристики - экран, клавиатуру, набор и последовательность команд. Поэтому в абонентской системе должен быть функциональный блок, преобразующий эти характеристики в те, которые приняты в сетевой службе VT.

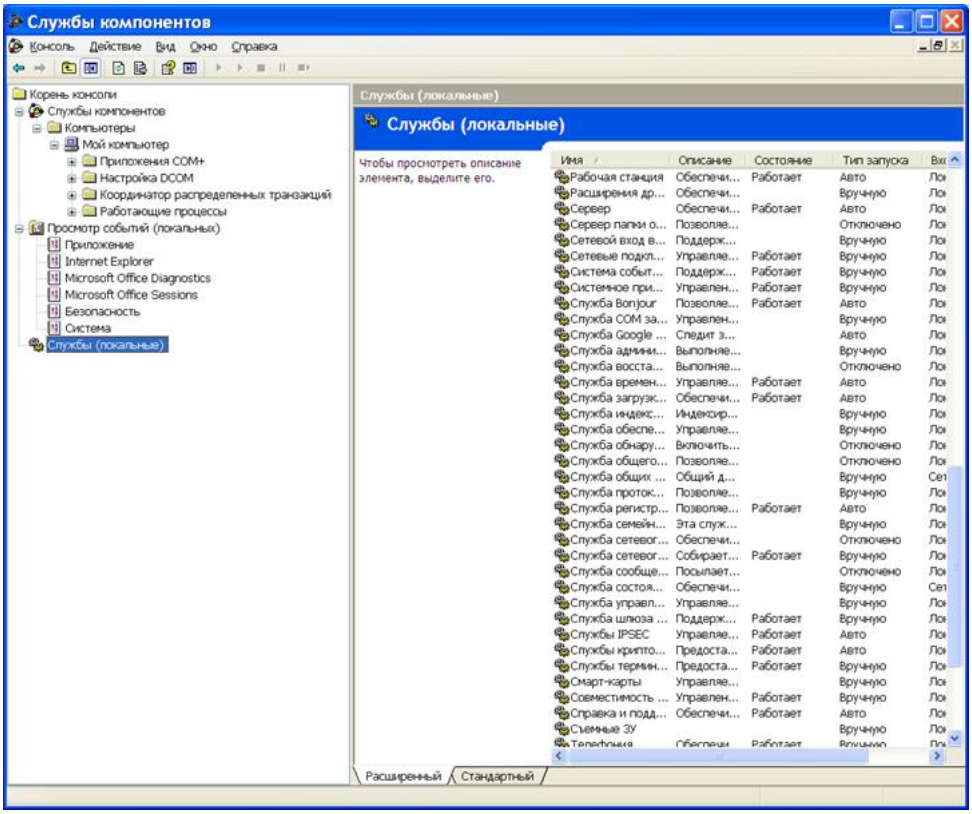
Контрольные вопросы:

1. Что такое сетевая служба?
2. Что такое сервис сетевой службы?
3. Рассказать об одной из первых сетевых служб – телефонная сеть.
4. Каким стандартом международным определяются сетевые службы? Перечислить другие стандарты, которые работаю со службами?
5. Назовите особенности сетевой службы справочной информации.
6. Назовите особенности сетевой службы обменом электронными данными.
7. Назовите особенности сетевой службы управлением файлами и доступом к ним.
8. Назовите особенности сетевой службы передачи заданий и управления их выполнением.
9. Назовите особенности сетевой службы обеспечивающей работу электронной почты.
10. Назовите особенности сетевой службы выполняющую процессы управления сетью.

Практические задания:

ЗАДАНИЕ № 10.1. Оснастка «Службы».

1. Чтобы открыть оснастку «Службы», нажмите кнопку **Пуск**, выберите команду **Панель управления**, щелкните категорию **Производительность и обслуживание**, щелкните значок **Администрирование**, затем дважды щелкните значок **Службы**.
2. Для выполнения этой процедуры необходимо войти в систему с учетной записью «Администратор» или члена группы «Администраторы». Если компьютер подключен к сети, то параметры сетевой политики могут запретить выполнение данной процедуры.
3. Если служба включена или отключена и возникли неполадки при запуске компьютера, возможно удастся запустить компьютер в ***безопасном режиме***. Затем можно изменить настройку службы или восстановить настройки по умолчанию. Для получения дополнительных сведений щелкните ссылку «См. также».
4. При установке флажка **Разрешить взаимодействие с рабочим столом** служба предоставляет пользователю интерфейс на рабочем столе. Эта возможность доступна только при установке переключателя в положение **С системной учетной записью** и только если служба настроена для взаимодействия с рабочим столом.



Чтобы настроить запуск службы:

1. Откройте оснастку **Службы.**
2. В области сведений выполните следующие действия.

a. Выберите службу. В меню **Действие** выберите команды **Пуск**, **Стоп**, **Остановка**, **Продолжение** или **Перезапуск**.

b. Щелкните команду правой кнопкой мыши и выберите команды **Пуск**, **Стоп**, **Остановка**, **Продолжение** или **Перезапуск**.

3. Щелкните правой кнопкой службу, которую требуется настроить, и выберите команду **Свойства**.
4. На вкладке **Общие** в поле **Тип запуска** выберите **Авто**, **Вручную** или **Отключено**.
5. Чтобы указать учетную запись пользователя, которую служба может использовать для входа в систему, выберите вкладку **Вход в систему** и выполните одно из следующих действий.

a. Чтобы указать использование службой учетной записи «Локальный компьютер», установите переключатель в положение **С системной учетной записью**.

b. Чтобы указать использование службой учетной записи «LocalService», установите переключатель в положение **С учетной записью** и введите **NTAUTHORITY\LocalService**.

c. Чтобы указать использование службой учетной записи «NetworkService», установите переключатель в положение **С учетной записью** и введите **NTAUTHORITY\NetworkService**.

d. Чтобы указать использование другой учетной записи, установите переключатель в положение **С учетной записью**, нажмите кнопку **Обзор** и укажите учетную запись пользователя в диалоговом окне **Выбор пользователей**. Для продолжения нажмите кнопку **ОК**.

6. Введите пароль для выбранной учетной записи в полях **Пароль** и **Подтверждение** и нажмите кнопку **ОК**.

v Важно!

· Изменение стандартной настройки служб может привести к неправильной работе ключевых служб. Особенно важно соблюдать осторожность при изменении параметров «Тип запуска» и «Вход в систему» для служб, настроенных для автоматического запуска.

· При остановке, запуске и перезапуске службы, оказывается влияние на любые зависимые от нее службы.

· Изменение стандартной настройки служб может привести к неправильной работе ключевых служб. Особенно важно соблюдать осторожность при изменении параметров «Тип запуска» и «Вход в систему» для служб, настроенных для автоматического запуска.

ЗАДАНИЕ № 10.2. Установка сетевой службы.

Для выполнения некоторых задач может потребоваться войти в систему с учетной записью «Администратор» или члена группы «Администраторы».

Службы предоставляют такие возможности, как совместный доступ к файлам и принтерам. Например, служба доступа к файлам и принтерам сетей Microsoft делает возможным доступ с других компьютеров к ресурсам на данном компьютере с помощью сети Microsoft. Ниже приведена процедура добавления сетевой службы на компьютер.

Чтобы добавить на компьютер сетевую службу, выполните следующие действия.

1. Откройте компонент Сетевые подключения.
2. В группе **ЛВС или высокоскоростной Интернет** щелкните значок **Подключение по локальной сети**.
3. В меню **Файл** выберите команду **Свойства**.
4. В диалоговом окне **Свойства: Подключение по локальной сети** нажмите кнопку **Установить**.
5. В диалоговом окне **Выбор типа сетевого компонента** выберите **Служба** и нажмите кнопку **Добавить**.

6. В диалоговом окне **Выбор сетевой службы** выберите службу, которую требуется установить, и нажмите кнопку **OK**.

v Примечания:

· Чтобы открыть компонент «Сетевые подключения», нажмите кнопку **Пуск**, выберите пункт **Панель управления**, а затем дважды щелкните значок **Сетевые подключения**.

· Для получения дополнительных сведений о работе с компонентом «Сетевые подключения» обращайтесь к меню **Справка** в окне «Сетевые подключения».

· Для получения дополнительных сведений щелкните ссылку **См. также**.

ЗАДАНИЕ № 10.3. Команды сетевых служб.

Рассмотреть несколько команд сетевых служб в «Центре справки и поддержки»

· ***Net accounts* —** Служит для обновления базы учетных данных пользователей, изменения паролей и параметров подключения для всех пользователей.

· ***Net compute* —** Служит для добавления или удаления имени компьютера из базы данных домена.

· ***Net config* —** Служит для вывода сведений о запущенных настраиваемых службах, а также просмотра и изменения параметров службы «Сервер» или «Рабочая станция». Команда **net config** без параметров выводит список настраиваемых служб.

· ***Net statistics* —** Вывод журнала статистики для служб локальной рабочей станции, сервера или запущенных служб, для которых доступна статистика. При использовании команды **net statistics** без параметров выводится список запущенных служб, для которых возможен вывод статистических сведений.

· ***Net continue* —** Служит для возобновления работы службы, приостановленной командой **net pause**.

· ***Net file* —** Вывод имен открытых общих файлов на сервере и количества блокировок для каждого файла, если они установлены. Также команда позволяет закрыть общий файл и удалить блокировки. Команда **net file** без параметров выводит список открытых файлов на сервере.

· ***Net group* —** Добавление, отображение и изменение глобальных групп в доменах.

· ***Net help* —** Служит для вывода списка команд и разделов, по которым можно получить справку, либо справки по указанной команде. Команда net help без параметров выводит список команд и разделов, по которым может быть получена справка.

· ***Net helpmsg***

· ***Net localgroup* —** Добавление, отображение и изменение локальных групп. Команда net localgroup без параметров выводит имя сервера и имена локальных групп компьютера.

· ***Net name***

· ***Net pause***

· ***Net print***

· ***Net send***

· ***Net session***

· ***Net share***

· ***Net stop***

· ***Net time***

· ***Net use***

· ***Net user***

· ***Net view***

Рассмотреть более подробно службу **Net Start.**

· ***Net start*** - Служит для запуска службы. При запуске команды **net start** без параметров выдается список запущенных служб.

Синтаксис.

net start [*служба*]

Запуск указанной службы. В следующей таблице перечислены значения атрибута *служба*.

Значение	Описание	Заметки
alerter	Запуск службы «Оповещатель».	u Служба Оповещатель позволяет отправлять сообщения отдельному пользователю или пользователям, подключенным к данному серверу. Эти сообщения служат для оповещения пользователей о проблемах безопасности, доступа и пользовательских сеансов. u Используйте диспетчер серверов (*системный_корневой_каталог*\System32\Srvmgr.exe) для указания администраторов, которые будут получать административные оповещения. Диспетчер серверов входит в состав только WindowsServer2000. u Оповещения отправляются с сервера на пользовательский компьютер как сообщения. Для приема оповещений на компьютере пользователя должна быть запущена служба сообщений.
browser	Запуск службы «Обозреватель компьютеров».	Служба «Обозреватель компьютеров» поддерживает текущий список компьютеров в локальной сети и предоставляет этот список запрашивающим его приложениям.
"Клиент для сетей NetWare"	Запуск службы «Клиент для сетей NetWare».	Эта команда доступна, только если установлена служба «Клиент для сетей NetWare».

"Сервер папки обмена"	Запуск службы «Сервер папки обмена».	u Служба «Сервер папки обмена» позволяет копировать и вставлять текстовые и графические данные по сети. u Служба «Сервер папки обмена» поддерживает окно папки обмена, с помощью которой можно просматривать страницы удаленных папок обмена.
dhcp client	Запуск службы «DHCP-клиент».	u Эта команда доступна, только если установлен протокол TCP/IP. u Служба «DHCP-клиент» поддерживает сетевую конфигурацию, запрашивая и обновляя IP-адреса и имена DNS. Служба «DHCP-клиент» поддерживает получение IP-адреса от DHCP-сервера. u Служба «DHCP-клиент» не может быть приостановлена или остановлена.
eventlog	Запуск службы «Журнал событий».	u Служба «Журнал событий» заносит в журнал сообщения о событиях, получаемые от программ и WindowsXP. Отчеты журнала событий содержат сведения, которые могут быть полезны при поиске причины неполадок. Эти отчеты можно просматривать в окне «Просмотр событий». Просмотр этих событий возможен только после запуска службы «Журнал событий». u Эту службу нельзя остановить или приостановить.
file replication	Запуск службы репликации файлов.	
messenger	Запуск службы сообщений.	u Эта служба позволяет компьютеру получать сообщения. u Сообщения отправляются компьютеру с использованием идентификационного имени компьютера.
netlogon	Запуск службы «Сетевой вход в систему».	u Служба «Сетевой вход в систему» проверяет запросы на подключение и управляет репликацией учетных записей пользователей в домене. u Служба «Сетевой вход в систему» должна быть запущена на всех серверах домена, где хранятся копии учетных данных пользователей.
"Поставщик поддержки безопасности NT LM"	Запуск службы «Поставщик поддержки безопасности NT LM».	Эта команда доступна после установки системы обеспечения защиты NT LM.
"plug and play"	Запуск службы «Plug and Play».	
"Диспетчер подключений удаленного доступа"	Запуск службы диспетчера подключений удаленного доступа.	Эта команда доступна, только если установлена служба удаленного доступа.
"Маршрутизация и удаленный доступ"	Запуск службы «Маршрутизация и удаленный доступ».	
rpclocator	Запуск службы «Локатор удаленного вызова процедур (RPC)».	u Эта служба позволяет распределенным приложениям использовать службу имени RPC Microsoft. u Служба «Локатор удаленного вызова процедур (RPC)» является службой имен RPC для Microsoft WindowsXP. Служба локатора RPC управляет базой данных службы имен RPC. u Серверная часть распределенного приложения регистрирует свою доступность с помощью службы локатора RPC. Клиентская служба распределенного приложения запрашивает службу локатора RPC для поиска доступного серверного компонента приложения.
rpcss	Запуск службы «Удаленный вызов процедур (RPC)».	u Служба «Удаленный вызов процедур (RPC)» является подсистемой удаленного вызова процедур WindowsXP. Эта подсистема включает определитель точек вызова и другие службы протокола RPC. Команда **Net start rpcss** запускает службу удаленного вызова процедур, что позволяет распределенным приложениям использовать динамические удаленные вызовы. Служба удаленного вызова процедур управляет базой данных регистрации распределенных приложений. u Серверная часть распределенного приложения регистрирует свое местоположение на сервере службы удаленного вызова процедур. Библиотека времени исполнения клиентской части приложения запрашивает службу удаленного вызова процедур для определения местоположения серверной части и получения информации о серверной части приложения. Сведения об использовании распределенным приложением службы определителя точек вызова должны быть приведены в документации к приложению.
schedule	Запуск службы	u Планировщик заданий позволяет запускать программы

	«Планировщик заданий».	в указанное время с помощью команды **at**. Перед запуском команд по расписанию может потребоваться запуск других служб. u Первоначально планировщик заданий настраивается на запуск всех программ с системной учетной записью на локальном компьютере. Запуск планировщика заданий с этой учетной записью позволяет выполнять любые программы без ограничений. Однако доступ к сети будет ограничен, так как системные привилегии на локальном компьютере могут не распознаваться другими компьютерами. u Для преодоления этого ограничения можно настроить планировщик заданий на запуск с учетной записью пользователя. В этом случае выполнение задач планировщиком заданий определяется правами доступа учетной записи пользователя. Однако, так как в этом случае планировщик заданий не имеет системных прав доступа в локальной системе, могут быть запущены только программы, не требующие вывода в окно.
server	Запуск службы «Сервер».	Пользователь имеет возможность применить службу сервера для совместного использования ресурсов сервера с другими пользователями сети.
spooler	Запуск службы «Диспетчер очереди печати».	Служба диспетчера очереди печати загружает файлы в память для печати.
"Модуль поддержки NetBIOS через TCP/IP"	Запуск службы поддержки NetBIOS через TCP, позволяющей работать службам NetBIOS через TCP/IP (NetBT).	u Службы NetBT поддерживают датаграммы NetBIOS, сеансы NetBIOS и управление именами NetBIOS (регистрацию имен и их разрешение в адреса) для приложений NetBIOS, использующих протокол TCP/IP. u Эта команда доступна, только если в свойствах сетевого адаптера в объекте Сетевые подключения в качестве компонента установлен **протокол Интернета (TCP/IP)**.
ups	Запуск службы «Источник бесперебойного питания».	u Служба бесперебойного питания управляет подключенным к компьютеру источником бесперебойного питания (ИБП). u Настройка службы бесперебойного питания задается в окне «Электропитание» панели управления. Если в настройке службы бесперебойного питания задается выполнение командного файла при выключении компьютера, то выполнение файла должно заканчиваться за 30 секунд. Большее время выполнения создает угрозу безаварийному завершению работы WindowsXP.
workstation	Запуск службы «Рабочая станция».	Эта служба позволяет компьютеру подключаться и использовать общие сетевые ресурсы.

Заметки.

· Набор отображаемых служб и приложений может изменяться в зависимости от параметров, выбранных при установке или настройке.

· Дополнительные сведения о службах на английском языке см. в руководстве «System Essentials Guide» на веб-узле корпорации Майкрософт.(http://www.microsoft.com/)

· Некоторые службы могут зависеть от других служб.

· Кроме того, для настройки автоматического запуска или остановки служб можно использовать оснастку «Службы». Эта оснастка позволяет запускать, останавливать, приостанавливать и возобновлять работу сетевых служб.

· Команду **Net start** можно использовать и для запуска служб, не входящих в состав WindowsXP.

· Если имя службы содержит пробелы, его следует заключать в кавычки (например **"*имяслужбы*"**).

Примеры.

Чтобы запустить службу клиента для сетей Netware, введите:

net start "Клиент для сетей NetWare"

ЗАДАНИЕ № 10.4. Оснастка управления службами *services.msc.*

Важную роль в сетевой настройки Windows XP может сыграть настройка системы служб. Управлять ими можно, вызвав оснастку управления службами через *Пуск ->Выполнить-> services.msc*. При стандартной установке тип запуска многих служб настроен как «авто», т.е. они автоматически запускаются при старте системы или при первом вызове службы. При настройке типа запуска службы «вручную» для задействования службы ее необходимо запустить вручную. Если тип запуска настроен как «отключено», службу нельзя запустить ни автоматически, ни вручную.

Многие службы зависимы от других, поэтому если отключить слишком много лишнего, то можно столкнуться с такой ситуацией, что не удастся включить все обратно. Чтобы этого избежать, советую, перед тем как производить эксперименты со службами, сохранить раздел реестра, отвечающий за запуск системных служб - [*HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServices*], например, щелкнув на указанном разделе правой кнопкой мыши и выбрав пункт «Экспортировать».

Далее указаны стандартные службы при обычной установке Windows XP Porfessional, их функции, рекомендации по изменению типа запуска служб, зависимости служб, а также тип запуска/вход от имени, действующие по умолчанию. Для

оптимизации работы системы часть служб можно подвергнуть отключению, причем внимание нужно обратить на службы с типом запуска «авто».

DHCP-клиент. Управляет конфигурацией сети посредством регистрации и обновления IP-адресов и DNS-имен. Если нет сети (ни локальной, ни модема), то можно отключить. Зависит от служб «NetBios через TCP/IP», «Драйвер протокола TCP/IP» и «Среда сетевой поддержки AFD». Тип запуска/Вход от имени - Авто/Локальная система.

DNS-клиент. Разрешает для данного компьютера DNS- имена в адресе и помещает их в кэш. Если служба остановлена, не разрешаются DNS-имена и нельзя разместить службу каталогов Active Directory контроллеров домена. Если Active Directory не используется и нет сети, службу можно отключить. Зависит от службы «Драйвер протокола TCP/IP». Тип запуска/Вход от имени - Авто/Сетевая служба.

NetMeeting Remote Desktop Sharing. Разрешает проверенным пользователям получать доступ к рабочему столу Windows, используя NetMeeting. Можно отключить. Тип запуска/Вход от имени - Вручную/Локальная система.

QoS RSVP. Обеспечивает рассылку оповещений в сети и управление локальным трафиком для QoS-программ и управляющих программ. Рекомендуется отключить. Простое отключение службы ни к чему не приведет - система по-прежнему будет резервировать 20% от канала связи. Поэтому поступаем следующим образом (под правами«Администратора»):

1. Запускаем оснастку «*Групповая политика*» (*Пуск -> Выполнить ->gpedit.msc*).
2. Далее раздел «*Конфигурация компьютера*» -> «*Административные шаблоны*» -> «*Сеть*» -> «*Диспетчер пакетов QoS*» -> «*Ограничить резервируемую пропускную способность*».
3. В открывшемся окне отметить пункт «Включен» и указать лимит канала в 0%. Затем ОК - и выходим из программы.
4. Заходим в свойства «Сетевого подключения», где на закладке Сеть убедимся, что протокол «Планировщик пакетов QoS» подключен. Если его там нет, то добавьте его (через кнопку «*Установить*»).
5. Перегружаем компьютер. Зависит от «*Драйвера протокола TCP/IP*», «*Среды сетевой поддержки AFD*» и «*Удаленного вызова процедур (RPC)*». Тип запуска/Вход от имени - Вручную/Локальная система.

Telnet. Позволяет удаленному пользователю входить в систему и запускать программы, поддерживает различных клиентов TCP/IP Telnet, включая компьютеры с операционными системами UNIX и Windows. Если эта служба остановлена, то удаленный пользователь не сможет запускать программы. Лучше отключить. Зависит от служб «Драйвер протокола TCP/IP», «Поставщик поддержки безопасности NT LM» и «Удаленный вызов процедур (RPC)». Тип запуска/Вход от имени - Вручную/Локальная система.

Беспроводная настройка. Предоставляет автоматическую настройку 802.11 адаптеров. Если таковых нет, тогда отключаем. Зависит от служб «Удаленный вызов процедур (RPC)» и «NDIS - протокол ввода/вывода пользовательского режима». Тип запуска/Вход от имени - Авто/Локальная система.

Брандмауэр Интернета (ICF) /Общий доступ к Интернету (ICS). Обеспечивает поддержку служб трансляции адресов, адресации и разрешения имен, предотвращает вторжение служб в домашней сети или сети небольшого офиса. Можно отключить, тем более что сторонние программы намного лучше справляются с такой же функцией. Зависит от служб «Диспетчер удаленного доступа», «Сетевые подключения», «Службы сетевого расположения (NLA)» и «Службы шлюза уровня приложения». Тип запуска/Вход от имени - Вручную/Локальная система.

Веб-клиент. Позволяет Windows-программам создавать, получать доступ и изменять файлы, хранящиеся в Интернете. Если отключить, то могут быть проблемы с FTP. Зависит от «Службы переадресации клиентов WebDav». Тип запуска/Вход от имени - Авто/Локальная служба.

Диспетчер подключений удаленного доступа. Создает сетевое подключение. Если есть модем, то оставляем »Вручную». Зависит от службы «Телефония». От данной службы зависят «Брандмауэр Интернета (ICF) /Общий доступ к Интернету (ICS)» и «Диспетчер авто-подключений удаленного доступа». Тип запуска/Вход от имени - Вручную/Локальная система.

Маршрутизация и удаленный доступ. Предлагает услуги маршрутизации организациям в локальной и глобальной сетях. Зависит от служб «NetBIOSGroup» и «Удаленный вызов процедур (RPC)». При отсутствии сети отключаем. Тип запуска/Вход от имени - Отключено/Локальная система.

Модуль поддержки NetBIOS через TCP/IP. Включает поддержку службы NetBIOS разрешения NetBIOS-имен в адреса. Зависит от служб «NetBIOS через TCP/IP» и »Среда сетевой поддержки AFD». Целесообразность отключения определяется наличием сети. Тип запуска/Вход от имени - Авто/Локальная служба.

Сервер. Обеспечивает поддержку общего доступа к файлам, принтерам и именованным каналам для локального компьютера через сетевое подключение. Отключаем, если не нужно. От данной службы зависит »Обозреватель компьютеров». Тип запуска/Вход от имени - Авто/Локальная система.

Сетевые подключения. Управляет объектами папки «Сеть и удаленный доступ к сети», отображающей свойства локальной сети и подключений удаленного доступа. Оставляем «Вручную», хотя, если нет сети и модема, то эту службу можно отключить. Зависит от службы «Удаленный вызов процедур (RPC)». А от данной службы зависит «Брандмауэр Интернета (ICF) /Общий доступ к Интернету (ICS)». Тип запуска/Вход от имени - Вручную/Локальная система.

Служба сетевого DDE. Обеспечивает сетевой транспорт и безопасность динамического обмена данными (DDE) для программ, выполняющихся на одном или на различных компьютерах. Если сети нет, то отключаем. Зависит от службы «Диспетчер сетевого DDE». От данной службы зависит «Сервер папки обмена». Тип запуска/Вход от имени - Вручную/ Локальная система.

Служба сетевого расположения (NLA). Собирает и хранит сведения о размещении и настройках сети, а также уведомляет приложения об их изменении. Опять же, если сети нет, то и нет надобности в этой службе. Зависит от служб «Драйвер протокола TCP/IP», «Среда сетевой поддержки AFD». А от данной службы зависит »Брандмауэр Интернета (ICF) /Общий доступ к Интернету (ICS)». Тип запуска/Вход от имени - Вручную/Локальная система.

Службы IPSEC. Сервис безопасности протокола TCP/IP. Если Вы не пользуетесь этим протоколом, то можно этот сервис выключить. Эта служба зависит от «Драйвер IPSEC» и «Драйвер протокола TCP/IP», «Удаленный вызов процедур (RPC)». Тип запуска/Вход от имени - Авто/Локальная система.

Службы терминалов. Раньше эта служба была доступна только в серверных вариантах ОС. Она позволяет подключаться к локальной машине по сети и удаленно работать на ней. В XP Pro эта служба предназначена для удаленного администрирования локального компьютера. Кроме этого, через эту службу работает переключение пользователей на одной машине (Switch User). Если эти возможности не нужны, то можете отключить эту службу. Зависит от компонента «Удаленный вызов процедур (RPC)».

Обратная зависимость от компонента «Совместимость быстрого переключения пользователей». Тип запуска/Вход от имени - Вручную/Локальная система.

Удаленный вызов процедур (RPC). Обеспечивает сопоставление конечных точек и иных служб RPC. От этой службы зависит более 39 компонентов, поэтому лучше не рисковать - оставляем как «Авто». Тип запуска/Вход от имени - Авто/Локальная система.

В заключение хочу отметить, что список служб может быть различным и зависит от компонентов, выбранных при установке, от дополнительных установленных программ. Необходимость того или иного сервиса определяется задачами, которые выполняются на конкретной машине, и установленным аппаратным обеспечением. Поэтому каждый должен сам решать, что можно отключить.

Перечень литературы и Интернет-ресурсов:

1. Андерсон К. с Минаси М. Локальные сети. Полное руководство. К.: ВЕК+, М.:ЭНТРОП, СПб.:КОРОНА 1999, 624 с.
2. Блэк Ю. Сети ЭВМ: протоколы, стандарты, интерфейсы. – М.: Мир, 1990.–506 с.
3. Бэрри Нанс. Компьютерные сети пер. с англ. – М.: БИНОМ, 1996.
4. Власов Ю.В., Рицкова Т.И. Лекция: Сетевые протоколы и службы http://www.intuit.ru/department/os/sysadmswin/10/
5. Вычислительные сети и сетевые протоколы/Д.Дэвис, Д.Барбер, У.Прайс, С.Соломонидес. – М. : Мир, 1982. – 564 с.
6. Жеретинцева Н.Н. Курс лекций по компьютерным сетям – Владивосток: ДВГМА, 2000. – 158 с.
7. Информационный портал - http://www.winline.ru/
8. Компьютерные сети: Учебный курс Microsoft Corporation – М.: Издательский отдел «Русская редакция», 1999.
9. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. (рекомендовано Мин. образования РФ). СПб: Питер, 2001,668 с.
10. Олифер В.Г., Олифер Н.А. Сетевые операционные системы. СПб.: Питер, 2001. 544 с.
11. Протоколы информационно-вычислительных сетей : Справочник / С.А. Аничкин, С.А. Белов, А.В. Бернштейн и др.; Под ред. И.А. Мизина, А.П. Кулешова. – М.: Радио и связь, 1990. – 504 с.
12. Протоколы TCP/IP Д. Комер "Межсетевой обмен с помощью TCP/IP" http://www.citforum.ru/internet/comer/contents.shtml.
13. Роль коммуникационных протоколов и функциональное назначение основных типов оборудования корпоративных сетей. Н. Олифер, В. Олифер, ЦИТ - http://www.citforum.ru/nets/protocols/index.shtml
14. Семейство протоколов TCP/IP - http://www.citforum.ru/internet/tcpip/index.shtml
15. Сетевые службы - http://vv303.narod.ru/files/inst/olifer/chapter10/default.htm
16. Службы и сетевые порты в серверных системах Microsoft Windows - http://support.microsoft.com/kb/832017/
17. Службы Windows XP - http://www.winblog.ru/2007/02/16/16020704.html
18. Стэн Шатт Мир компьютерных сетей пер. с англ. – К.: BHV, 1996 – 288 с.: – ISBN 5–7733–0028–1.
19. Технология корпоративных сетей. М. Кульгин. – СПб ПИТЕР, 1999.
20. Титтел Эд, Хадсон Курт, Дж. Майкл Стюард Networking Essentials – СПб ПИТЕР, 1999.
21. Титтел Эд, Хадсон Курт, Дж. Майкл Стюард TCP/IP – СПб ПИТЕР, 1999.
22. Якубайтис Э.А. Информационные сети и системы: Справочная книга. – М.: Финансы и статистика, 1996.

Тема 11. Модель распределенной обработки информации. Безопасность информации

Цели:

· Получить представление о распределённой обработки данных.

· Рассмотреть научно-технические принципы построения систем обеспечения безопасности информационных ресурсов информационных сетей с учетом современных тенденций развития сетевых информационных технологий.

· Изучить методы и средства анализа защищенности корпоративных сетей, технологии межсетевого экранирования.

11.1. Распределенная обработка данных.

Данные и обработка являются "распределенными" или "разделенными", если, выполнение операции требует использования нескольких процессоров. Термин "совместный" (cooperatif) является более специфическим: диалог между двумя прикладными системами с целью осуществления некой задачи. Основное назначение информационно-вычислительных сетей состоит в организации удобного и надежного доступа к ресурсам, распределенным в этой сети. Целью распределенной обработки данных является оптимизация использования ресурсов и упрощение работы пользователя. Необходимость распределенной обработки данных обусловлена территориальной удаленностью специалистов, участвующих в управлении организацией. Обработка данных, выполняемая на независимых, но связанных между собой компьютерах называется распределенная обработка данных. Основным назначением большинства информационно-вычислительных сетей является предоставление пользователям услуг в сфере информационного обслуживания.

Распределенная обработка данных — методика выполнения прикладных программ группой систем. Сущность DDP заключается в том, что пользователь получает возможность работать с сетевыми службами и прикладными процессами, расположенными в нескольких взаимосвязанных абонентских системах. При этом возможны несколько видов работ, которые он может выполнять: удаленный запрос, например, команда, позволяющая посылать одиночную заявку на выполнение обработки данных; удаленная транзакция, осуществляющая направление группы запросов прикладному процессу; распределенная транзакция, дающая возможность использования нескольких серверов и прикладных процессов, выполняемых в группе абонентских систем. Для распределенной обработки осуществляется сегментация прикладных программ — разделение сложной прикладной программы на части, которые могут быть распределены по системам локальной сети.

Сегментация осуществляется с помощью специального инструментального ПО, которое автоматизирует рассматриваемый процесс. С помощью технологии, предоставляемой объектно-ориентированной архитектурой в результате выполнения указанного процесса прикладная программа делится на самостоятельные части, загружаемые в различные системы. Благодаря этому, создается возможность перемещения программ из одной системы в другую и распределенной обработки данных. В результате сегментации каждая выделенная часть программы включает управление данными, алгоритм и блок презентации. Благодаря этому, она может быть оптимальным образом выполнена на основе платформ, используемых в сети. Передача данных для распределенной обработки происходит при помощи удаленного вызова процедур либо электронной почты. Первая технология характеризуется высоким быстродействием, а вторая - низкой стоимостью. Удаленный вызов процедур работает аналогично местному вызову процедур и обеспечивает организацию обработки данных. Этой цели служит механизм навигации в сети, поиска информации, запуска процесса в нескольких системах, передачи полученных результатов пользователям, пославшим запросы. Выполняемый процесс характеризуется прозрачностью. Выполнение удаленного вызова процедур является дорогостоящей операцией, ибо на все время ее выполнения системы, участвующие в работе, должны по каналам передавать данные друг другу. Альтернативной удаленного вызова является применение интеллектуальных агентов или выполнение распределенной обработки данных с использованием электронной почты. Этот метод не требует больших затрат, но работает значительно медленнее.

Известны также программные средства Системы Управления Распределенной Базой Данных (СУРБД), содержимое которой располагается в нескольких абонентских системах информационной сети. Задачей СУРБД является обеспечение функционирования распределенной базы данных. СУРБД должна действовать так, чтобы у пользователей возникла иллюзия того, что они работают с Базой Данных (БД), расположенной в одной абонентской системе. Использование СУРБД, по сравнению с группой невзаимосвязанных баз данных, позволяет сокращать затраты на передачу данных в информационной сети. СУРБД так распределяет файлы по сети, что в каждой системе хранятся те данные, которые чаще всего используются именно в этом месте. В СУРБД осуществляется тиражирование данных. Его сущность заключается в том, что изменение, вносимое в одну часть базы данных, в течение определенного времени отражается и в других частях базы. При планировании обработки данных могут рассматриваться три модели обработки: обработка в одноранговой локальной сети; централизованная обработка; обработка в модели клиент/сервер. При любой обработке имеются три основных уровня манипулирования данными: хранение данных; выполнение приложений, т.е. выборка и обработка данных для нужд прикладной задачи; представление данных и результатов обработки пользователю.

При обработке в одноранговой сети все три уровня, как правило, выполняются на одном - персональном - рабочем месте. В современных технологиях применения вычислительной техники персональная обработка информации, когда все данные и средства их обработки сосредоточены в пределах одного рабочего места, и обмен данными между рабочими местами не происходит или выполняется эпизодически (например, средствами электронной почты), постепенно уходит в прошлое. Современные информационные, управленческие, офисные системы в большей или меньшей степени ориентируются на многопользовательскую обработку, при которой данные доступны (возможно, одновременно доступны) многим пользователям с разных рабочих мест. Соображения эффективности и надежности требуют централизации процессов хранения и обработки данных. И централизованная обработка, и модель клиент/сервер в равной мере используют преимущества централизации. Различие между этими двумя моделями состоит в том, что при централизованной обработке представление информации конечному пользователю также выполняется средствами центральной вычислительной системы - на ее терминалах (неинтеллектуальных), подключенных к вычислительной системе через порты/каналы ввода-вывода. В модели же клиент/сервер терминалы, представляющие информацию, являются интеллектуальными - самостоятельными вычислительными системами (обычно ПЭВМ) и связаны с сервером через сетевые средства.

Вычислительный ресурс (это может быть отдельная ЭВМ в сети или отдельный процесс в многозадачной вычислительной системе), обеспечивающий хранение, администрирование, предоставление доступа к данным, называется сервером. Вычислительные ресурсы обеспечивающие использование данных и представление их конечному пользователю, называются клиентами. Вся модель, обеспечивающая такое распределение функций, называется моделью клиент/сервер. При перемещении

большей части функций манипулирования данными на высокопроизводительный и высоконадежный сервер могут быть обеспечены следующие *преимущества:* экономия вычислительных ресурсов всей системы в целом; экономия ресурсов средств коммуникаций; обеспечение работы всех пользователей с одной и той же копией данных; предотвращение фатальных конфликтов между клиентами при обращении их к одним и тем же данным; обеспечение надежного администрирования базы данных, в т.ч. резервного копирования и разграничения доступа к данным. Хотя централизованная обработка обеспечивает большую эффективность в сопровождении системы и в скорости обмена, предпочтительной все же представляется модель клиент/сервер, к числу достоинств которой следует отнести прежде всего гибкость - возможность строить клиентские рабочие места на разных платформах и в разных операционных средах и, таким образом, гибко приспосабливать возможности интеллектуального терминала АИРС к стоящим перед данным рабочим местом задачам.

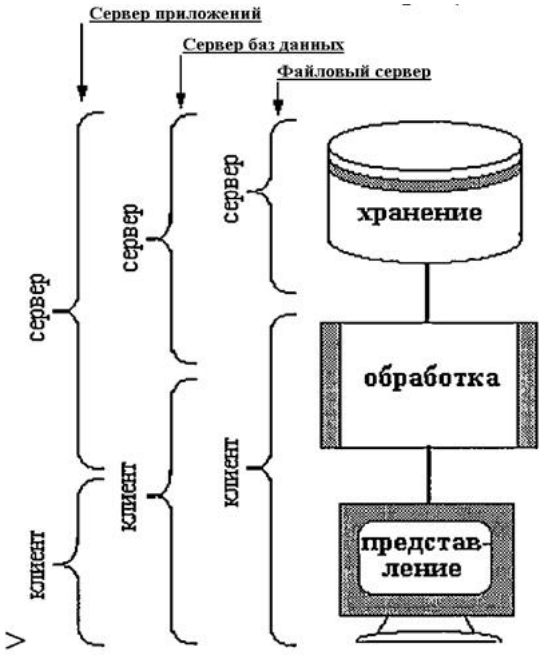


Рис. 11.1. Распределение функций манипулирования данными между клиентом и сервером

11.1.1. Технологии распределенных вычислений

Программное обеспечение (ПО) организации распределенных вычислений называют программным обеспечением *промежуточного слоя* (Middleware). Новое направление организации распределенных вычислений в сетях Internet-Intranet основано на создании и использовании программных средств, которые могут работать в различных аппаратно-программных средах. Совокупность таких средств называют *многоплатформенной распределенной средой* - MPC (crossware).

Находят применение технологии распределенных вычислений RPC (Remote Procedure Call), ORB (Object Request Broker), MOM (Message-oriented Middleware), DCE (Distributed Computing Environment), мониторы транзакций, ODBC.

RPC - процедурная блокирующая синхронная технология, предложенная фирмой Sun Microsystems. Вызов удаленных программ подобен вызову функций в языке С. При пересылках на основе транспортных протоколов TCP или UDP данные представляются в едином формате обмена XDR. Синхронность и блокирование означают, что клиент, обратившись к серверу, для продолжения работы ждет ответа от сервера. Для систем распределенных вычислений разработаны специальные языки программирования, для RPC это язык IDL (Interface Definition Language), который дает пользователю возможность оперировать различными объектами безотносительно к их расположению в сети. На нём можно записывать обращения к серверам приложений. Другой пример языка - NewEra в среде Informix. RPC входит во многие системы сетевого ПО.

ORB - технология объектно-ориентированного подхода, включает 13 пунктов (служб). Основные службы: служба именования, присваивает объектам уникальные имена, в результате пользователь может искать объект в сети; служба обработки транзакций, осуществляет управление транзакциями из приложений или из операционных систем; служба событий, обеспечивает асинхронное распространение и обработку сообщений о событиях; служба обеспечения безопасности - поддержки целостности данных. При применении ORB (в отличие от RPC) в узле-клиенте хранить сведения о расположении серверных объектов не нужно, достаточно знать расположение в сети программы-посредника ORB. Поэтому доступ пользователя к различным объектам существенно упрощен. Посредник должен определять, в каком месте сети находится запрашиваемый ресурс, направлять запрос пользователя в соответствующий узел, а после выполнения запроса возвращать результаты пользователю.

MOM - также объектная технология. Связь с серверами асинхронная. Это одна из наиболее простых технологий, включает команды "послать" и "получить", осуществляющие обмен сообщениями. Отличается от E-mail реальным масштабом времени. Однако могут быть варианты MOM с очередями, тогда режим on-line необязателен и при передаче не требуется подтверждений, т.е. опора на протокол IP без установления соединения.

11.1.2. Распределенная среда обработки данных

Таблица 12.1.

Основные компоненты DCE*

№ п/п	Служба	Выполняемые функции

1.	Имена	База Данных (БД) имен пользователей и средств, предназначенных для доступа пользователей к сетевым службам.
2.	Удаленный доступ	Технология, обеспечивающая взаимодействие двух прикладных программ, расположенных в различных абонентских системах.
3.	Защита данных	Программное Обеспечение (ПО) разрешения на доступ к ресурсам системы или сети.
4.	Многопоточность	Программы, обеспечивающие одновременное выполнение нескольких задач.

(Distributed Computing Environment (DCE*)) **—** технология распределенной обработки данных, предложенная фондом открытого программного обеспечения. Она не противопоставляется другим технологиям (RPC, ORB), а является средой для их использования. Среда DCE*, разработанная в 1990 г., представляет собой набор сетевых служб, предназначенный для выполнения прикладных процессов, рассредоточенных по группе абонентских систем гетерогенной (неоднородной) сети.

Системы, имеющие программы распределенной среды, соответственно, являются серверами и клиентами. Серверы связаны друг с другом логическими каналами, по которым передают друг другу файлы (рис.11.2.).

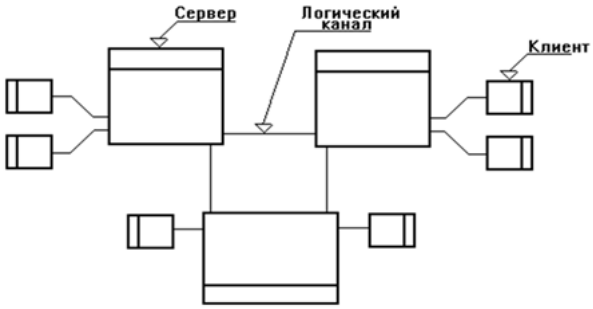


Рис. 11.2. Логическая структура среды DCE

Каждый сервер имеет свою группу клиентов. Среда имеет трехступенчатую архитектуру: прикладная программа **—** база данных **—** клиент.

Функции, выполняемые средой, включают прикладные службы: каталогов, позволяющую клиентам находить нужные им серверы; интерфейса многопоточной обработки; удаленного вызова процедур; обслуживания файлов; безопасности данных; времени, синхронизирующей часы в абонентских системах. Программное Обеспечение (ПО) среды погружается в Сетевую Операционную Систему (СОС). Серверы имеют свои, различные, Операционные Системы (ОС).

Функционирование распределенной среды требует выполнения ряда административных задач. К ним, в первую очередь, относятся средства:

- регистрации и контроля за лицензиями пользователей на работу с прикладными программами;
- унифицированных интерфейсов прикладных программ;
- обеспечения безопасности данных;
- инвентаризации программного и технического обеспечения абонентских систем, работающих в сети.

С точки зрения логического управления среда обработки данных делится на ячейки DCE*. В каждую из них может включаться от нескольких единиц до тысяч абонентских систем. Размеры ячеек территориально не ограничены. Входящие в одну и ту же ячейку системы могут быть расположены даже на разных континентах. В ячейках выполняются службы: контроля права работы с прикладными программами и базами данных; каталогов, назначающих адреса объектов; времени, синхронизирующей часы систем; лицензии, отслеживающей использование видов сервиса. Распределение прикладных процессов по ячейкам защищает от сбоев, позволяет приспособить процессы к конкретным нуждам групп пользователей. Последние могут иметь доступ только к определенным ячейкам.

11.2. Безопасность информационных сетей.

По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышается зависимость общества от степени безопасности используемых им информационных технологий. Цель ревизии средств защиты сети **—** это определение состава аппаратно-программного комплекса, требующегося для обеспечения защиты сети. Обеспечение информационной безопасности информационных систем и сетей является одним из ведущих направлений развития информационных технологий Актуальность и важность проблемы обеспечения информационной безопасности обусловлена следующими факторами:

u Современные уровни и темпы развития средств информационной безопасности значительно отстают от уровней и темпов развития информационных технологий.

u Высокие темпы роста парка персональных компьютеров, применяемых в разнообразных сферах человеческой деятельности.

u Резкое расширение круга пользователей, имеющих непосредственный доступ к вычислительным ресурсам и массивам данных;

u Значительное увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью компьютеров и других средств автоматизации;

u Многочисленные уязвимости в программных и сетевых платформах;

u Бурное развитие глобальной сети Интернет, практически не препятствующей нарушениям безопасности систем обработки информации во всем мире;

u Современные методы накопления, обработки и передачи информации способствовали появлению угроз, связанных с возможностью потери, искажения и раскрытия данных, адресованных или принадлежащих конечным пользователям.

Под ***угрозой*** безопасности понимается возможная опасность (потенциальная или реально существующая) совершения какого-либо деяния (действия или бездействия), направленного против объекта защиты (информационных ресурсов), наносящего ущерб собственнику или пользователю, проявляющегося в опасности искажения, раскрытия или потери информации. Реализацию угрозы в дальнейшем будем называть атакой.

Реализация той или иной угрозы безопасности может преследовать следующие цели: нарушение конфиденциальности информации; нарушение целостности информации; нарушение доступности (частичное или полное) работоспособности корпоративной сети.

11.2.1. Комплексный подход к обеспечению информационной безопасности

К основным способам обеспечения информационной безопасности относят:

1. ***Законодательные меры защиты*** определяются законодательными актами страны, которыми регламентируются правила использования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил. Применительно к России сюда относятся: Конституция РФ от 23 февраля 1996 года; Доктрина информационной безопасности РФ от 9 сентября 2000 г.; Кодексы РФ и Законы РФ; Указы Президента РФ и Постановления Правительства РФ; Государственные стандарты в области защиты информации (ГОСТы); Руководящие документы (РД).

2. ***К морально-этическим мерам*** противодействиям относятся нормы поведения, которые традиционно сложились или складываются по мере распространения сетевых и информационных технологий. Эти нормы большей частью не являются обязательными, однако несоблюдение их ведет обычно к потере авторитета и престижа человека. Данные нормы могут быть оформлены в некоторый свод правил и предписаний.

3. ***Организационные (административные) средства защиты*** представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации аппаратуры телекоммуникаций для обеспечения защиты информации. Организационные мероприятия охватывают все структурные элементы аппаратуры на всех этапах их жизненного цикла (строительство помещений, проектирование системы, монтаж и наладка оборудования, испытания и эксплуатация).

4. ***Технические средства*** реализуются в виде механических, электрических, электромеханических и электронных устройств, предназначенных для препятствования на возможных путях проникновения и доступа потенциального нарушителя к компонентам защиты. Вся совокупность технических средств делится *на аппаратные и физические* .***Под аппаратными техническими средствами*** принято понимать устройства, встраиваемые непосредственно в телекоммуникационную аппаратуру, или устройства, которые сопрягаются с подобной аппаратурой по стандартному интерфейсу. ***Физические средства*** реализуются в виде автономных устройств и систем. Например, замки на дверях, где размещена аппаратура, решетки на окнах, электронно-механическое оборудование охранной сигнализации.

5. ***Программные средства*** представляют из себя программное обеспечение, специально предназначенное для выполнения функций защиты информации. Программные средства и составляли основу механизмов защиты на первой фазе развития технологии обеспечения безопасности связи в каналах телекоммуникаций. При этом считалось, что основными средствами защиты являются программные. К данному классу средств защиты относятся: антивирусные, криптографические средства, системы разграничения доступа, межсетевые экраны, системы обнаружения вторжений и т.п.

11.2.2. Основные принципы обеспечения информационной безопасности

Построение системы защиты должно основываться на следующих основных принципах:

О Системность подхода. Комплексности решений.

О Разумная достаточность средств защиты.

О Разумная избыточность средств защиты.

О Гибкость управления и применения. Унификация средств защиты.

О Открытость алгоритмов и механизмов защиты.

О Простота применения защиты, средств и мер.

Система обеспечения безопасности информации должна иметь многоуровневую структуру и включать следующие уровни:

О уровень защиты автоматизированных рабочих мест (АРМ);

О уровень защиты локальных сетей и информационных серверов;

О уровень защиты корпоративной АС.

Защищенность является одним из важнейших показателей эффективности функционирования ИС, наряду с такими показателями как надежность, отказоустойчивость, производительность и т. п. Под защищенностью ИС будем понимать степень адекватности реализованных в ней механизмов защиты информации существующим в данной среде функционирования рискам, связанным с осуществлением угроз безопасности информации. Под угрозами безопасности информации традиционно понимается возможность нарушения таких свойств информации, как конфиденциальность, целостность и доступность.

Методы тестирования системы защиты

Тестирование системы защиты АС проводится с целью проверки эффективности используемых в ней механизмов защиты, их устойчивости в отношении возможных атак, а также с целью поиска уязвимостей в защите. Традиционно используются два основных метода тестирования:

О тестирование по методу «черного ящика»;

О тестирование по методу «белого ящика».

11.2.3. Сетевые сканеры

Основным фактором, определяющим защищенность ИС от угроз безопасности, является наличие в ИС уязвимостей защиты. Уязвимости защиты могут быть обусловлены как ошибками в конфигурации компонентов ИС, так и другими причинами, в число которых входят ошибки и программные закладки в коде ПО, отсутствие механизмов безопасности, их неправильное использование, либо их неадекватность существующим рискам, а также уязвимости, обусловленные человеческим фактором. Наличие уязвимостей в системе защиты ИС, в конечном счете, приводит к успешному осуществлению атак, использующих эти уязвимости. Сетевые сканеры являются, пожалуй, наиболее доступными и широко используемыми средствами анализа защищенности. Основной принцип их функционирования заключается в эмуляции действий потенциального злоумышленника по осуществлению сетевых атак. Поиск уязвимостей путем имитации возможных атак является одним из наиболее эффективных способов анализа защищенности ИС, который дополняет результаты анализа конфигурации по шаблонам, выполняемый локально с использованием шаблонов (списков проверки). Сканер является необходимым инструментом в арсенале любого администратора либо аудитора безопасности ИС. Существует два основных механизма, при помощи которых сканер безопасности проверяет наличи уязвимости - сканирование (scan) и зондирование (probe).

Современный сетевой сканер выполняет четыре основные задачи:

u Идентификацию доступных сетевых ресурсов;

u Идентификацию доступных сетевых сервисов;

u Идентификацию имеющихся уязвимостей сетевых сервисов;

u Выдачу рекомендаций по устранению уязвимостей.

11.2.4. Межсетевые экраны

МЭ называют локальное или функционально распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему и/или выходящей из неё. МЭ основное название, определенное в РД Гостехкомиссии РФ, для данного устройства. Также встречаются общепринятые названия брандмауэр и firewall (англ. огненная стена).

Выделяют следующую классификацию МЭ, в соответствие с функционированием на разных уровнях МВОС (OSI):

u Мостиковые экраны (2 уровень OSI);

u Фильтрующие маршрутизаторы (3 и 4 уровни OSI);

u Шлюзы сеансового уровня (5 уровень OSI);

u Шлюзы прикладного уровня (7 уровень OSI);

u Комплексные экраны (3-7 уровни OSI).

11.2.5. Системы обнаружения атак

Наряду со стандартными средствами защиты, без которых немыслимо нормальное функционирование ИС (таких как МЭ, системы резервного копирования и антивирусные средства), существует необходимость использования СОА (IDS, систем обнаружения атак или вторжений), которые являются основным средством борьбы с сетевыми атаками. Типовая архитектура системы выявления атак, как правило, включает в себя следующие компоненты:

v Сенсор (средство сбора информации);

v Анализатор (средство анализа информации);

v Средства реагирования;

v Средства управления.

11.2.6. Внутренние злоумышленники в информационных сетях. Методы воздействия.

Рассмотрим, при каких условиях легального сотрудника организации можно назвать внутренним нарушителем. Для эффективного функционирования организации необходимо, чтобы в ней имелась общая стратегия деятельности и четкие должностные инструкции каждому сотруднику. Следующим организационным документом должна ***быть политика безопасности*** организации, в которой изложены принципы организации и конкретные меры по обеспечению информационной безопасности предприятия. *Классификационный раздел* политики безопасности описывает имеющиеся в организации материальные и информационные ресурсы и необходимый уровень их защиты. В *штатном разделе* приводятся описания должностей с точки зрения информационной безопасности. Наконец, раздел, описывающий *правила разграничения доступа к корпоративной информации*, является ключевым для определения внутреннего нарушителя.

11.2.7. Концепция информационной безопасности

Основная цель концепции - определение методов и средств защиты и обеспечения безопасности информации, отвечающих интересам, требованиям и законодательству РФ в современных условиях необходимости использования ресурсов глобальных сетей передачи данных общего пользования для построения корпоративных защищенных и безопасных сетей. Концепция формулирует научно-технические принципы построения систем обеспечения безопасности информационных ресурсов корпоративных сетей (СОБИ КС) с учетом современных тенденций развития сетевых информационных технологий, развития видов сетевых протоколов, их взаимной инкапсуляции и совместного использования.

Контрольные вопросы:

1. Чем отличается технологии RPC, ORB, MOM, DCE, ODBC?
2. В чём состоит методика распределённой обработки данных в информационной сети?
3. Что такое угроза безопасности?
4. В чём заключается комплексный подход обеспечения информационной безопасности сети?
5. Какие методы тестирования системы защиты Вы знаете?

6. Как работает сетевой сканер?
7. Что такое защищённость сети?
8. Какова современная концепция информационной безопасности информационной сети. Есть ли она в МФПА?
9. Что такое система обнаружения атак?
10. Что такое внутренние злоумышленники?

Практические задания:

ЗАДАНИЕ № 11.1. Изобразить типовую архитектуру системы обнаружения атак (СОА), с помощью Microsoft Office Visio. В составе: межсетевой экран, хостовый и сетевой сенсор, средства управления, средства реагирования и сервер безопасности.

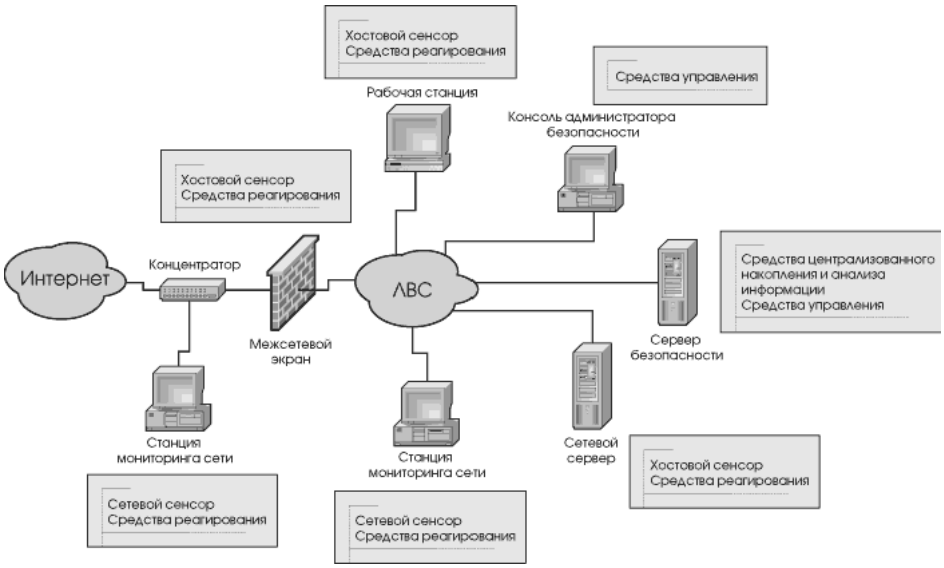


Рис. 11.3. Типовая архитектура СОА

ЗАДАНИЕ № 11.2. Создать виртуальную ловушку. В качестве виртуальной ловушки использовать эмуляцию полноценного компьютера со своей ОС. Такая эмуляция осуществляется с использованием специального ПО – виртуальной машины. Например,VMWare Workstation или Microsoft Virtual PC. Данные программы позволяют запускать на одном физическом компьютере множество ОС, полностью эмулируя их работу. Механизм подготовки виртуальной ловушки заключается в установке ОС, выделении ей IP-адреса из диапазона адресов корпоративной сети и присвоение имени. Имя можно подобрать так, чтобы в первую очередь привлечь внимание потенциального нарушителя, например, mailserver или domain. Возможно эмулирование некоторых сервисных служб на виртуальной ловушке. Причем для эмуляции можно воспользоваться описанными выше KFSensor или BOF. Эмулируемую систему можно намеренно оставить уязвимой для применения эксплойтов, с целью проникновения злоумышленника. Популярные виртуальные ловушки KFSensor и NFR Back Officer Friendly (BOF) способны эмулировать работу различных сервисов. Например, возможна эмуляция FTP-сервера, POP3-сервера, SMTP-сервера, TELNET-сервера, HTTP-сервера, SQL-сервера и многих других, в том числе серверной части троянской программы BackOrifice. При любой попытке доступа к данной службе выдается оповещение для администратора и протоколирование всей активности. Имеется возможность извещения администратора через электронную почту. KFSensor также предлагает разную степень эмуляции служб – от простой до максимально правдоподобной. С помощью принтскрина показать изображение программы-ловушки.

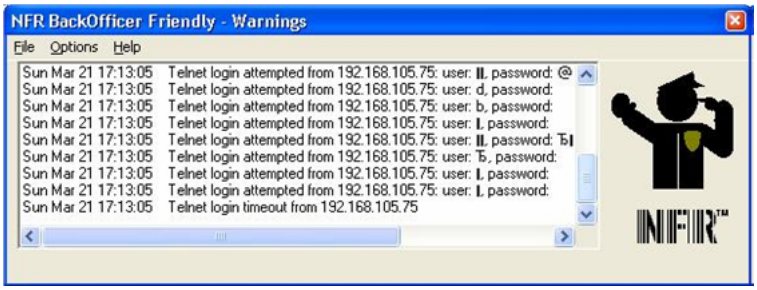


Рис. 11.4. NFR BackOfficer Friendly, эмулирующий работу TELNET-сервера, оповещает о процессе подбора злоумышленником (IP-адрес 192.168.105.75) паролей к ложному серверу

ЗАДАНИЕ № 11.3. Активизируйте опцию «Password must meet complexity requirements» («Пароли должны удовлетворять требованиям сложности») в политике безопасности Windows 2000/XP/2003. Данная функция предъявляет следующие требования к сложности паролей, назначаемых пользователю:

1.1. Пароль не может содержать какие-либо части пользовательского имени;
1.2. Длина пароля должна быть не менее 6 символов;
1.3. Пароль обязательно должен быть составлен из следующих символов:
· символы латинского алфавита в верхнем регистре;
· символы латинского алфавита в нижнем регистре;
· цифры от 0 до 9;

· специальные символы, например, !, $, #, %.

Примером пароля, удовлетворяющего указанным требованиям сложности, является пароль P@ssw0rd. Как показано выше, подбор паролей, созданных по такому принципу, гораздо сложнее как по методу перебора, так и по методу вычисления таблиц. Используя Microsoft Platform Software Development Kit можно создавать специализированные фильтры паролей для особенных целей.

ЗАДАНИЕ № 11.4. Методом пинга (Ping method) определить наличия запущенного сниффера влокальной сети использует уловку, заключающуюся в отсылке «ICMP Echo request» (Ping запроса) не на MAC-адрес машины, а на ее IP-адрес. Проиллюстрируем использование данного метода на примере.

1. Допустим, хост, который мы подозреваем на использование сниффера, имеет IP-адрес 10.1.1.1 и MAC-адрес 00-40-05-A4-79-3**2**.
2. Ваш компьютер должен находиться в том же сегменте ЛВС, что и подозреваемый компьютер.
3. Вы посылаете «ICMP Echo request», указав в запросе IP-адрес подозреваемого хоста и его слегка измененный MAC-адрес, например, 00-40-05-A4-79-3**3**.
4. Каждый хост, получив данный запрос, сравнивает указанный в запросе MAC-адрес со своим MAC-адресом. В случае совпадения MAC- адресов, хост отвечает источнику запроса с помощью «ICMP Echo Reply», иначе пакет игнорируется. В данном случае, ни один из хостов в ИС не должен увидеть данный пакет.
5. Если же получен ответ от какого-либо хоста, это значит что у него не используется фильтр MAC-адресов, т.е. его сетевой адаптер находится в «беспорядочном режиме». Следовательно на данном хосте используется сниффер.

Метод пинга может быть перенесен на другие протоколы, которые генерируют ответы на запросы, например, запрос на установление TCP-соединения или запрос по протоколу UDP на порт 7 (эхо).

ЗАДАНИЕ № 11.5. Метод ARP (ARP method) использует похожую технику, а также особенности реализации протокола ARP в Windows и Linux. Рассмотрим действие данного метода на примере определения хоста под управлением Windows с запущенным сниффером.

1. Вы подозреваете, что на хосте (A) с IP-адресом 192.168.86.19 запущен сниффер. Если вы разошлете широковещательный ARP-запрос, которому соответствует Ethernet-адрес «FF:FF:FF:FF:FF:FF», с целью выяснения MAC-адреса хоста (A), все хосты должны получить ваш запрос, но ответит только тот, чей IP-адрес указан в ARP-запросе (т.е. подозреваемый). В таблице приведены поля пакета рассылаемого ARP-запроса.

Ethernet-адрес хоста-получателя	FF:FF:FF:FF:FF:FF
Ethernet-адрес хоста-отправителя	Собственный MAC–адрес
Тип протокола (ARP=0806)	08 06
Адресное пространство (Ethernet=01)	00 01
…	
Аппаратный адрес хоста-отправителя	Собственный MAC–адрес
IP-адрес хоста-отправителя	Собственный IP-адрес
Аппаратный адрес хоста-получателя	00 00 00 00 00 00
IP-адрес хоста-получателя	IP-адрес хоста (A)

Однако было обнаружено, что если на хосте запущен сниффер, то в некоторых случаях он неправильно обрабатывает ARP-запросы.

2. Используя предложенный метод, вы посылаете точно такой же ARP-запрос, но где вместо широковещательного адреса «FF:FF:FF:FF:FF:FF» указан адрес «FF:FF:FF:FF:FF:FE» (ложный широковещательный адрес, из которого вычли один бит). Поскольку адрес не является широковещательным, теоретически ни один из хостов не должен ответить на такой запрос. Однако практические эксперименты, что Windows 2000/XP/2003 при условии, что сетевой адаптер, работает в беспорядочном режиме, посчитает такой запрос широковещательным. Соответственно хост (A), на котором запущен сниффер, сравнив IP-адрес в запросе со своим IP-адресом, пошлет ответ ARP-reply. Таким образом, хост (A) выдаст, что он прослушивает весь сетевой трафик. Ситуацию проиллюстрировать экранные снимками, сделанные с анализатора протоколов Sniffer Pro.

Перечень литературы и Интернет-ресурсов:

1. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты, ТИД "ДС", 688 стр., 2002 г.
2. Зима В., Молдовян А., Молдовян Н. Безопасность глобальных сетевых технологий, БХВ-Санкт-Петербург, 368 стр., 2002 г.
3. Информационная безопасность — http://ru.wikipedia.org/wiki/Information_security
4. Как обосновать затраты на информационную безопасность — http://www.iitrust.ru/articles/zat_ibezop.htm
5. Конев И., Беляев А. Информационная безопасность предприятия СПб-БХВ-Санкт-Петербург, 2003 – 752 с.
6. Лукацкий А.В. Обнаружение атак, БХВ-Санкт-Петербург, 596 стр., 2003 г.
7. Медведковский И. Д., Семьянов Б. В., Леонов Д. Г., Лукацкий А. В. Атака из Internet, 368 стр., 2002 г.
8. Методы распределённойобработка данных — http://www.find-info.ru/doc/cpp/009/portioned-methods.htm
9. Остерлох Х. TCP/IP. Семейство протоколов передачи данных в сетях компьютеров. «ДиаСофтЮП», 576 стр., 2002 г.
10. Распределенная среда обработки данных DCE — http://www.slomax.ru/index.php?option=com_content&task=view&id=47&Itemid=38
11. Скляров Д. Искусство защиты и взлома информации, БХВ- Петербург, 288 стр., 2004 г.
12. Соколов А. В., Шаньгин В. Ф. Защита информации в распределенных корпоративных сетях и системах, ДМК Пресс, 656 стр., 2002 г.

13. Ховард М., Лебланк Д. Защищенный код/Пер. с англ. – М.: Издательско-торговый дом «Русская редакция», 2003. – 704 стр.

14. Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа, Наука и Техника, 384 стр., 2004 г.

15. ISO27000.ru - первый русскоязычный информационный портал — http://www.iso27000.ru/o-proekte

Тема 12. Функциональные профили. Базовые и полные функциональные профили

Цели:

- Изучить процессы формирования, развития и применения профилей информационных систем.
- Разобраться в классификации функциональных профилей.
- Разобраться в типах функциональных профилей.
- Понять назначение полного функционального профиля.
- Получить представление об открытых сетевых архитектурах.
- Изучить процессы формирования, развития и применения профилей информационных систем.

12.1. Процессы формирования, развития и применения профилей ИС.

На стадии стратегического планирования и анализа требований уточняются исходные данные и разрабатываются спецификации требований к прикладному программному обеспечению (ПО) и к среде. Принимаемые на этой стадии решения исходят из альтернативного выбора методологии и принципов построения ИС между функционально-модульным подходом и объектным подходом. В плане создания ИС, разрабатываемом на этой стадии, должны быть учтены работы, связанные с построением и оформлением функциональных профилей ИС. Полнота функций, выполняемых информационно-вычислительной сетью – это обеспечение выполнения всех предусмотренных функций и по доступу ко всем ресурсам, и по совместной работе узлов, и по реализации всех протоколов и стандартов работы.

Аппаратно-программные платформы, на которых выполняются клиентские и серверные части приложений, должны соответствовать требованиям профиля среды ИС. После детального проектирования версии прикладных программных средств, начиная со стадии разработки вплоть до стадии интеграции и тестирования комплекса прикладных программ в составе ИС, все работы должны проводиться в соответствии с требованиями функциональных профилей ИС.

Применение функциональных профилей ИС в этих случаях позволяет обусловить пределы изменений в системе, связанных с ее адаптацией, и границы значений параметров, в рамках которых может производиться настройка. При сопровождении ИС важнейшее значение имеют регламенты процессов сопровождения и применение инструментальных средств, встроенных в ИС, в частности средств управления конфигурацией. Эти регламенты рекомендуется устанавливать с использованием стандартов ISO 687: 1983, ISO 12207:1995 и ANSI/IEEE 1042: 1987.

В международной функциональной стандартизации ИТ принята жесткая трактовка понятия профиля. Считается, что его основой могут быть только международные и национальные, утвержденные стандарты - не допускается использование стандартов де-факто и нормативных документов фирм. Подобное понятие профиля активно используется в гамме международных функциональных стандартов, конкретизирующих и регламентирующих основные процессы и объекты взаимосвязи открытых систем (ВОС), в которых возможна и целесообразна жесткая формализация профилей (функциональные стандарты ИСО 10607 - 10613 и соответствующие им ГОСТ Р). Однако при таком подходе невозможны унификация, регламентирование и параметризация множества конкретных функций и характеристик сложных объектов архитектуры и структуры современных ИС.

12.2. Классификация функциональных профилей.

Существует несколько классификаций профилей, по смысловому содержанию во многом несхожих, а в чем-то даже противоречивых. Это связано прежде всего со взаимной противоречивостью различных концепций. Например, с точки зрения общей концепции открытых систем вся взаимосвязь открытых систем (ВОС) относится к коммуникационным функциям, а с точки зрения самой ВОС к коммуникационным функциям относятся только функции четырех нижних уровней эталонной модели ВОС, функции же трех ее верхних уровней - к прикладным. Кроме того, некоторые функции, разработанные в рамках ВОС совместным техническим комитетом СТК1 ИСО/МЭК (и еще ранее техническим комитетом ТС 97), например административное управление (Management) системой и данными, справочные службы (Directory), машинная графика, в концепции открытых систем вынесены за рамки ее коммуникационных функций, т. е. отняты у ВОС. Такие несоответствия в классификации и терминологии характерны для начального этапа развития многих концепций и в данном случае — для концепции открытых систем.

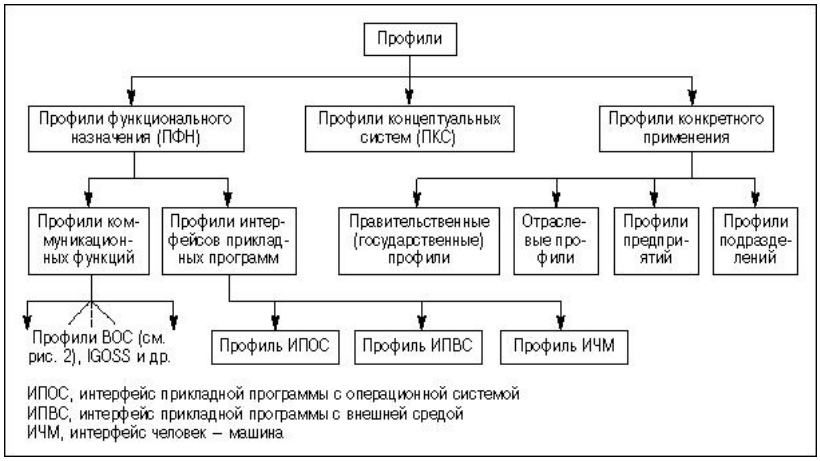


Рис. 12.1. Классификация профилей

Все известные к настоящему времени профили предлагается разделить на три крупных класса: назовем их профили функционального назначения (ПФН), профили концептуальных систем (ПКС) и профили конкретного применения (ПКП). ПФН охватывают лишь отдельные прикладные или коммуникационные функции и не распространяются на всю систему. Это некие

модули, блоки (как в крупнопанельном строительстве), только здесь эти блоки изготовлены не из бетона, а из тех же кирпичей (базовых стандартов), подобранных, обрубленных, подогнанных и сцементированных в расчете на заданный размер объекта (прикладную или коммуникационную функцию). К этому классу относятся как раз те профили, которые разрабатывает СГФС, сформулировавшая в ISO/IEC TR 10000-1 приведенное выше определение профилей. В настоящее время правительственные профили (GOSIP) и госпрофиль ВОС представляют собой некоторые выборки из всей совокупности базовых стандартов ВОС (версии профилей ВОС). Отраслевые профили строятся в зависимости от применяемого в отрасли набора прикладных программ, режимов работы сети (с установлением или без установления соединения), типов используемых сетей и сетевых технологий. Профили предприятий (подразделений) могут строиться в виде подмножества отраслевых профилей (профилей предприятий), а также независимо от них: например, если предприятие имеет свою локальную вычислительную сеть, не связанную с сетью отрасли.

12.3. Функциональный профиль.

Функциональный профиль **—** иерархия взаимосвязанных протоколов, предназначенная для определенного круга задач обработки и передачи данных.

В документах ISO и ITU определен широкий набор сетевых служб, и он все время расширяется. Выпущено большое число стандартов для всех семи уровней области взаимодействия. Все указанные стандарты являются гибкими и предусматривают множество вариантов. Кроме этого, производители могут использовать свои стандарты и интегрировать их в область взаимодействия. Реализовать все стандарты не только невозможно, но и не нужно. Поэтому для решения возникающих задач подбираются сетевые службы и множества определяющих их стандартов. В результате, создаются функциональные профили. При этом следует иметь в виду, что стандарт любого уровня содержит ядро (основу, обеспечивающую минимальные возможности функционирования уровня). Наряду с этим, имеется перечень необязательных функциональных блоков, расширяющих перечень видов сервиса.

Основными целями применения профилей при создании и использовании ИС являются:

- снижение трудоемкости проектов ИС;
- повышение качества компонентов ИС;
- обеспечение расширяемости ИС по набору прикладных функций и масштабируемости;
- обеспечение возможности функциональной интеграции в ИС задач, которые раньше решались раздельно;
- обеспечение переносимости прикладного программного обеспечения.

Выбор стандартов и документов для формирования профилей ИС зависит от того, какие из этих целей определены приоритетными.

Функциональный профиль определяет выбранные классы, подмножества, варианты и параметры стандартов, обеспечивающих работу нужного набора сетевых служб. Каждый из профилей определяет группу выбранных стандартов, имеющую международное признание. Существует множество типов функциональных профилей (рис.12.2).

Рис. 12.2. Классификация функциональных профилей

По числу используемых уровней области взаимодействия выделяют полные функциональные профили, коллапсные функциональные профили и базовые функциональные профили (рис.12.3).

Первые охватывают все семь уровней. Вторые включают, как минимум, физический уровень, канальный уровень и прикладной уровень. Все либо часть остальных уровней в профиле отсутствует (их функции резко упрощены и переданы на имеющиеся уровни). И, наконец, базовый профиль определяет лишь взаимосвязанные стандарты нескольких нижних уровней. Кроме этого, существуют смешанные функциональные профили, которые в одних случаях работают как полные, а в других - как коллапсные. Например, в Цифровой Сети с Интегральным Обслуживанием (ЦСИО).

В связи с использованием разнообразных наборов протоколов все большее распространение получают *многоштабельные профили*. Они характеризуются наличием разных штабелей протоколов. Например, тем, что на нижних (1-K) уровнях определяются различными, а на верхних (K+1-7) - одними и теми же протоколами (рис.12.4).

Важность проблемы создания и использования полных функциональных профилей настолько велика, что в наиболее развитых странах создаются правительственные профили взаимодействия открытых систем. Наряду с этим, ведутся работы по

созданию Международного стандартного профиля ISP.

Чаще всего, такие штабели определяются протоколами X.25, TPC/IP, 802.3.

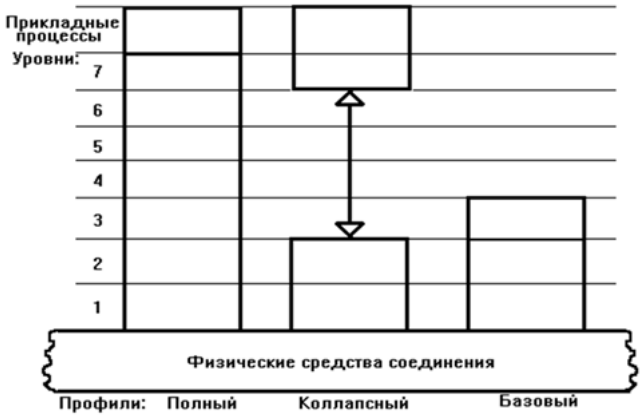


Рис.12.3. Типы функциональных профилей

В штабелях протоколов функциональных профилей выделяют точки со стандартными интерфейсами. Они определяют используемые платформы.

Рис.12.4. Схема многоштабельного профиля

12.3.1. Базовый функциональный профиль

Базовый функциональный профиль **—** функциональный профиль, включающий иерархию протоколов только несколько уровней.

Так как базовый функциональный профиль определяется стандартами лишь части уровней области взаимодействия, то он является фундаментом, на котором строится полный функциональный профиль либо коллапсный функциональный профиль. Поэтому базовый функциональный профиль самостоятельного значения не имеет. Пользуются популярностью базовые функциональные профили, именуемые оптоволоконный распределенный интерфейс данных, распределенная двойная шина с очередями, открытая сетевая обработка данных, базовый функциональный профиль ATM, сетевая базовая система ввода/вывода.

12.3.2. Коллапсный функциональный профиль

Коллапсный функциональный профиль **—** псевдо-полный функциональный профиль, в котором отсутствует один либо несколько уровней.

Коллапсным называют профиль, в котором функции отсутствующих уровней настолько упрощены, что включены в набор задач, выполняемых оставшимися уровнями. Появление коллапсных профилей открыло возможность создания очень простых и быстродействующих локальных сетей. Естественно, что эти преимущества получены за счет резкого упрощения ряда функций области взаимодействия. В этой связи, рассматриваемые профили имеют ограниченные возможности представления данных и организации сеансов. Кроме этого, здесь упрощена передача данных через коммуникационную сеть.

Примером коллапсного профиля является miniMAP, созданный фирмой General Motors.

Рис.12.5. Профиль miniMAP

Его архитектура характеризуется рядом важных особенностей, отличающих ее от Z функционального профиля MAP. Прежде всего, в miniMAP резко ограничены возможности создания разнообразных сетевых служб. Этот профиль предназначен только для управления такими технологическими процессами, в которых необходимо лишь передавать небольшие порции данных и получать короткие, но быстрые ответы. Подобные процессы используются в сетях считывающих устройств, интеллектуальных датчиков, систем машинного зрения, роботов.

12.3.3. Полный функциональный профиль

Полный функциональный профиль Full functional profile — функциональный профиль, включающий иерархию протоколов всех семи уровней. Полный функциональный профиль является законченным продуктом, обеспечивающим прикладные процессы всем набором видов сервиса, предоставляемых моделью OSI. Обычно базой профиля являются выбранные в качестве стандарта территориальные сети и локальные сети.

Полный функциональный профиль является целостным и законченным продуктом, обеспечивающим прикладные процессы всем набором видов сервиса, предоставляемых областью Взаимодействия Открытых Систем (ВОС). Состоит он из иерархической группы взаимосвязанных функциональных блоков.

Рис.12.6. Структура полного профиля

Базой профиля, как правило, являются выбранные в качестве стандарта территориальные сети и локальные сети. Они определяют физический уровень (1), канальный уровень (2) и сетевой уровень (3). Далее следует общий транспортный протокол, расположенный на транспортном уровне (4). Эти четыре уровня образуют транспортную платформу. В верхней части сеансовый уровень (5), представительный уровень (6) и прикладной уровень (7) создают прикладную платформу. Непосредственно на ней располагаются прикладные процессы. Полными функциональными профилями являются системная сетевая архитектура, архитектура дискретной сети, функциональный профиль MAP, функциональный профиль TOP, открытая сетевая архитектура. Во многих странах разработаны правительственные профили взаимодействия открытых систем, также являющиеся полными функциональными профилями.

12.4. Открытая сетевая архитектура.

Открытая сетевая архитектура — полный функциональный профиль, разработанный фирмой British Telecom.

British Telecom на всех семи уровнях использует в ONA (Open Network Architecture – Открытая Сетевая Архитектура) стандарты ISO и ITU. Разработка архитектуры поддерживается созданием средств тестирования для определения конформности изделий. На верхних уровнях ONA покрывает три области: передачи сообщений, диалога, обработки данных.

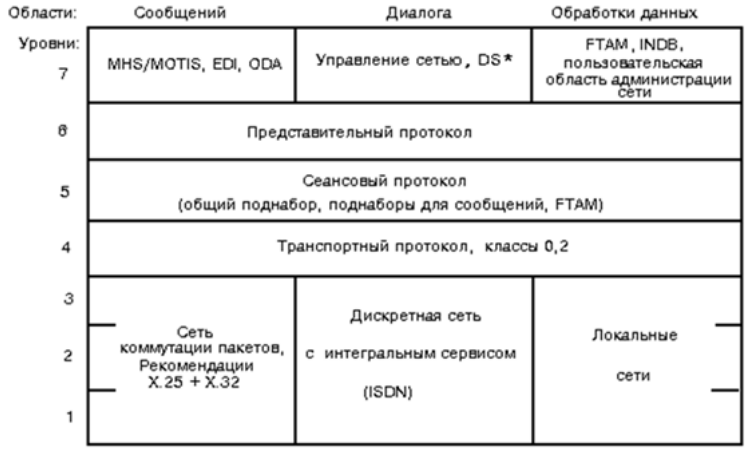


Рис. 12.7. Профиль открытой сетевой архитектуры

Сетевая служба MHS/MOTIS определяет работу электронной почты. При передаче сообщений применяется также сетевая служба EDI. Обработка сообщений осуществляется в соответствии со стандартом сетевая служба ODA.

Администрация сети выполняет задачи, связанные с управлением сетью. При управлении обеспечивается выполнение различных режимов передачи данных. С одной стороны, это - передача больших файлов для обработки статистики, счетов, удаленной загрузки сетевых программ. С другой стороны, это - посылка коротких сведений, например, управляющих команд. Для учета абонентских систем используется сетевая служба DS*.

Выполнение задач, связанных с передачей файлов, в архитектуре ONA обеспечивается сетевой службой FTAM. Хранение информации осуществляется Интеллектуальной сетевой базой данных INDB. Область обработки данных, также, используется для управления сетью. Что касается сетевой части структуры (уровни 1-3), то она опирается на сеть коммутации пакетов, Цифровую Сеть с Интегральным Обслуживанием (ЦСИО) и локальные сети. Такой подход определяет главные интересы British Telecom, связанные с организацией территориальных коммуникационных сетей.

Идея открытой сетевой архитектуры была впервые высказана Каном в 1972 году. Открытая сетевая архитектура подразумевает, что отдельные сети могут проектироваться и разрабатываться независимо, со своими уникальными интерфейсами, предоставляемыми пользователям или другим поставщикам сетевых услуг, включая услуги Интернета. При проектировании каждой сети могут быть приняты во внимание специфика окружения и особые требования пользователей.

В основу своих первоначальных рассуждений Кан положил четыре принципа:

u Каждая сеть должна сохранять свою индивидуальность. При подключении к Интернету сети не должны подвергаться внутренним переделкам.

u Коммуникации должны идти по принципу "максимум возможного". Если пакет не прибыл в пункт назначения, источник должен вскоре повторно передать его.

u Для связывания сетей должны использоваться черные ящики; позднее их назовут шлюзами и маршрутизаторами. Шлюзы не должны хранить информацию об отдельных протекающих через них потоках данных. Они должны оставаться простыми, без сложных средств адаптации и восстановления после разного рода ошибочных ситуаций.

u На эксплуатационном уровне не должно существовать глобальной системы управления.

12.4.1. RFC

Запрос комментариев (Request for Comments, RFC)— документ из серии пронумерованных информационных документов Интернета, содержащих технические спецификации и Стандарты, широко применяемые во Всемирной сети. Название RFC ещё можно перевести как «заявка на обсуждение» или «тема для обсуждения». В настоящее время первичной публикацией документов RFC занимается IETF под эгидой открытой организации Общество Интернета (Internet Society, ISOC). Правами на RFC обладает именно Общество Интернета. Несмотря на название, запросы комментариев RFC сейчас рассматриваются как стандарты Интернета (а рабочие версии стандартов обычно называют *драфтами*). Согласно RFC 2026, жизненный цикл стандарта выглядит следующим образом:

1. Выносится на всеобщее рассмотрение ***Интернетовский черновик (Internet Draft).*** Черновики не имеют официального статуса, и удаляются из базы через шесть месяцев после последнего изменения. Если черновик стандарта оказывается достаточно удачным и непротиворечивым, он получает статус ***Предложенного стандарта (Proposed Standard),*** и свой номер RFC. Наличие программной реализации стандарта желательно, но не обязательно.

2. Следующая стадия**—** ***Черновой стандарт (Draft Standard)*** означает, что предложенный стандарт принят сообществом, в частности, существуют две независимые по коду совместимые реализации разных команд разработчиков. В черновые стандарты ещё могут вноситься мелкие правки, но они считаются достаточно стабильными и рекомендуются для реализации.

3. Высший уровень**—** ***Стандарт Интернета (Internet Standard).*** Это спецификации с большим успешным опытом применения и зрелой формулировкой. Параллельно с нумерацией RFC они имеют свою собственную нумерацию STD. Список стандартов имеется в документе STD 1 (сейчас это RFC 5000, но нумерация может измениться). Из более чем трёх тысяч RFC этого уровня достигли только несколько десятков.

4. Многие старые RFC замещены более новыми версиями под новыми номерами, или вышли из употребления. Такие документы получают статус ***Исторических (Historic).***

Практически все стандарты Глобальной сети существуют в виде опубликованных заявок RFC. Но в виде документов RFC выходят не только стандарты, но также концепции, введения в новые направления в исследованиях, исторические справки, результаты экспериментов, руководства по внедрению технологий, предложения и рекомендации по развитию существующих Стандартов и другие новые идеи в информационных технологиях:

1. ***Экспериментальные (Experimental)*** спецификации содержат информацию об экспериментальных исследованиях, интересных для интернет-сообщества. Это могут быть, например, прототипы, реализующие новые концепции.

2. ***Информационные (Informational)*** RFC предназначены для ознакомления общественности, не являются стандартами и не являются результатом консенсуса или рекомендациями. Некоторые черновики, не получившие статуса Предложенного стандарта, но представляющие интерес, могут быть опубликованы как Информационные RFC.

3. ***Лучший современный опыт (Best Current Practice).*** Эта серия RFC содержит рекомендации по реализации стандартов, в том числе от сторонних организаций, а также внутренние документы о структуре и процедурах стандартизации.

Контрольные вопросы:

1. Расскажите о процессе формирования и применения профиля ИС?
2. Классификация функциональных профилей.
3. Что такое функциональный профиль?
4. Чем отличается коллапсный функциональный профиль от базового функционального профиля?
5. Какие типы функциональных профилей Вы знаете?
6. Какие RFC основные Вы знаете?
7. Что такое полный функциональный профиль?
8. Что такое структура полного профиля?
9. Основные профили открытой сетевой архитектуры?
10. Что такое открытая сетевая архитектура?

Практические задания:

ЗАДАНИЕ № 12.1-5. Управление учетными записями.

Цель: Научиться создавать учётные записи и группы учётных записей, предоставлять пользователям права доступа к папкам и файлам.

Ход работы:

1. Изучить теоретические положения, составить краткий конспект.
2. Предъявить конспект преподавателю.
3. Выполнить упражнения.
4. Ответить на контрольные вопросы.

Теоретические положения.

Управление учетными записями.

Создание учетных записей и групп занимает важное место в обеспечении безопасности Windows XP, поскольку, назначая им права доступа, администратор получает возможность ограничить пользователей в доступе к конфиденциальной информации компьютерной сети, разрешить или запретить им выполнение в сети определенного действия, например архивацию данных или завершение работы компьютера. Поскольку работа с учетными записями пользователей и групп в версиях Windows XP Professional и Windows XP Home Edition выполняется поразному, мы рассмотрим примеры для каждой системы отдельно.

Windows XP Professional.

В Windows XP Professional для работы с локальными учетными записями используется оснастка **Локальные пользователи и группы**. Если компьютер не является членом домена, то в качестве упрощенного средства администрирования можно также использовать утилиту *Учетные записи пользователей,* которая в Windows XP Home Edition является единственным инструментом для управления пользователями.

Оснастка *Локальные пользователи и группы.*

Оснастка **Локальные пользователи и группы** — это инструмент MMC, с помощью которого выполняется управление локальными учетными записями пользователей и групп — как на локальном, так и на удаленном компьютере. Запускать оснастку может любой пользователь, однако выполнять *администрирование* учетных записей могут только администраторы и члены группы Опытные пользователи.

Папка *Пользователи.*

Сразу после установки системы Windows XP папка **Пользователи** содержит четыре автоматически создаваемые *встроенные* учетные записи, перечисленные ниже. Две первые записи имеются и в системах Windows 2000, другие появились только в Windows XP.

Администратор — эту учетную запись используют при установке и настройке рабочей станции или сервера, являющегося членом домена. Она не может быть уничтожена, блокирована или удалена из группы Администраторы (Administrators), ее можно только переименовать.

Гость — эта учетная запись применяется для регистрации в компьютере без использования специально созданной учетной записи. Учетная запись Гость не требует ввода пароля и по умолчанию заблокирована.

(Обычно пользователь, учетная запись которого блокирована, но не удалена, при регистрации получает предупреждение, и входить в систему не может.) Она является членом группы Гости. Ей можно предоставить права доступа к ресурсам системы точно так же, как любой другой учетной записи.

Help Assistant — данная запись используется при работе с удаленным помощником.

SUPPORT_388945a0 — компания Microsoft зарезервировала эту запись за собой для поддержки службы поддержки; по умолчанию запись отключена.

Перечисленные учетные записи имеются и в Windows XP Home Edition. Можете проверить это сами, введя в командной строке net user. Кроме того, могут появляться и другие пользовательские учетные записи.

Например, после установки служб Интернета появляются записи следующего вида:

IUSR_<имяКомпьютера> — встроенная учетная запись для анонимного доступа к службам IIS (например, к веб-серверу или FTP-серверу);

IWAM_<имяКомпьютера> — встроенная запись, которую службы IIS используют для запуска приложений.

Папка *Группы.*

В системах Windows 2000 (рабочей станции или сервера, являющегося членом домена) папка **Группы** содержит шесть *встроенных* групп. Они создаются автоматически при установке системы. Ниже описаны свойства этих групп:

Администраторы — ее члены обладают полным доступом ко всем ресурсам системы. Это единственная встроенная группа, автоматически предоставляющая своим членам весь набор встроенных прав. По умолчанию содержит всех пользователей, зарегистрированных на компьютере в качестве администраторов (чьи имена были введены при первом запуске системы), включая встроенную учетную запись Администратор. Если компьютер подключен к домену, эта группа также содержит группу Пользователи домена.

Операторы архива — члены этой группы могут архивировать и восстанавливать файлы в системе независимо от того, какими правами эти файлы защищены. Кроме того, операторы архива могут входить в систему и завершать ее работу, но они не имеют права изменять настройки безопасности. По умолчанию пуста.

Гости — эта группа позволяет выполнить регистрацию пользователя с помощью учетной записи Гость и получить ограниченные права на доступ к ресурсам системы. Члены этой группы могут завершать работу системы. По умолчанию содержит пользователя Гость.

Опытные пользователи — члены этой группы могут создавать учетные записи пользователей, но они имеют право модифицировать настройки безопасности только для созданных ими учетных записей.

Кроме того, они могут создавать локальные группы и модифицировать состав членов созданных ими групп. То же самое они могут делать с группами Пользователи, Гости и Опытные пользователи . Члены группы Опытные пользователи не могут модифицировать членство в группах Администраторы и Операторы архива. Они не могут быть владельцами файлов, архивировать или восстанавливать каталоги, загружать и выгружать драйверы устройств и модифицировать настройки безопасности и журнал событий. По умолчанию пуста.

Репликатор — членом группы Репликатор должна быть только учетная запись, с помощью которой можно зарегистрироваться в службе репликации контроллера домена. Ее членами не следует делать рабочие учетные записи. По умолчанию пуста.

Пользователи — члены этой группы могут выполнять большинство пользовательских функций, например, запускать приложения, пользоваться локальным или сетевым принтером, завершать работу системы или блокировать рабочую станцию. Они также могут создавать локальные группы и регулировать состав их членов. Они не могут получить доступ к общему каталогу или создать локальный принтер. По умолчанию содержит служебные записи *прошедшие проверку* и интерактивные, а также созданные на компьютере учетные записи *с ограниченными правами*. Если компьютер подключен к домену, эта группа также содержит группу Пользователи домена.

В системах Windows XP появились три *дополнительных* группы:

О Операторы настройки сети (Network Configuration Operators) — группа, члены которой имеют некоторые права по настройке сетевых служб и параметров. По умолчанию пуста.

О Пользователи удаленного рабочего стола (Remote Desktop Users) — эта группа содержит имена пользователей, которым явно разрешен удаленный доступ к рабочему столу.

О HelpServicesGroup (Группа служб поддержки) — группа для поддержки справочной службы (Help and Support Service). По умолчанию содержит учетную запись SUPPORT_388945a0.

Внимание! Создание пользовательской учетной записи

Для создания учетной записи:

1. В оснастке **Локальные пользователи и группы** установите указатель мыши на папку **Пользователи** и нажмите правую кнопку. В контекстном меню выберите команду **Новый пользователь**.

2. Появится диалоговое окно **Новый пользователь**). В поле **Пользователь** введите имя входа для создаваемого пользователя, В поле **Полное имя** введите полное имя создаваемого пользователя — это имя будет отображаться в новом меню **Пуск** и в окне приветствия . (Если полное имя не задано, то отображается имя входа. На изолированном компьютере войти в систему можно с помощью любого имени.) В поле **Описание** введите описание создаваемого пользователя или его учетной записи. В поле **Пароль** введите пароль пользователя и в поле **Подтверждение** подтвердите его правильность вторичным вводом.

3. Установите или снимите флажки **Потребовать смену пароля при следующем входе в систему** , **Запретить смену пароля пользователем**, **Срок действия пароля не ограничен** и **Отключить учетную запись.**

4. Нажмите кнопку **Создать**. Чтобы создать еще одного пользователя, повторите шаги с 1 по 3. Для завершения работы нажмите кнопку **Закрыть**. Созданный пользователь включается в локальную группу Пользователи; вы можете открыть вновь созданную учетную запись и изменить членство пользователя в группах. Имя пользователя должно быть уникальным для компьютера. Оно может содержать до 20 символов верхнего и нижнего регистра. Ниже приведены символы, применение которых в имени пользователя недопустимо: " / \ И:; I =, + *?< >@

Имя пользователя не может состоять целиком из точек и пробелов.

Изменение и удаление учетных записей.

Изменять, переименовывать и удалять учетные записи можно с помощью контекстного меню, вызываемого елчком правой кнопки мыши на имени пользователя, либо посредством меню **Действие** на панели меню оснастки **Локальные пользователи и группы** (при этом в правом подокне оснастки должна быть выбрана модифицируемая или удаляемая учетная запись пользователя). На компьютере, входящем в домен, для работы с локальными учетными записями можно также использовать утилиту *Учетные записи пользователей*. Поскольку переименованная учетная запись сохраняет *идентификатор безопасности* , она сохраняет и все свои свойства, например, описание, полное имя, пароль, членство в группах и т. д. Поскольку SID уникален, нельзя после удаления пользователя или группы создать новую учетную запись со "старыми" свойствами. Поэтому иногда учетные записи пользователей просто временно блокируют.

Управление локальными группами.

Создание локальной группы.

Для создания локальной группы:

1. В окне оснастки **Локальные пользователи и группы** установите указатель мыши на папке **Группы** и нажмите правую кнопку. В появившемся контекстном меню выберите команду **Новая группа**.
2. В поле **Имя группы** введите имя новой группы.
3. В поле **Описание** введите описание новой группы.
4. В поле **Члены группы** можно сразу же добавить пользователей и группы, которые войдут в данную группу: для этого нужно нажать **кнопку Добавить** и выбрать их в списке.
5. Для завершения нажмите кнопку **Создать** и затем **— Закрыть**.

Имя локальной группы должно быть уникальным в пределах компьютера. Оно может содержать до 256 символов в верхнем и нижнем регистрах. Требования к символам, используемых в имени группы, такие же, как для имен пользователей.

Изменение членства в локальной группе.

Чтобы добавить или удалить учетную запись пользователя из группы:

1. В окне оснастки **Локальные пользователи и группы** щелкните на папке **Группы**.
2. В правом подокне установите указатель мыши на модифицируемую группу и нажмите правую кнопку. В появившемся контекстном меню выберите команду **Добавить в группу** или **Свойства**.
3. Для того чтобы добавить новые учетные записи в группу, нажмите кнопку **Добавить**. Далее следуйте указаниям диалогового окна **Выбор: Пользователи**.
4. Для того чтобы удалить из группы некоторых пользователей, в окне **Члены группы** окна свойств группы выберите одну или несколько учетных записей и нажмите кнопку **Удалить**.

На компьютерах **—** членах домена в локальную группу можно добавлять как локальных пользователей, созданных на компьютере, так и пользователей иглобальные группы, созданные в домене, к которому принадлежит компьютер, или в доверяемых доменах.

ЗАДАНИЕ № 12.1. Зайдите в **Панель управления**, добавьте 3 новые учётные записи и занесите их к разным группам пользователей - *ограниченный доступ, опытные пользователи, оператор архива*. Изучите, какими правами обладают различные группы пользователей.

ЗАДАНИЕ № 12.2. Зайдите в **Свойства системы**, затем на вкладку **Идентификация**, отнесите себя к группе с определённым именем (номер своей группы). Перезагрузитесь и посмотрите (**Моё сетевое окружение – Соседние компьютеры**) других членов группы. Посмотрите (контекстное меню на ярлычке «**Мой компьютер**») свою группу, имя и прочие атрибуты.

ЗАДАНИЕ № 12.3. Для установки параметров защиты файлов или папок, сделайте щелчок правой клавишей мыши на интересующем вас объекте. Выберите в контекстном меню команду **Свойства** и перейдите на вкладку **Безопасность.** Изучить предоставляемые возможности.

ЗАДАНИЕ № 12.4. Создайте файл в MS Word. Создайте папку «Моя папка» в папке «Мои документы». Поместите туда созданный файл. Предоставьте доступ к этой папке другим членам группы с разными приоритетами. Проверьте действие ограничений.

ЗАДАНИЕ № 12.5. Настройте папку «Моя папка» (**Свойства).** Измените фоновое изображение, добавьте комментарий для папки (Свойства\Доступ\Расширенные настройки (Примечание)). Проверить наличие комментария (Управление компьютером\Общие папки\Общие ресурсы (Описание)- при общем доступе).

ЗАДАНИЕ № 12.6. Запросы RFC. Найти и дать примеры популярных запросов комментариев RFC 768, RFC 791, RFC 792, RFC 793, RFC 821, RFC 822, RFC 826, RFC 894, RFC 951, RFC 959, RFC 977, RFC 1034, RFC 1035.

Перечень литературы и Интернет-ресурсов:

1. Информационные технологии и электронные коммуникации — http://emf.ulstu.ru/metod/ITEK/index.htm
2. Н.В. Максимов, И. И. Попов, Компьютерные сети: учебное пособие, М.:ФОРУМ, 2004.
3. Муштоватый И.Ф. Самоучитель по работе в Интернете/ Под общ. редакцией М.И. Монастырского. – Ростов н/Д.: «Феникс», 2001. – 320с.
4. Основы построения объединенных сетей — http://www.citforum.ru/nets/ito/index.shtml
5. Основы современных компьютерных технологий под редакцией А.Д. Хомоненко– СПб КОРОНА принт, 1998.
6. Пятибратов А.П. и др. Вычислительные системы, сети и телекоммуникации: Учебник/ Под редакцией А.П. Пятибратова. – М.: Финансы и статистика, 2001. – 512 с.

7. Системы передачи информации — http://kunegin.narod.ru/ref/lec/86.htm
8. Столлингс В. Компьютерные сети, протоколы и технологии Интернета. – СПб.: БХВ-Петербург, 2005. – 832 с.
9. Стэн Шатт Мир компьютерных сетей пер. с англ. – К.: BHV, 1996 – 288 с.
10. Технология корпоративных сетей. М. Кульгин. – СПб ПИТЕР, 1999.
11. Уолрэнд Дж. Телекоммуникационные и компьютерные сети: Вводный курс / Пер. с англ.- М.: Постмаркет, 2001.- 480с.
12. Якубайтис Э.А. Информационные сети и системы: Справочная книга. – М.: Финансы и статистика, 1996.

Тема 13. Методы оценки эффективности информационных сетей

Цели:

· Получить представление о требованиях, предъявляемые к сетям.
· Получить представление о показателях эффективности сети.
· Научиться рассчитывать показатели эффективности сети.

13.1. Требования к качеству услуг и критерии оценки сетей ЭВМ.

Основное требование – это обеспечение всем пользователям доступа к разделяемым ресурсам сети с заданным качеством обслуживания (QoS – Quality of Service). Основными критериями оценки качества обслуживания являются *производительность*, *надежность* и *безопасность*. В качестве показателей производительности используются *время реакции, пропускная способность* и *задержка передачи*.

Время реакции – это интервал времени между возникновением запроса пользователя к сетевой службе и получением ответа. Время реакции зависит от загруженности сегментов среды передачи и активного сетевого оборудования (коммутаторов,маршрутизаторов, серверов). *Пропускная способность* – это объем данных, передаваемых в единицу времени (бит/с, пакетов/с). Пропускная способность составного пути в сети определяется самым медленным элементом (как правило, это маршрутизатор). *Задержка передачи* – это интервал времени между моментом поступления пакета на вход сетевого устройства и моментом появления его на выходе устройства. *Безопасность* – это защищенность сетевых ресурсов от несанкционированного доступа.

В качестве показателей *надежности* используются: *среднее время наработки на отказ* $T_{\text{ОТК}}$, *среднее время ремонта* $T_{\text{РЕМ}}$ и *коэффициент готовности:* $K_{\text{Г}} = T_{\text{ОТК}} /(T_{\text{ОТК}} + T_{\text{РЕМ}})$, определяющий вероятность работоспособного состояния сети в любой момент времени.

Важным требованием к надежности вычислительных сетей является *отказоустойчивость*, т. е. сохранение работоспособности при отказе отдельных элементов.

Ряд требований к компьютерным сетям связан с их эксплуатацией и развитием, а также с обеспечением удобства работы для пользователей. *Совместимость* сетевого оборудования и программного обеспечения позволяет объединять разнообразные компоненты, приобретенные от разных производителей.

Расширяемость – это возможность расширения сети (добавления отдельных элементов, наращивания длины сегментов, замены оборудования на более мощное) без особых проблем.

Масштабируемость – это возможность расширения сети в широких пределах без снижения производительности. Важным требованием, характеризующим удобство работы пользователей, является

Прозрачность доступа к сетевым ресурсам. Прозрачность означает, что при работе в сети пользователю не требуется знать детали устройства системы.

Современные тенденции развития вычислительных сетей:

1. Сократился разрыв между локальными и глобальными сетями:
· за счет высокоскоростных территориальных каналов связи;
· за счет новых служб доступа к ресурсам Интернета.
2. В ЛВС используется коммуникационное оборудование: коммутаторы, маршрутизаторы, шлюзы.
3. В корпоративных сетях используются суперЭВМ (мэйнфреймы) в качестве серверов, поддерживающих технологии Ethernet и стек протоколов TCP/IP.
4.Внедряется обработка мультимедийной информации (аудио и видео).
5. Происходит слияние технологий ЛВС, глобальных сетей и любых информационных сетей (вычислительных, телефонных, телевизионных).

13.2. Прозрачность.

Прозрачность – это такое состояние сети, когда пользователь, работая в сети, не видит ее.

Коммуникационная сеть является прозрачной относительно проходящей сквозь нее информации, если выходной поток битов, в точности повторяет входной поток. Но сеть может быть непрозрачной во времени, если из-за меняющихся размеров очередей блоков данных изменяется и время прохождения различных блоков через узлы коммутации. Прозрачность сети по скорости передачи данных указывает, что данные можно передавать с любой нужной скоростью. Если в сети по одним и тем же маршрутам передаются информационные и управляющие (синхронизирующие) сигналы, то говорят, что сеть прозрачна по отношению к типам сигналов. Если передаваемая информация может кодироваться любым способом, то это означает, что сеть прозрачна для любых методов кодировок.

Прозрачная сеть является простым решением, в котором для взаимодействия локальных сетей, расположенных на значительном расстоянии друг от друга, используется принцип *Plug-and-play* (подключись и работай).

Прозрачное соединение. Служба *прозрачных* локальных сетей обеспечивает сквозное (end-to-end) соединение, связывающее между собой удаленные локальные сети. Привлекательность данного решения состоит в том, что эта служба объединяет удаленные друг от друга на значительное расстояние узлы как части локальной сети. Поэтому не нужно вкладывать средства в изучение новых технологий и создание территориально распределенных сетей (Wide-Area Network – WAN). Пользователям требуется только поддерживать локальное соединение, а провайдер службы прозрачных сетей обеспечит беспрепятственное взаимодействие узлов через сеть масштаба города (Metropolitan-Area Network – MAN) или сеть WAN. Службы *Прозрачной* локальной сети имеют много преимуществ. Например, пользователь может быстро и безопасно передавать большие объемы данных на значительные расстояния, не обременяя себя сложностями, связанными с работой в сетях WAN.

13.3. Производительность и управляемость.

Производительность – это характеристика сети, позволяющая оценить, насколько быстро информация передающей рабочей станции достигнет приемной рабочей станции. Производительность информационно-вычислительной сети – это среднее

количество запросов пользователей сети, исполняемых за единицу времени.

На производительность сети влияют следующие характеристики сети: конфигурация; скорость передачи данных; метод доступа к каналу; топология сети; технология.

Если производительность сети перестает отвечать предъявляемым к ней требованиям, то администратор сети может прибегнуть к различным приемам:

· изменить конфигурацию сети таким образом, чтобы структура сети более соответствовала структуре информационных потоков;

· перейти к другой модели построения распределенных приложений, которая позволила бы уменьшить сетевой трафик;

· заменить мосты более скоростными коммутаторами.

Но самым радикальным решением в такой ситуации является переход на более скоростную технологию. Если в сети используются традиционные технологии Ethernet или Token Ring, то переход на Fast Ethernet, FDDI или 100VG-AnyLAN позволит сразу в 10 раз увеличить пропускную способность каналов. С ростом масштаба сетей возникла необходимость в повышении их производительности. Одним из способов достижения этого стала их микросегментация. Она позволяет уменьшить число пользователей на один сегмент и снизить объем широковещательного трафика, а значит, повысить производительность сети. Более подходящими устройствами для микросегментации сетей стали коммутаторы.

ISO внесла большой вклад в стандартизацию сетей. *Модель управления* сети является основным средством для понимания главных функций систем управления сети. Эта модель состоит из 5 концептуальных областей:

· управление эффективностью;

· управление конфигурацией;

· управление учетом использования ресурсов;

· управление неисправностями;

· управление защитой данных.

13.4. Эффективность информационной сети.

Эффективность информационной сети — это ее способность достигать поставленную цель в заданных условиях применения и с определенным качеством.

Конкретизируя это понятие, можно сказать, что эффективность информационной сети — это характеристика, отражающая степень соответствия сети своему назначению, техническое совершенство и экономическую целесообразность. Понятие эффективности связано с получением некоторого полезного результата - эффекта использования информационных сетей. Эффект достигается ценой затрат определенных ресурсов, поэтому эффективность сети часто рассматривается в виде соотношения между эффектом (выигрышем) и затратами.

Показатель эффективности сети — количественная характеристика информационной сети, рассматриваемая применительно к определенным условиям ее функционирования. При оценке эффективности информационной сети необходимо учитывать характеристики трудовой деятельности человека, взаимодействующего с ЭВМ и другими техническими средствами сети. Следовательно, сеть рассматривается как система "человек-машина" (СЧМ). Показатель эффективности информационной сети определяется процессом ее функционирования, он является функционалом от этого процесса.

В общем виде:

$$W = W(t, L_П, L_{ТП}, L_A, L_Д, L_У)$$

где W — множество показателей эффективности сети,

t — время;

$L_П$, $L_{ТП}$, L_A, $L_Д$, $L_У$ — множества параметров соответственно входящих потоков запросов на обслуживание пользователей ($L_П$), технических и программных средств сети ($L_{ТП}$), алгоритмов обработки и передачи информации в сети (L_A), деятельности пользователей ($L_Д$), условий функционирования сети ($L_У$).

В свою очередь:

$$L_Д = \{L_Т, L_В, L_Н\},$$

где $L_Т$, $L_В$, $L_Н$ — множества выходных показателей деятельности пользователей информационной сети соответственно точностных ($L_Т$), временных ($L_В$), надежностных ($L_Н$).

Значения компонентов множеств $L_Т$, $L_В$, $L_Н$ определяются конкретными процессами деятельности пользователей в рассматриваемой информационной сети, средствами, которые имеются в их распоряжении для выполнения своих функций, и условиями работы.

В соответствии с конкретизацией понятия эффективности показатели множества W можно разделить на три группы:

$$W = \{W_Ц, W_Т, W_Э\},$$

где $W_Ц$ — показатели целевой эффективности информационной сети, или эффективности использования (целевого применения) информационной сети, это количественная мера соответствия сети своему назначению;

$W_Т$ — показатели технической эффективности информационной сети, это количественная мера, отражающая техническое совершенство сети;

$W_Э$ — показатели экономической эффективности информационной сети, это количественная мера экономической целесообразности сети.

13.4.1. Показатели целевой эффективности информационной сети

Выбор показателей целевой эффективности сети определяется ее назначением, в связи с чем имеет место большое многообразие показателей группы $W_Ц$. С помощью этих показателей оценивается эффект (целевой результат), получаемый за счет решения тех или иных прикладных задач на ЭВМ сети (с использованием общесетевых ресурсов - аппаратных, программных, информационных), а не вручную (если эти задачи вообще могут быть решены вручную в приемлемые сроки) или с использованием других, малоэффективных средств. Для количественной оценки этого эффекта могут применяться самые различные единицы измерения.

Примеры показателей целевой эффективности:

· точностные ($W_{ТН}$), надежностные ($W_Н$) и временные ($W_В$) показатели, применяемые в системах специального назначения для оценки эффективности использования в них сетевых структур. Например, прирост вероятности выполнения некоторого задания, сокращение времени на выполнение этого задания, повышение точности решения некоторой задачи;

· временные показатели целевого использования сетевых структур в управлении народным хозяйством на различных его уровнях, характеризующие повышение оперативности управления;

· показатели целевой эффективности информационной сети при решении задач планирования производства на различных его уровнях (отрасль, подотрасль, объединение, организация, фирма, предприятие и т.д.);

· показатели, характеризующие повышение качества продукции, технология производства которой включает использование информационной сети (например, использование ЛВС на предприятиях);

· показатели, характеризующие экономику производства продукции с применением сетевых структур (например, повышение производительности труда, увеличение объема выпускаемой продукции, снижение ее себестоимости, увеличение доли экспортируемой продукции и т.д.), если цель использования информационной сети заключается именно в улучшении характеристик производственно-хозяйственной деятельности предприятия или организации. В этом случае показатели целевой эффективности одновременно являются и показателями экономической эффективности.

Важнейшей характеристикой вычислительной сети является *надежность* - способность правильно функционировать в течение продолжительного периода времени. Это свойство имеет три составляющих: собственно надежность, готовность и удобство обслуживания.

Повышение надежности заключается в предотвращении неисправностей, отказов и сбоев за счет применения электронных схем и компонентов с высокой степенью интеграции, снижения уровня помех, облегченных режимов работы схем, обеспечения тепловых режимов их работы, а также за счет совершенствования методов сборки аппаратуры. Надежность измеряется *интенсивностью отказов и средним временем наработки на отказ*. Надежность сетей как распределенных систем во многом определяется надежностью кабельных систем и коммутационной аппаратуры.

Отказоустойчивость – это такое свойство вычислительной системы, которое обеспечивает ей как логической машине возможность продолжения действий, заданных программой, после возникновения неисправностей. Введение отказоустойчивости требует избыточного аппаратного и программного обеспечения. Направления, связанные с предотвращением неисправностей и отказоустойчивостью, основные в проблеме надежности. На параллельных вычислительных системах достигается как наиболее высокая производительность, так и, во многих случаях, очень высокая надежность. Имеющиеся ресурсы избыточности в параллельных системах могут гибко использоваться как для повышения производительности, так и для повышения надежности.

Повышение готовности предполагает подавление в определенных пределах влияния отказов и сбоев на работу системы с помощью средств контроля и коррекции ошибок, а также средств автоматического восстановления циркуляции информации в сети после обнаружения неисправности. Повышение готовности представляет собой борьбу за снижение времени простоя системы. Критерием оценки готовности является *коэффициент готовности*, который равен доле времени пребывания системы в работоспособном состоянии и может интерпретироваться как вероятность нахождения системы в работоспособном состоянии. Коэффициент готовности вычисляется как отношение среднего времени наработки на отказ к сумме этой же величины и среднего времени восстановления. Системы с высокой готовностью называют также отказоустойчивыми. Существуют различные градации отказоустойчивых компьютерных систем, к которым относятся и вычислительные сети. Приведем несколько общепринятых определений:

· ***высокая готовность*** - характеризует системы, выполненные по обычной компьютерной технологии, использующие избыточные аппаратные и программные средства и допускающие время восстановления в интервале от 2 до 20 минут;

· ***устойчивость к отказам*** - характеристика таких систем, которые имеют в горячем резерве избыточную аппаратуру для всех функциональных блоков, включая процессоры, источники питания, подсистемы ввода/вывода, подсистемы дисковой памяти, причем время восстановления при отказе не превышает одной секунды;

· ***непрерывная готовность*** - это свойство систем, которые также обеспечивают время восстановления в пределах одной секунды, но в отличие от систем устойчивых к отказам, системы непрерывной готовности устраняют не только простои, возникшие в результате отказов, но и плановые простои, связанные с модернизацией или обслуживанием системы. Все эти работы проводятся в режиме on-line. Дополнительным требованием к системам непрерывной готовности является отсутствие деградации, то есть система должна поддерживать постоянный уровень функциональных возможностей и производительности независимо от возникновения отказов.

13.4.2. Показатели технической эффективности информационной сети

С помощью этих показателей оценивается эффективность информационной сети как сложной аппаратно-программно-информационной кибернетической системы "человек-машина" при работе ее в различных режимах. При этом не принимается во внимание эффект, получаемый за счет реализации результатов решения задач (удовлетворения запросов) пользователей информационной сети. Показатели группы $W_Т$ могут использоваться для количественной оценки эффективности всей сети, ее отдельных систем и подсистем, звеньев и узлов сети. Для инвентаризационной ревизии и ревизии установленного оборудования предусмотрено использование центральной рабочей станции или сервера мониторинга которые работают с протоколом CMIP. Наряду с этим в настоящее время существует множество специализированных программ для сбора информации о работающих в сети устройствах. Цель инвентаризационной ревизии — Составление инвентаризационной описи всего программного и аппаратного обеспечения, используемого в сети. При этом цель ревизии установленного оборудования — это идентификация

местонахождения каждого элемента сети. Для анализа и решения проблемы в сети после сбора данных о работе следует составить список возможных причин; расставить приоритеты причин; используя средства управления сетью или метод замены, идентифицировать причины. Для оценки технической эффективности сети целесообразно использовать следующие показатели:

· $V_{ПД}$ — пропускная способность сети, т.е. средний поток данных, фактически передаваемых через сеть (измеряется в Мбит/с). Этот показатель может использоваться для оценки как многомагистральной информационной сети, так и одномагистральной (например, локальной сети, где данные передаются по моноканалу). Следует отличать фактическую пропускную способность канала или линии связи от физической пропускной способности V_K, которая определяется возможностями и свойствами передающей среды и является одним из главных ее параметров. Очевидно, что величина $V_{ПД}$ существенно зависит от физической пропускной способности канала или линии связи. Но она определяется и многими другими факторами: используемыми методами доступа в передающую среду, загрузкой канала, способами управления сетью, качеством и возможностями сетевой операционной системы и т.д. Все эти факторы обусловливают потоки передаваемых данных и фактическую скорость их передачи, т.е. фактическую (а не физическую) пропускную способность канала;

· $T_{ЗС}$ — задержка в сети, вносимая в передачу данных пользователя, т.е. время доставки сообщения от отправителя к получателю;

· $V_Ф$ — скорость передачи фреймов (коротких сообщений длиной 1000-2000 бит), т.е. количество фреймов, передаваемых за единицу времени по сети. Это дополнительный показатель, используемый в случае, когда поток данных (трафик) содержит в основном только короткие фреймы;

· $T_{ЗС} = f(V_{ПД})$ — зависимость времени задержки сообщения в сети от ее средней пропускной способности. Описание эффективности сети с помощью такой зависимости имеет большое значение, так как при увеличении загрузки сети (увеличении фактического потока данных) пользователь должен ожидать больше времени для начала передачи своих данных.

Для оценки технической эффективности отдельных звеньев информационной сети (узлов обработки информации, узлов связи, центров коммутации пакетов и т.д.), обслуживающих запросы пользователей сети, удобными оказываются следующие показатели.

1. Интегральная пропускная способность звена сети на отрезке времени $[0, t]$:

$$\delta_{И} = \frac{n_{о}(0, t)}{n_{п}(0, t)},$$

где $n_{о}(0, t)$, $n_{п}(0, t)$ — число запросов, соответственно обслуженных звеном сети на отрезке времени $[0, t]$ и поступивших на этом же отрезке.

Она показывает, как в среднем звено сети справляется с обслуживанием входящего потока запросов от момента начала отсчета работы до некоторого момента t (например, за смену, сутки, месяц).

2. Динамическая пропускная способность $\delta_{Д}(\Delta t, t)$, представляющая собой отношение числа запросов $n_{о}(\Delta t, t)$, обслуженных звеном сети на сравнительно небольшом интервале Δt к моменту времени t, к числу запросов $n_{п}(\Delta t, t)$, поступивших в звено на том же интервале Δt и к тому же моменту времени t:

$$\delta_{Д}(\Delta t, t) = \frac{n_{о}(\Delta t, t)}{n_{п}(\Delta t, t)}$$

Динамическая пропускная способность позволяет судить о том, как звено сети справляется с обслуживанием входящего потока запросов на любом заданном (наиболее характерном) отрезке времени к любому текущему моменту. Она дает возможность отслеживать работу звена сети в динамике и вырабатывать рекомендации по обеспечению ритмичности его функционирования.

3. Среднее время реакции звена сети на запрос пользователя - $T_Р$. Оно складывается из времени ожидания обслуживания запроса и времени собственно обслуживания. Этот показатель очень важен для оценки эффективности системы обслуживания при работе в интерактивном режиме.

4. Максимально возможное число активных абонентов, т.е. абонентов, обращающихся с запросами на обслуживание в данный момент.

5. Коэффициент задержки обслуживания абонентов; это отношение среднего времени реакции на запрос абонента при максимальном количестве активных абонентов к этому же времени при минимальном их количестве.

13.4.3. Показатели экономической эффективности информационной сети

Для оценки экономической эффективности всей сети или отдельных ее элементов и звеньев могут использоваться две группы показателей: интегральные показатели и частные показатели.

С помощью интегральных показателей оценивается общий (суммарный, интегральный) эффект, а затем и интегральная экономическая эффективность информационной сети (элемента или звена сети) с учетом всех капитальных и текущих (эксплуатационных) затрат и всей экономии за счет использования информационной сети, т.е. по всем источникам прямой и косвенной экономии и по всем ее видам.

Частные показатели необходимы для оценки частного экономического эффекта, получаемого по отдельным источникам экономии, которые создаются при внедрении новых аппаратных, программных, информационных средств или новых технологий работы информационной сети.

В качестве интегральных показателей экономической эффективности информационной сети можно рекомендовать давно апробированные показатели:

$Э_Г$ — годовой экономический эффект, руб;

$\tilde{Э}_г$ — среднегодовой экономический эффект, руб;

$Э_П$ — полный экономический эффект за расчетный период, руб;

$Е_Э$ — коэффициент экономической эффективности капитальных вложений (или единовременных затрат, имеющих характер капитальных вложений) на создание и внедрение всей сети или отдельных ее элементов или на совершенствование и развитие сети, 1/год;

$Т_{ОК}$ — срок окупаемости этих капитальных вложений, год.

Эти показатели могут быть как ожидаемыми (при априорной оценке), так и фактическими (при апостериорной оценке). Использование исследуемой системы экономически целесообразно, если выполняются условия:

$$Е_Э \geq Е_Н \text{ или } Т_{ОК} \geq Т_Н,$$

Где $Т_Н$ — нормативный срок окупаемости капитальных вложений,

$Е_Н$ — нормативный коэффициент экономической эффективности капитальных вложений.

Оценка частного экономического эффекта от внедрения новых аппаратных, программных, информационных средств или новых технологий работы информационной сети проводится с целью:

· обоснования экономической целесообразности их внедрения (особенно тех средств и технологий, экономическая эффективность которых вызывает сомнение и которые вместе с тем не дают сколько-нибудь заметного целевого эффекта, ради которого можно было бы пожертвовать экономическим эффектом);

· определения влияния этих средств и технологий на интегральную экономическую эффективность;

· сравнения конкурирующих вариантов внедряемых средств и технологий по частным показателям, поскольку в ряде случаев именно эти показатели имеют решающее значение при выборе того или иного варианта.

Частные показатели отличаются большим многообразием. Примеры частных показателей: сокращение численности обслуживающего персонала всей сети или отдельных ее систем, элементов, звеньев за счет внедрения новых средств и технологий; годовая экономия на текущих затратах за счет продления эффективного срока эксплуатации сети, вызванного совершенствованием профподготовки ее обслуживающего персонала; годовая экономия на текущих затратах за счет реализации мероприятий, направленных на улучшение условий труда обслуживающего персонала и, следовательно, способствующих повышению эффективности их трудовой деятельности, и др.

13.5. Методы оценки эффективности информационных сетей

Эффективность информационной сети оценивается на различных стадиях жизненного цикла сети — от этапа ее проектирования, когда выполняется априорная (доопытная) оценка с целью определения ожидаемой эффективности и решения вопроса о целесообразности реализации проекта, до этапа эксплуатации, когда проводится апостериорная (послеопытная, на основе конкретного опыта эксплуатации) оценка с целью определения фактической эффективности, подтверждающей или в какой-то степени опровергающей прогнозы. Апостериорная оценка обычно проводится методами прямого счета с использованием аналитических соотношений, характеризующих влияние различных факторов и параметров на показатели эффективности. Гораздо более сложной и трудоемкой задачей является априорная оценка, которая, как правило, осуществляется с помощью методов математическою моделирования. К математическим моделям сложных кибернетических человеко-машинных систем (информационные сети представляют собой именно такие системы), работающим в диалоговом режиме, когда необходимо учитывать характеристики человека (пользователя, оператора, администратора сети), предъявляется ряд требований.

Существуют два класса математических моделей - аналитические и имитационные, отличающиеся принципами построения и методами исследования. В аналитических моделях весь процесс функционирования исследуемой системы и отдельные его части представляются аналитически, в виде функциональных зависимостей (алгебраических и логических соотношений, интегрально-дифференциальных уравнений). В имитационных моделях процесс функционирования описывается (отображается) алгоритмически. Преимущества и недостатки аналитических и имитационных моделей широко известны. Задача состоит в том, чтобы при исследовании эффективности системы использовать те и другие модели комплексно, в рациональном сочетании.

Цель ревизии эффективности — это определение того, работает ли сеть в соответствии со своим потенциалом. В отчет о проведении оценки должны быть включены журналы, показывающие тенденцию к уменьшению скорости трафика в определенных сегментах сети.

Контрольные вопросы:

1. Какие основные требования предъявляются к сетям?
2. Что такое производительность сети?
3. Какие характеристики влияют на производительность сети?
4. Какие есть способы повышения производительности сетей?
5. Как обеспечить высокоскоростную пересылку трафика?
6. Чем обеспечивается надежность сети?
7. Что такое отказоустойчивость?
8. Что такое прозрачность сетей?
9. Что такое прозрачное соединение?
10. Назовите показатели целевой эффективности информационной сети.

Практические задания:

ЗАДАНИЕ № 13.1. Анализ сетевого трафика.

Подготовка. Для данной лабораторной работы требуется следующее.

1. Установить программное обеспечение сбора и анализа содержимого сетевых пакетов, например, Wireshark (наследник Ethereal, http://www.wireshark.org).

2. Желательно подготовить несколько протоколов прослушивания сетевых соединений. Для подготовки протокола (дампа) нужно запустить Wireshark, стартовать в нем захват трафика и выполнить какую-либо сетевую операцию.

? Получить или отправить почту.

? Передать или принять файл по ftp.

? Подключиться к удаленному узлу, используя telnet или ssh.

? Подключиться к сетевому диску.

? Выполнить команду ping или tracert (traceroute) и т.д.

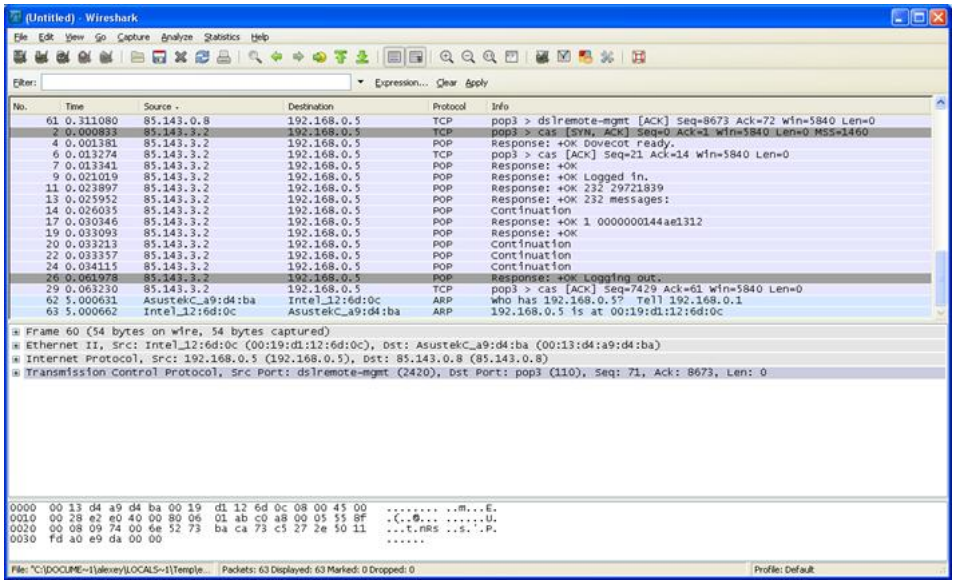
Когда накопится достаточное количество пакетов, захват трафика останавливается, протокол записывается в файл и может быть выдан слушателю для расшифровки.

Достаточно сохранить несколько десятков пакетов, но желательно, чтобы рассматриваемая операция была выполнена с начала до конца. **Внимание!** Если Вы используете при сборе данных собственный компьютер или информацию, то в случае использования небезопасных приложений (например, telnet) собранные протоколы могут содержать Вашу конфиденциальную информацию.

Цель работы: Получение практических навыков анализа сетевого трафика.

Краткое описание. Имеется фрагмент сетевого трафика, собранного на узле. Необходимо определить, в каких видах сетевого взаимодействия участвовал данный узел.

Постановка задачи: В качестве исходных данных можно использовать либо трафик, собранный непосредственно на практической работе, либо подготовленный преподавателем. Требуется провести анализ трафика и определить виды сетевого взаимодействия, в которых участвовал узел в период сбора его трафика.



Требуемые результаты.

Отчет о выполненной работе, содержащий:

v постановку задачи;

v описание типов взаимодействия с указанием пакетов, подтверждающих ваши выводы;

v если имеется – конфиденциальная информация, которую Вы извлекли из трафика.

ЗАДАНИЕ № 13.2. Инвентаризация ПО.

a. Собрать и описать общие сведения о своей инфраструктуре, сети.

b. Провести полную инвентаризацию программного обеспечения, установленного на всех ваших компьютерах. Как правило, ручной вариант инвентаризации не подходит, нужно пользоваться специальными программами по инвентаризации ПО, о них есть информация в следующем разделе.

c. Подсчитать приобретённые ранее лицензии, сравнить их с количеством установленных программных продуктов и проверить соблюдение лицензионных условий.

d. Разработать типовые конфигурации рабочих мест, правила использования программного обеспечения, приказы, инструкции и другие регулирующие документы.

e. Удалить лишние программы, докупить (если не хватает) лицензии, установить на компьютеры ПО в соответствии с разработанными типовыми конфигурациями. Подписать внутренние документы (правила использования ПО, приказы, регламенты, инструкции), довести их до сведения сотрудников.

Главные правила, которых нужно придерживаться, чтобы поддерживать порядок в ПО, после его наведения.

Некоторые из этих пунктов очень помогут Вам к тому же и при проверках правоохранительных органов:

v В компании должна быть разработана, подписана руководителем и донесена до сотрудников политика использования ПО (правила использования ПО) – нужно это для того, чтобы сотрудники не ставили на компьютеры неположенный софт и понимали, что компания серьезно относится к вопросам поддержания порядка в ПО. Полезно вывесить эту политику в рамочке на видном месте.

v Выпустить приказ об обязательном использовании только легально приобретённого программного обеспечения, о порядке его установки и удаления, включая наказания за нарушение этих правил.

v Регулярно, как минимум раз в полгода, нужно проводить инвентаризацию ПО и проверять соответствие используемого ПО купленным лицензиям.

v Поддерживать и своевременно обновлять базу данных (перечень) лицензий и хранилище документов, подтверждающих лицензионность (легальность использования) ПО. Назначить ответственного, который будет поддерживать эти базы в актуальном состоянии и при внутренних или внешних проверках быстро предоставит всю информацию.

v Хорошо бы описать и строго выполнять несколько базовых бизнес-процедур, описывающих:

1. Как и на каком основании вы приобретаете ПО.
2. Каким образом учитываются и хранятся приобретённые лицензии и комплектующие поставки.
3. Каким образом и на каком основании ПО устанавливается на компьютеры пользователей.

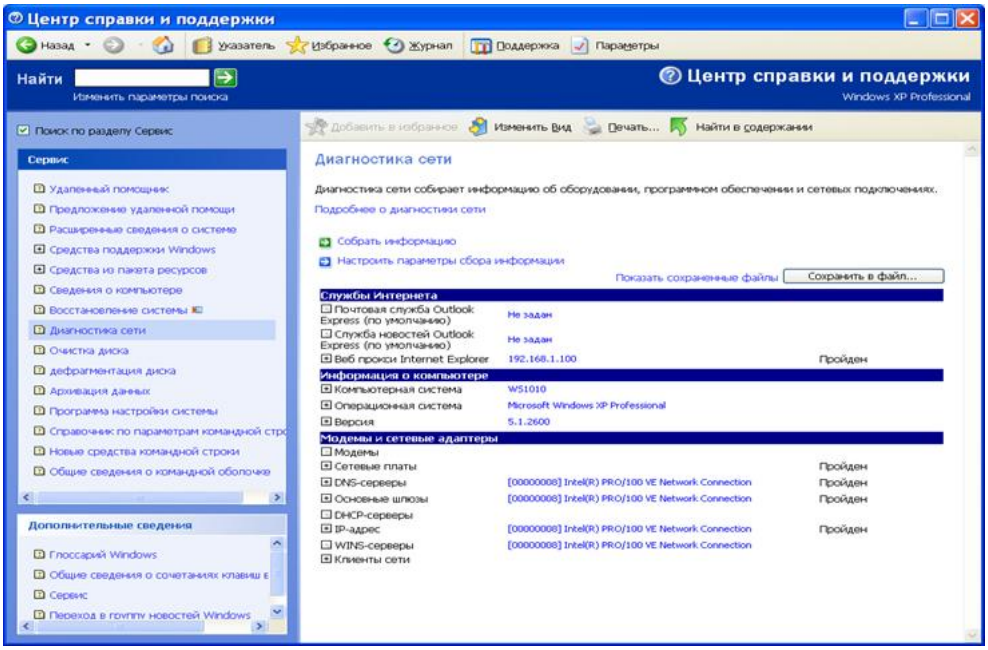
Бесплатные средства инвентаризации ПО.

· Бесплатное средство, позволяющее определять, какое программное обеспечение Майкрософт установлено на компьютерах – Microsoft Software Inventory Analyzer: http://go.microsoft.com/?linkid=9639471

· Другие бесплатные средства для инвентаризации ПО вы можете найти на следующем ресурсе: http://www.bsa.org/country/Tools%20and%20Resources/Free%20Software%20Audit%20Tools.aspx

ЗАДАНИЕ № 13.3. Диагностика сети.

Одна из наиболее полезных новых коммуникационных функций XP — утилита Network Diagnostics, программа для диагностики и устранения системных и сетевых проблем. Network Diagnostics позволяет узнать текущий статус Internet-служб (почты, новостей), получить сведения о компьютере (системное имя, тип загрузки, объем RAM), информацию об операционной системе (номер сборки, дату установки, номер версии), а также проверить статус модемов и сетевых адаптеров. Чтобы запустить Network Diagnostics, нужно выбрать пункт Scan your system (Start, Control Panel, Network and Internet Connections, Network Diagnostics). При тестировании сетевых адаптеров Network Diagnostics проверяет статус драйверов сетевых адаптеров и опрашивает шлюз, настроенный по умолчанию, основной и вторичный DNS-серверы, а также локальный IP-адрес. Утилита выводит отметки Passed или Failed для каждого проверяемого сетевого компонента и предоставляет другую полезную информацию о сети, в том числе IP-адреса шлюза, сервера DNS и сканируемого компьютера. Результаты работы Network Diagnostics могут быть сохранены в файле, который при необходимости можно переслать по электронной почте или FTP в службу поддержки. Усовершенствованы также коммуникационные возможности XP в области беспроводной связи. XP позволяет выполнять сканирование на наличие беспроводной сети и автоматически настраивать сетевые карты стандарта 802.11 для подключения к ней. Эта функция полезна для мобильных пользователей при подключении к общедоступным ресурсам. XP поддерживает стандарт IEEE 802.1X для выполнения аутентификации при сетевом доступе. С помощью «Центра справки и поддержки» запустить диагностику сети и просмотреть результаты. Также можно запустить диагностику с помощью команды : C:\WINDOWS\system32\netsh.exe diag gui



ЗАДАНИЕ № 13.4. Мониторинг и оптимизация системы.

Часть 1

МОНИТОРИНГ И ОПТИМИЗАЦИЯ СИСТЕМЫ.

1. Вызовите Диспетчер задач.

О Просмотрите все запущенные приложения.

О Какие процессы запущены в системе? Почему их больше, чем приложений?

О Для каждого процесса покажите в окне следующие счетчики:

u Имя образа

u Время ЦП

u Память максимум

u Объем виртуальной памяти

u Базовый приоритет

u Счетчик потоков

О Сравните процессы по этим показателям

О Как изменить приоритет некоторого процесса? На что это влияет? Какие процессы имеют высокие приоритеты? Почему?

О Посмотрите на вкладке Быстродействие общую картину потребления ресурсов вашего компьютера. Запустите несколько приложений. Проверьте, изменилась ли картина.

О Как можно убрать свернутое окно Диспетчера задач с панели задач, чтобы не занимать место на ней? Как тогда вызвать Диспетчер задач?

2. Вызовите оснастку Просмотр событий.

О Какие типы основных журналов можно просматривать в этой оснастке?

О Какие существуют типы событий?

О Какие параметры можно увидеть для каждого события? (Просмотрите их через окно свойств события.)

О Отсортируйте события в окнах журналов: журнал Приложений – по типу событий (Ошибки, Предупреждения, Уведомления); журнал системы – по дате возникновения событий).

О В окне журнала событий системы оставьте только столбцы: Тип, Дата, Время, Категория, Источник.

О В журнале Безопасности проведите фильтрацию событий: оставьте только аудит отказов за последние 2 недели.

О Создайте свой журнал событий, содержащий только сведения об ошибках приложений.

О Просмотрите окна свойств журналов. Для своего журнала установите максимальный размер журнала 100 кб и флажок: Затирать старые события по необходимости. Какие еще действия возможны при достижении максимального размера журнала?

О Сархивируйте ваш журнал. Какие типы файлов для архивации можно выбрать? Выберите двоичный файл (расширение .evt). Удалите свой журнал, а затем откройте сохраненный вами на диске файл журнала. Что изменилось в этом журнале по сравнению с тем, что вы сохраняли? Сохраните журнал в текстовом виде. Можно ли открыть затем такой журнал в данной оснастке? Откройте его в программе Блокнот.

О Создайте инструмент для просмотра событий на другом компьютере. Просмотрите их.

3. Запустите оснастку Производительность (работа с Системным монитором).

О Просмотрите, какие в системе существуют объекты производительности.

О Просмотрите основные счетчики оного из объектов. Как получить разъяснение, что отображает этот счетчик?

О Откройте объект процесс. Как можно добавить счетчик для конкретного процесса (Запустите, например, WORD и просмотрите для него некоторые счетчики.).

О Просмотрите, какие в системе есть потоки (например, потоки того же процесса WORD). Добавьте счетчики Текущий приоритет для потоков WORD, и посмотрите, как они изменяются при переходе в окно программы WORD и обратно.

О Удалите какой-нибудь счетчик (Кнопка Удалить панели инструментов).

О Создайте документ в программе WORD и поместите в него элемент управления System Monitor, в котором отражена степень загрузки центрального процессора.

О Ознакомьтесь с настройкой внешнего вида представления информации в окне вывода программы Системный монитор: введите названия графика. подпись по вертикальной оси, удаления панели инструментов.

О Рассмотрите возможность представления информации в окне вывода в виде гистограммы, отчета.

О Для диагностики узких мест:

u Для процессора проверьте счетчики: Процессор \ %загруженности процессора, Система \ длина очереди к процессору. Запустите несколько приложений, определите, какое из них в большей степени загружает процессор (через счетчики Процесс \ % загрузки процессора).

u Для проверки использования памяти введите счетчики Память \Доступно байт (не должен быть меньше 4 Мбайт), Память \ Обмен страниц. Затем запустите несколько приложений и проследите, как в динамике изменяются их рабочие множества (счетчик Процесс \ Рабочее множество).

u Для дисковой памяти: добавьте счетчики объекта Физический диск: Обращений чтения с диска / сек, Текущая длина очереди диска, % активности диска. Сравните, какие они для разных компьютеров в вашей сети. Эти счетчики определяют производительность вашей дисковой системы, если они стали с течением времени заметно увеличиваться, то необходимо дополнительно протестировать дисковую подсистему с использованием счетчиков: Физический диск \ Среднее время обращения к диску (должно быть не более 0,3 сек.), Физический диск \ Средний размер одного обмена с диском (хороший показатель должен быть в районе 20 кбайт).

О Встройте экраны с наиболее интересными показаниями счетчиков в отчет по практической работе.

4. Работа с оснасткой Оповещения и журналы производительности.

О Создайте свой журнал счетчиков. Файл должен быть двоичным, содержать счетчики, определяющие производительность ПК (счетчики, определяющие загруженность процессора отдельными процессами). Файл должен быть ограничен по размеру и собирать данные в течение ближайших 5 минут.

О Создайте текстовый журнал (типа TSV) и откройте его в программе EXCEl.

О В окне Системный монитор просмотрите в разных режимах (график, диаграмма, отчет) собранную информацию от разных счетчиков. Для этого:

u В окне вывода щелкните правой кнопкой мыши и выберите опцию Свойства.

u Перейдите на вкладку Источник и укажите свой файл журнала. Здесь же можно указать период времени, за который нужно вывести данные.

u Перейдите на вкладку Данные и укажите, данные каких счетчиков необходимо вывести.

О Создайте свой журнал оповещений. Задайте несколько условий, при которых будут возникать оповещения (например: Процессор \ % загрузки процессора больше некоторого значения, Система \ Длина очереди больше 1 и т.д.). Установите фиксацию таких событий в журнале. Затем через журнал приложений посмотрите, возникали ли такие ситуации. Задайте возможность посылки сообщения по сети.

5. Создайте изолированную оснастку по управлению службами.

О Посмотрите список запущенных на компьютере служб.

О Найдите службу сообщений. Получите вкладку свойств этой службы. На вкладке Общие посмотрите, какой файл обеспечивает работу этой службы, какие типы запуска служб существуют. Остановите службу.

О Изучите возможности других вкладок.

6. Запустите инструмент Управление компьютером. Откройте оснастку Управление дисками.

О На сколько разделов и какого типа разбит диск вашего компьютера.

О Какие логические диски сформированы в разделах.

О Сколько дисков можно создать в основном разделе, а сколько в дополнительном?

О Можно ли определить, на каком диске находится каталог с системными файлами ОС Windows 2000, а на каком находятся файлы, участвующие в процессе загрузки (файлы NTLDR, BOOT.INI, HAL.DLL и т.д.).

О Какие файловые системы сформированы на логических дисках.

О В каком режиме работает ваш диск?

О Есть ли на диске нераспределенное пространство. Есть ли возможность создать в нем или его части раздел. Если есть, создайте в нем основной раздел, сформируйте в нем логический диск и отформатируйте его для системы NTFS.

О Можно ли с помощью этой оснастки отформатировать дискету? Если нет, как это сделать. Можно ли на дискете создать ФС NTFS?

7. Посмотрите возможности оснастки Логические диски.

8. Посмотрите, фрагментированы ли ваши диски. Какие файловые системы подвержены фрагментации?

9. Посмотрите через Диспетчер устройств, какие устройства установлены на вашем ПК и все ли они работают нормально. Какие ресурсы заданы для устройств? Как определить, какой драйвер управляет устройством?

10. Все ли драйверы и системные файлы снабжены в системе цифровой подписью? Как определить реакцию системы на попытку установки драйвера без цифровой подписи?

11. Посмотрите возможности управления электропитанием. Какие схемы заданы и чем они отличаются? Ознакомьтесь с возможностями вкладки Дополнительно. Что такое спящий режим?

Часть 2

РАБОТА С ПОДСИСТЕМОЙ БЕЗОПАСНОСТИ.

1. Установите в системе срок действия пароля не менее 2 и не более 30 дней.

2. Запретите использование пустых паролей.

3. Установите неповторимость паролей (заставьте пользователя употреблять по крайней мере 3 разных пароля).

4. Проверьте возможности блокировки компьютера при 5 неудачных попытках регистрации. Кто может разблокировать компьютер?

5. Присвойте некоторому пользователю право в системе архивировать и восстанавливать все каталоги (проделайте это несколькими способами). Откажите некоторому пользователю в возможности регистрироваться локально.

6. Установите в системе правило не отображать имени последнего регистрировавшегося пользователя.

7. Установите консоль с оснасткой Групповая политика. Посмотрите и проверьте действенность ограничений на рабочую среду пользователя.

8. Как влияет добавление или удаление административных шаблонов на оснастку?

9. Создайте консоль, содержащую оснастку Шаблоны безопасности.

10. Возьмите за основу один из административных шаблонов и настройте свой, сохранив под другим именем.

11. Проанализируйте, насколько ваша система отличается от этого шаблона.

ЗАДАНИЕ № 13.5. Мониторинг сетевых протоколов и служб.

Практическая работа позволяет изучить применение Сетевого монитора для анализа сетевых пакетов, изучить применение программы "Диспетчер задач" для оперативного анализа производительности работы системы, изучить применение консоли "Производительность" для анализа производительности работы системы.

Упражнение 1. Диспетчер задач.

Цель упражнения: Изучить применение программы "Диспетчер задач" для оперативного анализа производительности работы системы.

Исходная конфигурация компьютера: Компьютеры с операционной системой Windows 2003 Server с созданными контроллерами домена.

Результат: Результаты наблюдений функционирования системы.

Предварительные навыки: Общие сведения о *Диспетчере задач.*

1. Запустите программу *Диспетчер задач:*

o Нажать комбинацию клавиш CTRL+SHIFT+ESC

o Щелкнуть правой кнопкой мыши на Панели задач и выбрать из меню *Диспетчер задач*

o Нажать комбинацию клавиш CTRL+ALT+DELETE, нажать кнопку *Диспетчер задач*

o Кнопка *"Пуск"* — *"Выполнить"* — Ввести *"taskmgr"* — Кнопка *"ОК"*

2. Настройте параметры программы:

Закладка *"Процессы"* —

Меню *"Параметры"* — Убрать галочку у поля *"Поверх остальных окон"* —

Меню *"Вид"* — *"Скорость обновления"* - *"Низкая"* —

Меню *"Вид"* — *"Выбрать столбцы"* - поставить галочки у полей

o *"Идентификация процесса (PID)"*

o *"Имя пользователя"*

o *"Объем виртуальной памяти"*

Кнопка *"ОК'*

3. Изучите работу с программой:

Запустите несколько приложений, изучите поведение системы на закладках *"Приложения", "Процессы", "Быстродействие"*

На закладке *"Процессы"* попробуйте остановить выполнение запущенных вами приложений — щелкнуть правой кнопкой мыши на имени процесса, выбрать *"Завершить процесс"*

На закладке *"Процессы"* попробуйте изменить приоритет какого-либо процесса — щелкнуть правой кнопкой мыши на имени процесса, выбрать *"Приоритет",* выбрать значение приоритета

4. Закройте программу.

Упражнение 2. Мониторинг производительности.

Цель упражнения: Изучить применение консоли "Производительность" для анализа производительности работы системы.

Исходная конфигурация компьютера: Компьютеры с операционной системой Windows 2003 Server с созданными контроллерами домена.

Результат: Проведенный анализ производительности работы системы.

Предварительные навыки: Общие сведения о консоли "Производительность"

Работа с Системным монитором.

1. Откройте консоль *Производительность:*

Кнопка *"Пуск"* — *"Все программы"* — *"Администрирование"* — *"Производительность"*

2. Добавьте счетчик *"Система/Длина очереди процессора"*

Щелкнуть кнопку на  панели инструментов (или CTRL+I) —

Выберите объект "Система" —

Выберите счетчик "Длина очереди процессора" —

Кнопка "Добавить" —

Кнопка "Закрыть"

3. Понаблюдайте за значениями счетчиков в процессе работы системы.

Работа с Журналами производительности.

1. Создайте новый журнал счетчиков:

В левой части окна консоли раскройте "Журналы и оповещения производительности", выберите "Журналы счетчиков" —

2. Создайте новый журнал:

Меню *"Действие"* — "Новые параметры журнала" —

Введите имя журнала (например, NewLog) — Кнопка *"ОК'* —

Добавьте счетчики (кнопка *"Добавить счетчики")*

- *"Процессор\% загруженности процессора"* (кнопка *"Добавить"*)
- *"ПамятьОбмен страниц в сек"* (кнопка *"Добавить"*)
- *"Физический диск\Средняя длина очереди диска"* (кнопка *"Добавить"*)
- *"Система/Длина очереди процессора"* (кнопка *"Добавить"*)

Кнопка *"Закрыть"*

3. Задайте интервал снятия показаний — *1 сек*

Кнопка *"Применить"*

4. Задайте режим запуска журнала:

Закладка *"Расписание*" —

Выберите *"Вручную (с помощью контекстного меню)"*

Кнопка *"ОК"*

5. Запустите журнал:

Щелкнуть правой кнопкой мыши на имени журнала —

Выбрать *"Запуск"*

6. Закройте консоль

7. Запустите приложения, использующие большой объем ресурсов компьютера (например, копирование большого объема данных с одного раздела диска на другой)

8. После завершения работы приложений снова запустите консоль *Производительность*

9. Остановите журнал:

Щелкнуть правой кнопкой мыши на имени журнала —

Выбрать "Остановка"

10. Изучите накопленные значения счетчиков:

Перейдите в окно *Системного монитора* —

Удалите все счетчики реального времени —

Откройте журнал счетчиков (кнопка на панели инструментов ) —

Выберите источник данных (выберите *"Файлы журнала",* кнопка *"Добавить"*, укажите путь к сохраненному журналу, например, "X:\Perflogs\NewLog_000001.blg') —

Кнопка *"Открыть"* — Кнопка *"Применить"* —

Добавьте счетчики (закладка *"Данные",* кнопка *"Добавить",* добавьте все накопленные счетчики) —

Кнопка *"Закрыть"* — Кнопка *"ОК'*

Упражнение 3. Сетевой монитор.

Цель упражнения: Изучить применение *Сетевого монитора* для анализа сетевых пакетов.

Исходная конфигурация компьютера: Компьютеры с операционной системой Windows 2003 Server с созданными контроллерами домена.

Результат: Проведенный анализ захваченных сетевых пакетов

Предварительные навыки: Общие сведения о *Сетевом мониторе.*

Установка Сетевого монитора.

Установите *Сетевой монитор:*

Кнопка *"Пуск"* — "*Панель управления"* —

"*Установка и удаление программ"* —

Кнопка *"Установка компонентов Wndows*" —

"*Средства управления и наблюдения"* — кнопка *"Состав"* —

Выбрать "*Средства сетевого монитора"* —

Кнопка *"ОК'* — Кнопка "*Далее"* (если потребуется, укажите путь к дистрибутиву операционной системы) —

Кнопка "*Готово"*

Работа с Сетевым монитором.

1. Запустите *Сетевой монитор:*

Кнопка *"Пуск"* — *"Все программы"* — *"Администрирование"* — *"Сетевой монитор"*

2. Выберите сетевой адаптер:

Кнопка *"ОК'* —

Раскрыть *"Локальный компьютер"* — Выбрать сетевой адаптер — Кнопка *"ОК'*

3. Запустите захват сетевых пакетов:

Меню *"Запись"* — *"Запустить"*

4. Запустите какой-либо процесс передачи данных по сети (например, копирование данных из сетевой папки с компьютера партнера на свой компьютер)

5. Остановите процесс захвата пакетов:

Меню *"Запись"* — *"Остановить"*

6. Просмотрите структуру и содержимое захваченных пакетов:

Меню *"Запись"* — *"Отобразить записанные данные"* (откроется список захваченных пакетов)

Щелкните двойным щелчком мыши на одном из пакетов, окно просмотра разделится на три части — список пакетов, структура выделенного пакета, содержимое выделенного пакета

В разделе структуры пакетов изучите заголовки пакетов (FRAME, ETHERNET, IP, TCP)

В разделе содержимого изучите содержимое пакетов (попробуйте найти пакет с текстом одного из файлов, которые в процессе захвата пакетов пересылался по сети)

7. Закройте *Сетевой монитор*

Перечень литературы и Интернет-ресурсов:

1. Брентон К. Разработка и диагностика многопротокольных сетей. – М.: Лори, 1999. –410 с.

2. Калачанов В.Д., Кобко Л.И. Экономическая эффективность внедрения информационных технологий. Учебное пособие - Москва: МАИ, 2006.- 180 с.,ISBN 5-7035-1674-9

3. Качество и эффективность информационных систем — http://rus-lib.ru/book/38/men/21/2.5.html

4. Оптимизация IP-трафика — http://www.citforum.ru/nets/hard/accelerator/

5. Средства анализа и оптимизации локальных сетей — http://www.citforum.ru/nets/optimize/index.shtml

6. Уилсон Э. Мониторинг и анализ сетей. Методы выявления неисправностей. – М.: Лори, 2002. – 350 с.

7. Хогдал А. Анализ и диагностика компьютерных сетей. – М.: Лори, 2000. –353 с.

Тема 14. Сетевые программные средства информационных сетей

Цели:

· Понять преимущества сетевых ОС.

· Получить представление о критериях для выбора ОС.

· Уметь организовать любую деятельность, связанную с передачей данных и выполнять функции прикладных программ сети.

Сетевая операционная система (ОС) составляет основу любой вычислительной сети. Каждый компьютер в сети в значительной степени автономен, поэтому под сетевой операционной системой в широком смысле понимается совокупность операционных систем отдельных компьютеров, взаимодействующих с целью обмена сообщениями и разделения ресурсов по единым правилам – протоколам. В узком смысле сетевая ОС – это операционная система отдельного компьютера, способная работать в сети.

Сетевые операционные системы (Network Operating System –NOS) – это комплекс программ, обеспечивающих обработку, хранение и передачу данных в сети.

Сетевая операционная система выполняет функции прикладной платформы, предоставляет разнообразные виды сетевых служб и поддерживает работу прикладных процессов, выполняемых в абонентских системах. Сетевые операционные системы используют клиент серверную либо одноранговую архитектуру. Компоненты NOS располагаются на всех рабочих станциях, включенных в сеть.

NOS определяет взаимосвязанную группу протоколов верхних уровней, обеспечивающих выполнение основных функций сети. К ним, в первую очередь, относятся:

· адресация объектов сети;

· функционирование сетевых служб;

· обеспечение безопасности данных;

· управление сетью.

Сетевые операционные системы ограничены областью своего действия. Сетевые супервизоры (управляющие программы) поддерживают работу одной или нескольких взаимодействующих локальных сетей. Если взаимодействуют несколько сетей (организована интерсеть), то сетевое программное обеспечение реализуется также в шлюзах и мостах, связывающих эти сети, а все сетевые объекты (рабочие станции, серверы), принадлежащие разным сетям, подчиняются общему адресному пространству.

Сетевые операционные системы, поддерживая распределенное выполнение процессов, их взаимодействие, обмен данными между процессорами, доступ пользователей к общим ресурсам и другие функции, выполняют важные системные требования к распределенной системе как к целостной и многопользовательской.

14.1. Сетевые оболочки и встроенные средства.

На практике сложилось несколько подходов к построению сетевых операционных систем (рис.14.1):

Использование существующей локальной ОС и надстроенной над ней *сетевой оболочки*. При этом в локальную ОС встраивался минимум сетевых функций необходимых для работы сетевой оболочки, которая выполняла основные сетевые функции. Такой подход был характерен для первых сетевых ОС персональных компьютеров (например, MS DOS и оболочка клиента NetWare), однако он используется и в современных ОС (например, LANtastic или Personal Ware).

Разработка операционных систем, изначально предназначенных для работы в сети. Сетевые функции у этих ОС глубоко *встроены* в основные модули системы, что обеспечивает ее логическую стройность, простоту эксплуатации и модификации, а также высокую производительность. Примером такой ОС является система Windows NT фирмы Microsoft.

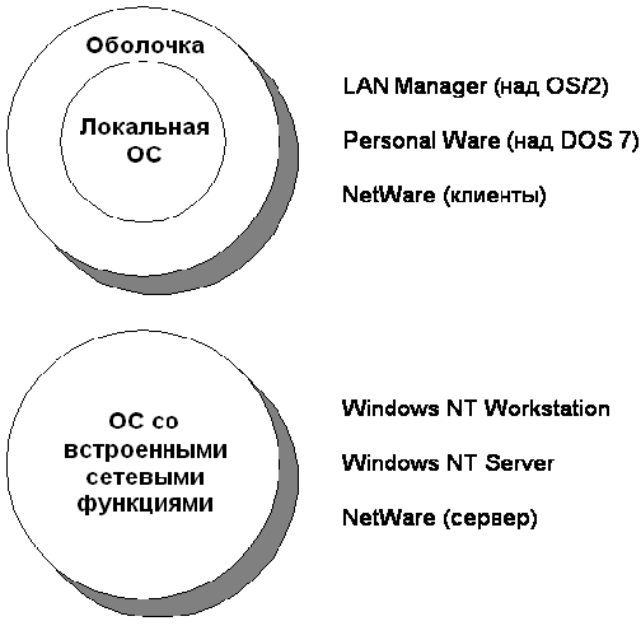


Рис.14.1. Варианты построения сетевых ОС

14.2. Основные компоненты сетевой ОС.

В сетевой операционной системе отдельной машины можно выделить несколько частей
1. Средства управления локальными ресурсами компьютера.
2. Средства предоставления собственных ресурсов и услуг в общее пользование - серверная часть ОС (сервер).
3. Средства запроса доступа к удаленным ресурсам и услугам и их использования - клиентская часть ОС (редиректор).
4. Коммуникационные средства ОС, с помощью которых происходит обмен сообщениями в сети.

В зависимости от функций, возлагаемых на конкретный компьютер, в его операционной системе может отсутствовать либо клиентская, либо серверная части.

Рис.14.2. Структура сетевой ОС

14.3. Требования к сетевым операционным системам.

Различают следующие системные требования:
- единая системная архитектура;
- обеспечение требуемого высокого уровня прозрачности;
- высокоуровневая и высоконадежная файловая система.

Единая системная архитектура. Понятие "системная архитектура" охватывает следующие вопросы:
- распределение функций между узлами сети;
- принципы построения коммуникационных протоколов;
- методы выполнения отдаленных операций типа «клиент-сервер»;
- структуру сетевой файловой системы;
- уровни прозрачности доступа к сети;
- принципы защиты данных;
- свойства общесетевого адресного пространства. Примером может служить адресация в Internet.

Обеспечение требуемого высокого уровня прозрачности. Сетевая операционная система должна обеспечивать для пользователей доступ к многообразным сетевым ресурсам независимо от степени распределенности, неоднородности и мобильности данных, программ и устройств. Высокий уровень прозрачности означает, что обеспечиваются прозрачность доступа, прозрачность имен, прозрачность физических устройств и сетевой среды и т.д. Сетевая операционная система изолирует от пользователя все различия, особенности и физические параметры привязки процессов к обрабатываемым сетевым ресурсам. Например, пользователь может обратиться к процессу печати определенных данных, называя их уникальными составными именами, но совершенно не заботится о том, где практически находятся эти данные, и на каком физическом принтере они будут распечатаны.

Высокоуровневая и высоконадежная файловая система. Файловая система, поддерживаемая сетевой операционной системой и входящая в ее состав, должна эффективно организовать хранение информации общего пользования и обеспечивать одновременный доступ к ней многих пользователей. Высокоуровневость означает, что доступ обеспечивается как к локальным файлам (расположенным на рабочих станциях), так и к удаленным (на серверах) на различных уровнях (справочник файлов; файл; именованный блок; сегмент файла). В сетевом режиме должны поддерживаться разнообразные операции с файлами (читать, писать, удалять, модифицировать). Протокол удаленного доступа и управления файлами должен обеспечивать все необходимые сетевые функции создания, обработки, пересылки и защиты файла.

Файловая система - центральный элемент сетевой операционной системы, определяющий производительность и надежность всей распределенной системы в целом.

По предназначению файловые системы можно классифицировать на следующие категории:

o Для носителей с произвольным доступом (например, жёсткий диск): FAT32, HPFS, ext2 и др. Поскольку доступ к дискам в разы медленнее, чем доступ к оперативной памяти, для прироста производительности во многих файловых системах применяется асинхронная запись изменений на диск. Для этого применяется либо журналирование, например в ext3, ReiserFS, JFS, NTFS, XFS, либо механизм soft updates и др. Журналирование широко распространено в Linux, применяется в NTFS. Soft updates — в BSD системах.

o Для носителей с последовательным доступом (например, магнитные ленты): QIC и др.

o Для оптических носителей — CD и DVD: ISO9660, ISO9690, HFS, UDF и др.

o Виртуальные файловые системы: AEFS и др.

o Сетевые файловые системы: NFS, CIFS, SSHFS, GmailFS и др.

o Для флэш-памяти: YAFFS, ExtremeFFS.

o Немного выпадают из общей классификации специализированные файловые системы: ZFS (собственно файловой системой является только часть ZFS), VMFS (т.н. кластерная файловая система, которая предназначена для хранения других файловых систем) и др.

Возможны следующие варианты структур сетевых операционных систем (СОС) ЛВС:

· каждая ЭВМ сети реализует все функции СОС, т.е. хранит в своей ОП резидентную часть СОС и имеет доступ к любой нерезидентной части, хранящейся на внешних носителях;

· каждая ЭВМ сети имеет копии программ только часто реализуемых функций СОС, копии программ редко реализуемых функций имеются в памяти только одной (или нескольких) ЭВМ;

· каждая ЭВМ сети выполняет только определенный набор функций СОС, причем этот набор является либо индивидуальным, либо некоторые функции будут общими для нескольких ЭВМ. Различия в структурах СОС обусловлены принятыми способами управления ЛВС (децентрализованное или централизованное управление). Отличительной особенностью СОС ЛВС является наличие слоя операционных систем, обеспечивающего обмен информацией между ЭВМ сети.

14.4. Обзор и выбор сетевых операционных систем.

Большое разнообразие типов компьютеров, используемых в вычислительных сетях, влечет за собой разнообразие операционных систем: для рабочих станций, для серверов сетей уровня отдела и серверов уровня предприятия в целом. К ним могут предъявляться различные требования по производительности и функциональным возможностям, желательно, чтобы они обладали свойством совместимости, которое позволило бы обеспечить совместную работу различных ОС.

Сетевые ОС могут быть разделены на две группы: масштаба отдела и масштаба предприятия. ОС для отделов или рабочих групп обеспечивают набор сетевых сервисов, включая разделение файлов, приложений и принтеров. Они также должны обеспечивать свойства отказоустойчивости, например, работать с RAID-массивами, поддерживать кластерные архитектуры. Сетевые ОС отделов обычно более просты в установке и управлении по сравнению с сетевыми ОС предприятия, у них меньше функциональных свойств, они меньше защищают данные и имеют более слабые возможности по взаимодействию с другими типами сетей, а также худшую производительность.

Сетевая операционная система масштаба предприятия прежде всего должна обладать основными свойствами любых корпоративных продуктов, в том числе:

· масштабируемостью, то есть способностью одинаково хорошо работать в широком диапазоне различных количественных характеристик сети;

· совместимостью с другими продуктами, то есть способностью работать в сложной гетерогенной среде интерсети в режиме plug-and-play.

Корпоративная сетевая ОС должна поддерживать более сложные сервисы. Подобно сетевой ОС рабочих групп, сетевая ОС масштаба предприятия должна позволять пользователям разделять файлы, приложения и принтеры, причем делать это для большего количества пользователей и объема данных и с более высокой производительностью. Сетевая ОС масштаба предприятия обеспечивает возможность соединения разнородных систем - как рабочих станций, так и серверов. Например, даже если ОС работает на платформе Intel, она должна поддерживать рабочие станции UNIX, работающие на RISC-платформах. Аналогично, серверная ОС, работающая на RISC-компьютере, должна поддерживать DOS, Windows и OS/2. Сетевая ОС должна поддерживать несколько стеков протоколов (таких как TCP/IP, IPX/SPX, NetBIOS, DECnet и OSI), обеспечивая простой доступ к удаленным ресурсам, удобные процедуры управления сервисами, включая агентов для систем управления сетью. Важным элементом сетевой ОС является централизованная справочная служба, в которой хранятся данные о пользователях и разделяемых ресурсах сети. Такая служба, называемая также службой каталогов, обеспечивает единый логический вход пользователя в сеть и предоставляет ему удобные средства просмотра всех доступных ему ресурсов. Администратор, при наличии в сети централизованной справочной службы, избавлен от необходимости заводить на каждом сервере повторяющийся список пользователей, а значит избавлен от большого количества рутинной работы и от потенциальных ошибок при определении состава пользователей и их прав на каждом сервере. Важным свойством справочной службы является ее масштабируемость, обеспечиваемая распределенностью базы данных о пользователях и ресурсах.

Такие сетевые ОС, как Banyan Vines, Novell NetWare 4.x, IBM LAN Server, Sun NFS, Microsoft LAN Manager и Windows NT Server, могут служить в качестве операционной системы предприятия, в то время как ОС NetWare 3.x, Personal Ware, Artisoft LANtastic больше подходят для небольших рабочих групп.

При выборе сетевой операционной системы необходимо учитывать:

· совместимость оборудования; тип сетевого носителя;

· размер сети; сетевую топологию;

· требования к серверу;

· операционные системы на клиентах и серверах;

· сетевая файловая система;

· соглашения об именах в сети;

· организация сетевых устройств хранения;

· набор сетевых служб, которые предоставляет сеть;

· возможность наращивания имен, определяющих хранимые данные и прикладные программы;
· механизм рассредоточения ресурсов по сети;
· способ модификации сети и сетевых служб;
· надежность функционирования и быстродействие сети;
· используемые или выбираемые физические средства соединения;
· типы компьютеров, объединяемых в сеть, их операционные системы;
· предлагаемые системы, обеспечивающие управление сетью;
· используемые средства защиты данных;
· совместимость с уже созданными прикладными процессами;
· число серверов, которое может работать в сети;
· перечень ретрансляционных систем, обеспечивающих сопряжение локальных сетей с различными территориальными сетями;
· способ документирования работы сети, организация подсказок и поддержек.

Конечно, ни одна из существующих сетевых ОС не отвечает в полном объеме перечисленным требованиям, поэтому выбор сетевой ОС, как правило, осуществляется с учетом производственной ситуации и опыта. Операционные системы могут различаться особенностями реализации внутренних алгоритмов управления основными ресурсами компьютера (процессорами, памятью, устройствами), особенностями использованных методов проектирования, типами аппаратных платформ, областями использования и многими другими свойствами.

14.5. Клиентское и серверное программное обеспечение.

Некоторые из сетевых операционных систем, в том числе Windows NT, имеют программные компоненты, обеспечивающие компьютеру как клиентские, так и серверные возможности. Это позволяет компьютерам поддерживать и использовать сетевые ресурсы и преобладает в одноранговых сетях. В общем, этот тип сетевых операционных систем не так мощен и надежен, как законченные сетевые операционные системы. Главное преимущество комбинированной клиентско–серверной сетевой операционной системы заключается в том, что важные ресурсы, расположенные на отдельной рабочей станции, могут быть разделены с остальной частью сети. Недостаток состоит в том, что если рабочая станция поддерживает много активно используемых ресурсов, она испытывает серьезное падение производительности. Если такое происходит, то необходимо перенести эти ресурсы на сервер для увеличения общей производительности.

14.5.1. Серверное программное обеспечение

Для того чтобы компьютер мог выступать в роли сетевого сервера необходимо установить серверную часть сетевой операционной системы, которая позволяет поддерживать ресурсы и распространять их среди сетевых клиентов. Важным вопросом для сетевых серверов является возможность ограничить доступ к сетевым ресурсам. Это называется сетевой защитой (network security). Она предоставляет средства управления над тем, к каким ресурсам могут получить доступ пользователи, степень этого доступа, а также, сколько пользователей смогут получить такой доступ одновременно. Этот контроль обеспечивает конфиденциальность и защиту и поддерживает эффективную сетевую среду.

В дополнение к обеспечению контроля над сетевыми ресурсами сервер выполняет следующие функции: предоставляет проверку регистрационных имен (logon identification) для пользователей; управляет пользователями и группами; хранит инструменты сетевого администрирования для управления, контроля и аудита; обеспечивает отказоустойчивость для защиты целостности сети.

14.5.2. Клиентское программное обеспечение

Для работы с сетью на клиентских рабочих станциях должно быть установлено клиентское программное обеспечение. Это программное обеспечение обеспечивает доступ к ресурсам, расположенным на сетевом сервере. Тремя наиболее важными компонентами клиентского программного обеспечения являются редиректоры (redirector), распределители (designator) и имена UNC.

14.5.3. Редиректоры

Редиректор – сетевое программное обеспечение, которое принимает запросы ввода/вывода для удаленных файлов, именованных каналов или почтовых слотов и затем переназначает их сетевым сервисам другого компьютера. Редиректор перехватывает все запросы, поступающие от приложений, и анализирует их.

Фактически существуют два типа редиректоров, используемых в сети:

« клиентский редиректор (client redirector)

« серверный редиректор (server redirector).

Оба редиректора функционируют на представительском уровне модели OSI. Когда клиент делает запрос к сетевому приложению или службе, редиректор перехватывает этот запрос и проверяет, является ли ресурс локальным (находящимся на запрашивающем компьютере) или удаленным (в сети). Если редиректор определяет, что это локальный запрос, он направляет запрос центральному процессору для немедленной обработки. Если запрос предназначен для сети, редиректор направляет запрос по сети к соответствующему серверу. По существу, редиректоры скрывают от пользователя сложность доступа к сети. После того как сетевой ресурс определен, пользователи могут получить к нему доступ без знания его точного расположения.

14.5.4. Распределители

Распределитель (designator) представляет собой часть программного обеспечения, управляющую присвоением букв накопителя (drive letter) как локальным, так и удаленным сетевым ресурсам или разделяемым дисководам, что помогает во взаимодействии с сетевыми ресурсами. Когда между сетевым ресурсом и буквой локального накопителя создана ассоциация,

известная также как отображение дисковода (mapping a drive), распределитель отслеживает присвоение такой буквы дисковода сетевому ресурсу. Затем, когда пользователь или приложение получат доступ к диску, распределитель заменит букву дисковода на сетевой адрес ресурса, прежде чем запрос будет послан редиректору.

14.5.5. Имена UNC

Редиректор и распределитель являются не единственными методами, используемыми для доступа к сетевым ресурсам. Большинство современных сетевых операционных систем, так же как и Windows 95, 98, NT, распознают имена UNC (Universal Naming Convention — Универсальное соглашение по наименованию). UNC представляют собой стандартный способ именования сетевых ресурсов. Эти имена имеют форму *\\Имя_сервера\имя_ресурса*. Способные работать с UNC приложения и утилиты командной строки используют имена UNC вместо отображения сетевых дисков.

14.6. Прикладные программы сети.

Системные программные средства, управляющие процессами в компьютерных сетях, объединенные общей архитектурой, определенными коммуникационными протоколами и механизмами взаимодействия вычислительных процессов, называются сетевыми операционными системами. Они предназначены для эффективного решения задач распределенной обработки данных, т.е. обработки данных не на отдельном локальном компьютере, а на нескольких объединенных сетью, причем часто бывает неважно - локальной или глобальной. Важным требованием к большинству современных пакетов прикладных программ (ППП) является их способность работать в условиях локальных сетей, то есть выполнять функции прикладных программ сети (ППС).Эти ППС должны обеспечивать возможность функционирования в сети определенного типа. В конце прошлого века 90% рынка было объединено вокруг сетей Ethernet, ARC-Net и Token Ring. Именно к этим типам сетей приспосабливалось большинство разработчиков. Перспективными технологиями являются технологии беспроводной передачи данных (Wi-Fi, bluetooth).

В состав наиболее известных ППС входят:

- текстовые процессоры (MS Office Word 2003 SP2);
- пакеты электронных таблиц или табличных процессоров (Quattro Pro, MS Office Excel 2003);
- СУБД (Access, dBase IV, V, Clipper, Paradox и др.);
- пакеты группового обеспечения (Lotus Notes, Office Vision);
- пакеты электронной почты (Microsoft Mail, MS Office Outlook, The Bat!);
- интегрированные пакеты (Symphony, FrameWork);
- пакеты телесвязи для обеспечения передачи файлов между ПК (Crosstalk, Smartterm, Smartcom II, Kermit).

14.7. Специализированные программные средства.

В эпоху internet требуется огромное количество специализированных программных средств, выполняющих конкретные задачи. В качестве примеров можно привести:

- браузеры (Internet Explorer, Opera, Mozilla Firefox, Netscape Navigator) ;
- даунлоадеры (ReGet, FlashGet, WinMX, GetRight, eDonkey) ;
- сканнеры сетевых ресурсов и уязвимостей (nmap, Guardian, netcat, port mapper, secure CRT) ;
- брандмауэры (Kerio Firewall Personal, Agnitum Outpost, Windows Firewall) ;
- терминалы (telneat) ;
- мессенджеры (Mirabilis ICQ, SIM, RQ, Jabber, MSN, Yahoo, xchat, licq) ;
- чат-клиенты (Miranda IM, Y-Chat, BORGChat) ;
- информационно-поисковые машины (yandex, rambler, google и другие) ;
- программы-прокси (Kerio Winroute, WinGate) ;
- мэйл-клиенты и серверы (Outlook Express, The Bat!, smtpd, Kerio Mail-Server) ;
- ftp-клиенты и серверы (Total Commander, putty, CuteFTP, Gene FTP Server U-FTP) ;
- HTTP-серверы (apache) ;
- снифферы (ZXSniffer, Kain) ;
- утилиты удаленного администрирования (RAdmin, Tiramisu, Citrix Metaframe, Team Viewer) ;
- другие разнообразные утилиты и программы (VideoLAN Center, LANScope, coockie editors, streambox VCR, WEBCopier, DynDNS Updater, KDE Bluetooth Framework, Wi-Fi Manager, 3d traceroute, AdvancedRe-motelnfo, MyVoice Email и др.).

Все эти и многие другие программные средства позволяют наиболее удобно организовать любую деятельность, связанную с передачей данных удаленным клиентам, либо обеспечением сетевых сервисов.

Контрольные вопросы:

1. Какие функции сети выполняет сетевая операционная система?
2. Что такое редиректор?
3. Из каких частей состоит структура NOS?
4. Что такое NOS и каково ее назначение?
5. Как подразделяются сетевые операционные системы по правам доступа к ресурсам?
6. Как подразделяются сетевые операционные системы по масштабу сетей?
7. Что такое распределитель?
8. Перечислите наиболее употребляемые браузеры.
9. Что такое файловая система?
10. Какие стеки протоколов поддерживает сетевая операционная система?

Практические задания:

Работа с почтовой программой Outlook Express.

Почтовая программа **Outlook Express** входит в пакет **Internet Explorer**.

Электронная почта (*e-mail*) является самым широко используемым приложением для большинства сетей. Поскольку Интернет является самым популярным и большим объединением компьютерных сетей, и миллионы частных пользователей компьютеров имеют возможность подключения к сети Интернет, общение посредством электронной почты приобретает большое значение.

Электронная почта - это очень быстрый и удобный способ общения через сеть Интернет. С помощью электронной почты можно не только обмениваться сообщениями с людьми, но и найти разнообразную информацию, получить любой файл или Web-страницу, используя специальные почтовые серверы. Чтобы ваше электронное письмо (сообщение, передаваемое по электронной почте) не потерялось, каждому пользователю электронной почты присваивается уникальный адрес, который представляет собой текстовую строку, например, **ivanov@server.inet.ru.** Электронный адрес вводится *строчными буквами латинского алфавита*. Текст электронного адреса, расположенный слева от символа @, идентифицирует конкретного пользователя, а информация, расположенная справа, является адресом почтового сервера, на котором находится почтовый ящик пользователя. Электронное письмо состоит из *заголовка* и тела письма.

В заголовке письма помещается адрес получателя, адрес отправителя и тема сообщения. Текст самого сообщения помещается в тело письма. Для создания, отправки, получения и просмотра электронных писем используются специальные почтовые программы. Программа **Outlook Express** является одной из таких почтовых программ. Для удобства работы с электронной корреспонденцией почтовые программы распределяют все почтовые сообщения по папкам. Программа **Outlook Express** создает пять папок.

· В папку **Входящие** (Inbox) помещаются все получаемые сообщения, откуда впоследствии они могут быть перемещены или скопированы в любые другие папки.

· В папку **Исходящие** (Outbox) помещаются письма, готовые к отправке, но еще не отправленные (если в пункте меню **Сервис⇒Параметры** на вкладке **Отправка** не установлена опция **Отправлять сообщение немедленно**).

· После отправления сообщений из папки **Исходящие** (Outbox), их копии помещаются в папку **Отправленные** (Sent Items) для хранения.

· После удаления писем из любой имеющейся папки, они попадают в папку **Удаленные** (Deleted Items) и хранятся там некоторое время на случай, если вдруг снова потребуются.

· Папка **Черновики** (Draft) предназначена для хранения заготовок писем или незаконченных сообщений. Вы можете создавать новые и удалять ненужные папки по своему желанию. Как это сделать, описано в одном из последующих заданий.

ЗАДАНИЕ № 14.1. Запуск программы Outlook Express и Подключение к сети Интернет.

· Запустите программу **Outlook Express** двойным щелчком мыши на ярлыке программы  , расположенном на **Рабочем столе** (*Desktop*). На экране появится рабочее окно программы **Outlook Express**.

· Если на рабочем столе отсутствует ярлык программы **Outlook Express**, то выполните следующее:

· Щелкните по пиктограмме **Мой компьютер** на рабочем столе.

· Перейдите в папку **Outlook Express**, где находится ярлык программы: **C:\ Program Files\Outlook Express**.

· Дважды щелкните ярлык мышью, чтобы запустить программу.

После запуска программы **Outlook Express** на экран выводится мастер **Подключение к Интернету**. *Мастер* – это последовательность диалогов, которая ведет вас к определенной цели. Последовательно выполните следующие действия.

· В 1-м окно мастера **– Подключайтесь! –** нажмите кнопку **Далее**.

· Во 2-м окне **Как вы предполагаете подключиться?** установите переключатель на опции **У меня уже налажена связь с Интернетом на этом компьютере и я не хочу ничего изменять** и нажмите кнопку **Далее**.

· В 3-м окне **Использовать текущую настройку?** нажмите кнопку **Готово**.

На экран выводится окно **Обзор папок**. По умолчанию выделена папка *Outlook Express*. Нажмите кнопку **ОК**. На экран выводится окно программы **Outlook Express**.

При первом запуске программа **Outlook Express** загружает в правую часть рабочего окна страницу, предназначенную для быстрого вызова часто используемых действий программы. В нижней части страницы отображается **Совет дня** (*Tip of the day*), который выбирается случайным образом при каждом запуске **Outlook Express**. Чтобы при запуске программа **Outlook Express** сразу отображала содержимое папки **Входящие** (*Inbox*), необходимо установить флажок **Переходить в папку «Входящие» при запуске** (*When starting, go directly to may «Inbox» folder*), расположенный в нижней части страницы.

Теперь перейдем в папку **Входящие** (*Inbox*), чтобы познакомиться с рабочим окном программы **Outlook Express**. Для этого необходимо выполнить следующие действия.

· Подведите указатель мыши к надписи **Чтение почты** (*Read mail*) на странице, расположенной в правой части рабочего окна. Когда указатель мыши изменится на “перст указующий”, щелкните мышью, рабочее окно программы **Outlook Express** отобразит папку **Входящие** (*Inbox*).

ЗАДАНИЕ № 14.2. Настройка программы *Outlook Express.*

Прежде чем получить доступ к почте вам необходимо выполнить ряд настроек путем диалога с мастером **Подключение к Интернету**.

· В 1-м окне **Ваше имя** введите свое имя (латинскими буквами), которое будет помещаться в поле **От** заголовка исходящих сообщений перед вашим электронным адресом, и нажмите кнопку **Далее**.

· Во 2-м окне **Адрес электронной почты сети Интернет** введите свой электронный адрес и нажмите кнопку **Далее**.

· В 3-м окне **Имена серверов электронной почты** в поле **Тип сервера для входящих сообщений** установите **POP3**. В полях **Сервер для входящих сообщений** и **Сервер для исходящих сообщений** введите **mail-win.iile.ru**. Нажмите кнопку

Далее.

· В 4-м окне **Вход на сервер почты сети Интернет** заполните поле ввода **Учетная запись POP** (по умолчанию введена) и введите пароль в поле **Пароль**. Учетная запись **–** это, как правило, левая часть вашего электронного адреса до символа **@**, которая идентифицирует вас как пользователя почтового ящика. Нажмите кнопку **Далее**.

· В 5-м окне **Удобное имя** введите в поле ввода **Имя учетной записи почты сети Интернет** любое удобное для вас имя. Нажмите кнопку **Далее**.

· В 6-м окне **Какой тип соединения?** установите переключатель *Каким способом вы предпочитаете подключаться к Интернету?* в положение **Через локальную компьютерную сеть организации**.

· В последнем окне **Поздравляем!** нажмите кнопку **Готово**.

ЗАДАНИЕ № 14.3. Знакомство с рабочим окном Outlook Express.

Познакомимся подробнее с рабочим окном программы **Outlook Express**.

· **Заголовок окна и строка меню -** стандартные атрибуты окна в операционной системе *Windows95/NT*. С помощью меню вы можете выбрать любую команду программы **Outlook Express**.

· На **Панели инструментов** (*Toolbar*) расположены значки с надписями, обозначающие часто выполняемые действия. Если подвести указатель мыши к значку, то значок “превращается” в объемную кнопку. Если щелкнуть мышью на этой кнопке, то выполнится связанная с этой кнопкой команда. При необходимости надписи к кнопкам можно отключить, можно изменить местоположение панели инструментов, а также добавить новые или удалить редко используемые кнопки. Основная часть окна программы может быть поделена на несколько областей. При первом запуске программы и выборе любой папки окно программы делится на три части:

О в левой части окна **–** *Список папок*,

О в правой части окна в верхней половине **–** *Список писем*,

О в правой части окна в нижней половине **–** *Область просмотра*.

· **Список папок** (*Folders List*) содержит имена папок, предназначенных для хранения и сортировки принимаемой и отправляемой почты. В этих папках вы можете создавать и удалять новые папки, раскладывать в них письма, получаемые из разных почтовых ящиков.

· **Список писем** предназначен для отображения содержимого папки, открытой в настоящий момент. В нем отображаются заголовки писем.

· **Область просмотра** содержит **Заголовок области просмотра** (заголовок выбранного письма) и текст выбранного письма.

· При первом запуске программа **Outlook Express** помещает в папку **Входящие** (*Inbox*) два письма от группы разработчиков, адресованные вам с приветствием и интересной информацией. Можно изменить размеры списка папок, списка писем и области просмотра, перетаскивая мышью разделяющие их границы.

· **В Строке состояния** отображается вспомогательная информация, например, количество писем в выбранной папке или выполняемые в данный момент действия: подключение к почтовому серверу, получение почты и т. п.

Вид рабочего окна программы **Outlook Express** можно менять путем установки флажков и переключателей на вкладке меню **Вид ⇒ Раскладка**. Ознакомимся с текущими установками.

· Выберите команду меню **Вид\Раскладка** (*View\Layout*). На экране появится диалог **Свойства: *Раскладка окна*** *(Window Layout)*.

· В группе элементов управления **Основное окно** установите флажок **Список папок** (*Folders list*) и сбросьте флажки **Панель Outlook** (*Outlook Bar*), **Панель папок** (*Folder Bar*), **Совет дня** (*Tip of the day*).

· В группе элементов управления **Панель инструментов** (*Toolbar*) установите переключатель в положение **Сверху** (*Top*) и установите флажок **Показывать подсказки на кнопках** (*Show text on toolbar buttons*).

· В группе элементов управления **Область просмотра** (*Preview Pane*) установите флажки **Показывать область просмотра** (*Use preview pane*) и **Показывать заголовок области просмотра** (*Show preview pane Header*), установите переключатель в положение **Под сообщениями** (*Bellow Messages*).

· Нажмите кнопку **ОК,** чтобы закрыть диалог.

Программа **Outlook Express** может быть настроена так, что будет немедленно осуществлять отправку созданных вами сообщений. Чтобы этого не происходило, выполните следующие действия.

· Выберите команду меню **Сервис\Параметры** (*Tools\Options*). На экране появится диалог **Параметры** (*Options*).

· Перейдите на вкладку **Отправка** (*Send*) и сбросьте флажок **Отправлять сообщения немедленно** (*Send messages immediately*).

· Нажмите кнопку **ОК,** чтобы закрыть диалог.

Справка: Чтобы просмотреть, удалить, добавить или внести изменения в *Учетную запись*, нужно выполнить следующие действия.

· Выбрать команду меню **Сервис\Учетные записи** (*Tools\Accounts*). На экране появится диалог **Учетные записи Интернета** (*Internet Accounts*).

· Выбрать вкладку **Почта** (*Mail*).

· Выделить мышью строку, соответствующую вашей учетной записи, и нажмите кнопку **Свойства** (*Properties*). На экране появится диалоговое окно **Свойства** (*Properties*) вашей учетной записи.

· Закройте окна диалога.

ЗАДАНИЕ № 14.4. Настройка почтового сервера на компьютере с операционной системой Windows Server 2003. Создание почтовых ящиков.

Установка сервера электронной почты:

1. Войдите в систему как пользователь с правами администратора домена.
2. В меню **Пуск, Администрирование** выберите команду **Мастер настройки сервера.**
3. На первой странице Мастера настройки щёлкните мышкой на кнопке **Далее.**
4. На странице **Предварительные шаги** щёлкните мышкой на кнопке **Далее.**
5. На странице **Роль сервера** убедитесь, что в строке с ролью **Почтовый сервер (POP3, SMTP**) в колонке **Настроено** указано значение **Нет**.
6. Выберите в списке значение **Почтовый сервер (POP3, SMTP),** после чего щелкните мышью на кнопке **Далее**.
7. На странице **Настройка службы POP3** в списке **Метод проверки подлинности** выберите значение **Интегрированные с Active Directory**, а в поле **Имя домена электронной почты** введите удобное вам название домена, для которого ваш сервер будет принимать электронную почту (например, *mfpa.ru*).
8. На странице **Сводка выбранных параметров** убедитесь, что в поле **Сводка** присутствует строка **Установка POP3 и протокола SMTP для обеспечении отправки и получения почты почтовыми клиентами POP3**, и щелкните мышью на кнопке **Далее**. Если при этом откроется окно **Вставка диска**, то щелкните на кнопке **ОК**., затем в диалоговом окне **Требуемые файлы** укажите в поле **Размещение файлов** путь к дистрибутиву операционной системы Windows Server 2003 и щелкните на кнопке **ОК**.
9. На странице **Этот сервер теперь является почтовым сервером** щелкните на кнопке **Готово**. Автоматически запустится программа **Управление данным сервером.**
10. Убедитесь, что в списке ролей сервера, который вы видите в окне **Управление данным сервером**, появилась строка **Почтовый сервер (POP3, SMTP).**

ЗАДАНИЕ № 14.5. Работа с адресной книгой.

· Нажмите кнопку **Адресная книга** на панели инструментов **Outlook Express**.
· Выберите команду **Файл\Создать адрес**.
· В диалоговом окне **Свойства** в поле ввода *Имя* введите текст **Почтовый робот**. Клавишу **<Enter>** после ввода нажимать не надо.
· Щелкните мышью на поле ввода **Добавить новый** в группе элементов **Адреса электронной почты**, введите текст test@triumph.ru и нажмите **Enter**.
· Нажмите кнопку **ОК**.
· Закройте окно адресной книги с помощью команды **Файл\Закрыть**.

Если при вводе адреса имеются ошибки, то для их исправления необходимо выполнить следующие операции:
· Вновь откройте адресную книгу.
· Двойным щелчком мыши на строке адресата откройте диалог **Свойства**.
· В списке адресатов выделите мышью строку адреса, который нужно исправить.
· Нажмите кнопку **Изменить** в группе элементов **Адреса электронной почты**, при этом выделенный адрес будет помещен в рамку.
· Внесите необходимые исправления.
· Закройте диалог **Свойства адресата**, нажав кнопку **ОК**.
· Закройте окно адресной книги с помощью команды **Файл\Закрыть**.

Адресная книга программы **Outlook Express** позволяет объединять адресатов в группы по определенным признакам.

Если создать группы адресатов (например, ваших коллег по работе или родственников), то посылать им электронную почту будет проще. Чтобы отправить сообщение всем участникам группы, достаточно указать в нем имя группы, и вам не придется вводить каждое имя в отдельности. Использование групп помогает также более удобно организовать большую адресную книгу.

Можно создать несколько групп; любой адресат может входить более чем в одну группу. Для этого необходимо выполнить следующее:
· Нажмите на панели инструментов адресной книги кнопку **Создать группу**.
· В поле **Название группы** введите имя группы.
· Нажмите кнопку **Выбрать участников** и щелкните нужное имя в списке адресной книги.
· Нажмите кнопку **OK**, а затем еще раз нажмите **OK**, чтобы закрыть диалоговое окно.

ЗАДАНИЕ № 14.6. Отправка электронного письма.

Как отправить сообщение электронной почты:
· Откройте адресную книгу, нажав на кнопку **Адресная книга** на панели инструментов.
· В списке адресатов выберите **Почтовый робот**, и щелкните на нём правой кнопкой мыши, чтобы вывести контекстное меню.
· Из контекстного меню выберите команду **Отправить сообщение.** На экран будет выведено окно **Создать сообщение** с адресом почтового робота.
· В поле ввода **Тема** введите текст: **Kodirovka KOI8**
· Нажмите кнопку **Отправить**. Ваше письмо будет помещено в папку **Исходящие**.
· Закройте адресную книгу.

Создадим ещё одно сообщение почтовому роботу:
· Нажмите кнопку **Создать сообщение** на панели инструментов, на экране появится окно **Создать сообщение.**
· Нажмите кнопку рядом с надписью **Кому**, и в появившемся диалоге **Выбрать получателя** из списка адресатов выберите **Почтовый робот** и нажмите кнопку **Кому.**
· Закройте диалог кнопкой **ОК.**
· В поле ввода **Тема** введите текст: **Kodirovka Windows.**

· Нажмите кнопку **Отправить** на панели инструментов, чтобы переместить письмо в папку **Исходящие.** Окно **Создать сообщение** при этом закроется.

Создадим для примера сообщение несуществующему адресату:

· Нажмите кнопку **Создать сообщение** на панели инструментов, появится окно **Создать сообщение**.

· В поле ввода **Кому** введите текст: internet@internet.no.

· В поле ввода **Тема** введите текст: **test** и нажмите кнопку **Отправить**. Окно будет закрыто, и сообщение будет помещено в папку **Исходящие**.

· Нажмите кнопку **Доставить почту** на панели инструментов.

ЗАДАНИЕ № 14.7. Получение электронного письма.

Ответ от почтового сервера вы сможете получить через 15 – 20 минут, если ответ не пришел, то повторите попытку еще раз.

Для получения почты выполните следующие действия:

· Нажмите кнопку **Доставить почту** на панели инструментов. В списке писем папки **Входящие** будут находиться заголовки полученных писем. В скобках рядом с папкой указано общее число непрочитанных писем.

· Первое письмо получено от *Mail Delivery Subsystem* вашего интернет-провайдера с уведомлением о том, что internet@internet.no не существует. К письму присоединен файл с вашим исходным сообщением, о чем свидетельствует «скрепка» перед заголовком сообщения в списке писем.

· Следующее письмо получено от почтового робота издательства *Триумф* в ответ на письмо с темой: **Kodirovka KOI8.** Чтобы просмотреть содержание письма, щелкните мышью на заголовке письма с темой: **Ответ от издательства Триумф KOI**. В области просмотра появится текст сообщения.

· При просмотре содержимого третьего письма, в теме которого содержится нечитаемый текст, в области просмотра появится нечитаемый текст сообщения.

· Выберите команду меню **Вид\Язык\Кириллица**. Текст и заголовок сообщения в области просмотра примут читаемый вид. К сожалению, тема письма в списке писем остается нечитаемой, но она будет продублирована в заголовке сообщения в области просмотра в читаемом виде.

Примечание: К сожалению, выбор кодировки **Вид\Язык\Кириллица** не всегда помогает, так как по пути следования письмо может быть испорчено программами пересылки почты.

ЗАДАНИЕ № 14.8. Ответ на полученное письмо.

Чтобы быстро составить ответ на полученное письмо, и при этом не заносить адрес отправителя в адресную книгу, проще всего воспользоваться специальной командой **Ответить автору**, кнопка которой находится на панели инструментов. При выполнении этой команды программа создает письмо с адресом отправителя в поле **Кому** и темой исходного сообщения с пометкой **Ответ:** (**Re:**) в поле **Тема**. Кроме того, в тело самого письма помещается текст полученного сообщения, помеченный символом **>** в начале каждой строки, чтобы вы могли напомнить автору полученного письма, о чем шла речь.

Чтобы продемонстрировать, каким образом отвечать на полученные письма, создадим ответ на сообщение подсистемы доставки почты:

· Выделите в списке сообщений папки **Входящие** заголовок письма, в поле **От** которого содержится текст: *Mail Delivery Subsystem*.

· Нажмите кнопку **Ответить автору** на панели инструментов и ознакомьтесь с подготовленным шаблоном ответа.

· Поместите текстовый курсор в тело ответа, удалите ненужный текст исходного письма и вставьте свои комментарии после строк исходного письма. После редактирования ответ необходимо поместить в папку **Исходящие**. Для этого:

· Нажмите кнопку **Отправить**, расположенную на панели инструментов окна **Ответ** (**Re:**) программы **Outlook Express**. При этом окно закроется, и ответ будет помещен в папку **Исходящие**.

· Кнопку **Доставить почту** на панели инструментов нажимать не надо, так как это письмо никуда отправлять не нужно, а в следующем задании мы его удалим.

ЗАДАНИЕ № 14.9. Удаление и восстановление писем.

Удалим письмо с ответом в адрес подсистемы доставки почты. Для этого:

· Щелкните мышью на надписи **Исходящие** в списке папок. Рабочее окно программы **Outlook Express** отобразит содержимое этой папки.

· Щелкните мышью на заголовке письма в списке писем, чтобы его выделить.

· Нажмите кнопку **Удалить** на панели инструментов. При этом письмо не удаляется совсем, а помещается в папку **Удаленные**, откуда при желании его можно восстановить. Для этого:

· Щелкните мышью на надписи **Удаленные** в списке папок. Рабочее окно программы **Outlook Express** отобразит содержимое этой папки.

· Выделите в списке писем письмо, которое необходимо восстановить, и нажмите правую кнопку мыши.

· Выберите команду контекстного меню **Переместить в …**.

· В диалоговом окне **Переместить** выберите папку (например, **Входящие**), в которую хотите поместить восстановленное письмо, и нажмите кнопку **ОК**.

Примечание: Описанным выше способом вы можете переместить удаленное письмо в любую папку, кроме папки **Исходящие**. Чтобы переместить письмо из любой папки в папку **Исходящие**, необходимо сначала открыть письмо двойным щелчком мыши на его заголовке в списке писем открытой папки, а затем в появившемся окне письма нажать кнопку **Отправить**.

· Повторно удалите из папки **Входящие** письмо, восстановленное из папки **Удаленные**.

Примечание: Письма, удаляемые из папки **Удаленные**, восстановить будет невозможно.

ЗАДАНИЕ № 14.10. Автоматическая сортировка входящей почты.

Программа **Outlook Express** позволяет автоматически сортировать входящую почту, то есть в зависимости от адреса отправителя, темы письма или ключевых слов в теле письма, помещать их при поступлении в разные папки. Рассмотрим это на примере письма, которое вы получите от почтового робота. Для этого:

· Откройте адресную книгу. В открывшемся окне в списке адресатов будет надпись: **Почтовый робот**.
· Щелкните правой кнопкой мыши на адресата **Почтовый робот**.
· В контекстном меню выберите команду **Отправить сообщение**.
· В появившемся окне **Отправить сообщение** щелкните мышью на поле ввода **Тема** и введите текст: **Kodirovka KOI8**.
· Нажмите кнопку **Отправить** и закройте адресную книгу.

Теперь создадим папку **От робота**, для чего:

· Щелкните правой кнопкой мыши на папке **Входящие** в **Списке папок**.
· В появившемся на экране контекстном меню выберите команду **Создать папку**.
· В поле ввода **Название папки** введите текст: **От робота**.
· Закройте папку, нажав кнопку **ОК**.

Теперь зададим условие сортировки:

· Выберите команду меню **Сервис\Сортировщик сообщений**.
· В диалоговом окне **Сортировщик сообщений** нажмите кнопку **Добавить**.
· В диалоговом окне **Свойства** в группе элементов управления **Для сообщений, удовлетворяющих условиям**, в строке **От:** нажмите кнопку, расположенную перед полем ввода. На экране появится окно **Выбрать получателей**.
· Щелкните мышью на строке **Почтовый робот** в списке адресатов, расположенном в левом окне диалога, и нажмите кнопку **От:**, чтобы скопировать адресата в список **Получатели сообщения**.
· Нажмите кнопку **ОК**, чтобы закрыть диалоговое окно **Выбрать получателей**. При этом в поле ввода **От:** диалогового окна **Свойства** появится адрес почтового робота.
· В группе элементов управления **Выполнить следующие действия:** диалогового окна **Свойства** установите флажок **Переместить в:** и нажмите кнопку **Папка**. На экране появится диалоговое окно **Переместить**.
· Щелкните на + рядом с папкой **Входящие**. Папка **Входящие** раскроется.
· Выберите папку **От робота** и нажмите кнопку **ОК**. Диалоговое окно **Переместить** закроется, а в поле ввода **Переместить в:** диалогового окна **Свойства** появится имя выбранной папки.
· Нажмите кнопку **ОК**, чтобы закрыть диалоговое окно **Свойства**. В списке **Описание** диалогового окна **Сортировщик сообщений** появится условие сортировки с установленным перед ним флажком, означающим, что данное условие сортировки вступило в силу. В дальнейшем, чтобы отключить это условие, необходимо просто сбросить флажок, щелкнув по нему мышью.
· Нажмите кнопку **ОК**, чтобы закрыть диалоговое окно **Сортировщик сообщений**.
· Нажмите кнопку **Доставить почту**.

ЗАДАНИЕ № 14.11. Присоединение файлов к письму.

При работе с электронной почтой часто бывает необходимо переслать либо получить файл. Это может быть программа или большой текстовый файл, упакованный каким-либо архиватором. **Outlook Express** позволяет присоединить к письму любой файл. Для этого:

· Нажмите кнопку **Создать сообщение** на панели инструментов.
· В диалоговом окне **Создать сообщение** нажмите кнопку рядом с полем **Кому:** в заголовке письма.
· В диалоговом окне **Выбрать получателей** из списка адресатов слева выберите **Почтовый робот** и нажмите кнопку **Кому**. В поле **Получатели сообщения** появится имя почтового робота.
· Нажмите **ОК**, чтобы закрыть диалоговое окно. В поле **Кому:** в заголовке сообщения в окне **Создать сообщение** появится надпись **Почтовый робот**. Это означает, что адрес получателя сообщения введен.
· Нажмите кнопку «скрепка» на панели инструментов окна **Создать сообщение**. На экране появится диалоговое окно **Вставка вложений**.
· Выберите любой файл из любой папки и нажмите кнопку **Вложить**. В нижней части окна **Создать сообщение** появится зона, в которой будет показано имя и длина присоединенного файла.
· Нажмите кнопку **Отправить**, чтобы отправить письмо с вложенным файлом.

ЗАДАНИЕ № 14.12. Отсоединение файлов, пришедших вместе с письмом.

Мы пошлем специальный запрос почтовому роботу, чтобы получить письмо с присоединенным файлом, а затем прочитаем содержимое полученного письма. Для этого:

· Откройте адресную книгу.
· В появившемся окне в списке адресатов будет надпись **Почтовый робот**.
· Щелкните правой кнопкой мыши на адресате.
· Выберите в контекстном меню команду **Отправить сообщение**.
· В появившемся окне **Создать сообщение** с адресом почтового робота щелкните мышью на поле ввода **Тема** и введите текст: **Risunok BMP**.

· Нажмите кнопку **Отправить**.

После получения ответа выполните следующее:

· Выберите в **Списке папок** папку **От робота**. Рабочее окно программы **Outlook Express**. Значок «скрепка» перед строкой заголовка письма в списке писем означает, что сообщение имеет присоединенный файл.

В области просмотра выбранного сообщения программа автоматически отображает присоединенные файлы известных ей типов, либо просто выводит название присоединенного файла. Присоединенные файлы хранятся вместе со всеми полученными письмами. Но можно отсоединить присланный файл, просмотреть и хранить его отдельно.

· В списке писем папки **От робота** выберите письмо с присоединенным файлом. В окне просмотра сообщения появится содержимое выбранного письма с присоединенным к нему файлом.

· В области просмотра в правой части заголовка письма нажмите кнопку «скрепка», появится контекстное меню с именем и размером вложенного файла.

· Щелкните мышью на имени присоединенного файла в контекстном меню. На экране появится предупреждение об открытии вложения. Если установить переключатель в положение **Открыть**, то будет запущена связанная с типом вложенного файла программа, которая отразит его содержание. В данном случае будет запущена программа, связанная с расширением **.bmp**, это может быть либо графический редактор, либо программа просмотра рисунка.

· Установите переключатель **Что следует сделать с этим файлом?** в положение **Сохранить на диске**. На экране появится диалоговое окно **Сохранить вложение как…**.

· Выберите папку, в которой хотите сохранить вложенный файл, и нажмите кнопку **Сохранить**.

Перечень литературы и Интернет-ресурсов:

1. Гордеев А.В. Операционные системы. Санкт Петербург, Питер, 2006 год.
2. Дроздов С. Н. Операционные системы: Конспект лекций. – Таганрог: Изд-во ТРТУ, 2003. – 136 с.
3. Коллекция компьютерных документов — http://www.emanual.ru
4. Олифер В.Г. Сетевые операционные системы. СПб.:Питер, 2002.-538с.
5. Партыка Т.Л., Попов И.И. Операционные системы, среды и оболочки: Учебное пособие. - М.: ФОРУМ; ИНФРА-М, 2004. - 400 с.: ил.
6. Петерсон Р. LINUX: руководство по операционной системе: В 2т.:Пер. с англ. - 2-е изд., перераб. и доп. - К.: Издательская группа BHV, 1998. 590с.
7. Пог Д. Macintosh для «чайников» – перев. с англ. – К.: Диалектика, 1997.352 с.
8. Портал «CIT Forum» — http://www.citforum.ru – IT
9. Проект «Russian Fedora» — http://www.russianfedora.ru
10. Робачевский А.М. Операционная система UNIX СПб. БХВ-Петербург 2002. 528 с.
11. Столлингс В. Операционные системы. – М.: Вильямс, 2002. – 848 с.
12. Таненбаум Э. Современные операционные системы. – СПб.: Питер, 2002. – 1040 с.
13. Эбен М., Таймэн Б. «FreeBSD. Энциклопедия пользователя» - К: ООО «ТИД «ДС», 2002. 864с.
14. InterSystems International Corporation в России — http://www.intersystems.ru

Тема 15. Сетевые технические средства информационных сетей

Цели:

· Получить представление о критериях выбора проводной и беспроводной сети.
· Научиться объединять две локальные сети в одну.
· Понять преимущества коммуникационное оборудования.
· Научиться подключать сеть к другим сетям и компьютерным средам для объединения их в большую разнородную систему.

Техническое обеспечение **—** комплекс электронных, электрических и механических устройств, входящих в состав системы или сети. Техническое или аппаратное обеспечение включает компьютеры и логические устройства. К ним добавляются внешние устройства и диагностическая аппаратура. Вспомогательную, но важную роль играют энергетическое оборудование, батареи и аккумуляторы. Нередко, для обеспечения безопасности данных, используются аппараты шифрования информации.

15.1. Линии связи.

15.1.1. Кабельные системы вычислительных сетей

В широком ассортименте кабелей нетрудно запутаться. Так, фирма Belden, ведущий производитель кабелей, публикует каталог, где предлагает более 2200 их типов. К счастью, в большинстве сетей применяются только три основные группы кабелей:
· коаксиальный кабель (coaxial cable);
· витая пара (twisted pair);
· неэкранированная (unshielded);
· экранированная (shielded);
· оптоволоконный кабель (fiber optic).

15.1.2. Коаксиальный кабель

Не так давно коаксиальный кабель был самым распространенным типом кабеля. Во-первых, он был относительно недорогим, легким, гибким и удобным в применении. А во-вторых, широкая популярность коаксиального кабеля привела к тому, что он стал безопасным и простым в установке. Самый простой коаксиальный кабель состоит из медной жилы (core), изоляции, ее окружающей, экрана в виде металлической оплетки и внешней оболочки. Если кабель, кроме металлической оплетки, имеет и слой фольги, он называется кабелем с двойной экранизацией.

Существует два типа коаксиальных кабелей:
· тонкий коаксиальный кабель;
· толстый коаксиальный кабель.

Рис. 15.1. Структура коаксиального кабеля

Тонкий коаксиальный кабель **—** гибкий кабель диаметром около 0,5 см (около 0,25 дюймов). Тонкий (thin) коаксиальный кабель способен передавать сигнал на расстояние до 185 м (около 607 футов) без его заметного искажения, вызванного затуханием.

Толстый (thick) коаксиальный кабель **—** относительно жесткий кабель с диаметром около 1 см (около 0,5 дюймов). Иногда его называют «стандартный Ethernet», поскольку он был первым типом кабеля, применяемым в Ethernet. Толстый коаксиальный кабель передает сигналы дальше, чем тонкий, — до 500 м (около 1 640 футов).

15.1.3. Витая пара

Самая простая витая пара (twisted pair) **—** это два перевитых вокруг друг друга изолированных медных провода. Существует два типа тонкого кабеля: неэкранированная (unshielded) витая пара (UTP) и экранированная (shielded) витая пара (STP).

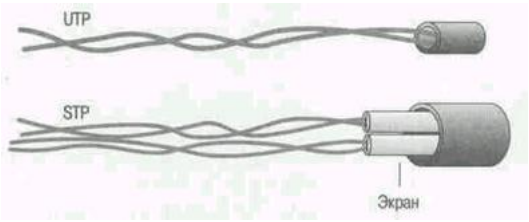


Рис. 15.2. Неэкранированная и экранированная витые пары

15.1.4. Волоконно-оптические линии.

Наиболее дорогими являются оптопроводники, называемые также стекло-волоконным кабелем. Скорость распространения информации по ним достигает от 100 Мбит/с до нескольких Гигабит в секунду. Допустимое удаление более 50 км. Внешнее воздействие помех практически отсутствует. На данный момент это наиболее дорогостоящее соединение для ЛВС. Применяются там, где возникают электромагнитные поля помех или требуется передача информации на очень большие расстояния без использования повторителей, а так же для достижения высоких пропускных способностей. Они обладают противоподслушивающими свойствами, так как техника ответвлений в оптоволоконных кабелях очень сложна.

Рис. 15.3. Оптоволоконный кабель

15.1.5. Выбор кабеля

Прежде чем выбрать наиболее подходящий для Вас тип кабеля, ответьте на следующие вопросы. Они помогут Вам сориентироваться среди огромного разнообразия кабельной продукции.

- Насколько интенсивным планируется сетевой трафик?
- Каковы требования защиты данных?
- На какое максимальное расстояние будет проложен кабель?
- Каковы требуемые характеристики кабеля?
- Сколько средств выделено на реализацию проекта?

15.1.6. Беспроводные сети

Кабели — общепринятая среда обмена данными между компьютерами. Однако сегодня появляются технологии беспроводной передачи, которые избавляют нас от трудностей физических соединений. Наиболее распространёнными на сегодняшний день являются: радиопередающие сети, сети с инфракрасным и лазерным излучением, мобильные (сотовые) сети, микроволновые системы и другие.

15.2. Коммутационное оборудование.

Коммутационное оборудование любой информационной сети служит связующим звеном между источниками (компьютерами, серверами, внешними периферийными устройствами, средствами отображения и воспроизведения мультимедиа).

Функции современного коммутационного оборудования включают:

- физическое соединение источников и средств;
- усиление и передачу сигналов на расстояние;
- разветвление сигналов, необходимое для подключения одного источника сразу к нескольким средствам отображения;
- коммутацию сигналов, позволяющую подключать несколько источников к одному входу средства отображения;
- регулировку параметров сигналов;
- преобразование сигналов из одного вида в другой, выполняемое, как правило, с целью обеспечения наилучшего соответствия параметров сигналов и возможностей средств отображения.

Коммутационные устройства могут выполнять ряд специальных функций, таких как контроль наличия сигналов, гальваническая развязка между устройствами, подключенными к разным контурам заземления, генерация настроечных тестовых изображений. Большинство коммутационных устройств может управляться дистанционно с помощью интерфейса RS-232. Весь спектр современного коммутационного оборудования может быть разбит на следующие группы в соответствии с выполняемыми ими функциями:

Усилители-разветвители выполняют две основные функции: усиление сигнала с целью компенсации его затухания при передаче на расстояние и разветвление, позволяющее подключать один источник к нескольким средствам демонстрации.

Переключатели, используются для подключения сразу несколько источников к одному средству отображения.. Имея несколько входов и несколько выходов, они позволяют переключать любой из входов на любой один или несколько выходов сразу, что обеспечивает максимальную гибкость при организации вывода информации.

Преобразователи сигнала меняют формат и параметры сигналов, обеспечивают точное соответствие типа, разрешения и частоты сигнала параметрам устройств. Среди устройств этой группы можно выделить универсальные преобразователи, способные произвольно менять многие сигналы, существенно расширяя спектр возможных источников и используемых средств отображения.

Комбинированные устройства объединяют в себе сразу несколько функций. Системные переключатели могут одновременно являться переключателями, разветвителями и иметь встроенный преобразователь для приведения сигналов к удобному формату. Дополнительной особенностью этих устройств является функция дистанционного управления оборудованием с помощью реле и последовательного порта, а также встроенное устройство для дешифровки команд инфракрасных пультов дистанционного управления. Некоторые комбинированные устройства имеют функцию бесшовного (seamless) переключения.

Важнейшей частью любой системы являются кабели. Качественные кабели отличаются высокой стабильностью таких параметров, как диаметр проводниковых жил и расстояние между ними, качество изоляции и экранировки. Использование качественных кабелей обеспечивает преимущество системы в целом, позволяя минимизировать потери качества сигналов. Важной характеристикой кабелей является коэффициент затухания, определяющий суммарные потери сигнала на единицу его длины. При выборе кабелей особую роль играет тип и параметры соответствующего сигнала, а также расстояние, на которое следует передавать данный сигнал. Также к коммутационному оборудованию относят: коммутационные шкафы, панели, стойки, кронштейны, щиты

15.2.1. Сетевые адаптеры

По выполняемым функциям сетевые адаптеры (СА) делятся на две группы:

1. Реализующие функции физического и канального уровней. Применяются в сетях с простой топологией, где почти отсутствует необходимость выполнения таких функций, как маршрутизация пакетов, формирование из поступающих пакетов сообщений, согласование протоколов различных сетей и др.
2. Реализующие функции первых четырех уровней модели ВОС - физического, канального, сетевого и транспортного. Эти адаптеры, кроме функций СА первой группы, могут выполнять функции маршрутизации, ретрансляции данных, формирования пакетов из передаваемого сообщения (при передаче), сборки пакетов в сообщение (при приеме), согласования ППД различных сетей, сокращая таким образом затраты вычислительных ресурсов ЭВМ на организацию сетевого обмен.

Адаптеры ориентированы на определенную архитектуру локальной сети и ее технические характеристики, поэтому по топологии ЛВС адаптеры разделяются на следующие группы: поддерживающие шинную топологию, кольцевую, звездообразную, древовидную, комбинированную (звездно-кольцевую, звездно-шинную). Дифференциация адаптеров по выполняемым функциям и ориентация их на определенную архитектуру ЛВС привели к большому многообразию типов адаптеров и разбросу их характеристик.

15.3. Коммуникационное оборудование.

Коммуникационное оборудование предназначено для подключения персональных компьютеров, а также других устройств к технологическим сетям, построенным на базе выделенных каналов тональной частоты, радиоканалов и цифровых каналов передачи данных, а также позволяет построить многоуровневые технологические сети с применением различных физических каналов передачи данных в различных сегментах сети. Это оборудование лучше всего изучать на примерах оборудования компании CISCO, которая разрабатывает и продаёт сетевое оборудование, а также ПО к этому оборудованию. Также на современном рынке существует множество фирм, работающих в области производства сетевого коммуникационного оборудования: D-Link, 3Com, ZyXEL, Linksys, Trendnet, Planet и многие другие зарубежные и отечественные фирмы.

15.3.1. Концентратор (Hub) и модем

Концентратор (Hub) — многопортовый повторитель сети с автосегментацией. Все порты концентратора равноправны. Получив сигнал от одной из подключенных к нему станций, концентратор транслирует его на все свои активные порты. При этом, если на каком-либо из портов обнаружена неисправность, то этот порт автоматически отключается (сегментируется), а после ее устранения снова делается активным. Обработка коллизий и текущий контроль за состоянием каналов связи обычно осуществляется самим концентратором. Концентраторы можно использовать как автономные устройства или соединять друг с другом, увеличивая тем самым размер сети и создавая более сложные топологии.

Модем, обеспечивая согласование цифровых сигналов компьютера с аналоговыми сигналами телефонной линии, при передаче данных осуществляет модулирование аналоговых сигналов цифровой информацией, а при приеме - демодулирование. Главное отличие между ними - способ модуляции. Различают модемы с частотной, амплитудной и фазовой модуляцией.

15.3.2. Приемопередатчики (Transceiver) и повторители (Repeater)

С помощью этих устройств можно объединить несколько сегментов сети с шинной топологией, увеличивая таким образом общую протяженность сети.

Приемопередатчик трансивер (Transceive)r (сокращение от TRANSmitter/reCEIVER) — это устройство, предназначенное для приема пакетов от контроллера рабочих станций сети и передачи их в шину. Он также разрешает коллизии в шине. Конструктивно приемопередатчик и контроллер могут объединяться на одной плате или находиться в различных узлах.

Повторитель, репитер (Repeater) — устройство, передающее сигналы из одного кабеля в другой без маршрутизации или фильтрации пакетов. В терминах OSI представляет собой промежуточное устройство физического уровня. Сигнал при

распространении по кабелю искажается, поскольку уменьшается его амплитуда. Причина этого явления — затухание. В результате, если кабель имеет достаточную длину, затухание может исказить сигнал до неузнаваемости. Однако благодаря репитерам сигналы способны распространяться на большие расстояния.

15.3.3. Коммутаторы (switch), мосты (bridge) и шлюзы (gateways)

Когда появились первые устройства, позволяющие разъединять сеть на несколько доменов коллизий (по сути фрагменты ЛВС, построенные на hub-ах), они были двух портовыми и получили название мостов (bridge-ей). По мере развития данного типа оборудования, они стали многопортовыми и получили название коммутаторов (switch-ей). Некоторое время оба понятия существовали одновременно, а позднее вместо термина "мост" стали применять "коммутатор".

Коммутаторы. Наиболее простую структуру имеет коммутатор. Это связано с тем, что он соединяет друг с другом только каналы передачи данных, образуя необходимую физическую базу тракта передачи информации между абонентскими системами. В том случае, когда к коммутатору подходит более двух каналов, он выполняет функции, связанные с коммутацией информации. Коммутация осуществляется прозрачным образом, т.е. без какой-либо обработки этой информации. Во всех случаях (при любом числе соединяемых каналов) коммутатор обеспечивает усиление передаваемых сигналов и корректирует крутизну их фронтов. Коммутатор не имеет буферов. Поэтому он прозрачен для информации. Более того, коммутатор требует, чтобы скорости передачи данных по соединяемым каналам были одинаковы. Физические процессы выполняемые коммутатором реализуются аппаратно. Коммутаторы используются для соединения в основном идентичных сетей, имеющих некоторые различия на физическом и канальном уровнях. Например, с помощью коммутатора могут соединяться на 3-м (сетевом) уровне две сети с различными более низкими уровнями, но одинаковыми более высокими уровнями.

Коммутатор является обучающимся устройством и действует по аналогичной технологии. В отличие от мостов, ряд коммутаторов не помещает все приходящие пакеты в буфер. Это происходит лишь тогда, когда надо согласовать скорости передачи, или адрес назначения не содержится в адресной таблице, или когда порт, куда должен быть направлен пакет, занят, а коммутирует пакеты "на лету". Коммутатор лишь анализирует адрес назначения в заголовке пакета и, сверившись с адресной таблицей, тут же (время задержки около 30-40 микросекунд) направляет этот пакет в соответствующий порт. Таким образом, когда пакет еще целиком не прошел через входной порт, его заголовок уже передается через выходной.

Шлюзы (gateways) обеспечивают связь между различными архитектурами и средами. Они переупаковывают и преобразуют данные, передаваемые из одной среды в другую, чтобы каждая среда могла понимать данные других сред. В частности, шлюз переупаковывает информацию в соответствии с требованиями системы назначения; изменяет формат сообщения, чтобы прикладная программа на принимающей стороне могла распознать данные. Например, шлюзы электронной почты (такие, как X.400) принимают сообщение в одном формате, транслируют его и пересылают в формате X.400, используемом получателем, и наоборот.

Шлюз связывает две системы, которые используют разные:

- коммуникационные протоколы;
- структуры и форматы данных;
- языки;
- архитектуры.

Шлюзы связывают гетерогенные сети, например Microsoft Windows NT Server с SNA (Systems Network Architecture фирмы IBM). Они изменяют формат данных, чтобы сделать их понятными прикладной программе на принимающей стороне. Наиболее сложной из систем преобразующих протоколы является шлюз. Он обеспечивает взаимодействие двух или более информационных сетей с различными «штабелями» протоколов семи уровней. Следует отметить, что шлюзы чаще всего используются в тех случаях, когда нужно объединить информационные сети, созданные по различным фирменным стандартам. Когда же проектируется группа сетей в соответствии со стандартами ISO, целесообразен другой подход. В этом случае в соединяемых сетях протоколы уровней 4-7 делаются одинаковыми. Это позволяет для соединения сетей использовать не шлюзы, а более простые ретрансляционные системы — маршрутизаторы, мосты.

Мост (bridge), как и репитер, может соединять сегменты или локальные сети рабочих групп. Однако в отличие от репитера, мост также служит для разбиения сети, что помогает изолировать трафик или отдельные проблемы. Например, если трафик одного-двух компьютеров или одного отдела «затопляет» сеть пакетами, уменьшая ее производительность в целом, мост изолирует эти компьютеры или этот отдел.

Мосты предназначены для соединения частей сетей, различных типов каналов передачи данных, например циклического кольца с моноканалом. Любой канал определяется протоколами уровней 1-2, поэтому логическая структура моста имеет двухуровневую структуру. Канальные процессы здесь преобразуют протоколы обоих уровней. При использовании мостов в соединяемых подсетях должны быть согласованы структура адресов и размер кадров. Более сложные интеллектуальные мосты наряду с указанными задачами выполняют также роль фильтров, не пропускающих сквозь себя пакеты, не адресованные другой части сети. Мосты не имеют механизмов управления потоками. Поэтому, если входной поток кадров больше выходного, то буферы переполняются и кадры выбрасываются. Нередко кадры, которые в течение заданного времени не могли быть переданы, также ликвидируются.

Мосты обычно решают следующие задачи.

- Увеличивают размер сети.
- Увеличивают максимальное количество компьютеров в сети.
- Устраняют узкие места, появляющиеся в результате подключения избыточного числа компьютеров и, как следствие, возрастания трафика. Мосты разбивают перегруженную сеть на отдельные сегменты с уменьшенным трафиком. В итоге каждая подсеть будет работать более эффективно.
- Соединяют разнородные физические носители, такие, как витая пара и коаксиальный кабель.
- Соединяют разнородные сегменты сети, например Ethernet и Token Ring, и переносят между ними пакеты.

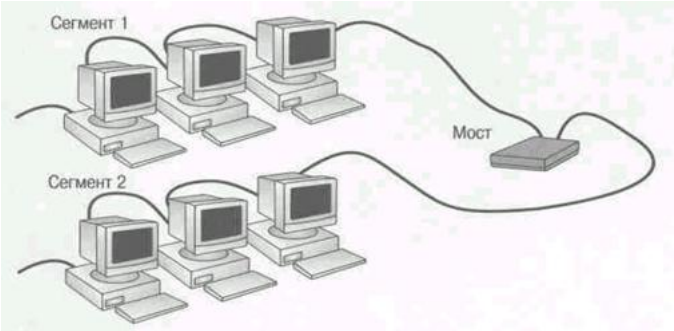


Рис. 15.4. Мост соединяет две сети

15.3.4. Маршрутизаторы (routers)

Маршрутизаторы (routers) работают на сетевом уровне модели OSI. Это значит, что они могут переадресовывать и маршрутизировать пакеты через множество сетей, обмениваясь информацией (которая зависит от протокола) между раздельными сетями. Маршрутизаторы считывают в пакете адресную информацию сложной сети и, поскольку они функционируют на более высоком по сравнению с мостами уровне модели OSI, имеют доступ к дополнительным данным. Маршрутизатор является сложным интеллектуальным устройством, построенным на базе одного, а иногда и нескольких мощных процессоров. Такой специализированный мультипроцессор работает, как правило, под управлением специализированной операционной системы.

Маршрутизаторы могут выполнять следующие функции мостов:

- фильтровать и изолировать трафик;
- соединять сегменты сети.
- соединять нескольких локальных сетей.
- подключать локальные сети (LAN) к территориально-распределенным сетям (WAN).

Маршрутизаторы зависят от используемого протокола (например, TCP/IP, IPX, AppleTalk) и, в отличие от мостов и коммутаторов, функционирующих на втором уровне, работают на третьем или седьмом уровне модели OSI. Маршрутизатор имеет в своем распоряжении базу топологической информации, которая говорит ему, например, о том, между какими подсетями общей сети имеются связи и в каком состоянии (работоспособном или нет) они находятся. Имея такую карту сети, маршрутизатор может выбрать один из нескольких возможных маршрутов доставки пакета адресату (он может принимать решение о наилучшем маршруте доставки данных, руководствуясь такими факторами, как стоимость, скорость доставки и т.д.). Кроме того, маршрутизаторы позволяют эффективно управлять трафиком широковещательной рассылки, обеспечивая передачу данных только в нужные порты. В отличие от моста/коммутатора, который не знает, как связаны сегменты друг с другом за пределами его портов, маршрутизатор видит всю картину связей подсетей друг с другом, поэтому он может выбрать правильный маршрут и при наличии нескольких альтернативных маршрутов. Решение о выборе того или иного маршрута принимается каждым маршрутизатором, через который проходит сообщение. Для того чтобы составить карту связей в сети, маршрутизаторы обмениваются специальными служебными сообщениями, в которых содержится информация о тех связях между подсетями, о которых они знают (эти подсети подключены к ним непосредственно или же они узнали эту информацию от других маршрутизаторов). Построение графа связей между подсетями и выбор оптимального по какому-либо критерию маршрута на этом графе представляют собой сложную задачу. Маршрутизаторы позволяют объединять сети с различными принципами организации в единую сеть, которая в этом, случае часто называется интерсеть (internet). В каждой из сетей, образующих интерсеть, сохраняются присущие им принципы адресации узлов и протоколы обмена информацией. Поэтому маршрутизаторы могут объединять не только локальные сети с различной технологией, но и локальные сети с глобальными. Маршрутизаторы не только объединяют сети, но и надежно защищают их друг от друга. Причем эта изоляция осуществляется гораздо проще и надежнее, чем с помощью мостов/коммутаторов. Кроме того, маршрутизатор предоставляет администратору удобные средства фильтрации потока сообщений за счет того, что сам распознает многие поля служебной информации в пакете. Задачей маршрутизатора является обеспечение взаимодействия коммуникационных подсетей. Последние характеризуются лишь тремя уровнями протоколов. Маршрутизатор “не знает” протоколов уровней 4-7 и является прозрачным для них. В его задачу входит преобразование протоколов трех нижних уровней. Иногда в информационных сетях маршрутизаторы связывают части коммуникационной подсети, в которых используются одинаковые протоколы уровней 1-3. В этих случаях в маршрутизаторах, именуемых узлами коммутации пакетов, преобразование протоколов не выполняется. Здесь сетевые процессы осуществляют лишь коммутацию и маршрутизацию информации. В соединяемых узлами подсетях должна быть осуществлена общая адресация абонентских систем.

15.3.5. Анализаторы ЛВС и сетевые тестеры

Анализаторы — это мощный диагностический инструмент, предназначенный для контроля качества функционирования сети. Контроль позволяет наблюдать за работой сети в режиме реального времени и регистрировать события, которые могут означать возникновение проблемы. Контроль сопровождается графическим или цифровым отображением информации. Анализаторы могут накапливать и хранить информацию о состоянии сети с целью последующего его воспроизведения и анализа.

Сетевые тестеры — это приборы, входящие в состав контрольно-измерительной аппаратуры, которая облегчает установку и техническое обслуживание локальных сетей. Тестеры линий передачи являются хорошим средством проверки нового кабеля и отыскания неисправностей в системе установленных кабелей. Они способны не только обнаруживать неисправность, но и сообщать сведения о ее характере и месте расположения.

15.4. Терминальное оборудование.

Терминальное оборудование **—** основная часть абонентской системы, выполняющая прикладные процессы и, возможно, часть функций области взаимодействия.

Главной задачей терминального оборудования является выполнение прикладных процессов для нужд пользователей. Кроме этого - прикладные процессы управления. Оно может также выполнять и функции верхних уровней области взаимодействия. Чаще всего используются те типы терминального оборудования, которые кроме прикладных процессов реализуют три, четыре либо пять верхних уровней. Подключается терминальное оборудование в информационную сеть при помощи дополнительного устройства, именуемого станцией. Станция выполняет недостающие в нем функции нижних уровней. В качестве терминального оборудования могут выступать самые разнообразные устройства: телефонный аппарат, телекс, факс-аппарат, дисплей, X-terminal (предназначенны для работы с изображениями), полиэкранный терминал, многофункциональный терминал (работает с любыми типами данных, в том числе - с речью и изображениями), персональный компьютер, мини-компьютер, суперкомпьютер и т.д.

Контрольные вопросы:

1. Назначение сетевого адаптера.
2. Каково назначение повторителя?
3. Что такое сетевой концентратор и каково его назначение?
4. На каком уровне сетевой модели OSI используется Hub?
5. Назначение моста.
6. На каком уровне сетевой модели OSI используется мост?
7. На каком уровне сетевой модели OSI используется коммутатор?
8. Назначение маршрутизатора.
9. Каково различие между маршрутизаторами и мостами?
10. Что такое шлюз и каково его назначение.

Практические задания:

ЗАДАНИЕ № 15.1. Типы сетевых кабелей. Найдите для варианта реализации в левой колонке соответствующий тип кабеля в правой.

Реализация	Тип кабеля
1. Используется в топологии «шина»	a. Неэкранированная витая пара
2. Использовался изначально в сетях Token Ring	b. Однорежимный оптоволоконный кабель
3. Подходит для сетей Gigabit Ethernet	c. Экранированная витая пара
4. Состоит из восьми проводов	d. Коаксиальный кабель
5. Используется в ЛВС, передающих данные на большие расстояния	e. Кабель типа UTP категории 5
6. Использует лазер в качестве источника света	f.Многорежимный оптоволоконный кабель

ЗАДАНИЕ № 15.2. Диагностика кабелей. Определите, будет ли функционировать сеть в описанных ситуациях. Если нет, объясните почему.

1. 25 компьютеров подключено к 300-метровому сегменту кабеля ≪тонкий≫ Ethernet с использованием топологии ≪шина ≫.

2. 10 компьютеров с сетевыми платами 100BaseT4 Fast Ethernet подключены к концентратору 100-метровыми отрезками кабеля UTP категории 3.

3. Сети в двух зданиях, расположенных на расстоянии 1000 м друг от друга, соединены с помощью однорежимного оптоволоконного кабеля с разъемами RJ45.

4. 15 компьютеров объединены в сеть Token Ring с физической топологией ≪кольцо≫.

5. Сеть Fast Ethernet построена с использованием оборудования 100BaseTX и кабеля UTP категории 5e. Две пары проводов в кабеле используются для передачи данных, а еще две **—** для передачи телефонного сигнала.

ЗАДАНИЕ № 15.3. Концентраторы. Найдите для понятия в левой колонке соответствующее описание в правой.

Понятие	Описание
1. Модуль множественного доступа в сети Token Ring	a. Усиливает сигналы
2. Интеллектуальный концентратор	b. Передает сообщения на консольуправления сетью
3. Каскадирующий порт	c. Используется для соединения модулей MAU
4. Закороченный порт	d. Пересылает пакеты последовательно
5. Повторитель	e. Исключен из сети Token Ring
6. Порт для входа и выхода	f. Используется для соединения концентратора Ethernet с обычным портом другого концентратора

ЗАДАНИЕ № 15.4. Назначение моста. Найдите для понятия в левой колонке соответствующее описание в правой.

Понятие	Описание
1. Мост-транслятор	a. Определяет выбор конкретного моста для обработки пакетов
2. Маршрутизация «источник-маршрут»	b. Позволяет мостам составлять таблицы адресов
3. Прозрачное соединение	c. Соединяет два сегмента сети с помощью технологии ГВС
4. Удаленный мост	d. Соединяет два сетевых сегмента, в которых используются кабели различных видов
5. STA	e. Позволяет компьютерам самим выбирать, каким мостом они будут пользоваться

ЗАДАНИЕ № 15.5. Коммутаторы. Дать сравнительную характеристику коммутаторов 3-го и 4-го уровня. С помощью программы Microsoft Visio соединить несколько групп компьютеров данными коммутаторами и обосновать своё решение.

Перечень литературы и Интернет-ресурсов:

1. Б. С. Гольдштейн, «Системы коммутации: Учебник для вузов», Издательство: «БХВ-Петербург», 2004 г., 318 стр. ISBN5-8206-0108-4,5-8206-0128-9.

2. А. Б. Гольдштейн, Б. С. Гольдштейн, «Softswitch», Издательство: «БХВ-Петербург», 2006 г., 368 стр., ISBN5-8206-0117-3.

3. Б. С. Гольдштейн, И. М. Ехриель, Р. Д. Рерле, «ОКС7. Подсистема SCCP. Справочник по телекоммуникационным протоколам», Серия: Телекоммуникационные протоколы ВСС РФ, Издательство: «БХВ-Петербург», 2006 г., 320 стр., ISBN5-94157-940-3.

4. перев. Тригуб С. Н., Программа сетевой академии Cisco CCNA 3 и 4: вспомогательное руководство (+ CD-ROM), Издательство: «М.:Вильямс», 2008г., 994 стр., ISBN: 978-5-8459-1120-9, 5-8459-1120-6.

5. Пролетарский А.В.,Баскаков И.В.,Чирков Д.Н.,Федотов Р.А.,Бобков А.В.,Платонов В.А., Беспроводные сети Wi-Fi. Учебное пособие, Издательство:М.: «Интернет-университет информ.технологий», 2010 г., 215 стр., ISBN:978-5-94774-737-9.

6. Уэнделл Одом, Официальное руководство по подготовке к сертификационным экзаменам CCENT/CCNA ICND1. 2-е изд. (+CD), Издательство: «М.:Вильямс», 2009г., 736стр., ISBN:978-5-8459-1442-2.

7. Шевкопляс Б.В. Синхронизация в телекоммуникационных системах: Сборник задач: Учебное пособие (ГРИФ) / Шевкопляс Б.В. Издательство: «РадиоСофт», 2009г., 368 стр., ISBN:978-5-93037-187-1.

Экзаменационные вопросы

1. Основные понятия информационных сетей (информация, сообщение, объект, абонент, пользователь, рабочая группа …).
2. Понятие открытой информационной системы.
3. Информационные сети. Классификация, краткие характеристики.
4. Основные концепции построения вычислительной сети.
5. Назначение информационной сети.
6. Архитектура вычислительных сетей.
7. Одноранговые сети.
8. Сети с выделенным сервером.
9. Комбинированные сети.
10. Сравнение одноранговых сетей и сетей на основе сервера.
11. Назначение информационных сетей. Классификация сетей ЭВМ (Локальные вычислительные сети, Корпоративная сеть, Глобальная сеть.
12. Протоколы IPX/SPX.
13. Локальные сети. Характеристики. Ассоциация локальных сетей.
14. Информационные ресурсы сетей.
15. Теория очередей. Пуассоновские процессы.
16. Теория очередей. Система обслуживания M/M/1.
17. Базовая эталонная модель взаимодействия открытых систем. Область взаимодействия. Прикладной, представительный и сеансовый уровни.
18. Базовая эталонная модель взаимодействия открытых систем. Транспортный, сетевой, канальный и физический уровни.
19. Соединения. Физические средства соединений. Абонентский канал. Порт. Физические и логические каналы.
20. Модель OSI ISO.
21. Модель IEEE 802.
22. Компоненты информационных сетей. Абонентская система. Ретрансляционная система.
23. Административная система. Управление сетью.
24. Коммуникационные подсети. Аналоговые и дискретные сети.
25. Моноканальные подсети. Моноканал. Множественный доступ.
26. Циклические подсети. Структуры.
27. Узловые подсети. Узлы коммутации.
28. Основные группы кабелей вычислительных сетей.
29. Сетевые адаптеры.
30. Методы маршрутизации информации.
31. Методы коммутации информации. Коммутация каналов. Коммутация пакетов.
32. Методы коммутации информации. Смешанная коммутация. Ретрансляция кадров. Ретрансляция ячеек. Сквозная коммутация.
33. Протоколы. Назначение. Классификация.
34. Сетевые протоколы.
35. Назначение сетевых протоколов.
36. Работа сетевых протоколов.
37. Маршрутизируемые и немаршрутизируемые сетевые протоколы.
38. Понятие протокола. Стандартные стеки коммуникационных протоколов (OSI, TCP/IP, Стек IPX/SPX, NetBIOS/SMB).
39. Сетевые службы.
40. Модель распределённой обработки информации.
41. Безопасность информации. Задачи. Методы обеспечения.
42. Концепция безопасности сети.
43. Базовые функциональные профили. Полные функциональные профили.
44. Показатели и методы оценки эффективности информационных сетей.
45. Сетевые программные и технические средства.
46. Методы коммутации информации. Коммутация каналов, сообщений, пакетов. Дейтаграммы. Виртуальные каналы.
47. Классификация коммуникационных подсетей локальных и территориальных компьютерных сетей. Основные принципы организации и функционирования сетей с селекцией и маршрутизацией информации. Моноканальные и циклические коммуникационные подсети.
48. Комплекс стандартов IEEE 802. Структура комплекса. Примеры стандартов IEEE 802. Соотношение IEEE 802 с моделью OSI ISO.
49. Физическая структура сетей Ethernet.
50. Метод CSMA/CD.
51. Коммутаторы. Основные принципы организации и функционирования.

Глоссарий

Русские термины:

1000Base–LX – стандарт на сегменты сети Gigabit **Ethernet на оптоволоконном кабеле с длиной волны света 1,3 мкм.**

1000Base–SX – стандарт на сегменты сети Gigabit **Ethernet на оптоволоконном кабеле с длиной волны света 0,85 мкм.**

1000Base–CX – стандарт на сегменты сети Gigabit **Ethernet на экранированной витой паре.**

100Base–FX – обозначение **технологии Fast Ethernet по** стандарту 802.3 сети Fast Ethernet для передачи больших сообщений по многомодовому оптоволокну в полудуплексном и полнодуплексном режимах.

100Base-T4 – обозначение **технологии Fast Ethernet** по стандарту 802.3 **со скоростью 100 Мб/с** для четырех парной витой пары. Вместо кодирования 4B/5B в этом методе используется кодирование 8B/6T.

100Base–TX – обозначение **технологии** сети Fast Ethernet по стандарту 802.3 для передачи больших сообщений с использованием метода MLT-3 для передачи сигналов 5-битовых порций кода 4B/5B по витой паре, а также наличие функции авто переговоров (Auto-negotiation) для выбора режима работы порта.

10Base2 – обозначение технологии Ethernet по стандарту 802.3 со скоростью передачи данных 10 Мб/с для тонкого коаксиального кабеля.

10Base5 – обозначение технологии Ethernet по стандарту 802.3 со скоростью передачи данных 10 Мб/с для толстого коаксиального кабеля.

10Base–FL – стандарт на сегменты сети **Ethernet на оптоволоконном кабеле.**

10BaseT – обозначение технологии Ethernet по стандарту 802.3 со скоростью передачи данных 10 Мб/с для кабеля «витая пара».

Адаптер (adapter) – устройство либо программа для согласования параметров входных и выходных сигналов в целях сопряжения объектов.

Административная система (management system) – система, обеспечивающая управление сетью либо ее частью.

Адрес (address) – закодированное обозначение пункта отправления либо назначения данных.

Адрес IP – адрес, однозначно определяющий компьютер в сети (адрес состоит из 32 двоичных разрядов и не может повторяться во всей сети TCP/IP). Адрес IP обычно разбивается на четыре октета по восемь двоичных разрядов (один байт); каждый октет преобразуется в десятичное число и отделяется точкой, например 102.54.94.97.

Аналоговый сигнал (analog signal) – сигнал, величина которого непрерывно изменяется во времени. Аналоговый сигнал обеспечивает передачу данных путем непрерывного изменения во времени.

Аналого-дискретное преобразование (analog-to-digital conversion) – процесс преобразования аналогового сигнала в дискретный сигнал.

Анонимные подключения – эта функция, которая разрешает удаленный доступ к ресурсам компьютера по учетной записи компьютера без предъявления имени и пароля с правами, определяемыми этой учетной записью.

Архитектура – концепция, определяющая модель, структуру, выполняемые функции и взаимосвязь компонентов сети. Архитектура охватывает логическую, физическую и программную структуры и функционирование сети, а также элементы, характер и топологию взаимодействия элементов.

Асинхронная передача – метод передачи основанный на пересылки данных по одному символу. При этом промежутки между передачами символов могут быть не равными.

База данных (БД) – совокупность взаимосвязанных данных, организованная по определенным правилам в виде одного или группы файлов.

Базовый порт ввода/вывода (base I/O port) – адрес памяти, по которому центральный процессор и адаптер проверяют наличие сообщений, которые они могут оставлять друг для друга.

Безопасность данных (data security) **–** концепция защиты программ и данных от случайного либо умышленного изменения, уничтожения, разглашения, а также несанкционированного использования.

Блок данных (data unit) – последовательность символов фиксированной длины, используемая для представления данных или самостоятельно передаваемая в сети.

Бод (baud) – термин, используемый для измерения скорости модема, который описывает количество изменений состояния, происходящих за одну секунду в аналоговой телефонной линии.

Булева алгебра – алгебраическая структура с тремя операциями И, ИЛИ, НЕ.

Буфер (buffer) – временная область, которую устройство использует для хранения входящих данных перед тем, как они смогут быть обработаны на входе, или для хранения исходящих данных до тех пор, пока не появится возможность их передачи.

Буфер (buffer) – запоминающее устройство, используемое между объектами при передаче данных для временного хранения данных с целью согласования скоростей.

Витая пара (twisted-pair cable) – два скрученных изолированных провода, которые используются для передачи электрических сигналов.

Виртуальная сеть – сеть, характеристики которой в основном определяются ее программным обеспечением.

Виртуальные локальные вычислительные сети (ВЛВС) – логические наложения на коммутируемое объединение сетей, определяющие группы пользователей. Это означает, что пользователь или система, подключенные к физическому порту, могут участвовать в нескольких ВЛВС – группах, поскольку логическая сеть не обязана подчиняться ограничениям физической. Границы ВЛВС задают область локального вещания. Обычно потоки данных в ВЛВС коммутируются на уровне 2, в то время как трафик между ВЛВС маршрутизируется, с использованием внешнего маршрутизатора.

Волновое сопротивление, импеданс (impedance) – полное электрическое сопротивление переменному току, включающее активную и реактивную составляющие. Измеряется в омах.

Выделенная линия (dedicated line) **–** (точка-точка) частная или адресуемая линия, наиболее популярная в глобальных вычислительных сетях. Обеспечивает полнодуплексную полосу пропускания, установив постоянное соединение каждой оконечной точки через мосты и маршрутизаторы с несколькими ЛВС.

Выделенный сервер (dedicated server) – сетевой сервер, который действует только как сервер и не предназначен для использования в качестве клиентской машины.

Гигабайт (gigabyte) – обычно 1000 мегабайтов. Точно 1024 мегабайт, где 1 мегабайт равен 1 048 576 байтам (2^{20}).

Гиперсреда – технология представления любых видов информации в виде блоков, ассоциативно связанных друг с другом, не требующая подтверждения о приеме от принимающей стороны.

Гипертекст – текст, представленный в виде ассоциативно связанных друг с другом блоков.

Гипертекстовый протокол HTTP – протокол сети Internet, описывающий процедуры обмена блоками гипертекста.

Главный контроллер домена (Primary Domain Controller, PDC) – компьютер, на котором устанавливается Windows NT Server в режиме PDC для хранения главной копии базы данных учетных записей.

Глобальная вычислительная сеть, ГВС (Wide Area Network, WAN) – компьютерная сеть, использующая средства связи дальнего действия.

Группа (group) – совокупность пользователей, определяемая общим именем и правами доступа ресурсам.

Данные (data**)** – информация, представленная в формализованном виде, пригодном для автоматической обработки при возможном участии человека.

Дейтаграммы (datagrams) – сообщения, которые не требуют подтверждения о приеме от принимающей стороны. Термин, используемый в некоторых протоколах для обозначения пакета.

Дефрагментация (defragmentation) – процесс воссоздания больших PDU (пакетных блоков данных) на более высоком уровне из набора более мелких PDU с нижнего уровня.

Диагностическое программное обеспечение (diagnostic software) – специализированные программы или специфические системные компоненты, которые позволяют исследовать и наблюдать систему с целью определения, работает она правильно или нет, и попробовать определить причину проблемы.

Дискретный сигнал (discrete signal**)** – сигнал, имеющий конечное, обычно небольшое, число значений. Практически всегда дискретный сигнал имеет два либо три значения. Нередко его называют также *цифровым сигналом.*

Домен (domain) – совокупность компьютеров, использующих операционную систему Windows NT Server, имеющих общую базу данных и систему защиты. Каждый домен имеет неповторяющееся имя.

Доменная система имен (DNS –Domain Name System) – система обозначений для сопоставления адресов IP и имен, понятных пользователю, используется в сети Internet. Система DNS иногда называется службой DNS.

Доступ (access) – операция, обеспечивающая запись, модификацию, чтение или передачу данных.

Драйвер (driver) – компонент операционной системы, взаимодействующий с внешним устройством или управляющий выполнением программ.

Драйвер устройства (device driver) – программа, которая обеспечивает взаимодействие между операционной системой и конкретными устройствами с целью ввода/вывода данных для этого устройства.

Единообразный локатор ресурсов (Uniform Resource Locator, URL) – идентификатор, или адрес ресурсов, в сети Internet. Обеспечивает гипертекстовые связи между документами WWW.

Жесткий диск (hard disk**)** – накопитель данных в вычислительных системах.

Заголовок кадра (frame preamble**)** – служебная информация Канального уровня модели OSI, добавляемая в начало кадра.

Запрос прерывания (IRQ – interrupt request) – сигнал, посылаемый центральному процессору от периферийного устройства. Сообщает о событии, обработка которого требует участие процессора.

Запросчик (requester, LAN requester) – (редиректор) программа, находящаяся на компьютере клиенте. Переадресует на соответствующий сервер запросы на сетевые услуги со стороны работающих на этом же компьютере приложений.

Затухание (attenuation) – ослабление сигнала при удалении его от точки испускания.

Звезда (star topology) – вид топологии, при котором каждый компьютер подключен к центральному компоненту, называемому концентратором.

Зеркальные диски (disk mirroring) – уровень 1 технологии RAID, при которой часть жесткого диска (или весь жесткий диск) дублируется на одном или нескольких жестких дисках. Позволяет создавать резервную копию данных.

Изображение (image**)** – графическая форма представления данных, предназначенная для зрительного восприятия.

Импульсно-кодовая модуляция – ИКМ **(**PCM – Pulse Code Modulation) – метод преобразования аналогового сигнала телефонии в дискретный сигнал.

Интернет – совокупность компьютеров, объединенных в глобальную сеть.

Информационная сеть (information network) – сеть, предназначенная для обработки, хранения и передачи данных.

Информационная система (information system) – объект, способный осуществлять хранение, обработку или передачу данных. К информационной системе относятся: компьютеры, программы, пользователи и другие составляющие, предназначенные для процесса обработки и передачи данных.

Информационно-поисковая система – (IRS – Information Retrieval System) – система, предназначенная для поиска информации в базе данных.

Информация (information) – совокупность фактов, явлений, событий, представляющих интерес, подлежащих регистрации и обработке.

Информация (information) – данные, обработанные адекватными им методами.

Инфракрасный канал (infrared channel) – канал, использующий для передачи данных инфракрасное излучение. Инфракрасный канал работает в диапазоне высоких частот, где сигналы мало подвержены электрическим помехам.

Кабель (cable) **—** один либо группа изолированных проводников, заключенных в герметическую оболочку.

Кадр (frame) – блок информации канального уровня.

Кадр данных (data frame) – базовая упаковка битов, которая представляет собой PDU (пакетный блок данных), посланный с одного компьютера на другой по сетевому носителю.

Канал (link) –среда или путь передачи данных.

Канал передачи данных (data channel) – кабели и инфраструктура сети.

Канальный уровень (Date link layer) –второй уровень модели OSI. Здесь из последовательности битов, поступающих от физического уровня, формируются кадры.

Клиент (client) – компьютер в сети, который запрашивает ресурсы или услуги от некоторых других компьютеров.

Клиент (client) – объект информационной сети, использующий сервис, предоставляемый другими объектами.

Клиент-сервер (client–server) – модель вычислений, при которой некоторые компьютеры запрашивают услуги (клиенты), а другие отвечают на такие запросы на услуги (сервер).

Коаксиальный кабель (coaxial cable) – кабель, состоящий из изолированных друг от друга внутреннего и внешнего проводников. Коаксиальный кабель имеет один либо несколько центральных медных проводников, покрытых диэлектрической изоляцией, которая для защиты центральных проводников от внешних электромагнитных воздействий покрыта металлической оплеткой (сеткой) либо трубкой.

Коаксиальный кабель (coaxial cable) – тип кабеля, который использует центральный проводник, обернутый изолирующим слоем, окруженный плетеной металлической сеткой и внешней оболочкой или экранирующим слоем.

Коллизия (collision) – ситуация, когда две рабочие станции пытаются одновременно занять канал (использовать рабочую среду – кабель).

Коммуникационная сеть – сеть, предназначенная для передачи данных, также она выполняет задачи, связанные с преобразованием данных.

Коммутатор (switch) – устройство или программа, осуществляющие выбор одного из возможных вариантов направления передачи данных.

Коммутаторы кадров – многопортовые мосты уровня доступа к среде передачи, работающие со скоростью этой среды и гарантирующие на порядок более высокую пропускную способность при связывании клиентских и серверных систем по сравнению с концентраторами для среды с разделяемым доступом. При сегментации ЛВС коммутаторы кадров обеспечивают лучшие показатели цена/производительность и меньшие задержки, чем традиционные связки мостов и маршрутизаторов.

Коммутаторы ячеек – устройства, реализующие ATM-коммутацию данных, разделенных на короткие ячейки фиксированного размера. Ориентация на установление соединений позволяют ATM обеспечивать классы (качество) обслуживания, пригодные для всех видов мультимедийного трафика, включая данные, голос и видео.

Концентратор или hub (concentrator or hub) – связующий компонент сети, к которому подключаются все компьютеры в сети топологии «Звезда». Концентратор обеспечивает связь компьютеров друг с другом при использовании витой пары, также используется в сетях FDDI для подключения компьютеров в центральном узле.

Концентратор MSAU (Multi Station Access Unit) – устройство для доступа к множеству станций, которое осуществляет маршрутизацию пакета к следующему узлу в сетях с метод доступа с передачей маркера.

Корпоративная сеть (enterprise network) – крупномасштабная сеть, обычно соединяющая многие локальные сети.

Лазерный принтер (laser printer) – принтер, в котором изображение символов печатаются лазерным лучом и переносятся на бумагу методом ксерографии.

Логический диск (logical disk) – часть физического диска, отформатированная под конкретную файловую систему и имеющая свое буквенное наименование.

Логический канал (logical channel) – путь, по которому данные передаются от одного порта к другому. Логический канал прокладывается в одном либо последовательности физических каналов и через уровни области взаимодействия.

Локальная группа (local group) – В Windows NT Server – учетная запись, определенная на конкретном компьютере. Включает учетные записи пользователей данного компьютера.

Локальная сеть (Local-Area Network) – сеть, системы которой расположены на небольшом расстоянии друг от друга.

Магистраль (backbone) – основной кабель, от которого кабели трансиверов идут к компьютерам, повторителям и мостам.

Манчестерское кодирование – схема передачи двоичных данных, применяемая во многих сетях. При передаче бита, равного 1, в течение временного интервала, который отведен для его передачи, значение сигнала меняется с положительного на отрицательное. При передаче бита равного 0, в течение временного интервала, который отведен для его передачи, значение сигнала меняется с отрицательного на положительное.

Маркер (token) – уникальная комбинация битов. Когда рабочая станция в ЛВС получает маркер, она имеет право начать передачу данных.

Маршрутизатор (router) – протокол – ориентированное устройство, соединяющее две сети, иногда с абсолютно разными уровнями MAC (канальный уровень, контроль доступа к среде).

Маршрутизация (routing) – процесс определения в коммуникационной сети пути, по которому блок данных может достигнуть адресата.

Маска сети (network mask) – 32-битовое число, по которому можно определить диапазон IP-адресов, находящихся в одной IP-сети/подсети.

Масштабируемость – это возможность увеличить вычислительную мощность Web-сайта или компьютерной системы (в частности выполнение большего числа операций или транзакций за определенный период времени) за счет установки большего числа процессоров или их замены на более мощные.

Мегабайт (megabyte) – 1 048 576 байтов (2^{20}).

Метод доступа – способ определения, какая рабочая станция сможет следующей использовать ЛВС. Кроме того, также называется набор правил, используемых сетевым оборудованием, чтобы направлять поток сообщений через сеть, а также один из основных признаков, по которым различают компоненты сетевого оборудования.

Метод доступа к каналу (channel access method) – правила, используемые для определения, какой компьютер может посылать данные по сети, тем самым предотвращающее потерю данных из-за коллизий.

Метод доступа – набор правил, обеспечивающих арбитраж доступа к среде передачи. Примерами методов доступа являются CSMA/CD (Ethernet) и передача маркера (Token Ring).

Метод множественного доступа с прослушиванием несущей и разрешением коллизий (CSMA/CD) – метод доступа к каналу связи, который устанавливает следующий порядок: если рабочая станция хочет воспользоваться сетью для передачи данных, она сначала должна проверить состояние канала, начинать передачу станция может, если канал свободен. В процессе передачи станция продолжает прослушивание сети для обнаружения возможных конфликтов. Если возникает конфликт, в случае, когда два узла попытаются занять канал, то обнаружившая конфликт интерфейсная плата, выдает в сеть специальный сигнал, и обе станции одновременно прекращают передачу.

Метод обработки запросов по приоритету – метод доступа к каналу связи, где всем узлам сети предоставляется право равного доступа. Концентратор опрашивает каждый порт и проверяет наличие запроса на передачу затем решает этот запрос в соответствии с приоритетом.

Метод с передачей маркера или полномочия (TPMA) – метод доступа к каналу связи, в котором от компьютера к компьютеру передается маркер, дающий разрешение на передачу сообщения. При получении маркера рабочая станция может передавать сообщение, присоединяя его к маркеру, который переносит его по сети. Каждая станция, находящаяся между передающей и принимающей «видит» это сообщение, но только станция-адресат принимает его. При этом она создает новый маркер.

Микроядро (microkernel) – центральная часть операционной системы , выполняющая основные функции управления системой.

Модем (modem) – сокращение от МОДулятор-ДЕМодулятор. Устройство связи, позволяющее компьютеру передавать данные по обычной телефонной линии. При передачи преобразует цифровые сигналы в аналоговые. При приеме преобразует аналоговые сигналы в цифровые.

Монитор сети (network monitor) – программно-аппаратное устройство, которое отслеживает сетевой трафик. Проверяет пакеты на уровне кадров, собирает информацию о типах пакетов и ошибках.

Мост (bridge) – это прибор, позволяющий рабочим станциям одной сети обращаться к рабочим станциям другой. Мосты используются для разделения ЛВС на маленькие сегменты. Выполняет соединение на канальном уровне модели OSI. Мост преобразует физический и канальный уровни различных типов. Используется для увеличения длины или количества узлов.

Мост - маршрутизатор (bridge-router) – сетевое устройство, которое объединяет лучшие функции моста и маршрутизатора.

Мультиплексор (multiplexor) – устройство, позволяющее разделить канал передачи на два или более подканала. Может быть реализован программно. Кроме того, используется для подключения нескольких линий связи к компьютеру.

Нейронная сеть (neural network) **–** сеть, образованная взаимодействующими друг с другом нервными клетками, либо моделирующими их поведение компонентами.

Несущая (carrier) **–** непрерывный сигнал, на который накладывается другой сигнал, несущий информацию.

Неэкранированная витая пара (UTP – Unshielded Twisted Pair) – кабель, в котором изолированная пара проводников скручена с небольшим числом витков на единицу длины. Скручивание проводов уменьшает электрические помехи извне при распространении сигналов по кабелю.

Оболочка (shell) **–** программное обеспечение, которое реализует взаимодействие пользователя с операционной системой (пользовательский интерфейс).

Обработка запросов по приоритету (demand priority) – высокоскоростной метод доступа к каналу, используемый сетями 100VG-Any LAN в топологии звезда.

Общий ресурс (shared resource) – любое устройство, данные или программа.

Одноранговая архитектура (peer-to-peer architecture) **–** концепция информационной сети, в которой каждая абонентская система может предоставлять и потреблять ресурсы.

Октет - байт.

Оперативная память (main memory) – память, предназначенная для хранения данных и команд, необходимых процессору для выполнения им операций.

Оптический кабель (optical cable) – кабель, передающий сигналы света. Для создания оптического кабеля используются световоды, каждый из которых имеет несколько слоев защитных покрытий, улучшающих механические и оптические характеристики этих световодов.

Оптический канал (optical channel) – канал, предназначенный для передачи сигналов света.

Оптоволокно (optical fiber) **–** среда, по которой цифровые данные передаются в виде модулированных световых импульсов.

Пакет – это единица информации, передаваемый между станциями сети. Используется на сетевом уровне модели OSI.

Пароль (password) – признак, подтверждающий право пользователя или прикладной программы на использование какого-нибудь ресурса.

Передача данных (data communications) – процесс транспортирования данных из одной системы в другую.

Повторитель или репитер (repeater) – устройство, усиливающее сигналы с одного отрезка кабеля и передающее их в другой отрезок без изменения содержания. Повторители увеличивают максимальную длину трассы ЛВС.

Полномочие (token) – специальный символ или группа символов, разрешающая системе передачу кадров.

Полоса пропускания (bandwidth) – разность между максимальной и минимальной частотой в заданном диапазоне; диапазон частот, на которых может работать носитель.

Пользователь (user) – юридическое либо физическое лицо, использующее какие-либо ресурсы, возможности.

Порт (port) **–** точка доступа к устройству либо программе. Различают физические и логические порты.

Провайдер (provider) – организация, которая обеспечивает подключение к Internet и другие услуги за определенную плату.

Протокол – набор правил, регламентирующих порядок сборки пакетов, содержащих данные и управляющую информацию, на рабочей станции-отправителе для передачи их по сети, а также порядок разборки пакетов по достижении ими рабочей станции-получателя.

Распределитель (hub) **–** центр ЛВС или кабельной системы с топологией звезда. В этой роли могут быть файл-серверы или концентраторы. Они содержат сетевое программное обеспечение и управляют коммуникациями внутри сети, а также могут работать как шлюзы к другим ЛВС.

Редиректор для ОС (redirector) – сетевое программное обеспечение, которое принимает запросы ввода/вывода для удаленных файлов, именованных каналов или почтовых слотов и затем переназначает их сетевым сервисам другого компьютера. Для Windows NT редиректоры выполнены как драйверы файловой системы.

Редиректор для протоколов (redirector) – компонент набора протоколов или сетевой операционной системы, ответственный за перехват запросов от приложений и распределение их между локальной или удаленной службами сети.

Реестр (registry) **–** архив БД Windows NT для хранения информации о конфигурации компьютера, включая аппаратные средства, установленное программное обеспечение, установки окружения и др.

Сеанс – сообщение, в котором предполагается создание логической связи для обмена сообщений. Сеанс должен быть сначала установлен, после этого происходит обмен сообщениями. После окончания обмена сеанс должен быть закрыт.

Сегмент (segment) – часть сети, ограниченная ретранслирующими устройствами (повторителями, мостами, маршрутизаторами и шлюзами).

Сервер – это компьютер сети, предоставляющий сервис другим объектам по их запросам.

Сервис – процесс обслуживания объектов.

Сетевая служба (network service) **–** вид сервиса, предоставляемого сетью

Сеть (network) – взаимодействующая совокупность сетевых узлов, связанных друг с другом каналами связи, предназначенная для передачи информации.

Слот адаптера (adapter slot) **–** гнездо, встроенное в материнскую плату.

Стандарт RS-232 – промышленный стандарт для последовательных соединений.

Телекоммуникация (telecommunication) **–** область деятельности, предметом которой являются методы и средства передачи информации.

Терминал (terminal) – устройство ввода/вывода данных и команд в систему или сеть.

Тестирование (testing) **–** процесс проверки правильности функционирования устройства либо программного обеспечения.

Технология RAID – используется для построения отказоустойчивости систем. Имеет пять уровней. 1 уровень **–** зеркализация дисков, 2 уровень **–** чередование дисков с записью кода коррекции ошибок, 3 уровень **–** код коррекции ошибок в виде четности, 4 уровень – чередование дисков блоками, 5 уровень – чередование с контролем четности.

Тип кадра (frame type) **–** один из четырех стандартов, которые определяют структуру пакета Ethernet: Ethernet 802.3, Ethernet 802.2, Ethernet SNAP или Ethernet II.

Транзакция – короткий во времени цикл взаимодействия объектов, включающий *запрос - выполнение задания – ответ*.

Трансивер – устройство, предназначенное осуществлять передачу данных с сетевых интерфейсных плат в физическую среду.

Трафик – поток данных.

Удаленная регистрация (remote logon) **–** подключение по сети к другому компьютеру пользователя, зарегистрированного на своем ПК по своей учетной записи.

Удаленный доступ (dial-up) **–** доступ к системе или по сети к другому компьютеру пользователя, зарегистрированного на своем ПК по своей учетной записи.

Удаленный доступ (remote access) **–** технология взаимодействия абонентских систем с локальными сетями через территориальные коммуникационные сети.

Утилита (utility) **–** программа, выполняющая какую-либо функцию сервиса.

Узел (node) **–** точка присоединения к сети; устройство, подключенное к сети.

Учетная запись (account) – информация, хранящаяся в базе данных Windows NT (учетная запись пользователя, компьютера, группы).

Факсимильная связь (facsimile) **–** процесс передачи через коммуникационную сеть неподвижных изображений и текста.

Физическая среда (physical media**) –** материальная субстанция, через которую осуществляется передача сигналов.

Фрагментация (fragmentation) – процесс разделения длинного пакета данных с более высокого уровня на последовательность более коротких пакетов на нижнем уровне.

Характеристический файл данных (characterization data file) **–** файл, содержащий информацию о конфигурационных возможностях конкретной модели принтера, включая поддерживающую разрешающую способность.

Центральный процессор (central processing unit) **–** управляющий и вычислительный модуль компьютера. Устройство, которое интерпретирует и выполняет команды.

Циклический избыточный код (CRC **–** Cyclical Redundancy Check) **–** число, получаемое в результате математических преобразований над пакетом данных и исходными данными. При доставке пакета вычисления повторяются. Если результат совпадает, то пакет принят без ошибок.

Цифровая линия (digital line) **–** линия связи, передающая информацию только в двоичной (цифровой) форме.

Цифровая сеть комплексных услуг (ISDN – Integrated Services Digital Network) **–** цифровая сеть связи, обеспечивающая коммутацию каналов и коммутацию пакетов.

Четность (parity) – способ контроля за безошибочной передачей блоков данных с помощью добавления контрольных битов.

Шина (bus) **–** специализированный набор параллельных линий в персональном компьютере.

Шина (bus) **–** канал передачи данных, отдельные части которого называются сегментами.

Широковещательная передача (broadcast) – технология передачи сигналов, таких как сетевые данные, посредством использования передатчика какого-либо типа для посылки этих сигналов по коммуникационному носителю.

Шифрование (encryption) **–** преобразование информации для ее защиты от несанкционированного доступа.

Шлюз (gateway) **–** устройство, посредством которого соединяются сети разных архитектур.

Экран (shielding) **–** металлическая оплетка или цилиндр, навитый из фольги. Защищает передаваемые данные, уменьшая внешние электрические помехи, которые называются шумом.

Экранированная витая пара (Shielded Twisted-Pair, STP) **–** витая пара, окруженная заземленной металлической оплеткой, которая служит экраном.

Электронная почта (email) **–** компьютерная система обмена сообщениями, где текст и файлы могут быть посланы от одного пользователя к одному или многим другим пользователям в той же сети.

Эталонная модель взаимодействия открытых систем (OSI – Open System Interconnection) **–** семиуровневая модель, которая стандартизирует уровни услуг и виды взаимодействия между системами в информационной сети при передаче данных.

Эфир (ether) **–** пространство, через которое распространяются волны электромагнитного спектра и прокладываются каналы радиосетей и инфракрасных сетей. Электромагнитное поле не нуждается в специальном носителе.

Язык HTML – инструментальное программное обеспечение, использующее технологию гипертекста.

Язык описания страниц (page description language) **–** язык программирования, который описывает вид страницы для печати. Используется для компоновки изображения страницы.

Язык структурированных запросов (SQL – Structured Query Language) **–** язык управления базами данных, используемый для запроса, обновления и управления реляционными базами данных.

Ячеистая топология сети (mesh network topology) – топология, используемая в глобальных вычислительных сетях. К любому узлу существует несколько маршрутов.

Английские термины:

Access – доступ.

Access auditing – контроль доступа.

Adapter – адаптер, устройство согласования параметров входных и выходных сигналов в целях сопряжения.

Address – адрес, закодированное обозначение пункта отправления либо назначения данных.

Addressing – адресация, способ указания объектов в сети либо в системе.

Administration – администрирование, управление сетью.

Analog network – аналоговая сеть, передающая и обрабатывающая аналоговые сигналы.

Analog signal – аналоговый сигнал, величина которого непрерывно изменяется во времени.

Analog-to-digital conversion – аналого-дискретное преобразование, процесс преобразования аналогового сигнала в дискретный.

Animation – анимация, виртуальная реальность, мнимый мир, создаваемый аудиовидиосистемой в воображении пользователя.

Application layer – прикладной уровень модели OSI, обеспечивающий прикладным процессам средства доступа к области взаимодействия.

Archivator – архиватор, программа, обеспечивающая сжатие данных.

Arithmetic and logical unit (ALU) **–** арифметико-логическое устройство, часть процессора, выполняющая арифметические и логические операции над данными

Asynchronous Transfer Mode (ATM) **–** асинхронный способ передачи данных, пакетно-ориентированный метод скоростной передачи.

Banyan network – баньяновая сеть, скоростная распределительная сеть с каскадной адресацией.

Baud – бод, единица скорости передачи данных. Число бод равно количеству изменений сигнала (потенциала, фазы, частоты), происходящих в секунду. Для двоичных сигналов, нередко, считают, что бод равен биту в секунду, например 1200 бод = 1200 бит/с.

Binary code – двоичный код, алфавит кода ограничен двумя символами (0, +1).

Bipolar code – биполярный код. Алфавит кода ограничен тремя символами (-1, 0, +1), где единицы представляются чередующимися импульсами. Отсутствие импульсов определяет состояние нуля.

Bit – бит, наименьшая единица информации в двоичной системе счисления.

Bridge – мост, сетевое оборудование для преобразования физического и канального уровней различных типов.

Broadband channel – широкополосный канал.

Broadcasting – широковещание.

Bus – шина.

Byte – байт, единица количества информации, равная восьми битам.

Cable – кабель, длинномерное изделие для передачи сигналов.

Cache memory – кэш-память, буферное запоминающее устройство, работающее со скоростью, обеспечивающей функционирование процессора без режимов ожидания.

Carrier – несущая, непрерывный сигнал, на который накладывается другой сигнал, дающий информацию.

Cellular packet radio network – сотовая пакетная радиосеть.

Channel – канал, среда или путь, по которому передаются данные.

Circuit switching – коммутация каналов, предоставление последовательности каналов сети для монопольного использования при передачи данных во время сеанса.

Client – клиент, объект использующий сервис, предоставляемый другими объектами.

Client-server architecture – архитектура клиент-сервер.

Clock rate – тактовая частота.

Closed channel – закрытый канал.

Coaxial cable – коаксиальный кабель, использующий центральный проводник, обернутый экранирующим слоем.

Communication network – коммуникационная сеть, предназначенная для передачи данных, также она выполняет задачи, связанные с преобразованием данных.

Compiler – компилятор, программа–транслятор преобразующая код в язык машинных команд (исполняемый файл).

Concentrator – концентратор, устройство, у которого суммарная пропускная способность входных каналов выше пропускной способности выходного канала.

Confidention – конфиденциальность, доверительность, секретность.

Conformance – конформность, соответствие объекта его нормативно-технической документации. Конформность объекта определяется в результате процесса его тестирования.

Connection – соединение.

Console – консоль, одна либо несколько абонентских систем для работы с платформой управления сетью.

Data link layer – канальный уровень, уровень модели OSI, отвечающий за формирование и передачу блоков данных и обеспечивающий доступ к каналу связи области взаимодействия.

Data management – управление данными.

Data processing – обработка данных.

Data protection – защита данных.

Data security – безопасность данных.

Data security architecture – архитектура безопасности данных, архитектура, определяющая методы и средства защиты данных.

Data transfer – пересылка данных.

Data unit – блок данных.

Databank – банк данных.

Database – база данных**.**

Database management system (DBMS) **–** система управления базой данных (СУБД).

Database server – сервер базы данных.

Datagram – дейтаграмма, сообщение, которое не требует подтверждения о приеме от принимающей стороны.

Decoding – декодирование.

Dedicated channel – выделенный канал.

Designator – распределитель.

Determinate access - детерминированный доступ, множественный доступ**.**

Device – устройство.

Diagnostic – диагностика.

Dialog – диалог.

Digital network – дискретная сеть.

Digital signal – цифровой сигнал, дискретный сигнал.

Digit-to-analog conversion – дискретно-аналоговое преобразование, процесс преобразования дискретного сигнала в аналоговый.

Direct Memory Access (DMA) **–** прямой доступ к памяти.

Directory – каталог.

Directory network service – сетевая служба каталогов.

DirectX – набор драйверов, образующий интерфейс между программами в среде Windows и аппаратными средствами.

DirectDraw – часть набора драйверов DirectX, поддерживающих непосредственную работу с видеокартой и позволяющих, например, прямую запись в видеопамять.

Disk – диск.

Disk drive – дисковод.

Disk Operating System (DOS) - дисковая операционная система (ДОС)**.**

Diskette – дискета.

Display – дисплей.

Distance learning – дистанционное обучение, технология обучения с помощью средств информационной сети.

Domain – домен, группа компьютеров, находящаяся в одном месте (здании, этаже, организации) и управляемая СОС.

Driver - компонент операционной системы, взаимодействующий с устройством либо управляющий выполнением программ.

Duplex channel - дуплексный канал, осуществляет передачу данных в обоих направлениях.

Electronic mail – электронная почта, средства передачи сообщений между пользователями в сети.

Emulation – эмуляция, организация структуры одного объекта, при которой его функционирование неотличимо от другого объекта.

Encryption – шифрование, способ изменения данных с целью засекречивания.

Enterprise network – корпоративная сеть, локальная сеть большого предприятия.

Ether – эфир, пространство, через которое распространяются волны электромагнитного спектра и прокладываются каналы, радиосетей и инфракрасных сетей.

Ethernet network –сеть Ethernet, тип локальной сети, предложенный корпорацией Xerox.

Explorer – программа – броузер для просмотра Web-страниц.

External device – внешнее устройство.

External memory – внешняя память, непосредственно не доступная процессору.

Facsimile – факсимильная связь, процесс передачи через коммуникационную сеть неподвижных изображений и текста.

Fast Ethernet – сеть Fast Ethernet, тип скоростной сети Ethernet со скоростью передачи данных 100 Мбит/с.

Fiber Channel network –сеть Fiber Channel, тип скоростной локальной сети, основанной на использовании оптических каналов.

Fiber Distributed Data Interface (FDDI) **–** оптоволоконный распределенный интерфейс данных.

Fiber-optic link - волоконно-оптическая линия связи.

File – файл.

Flash memory – флэш-память, память на основе полупроводниковой технологии.

Floppy disk – гибкий диск.

Folder – пиктограмма.

Font – шрифт.

Frame – кадр.

Frame relay – ретрансляция кадров.

Frequency band – полоса частот.

Frequency Division Multiple Access (FDMA) **–** множественный доступ с разделением частоты.

Frequency modulation – частотная модуляция.

Functional profile – функциональный профиль.

Gateway – шлюз.

Global network – глобальная сеть.

Gopher – интерактивная оболочка для поиска, присоединения и использования ресурсов и возможностей Internet. Интерфейс с пользователем осуществлен через систему меню.

Graphic interface – графический интерфейс.

Hacker – хакер.

Hard disk – жесткий диск.

Hardware – техническое обеспечение.

Hardware Description Language (HDL) **–** язык описания технических средств.

Hardware platform – аппаратная платформа.

Heterogeneous network – гетерогенная сеть, сеть в которой работают системы различных фирм производителей.

Hierarchical addressing – иерархическая адресация, адресация при которой адреса объединяют в группы, отражая их взаимосвязь.

High-level language – язык высокого уровня.

Host computer – главный компьютер в архитектуре терминал-главный компьютер.

Hypermedia – гиперсреда.

Hypertext – гипертекст.

Hypertext Markup Language (HTML) **–** гипертекстовый язык разметки.

Hypertext Transfer Protocol (HTTP) **–** гипертекстовый протокол передачи.

Identification – идентификация.

Image – изображение.

Index – индекс.

Information – информация.

Information network – информационная сеть.

Infrared channel – инфракрасный канал.

Infrared network – инфракрасная сеть.

Infrared radiation – инфракрасное излучение.

Infrastructure – инфраструктура.

Input/output device – устройство ввода/вывода.

Input/output interface – интерфейс ввода/вывода.

Integrated Services Digital Network (ISDN) **–** цифровая сеть с интегральным обслуживанием.

Intelligent Hub – интеллектуальный концентратор. Интеллект концентраторов состоит в том, что они могут выполнять операции мониторинга и управления сетью.

Interconnection area – область взаимодействия.

Interface – интерфейс.

Internet network – сеть Internet.

Interpreter – интерпретатор, программа, анализирующая построчно команды или операторы программы и непосредственно выполняющая их.

Java language – язык Java, объектно-ориентированной архитектуры, предложенный корпорацией SUN Microsystems

Java Script language – язык JavaScript.

Jet-printer – струйный принтер.

Job – задание.

Key – ключ.

Keyboard – клавиатура.

Knowledge base – база знаний (БЗ).

Laser printer – лазерный принтер.

Light guide – световод.

Link Access Procedure (LAP) **–** процедура доступа к каналу.

Loader – загрузчик, программа, выполняющая функции загрузки объектного модуля в операционную память и динамического формирования загрузочного модуля.

Local-area network (LAN) **–** локальная сеть.

Locking – блокировка.

Logical address – логический адрес, символический условный адрес объекта**.**

Logical channel – логический канал.

Low-level language – язык низкого уровня.

Machine language – машинный язык.

Macro instruction – макрокоманда.

Manageable Hub - управляемый концентратор. Еще одно название для интеллектуальных хабов. Каждый порт управляемого концентратора можно независимо конфигурировать, включать или выключать, а также организовать его мониторинг.

Manager – администратор.

Manchester coding - манчестерское кодирование.

Matrix printer – матричный принтер.

Message – сообщение, единица данных на прикладном уровне.

Mirroring – зеркализация.

Modular hub - модульный концентратор. В основе модульного хаба лежит шасси, в которое помещаются специальные платы или модули. Каждый из модулей функционирует подобно автономному концентратору, а модули взаимодействуют друг с другом через шину шасси.

Narrowband channel – узкополосный канал.

Navigator – навигатор.

NetWare network – сеть NetWare.

Network – сеть.

Network analyzer – анализатор сети.

Network Basic Input/Output System (NetBIOS) **–** сетевая базовая система ввода/вывода.

Network layer – сетевой уровень.

Network management – управление сетью.
Network Operating System (NOS) **–** сетевая операционная система (СОС).
Network printer – сетевой принтер.
Network service – сетевая служба.
Neural network – нейронная сеть.
Notebook personal computer – блокнотный персональный компьютер**.**
Object – объект.
Object Linking and Embedding technology (OLE) **–** технология связи и компоновки объектов
Object-oriented architecture – объектно-ориентированная архитектура**.**
Object-Oriented Database (OODB) - объектно-ориентированная база данных.
Optical fiber – оптическое волокно.
Optical disk – оптический диск.
Packet – пакет, единица данных на сетевом уровне.
Packet switching – коммутация пакетов.
Paging device – пейджер**,** устройство радиовызова.
Parity – четность.
Pascal language - язык Pascal.
Password – пароль.
PCI bus - шина PCI.
Peer-to-peer architecture - одноранговая архитектура.
Permission – разрешение.
Physical address – физический адрес.
Physical interconnection facility – физические средства соединения.
Physical layer – физический уровень.
Physical link – физический канал.
Physical medium – физическая среда.
Ping – утилита проверки связи с удаленной ЭВМ.
Postscript language - язык описания документов, в том числе изображений.
Presentation layer - представительский уровень**.**
Printer – принтер.
Protocol – протокол.
Quantization – квантование, разбиение диапазона значений аналогового сигнала на конечное число интервалов (квант).
Quantum – квант.
Radio channel – радиоканал.
Radio local-area network – локальная радиосеть.
Radio network – радиосеть.
Raster – растр, форма представления изображения в виде элементов, упорядоченных в строки и столбцы.
Raster image – растровое изображение, формируется построчно из отдельных точек различной степени яркости и различного цвета.
Real-time system – система реального времени. Системы, функционирование которых зависит не только от логической корректности вычислений, но и от времени, за которое эти вычисления производятся.
Record – запись.
Redirector – редиректор.
Relational database (RDB) **–** реляционная база данных.
Relay system - ретрансляционная система**.**
Remote access – удаленный доступ.
Repeater – повторитель.
Repeater – повторитель. Репитер.
Resource – ресурс.
Resource sharing – совместное использование ресурса.
Ribbon cable – плоский кабель.
Rout – маршрут, путь.
Scanner – сканер.
Screen – экран.
Semantics – семантика.
Serial interface – последовательный интерфейс.
Server – сервер.
Service – сервис.
Session – сеанс.
Session layer – сеансовый уровень.
Sharing (разделение) **–** совместное использование.
Shell – командный процессор. Оболочка.
Simulation – моделирование.
Software - программное обеспечение.
Sound board – звуковая плата.
Speech recognition - распознавание речи.
Stackable hub – стековый хаб. Стековые хабы действуют как автономные устройства с единственным отличием, они позволяют организовать стек - группу концентраторов, работающих как одно логическое устройство. С точки зрения сети стек

концентраторов является одним хабом.

Stand-alone – автономный.

Stand-alone hub - автономный хаб. Устройство с несколькими (обычно от 4 до 32) портами, способное функционировать независимо. Обычно автономные концентраторы поддерживают способ наращивания числа портов.

Switch – коммутатор.

Synchronizing – синхронизация.

Syntax – синтаксис.

Talk – одна из прикладных программ сети Internet. Дает возможность открытия разговора с пользователем удаленной ЭВМ.

Telecommunications – телекоммуникации.

Telefax – факс-аппарат.

Telephone mail – электронная почта.

Telephone network – телефонная сеть.

Telnet – удаленный доступ. Дает возможность абоненту работать на любой ЭВМ сети Internet как на своей собственной.

Testing – тестирование.

Time sharing - разделение времени.

Timer – таймер.

Token – полномочие.

Topology – топология.

Traffic – трафик.

Transaction – трансакция, короткий во времени цикл взаимодействия объектов, включающий *запрос-выполнение задания-ответ*.

Translator – транслятор, программа, преобразующая программу, написанную на одном языке, в программу представленную на другом языке.

Transparency – прозрачность, объект считается прозрачным для пользователя либо программы в том случае, когда они, работая через (сквозь) объект, не видят его.

Transport layer (транспортный уровень) **–** уровень, на котором пакеты передаются через коммуникационную сеть.

Three-dimensional image (трехмерное изображение) **–** изображение объемного предмета, выполненное на плоскости.

Unauthorized access – несанкционированный доступ.

Uninterruptible Power Supply (UPS) – источник бесперебойного питания.

Unique address – уникальный адрес.

Unipolar code – униполярный код.

Universal CODE (UNICODE) - универсальный код, стандарт 16-разрядного кодирования символов. Код идет на смену использовавшимся до сих пор 7-8-битовым обозначениям.

UNIX operating system (операционная система) UNIX – Сетевая Операционная Система (СОС), созданная фирмой Bell Laboratory.

User – пользователь, юридическое либо физическое лицо, использующее какие-либо ресурсы, возможности.

User interface – интерфейс пользователя.

Utility – утилита, программа, выполняющая какую-либо функцию сервиса.

Vector image – векторное изображение, характеризуется большим числом отрезков коротких прямых, каждый из которых имеет определенное направление, цвет и координаты точки.

Verification – верификация, процедура проведения анализа с целью установления подлинности, проверки истинности.

Video board – видео плата, одноплатный контроллер, вставляемых в компьютер, которые в режиме реального времени осуществляют аналого-дискретное преобразование в потоки дискретных сигналов.

Video bus – видео шина, предназначенная, в первую очередь, для передачи изображений.

Video conferencing – видеоконференция, методология проведения совещаний и дискуссий между группами удаленных пользователей с использованием движущихся изображений.

Viewer – визуализатор, программа просмотра документов на экране.

Virtual reality (виртуальная реальность) **–** мнимый мир, создаваемый аудио видеосистемой в воображении.

Wavequide – волновод.

Webster – сетевая версия толкового словаря английского языка.

Whois – адресная книга сети Internet.

Английские сокращения:

ACF (Advanced Communications Function) **–** дополнительная коммуникационная функция.

ACP (ANSI Code Page) **–** кодовая страница ANSI.

ACPI (Advanced Configuration and Power Interface) **–** современный интерфейс конфигурирования и управления энергопотреблением.

ACS (Advanced Connectivity System) **–** дополнительные системы связи.

ADC (Analog Digital Converter) **–** аналогово-цифровой преобразователь (АЦП). Предназначен для преобразования аналогового сигнала в цифровой.

AFP (Apple Talk File Protocol) **–** Файловый протокол Apple Talk). Протокол удаленного управления файлами Macintosh.

ANR (Automatic Network Routing) **–** автоматическая сетевая маршрутизация.

ANSI (American National Standards Institute) **–** американский институт национальных стандартов.

API (Application Programming Interface) **–** интерфейс прикладных программ. Набор процедур, которые вызываются прикладной программой для осуществления низкоуровневых операций, исполняемых операционной системой.

APPC (Advanced Program-to Program Communication) **–** высокоуровневый протокол для взаимодействия программ.

APPN (Advanced Program-to Program Communication) **–** высокоуровневый протокол для взаимодействия программ.

ARP (Address Resolution Protocol) – протокол разрешения адреса.

ASCII (American Standard Code for Information Interchange) – американский стандартный код для обмена информацией.

ASCII (American Standard Code for Information Interchange) – американский стандартный код для информационного обмена.

ASMP (ASymmetric Multi Processing) – асимметричная мультипроцессорная обработка.

ASP (Active Server Page) – технология, позволяющая создавать динамические Web-приложения.

AT (Advanced Technology) – усовершенствованная технология.

ATandT (American Telephone and Telegraph) – американский телефон и телеграф.

ATM (Asynchronous Transfer Mode) – асинхронной режим передачи. Тип коммутационной технологии, при котором по сети передаются небольшие ячейки фиксированного размера.

ATP (Apple Talk Protocol) – транзакционный сеансовый протокол Apple Talk.

AUI (Attachment Unit Interface) – интерфейс подключаемого модуля. Интерфейс для подключения внешнего трансивера, установленного на магистральном коаксиальном кабеле.

BASE – сокращение BASEband, основная полоса канала.

BASIC (Beginning All-purpose Symbolic Instruction Code) – система символического кодирования для начинающих.

BBS (Broadcast Bulletin System) – широковещательная система объявлений. Электронная доска объявлений, компьютерный аналог доски объявлений.

BDC (Backup Domain Controller) – вторичный контроллер домена.

BIOS (Basic Input/Output System) – базовая система ввода/вывода.

B-ISDN (Broadband-Integrated Services Digital Network) – широкополосная цифровая сеть с интегральным обслуживанием.

BNS (Broadband Network Service) – широкополосный сетевой сервис.

B-WIN (Broadband-Wissenchafts Nets) – широкополосная исследовательская сеть.

CAS (Column Address Strobe) – строб адреса столбца, сигнал, используемый при работе с динамической памятью.

CASE (Computer-Aided Software Engineering) – компьютерная разработка программного обеспечения.

CDPD (Cellular Digital Packet Date) – Сотовые дискретные пакетные данные, сотовая пакетная радиосеть.

CD-ROM (Compact Disk Read Only Memory) – компакт-диск с памятью только для чтения.

CGI (Common Gateway Interface) – общий интерфейс шлюза.

CGM (Computer Graphics Metafile) – метафайл компьютерной графики

CLNP (Connection Less Network Protocol) – сетевой протокол без организации соединений.

CMIP (Common Management Information Protocol) – общий протокол управления информацией.

CPI (Common Programming Interface) – общий программный интерфейс.

CPU (Central Processing Unit) – центральное процессорное устройство.

CRC (Cycle Redundancy Check) – контроль цикличной избыточности.

CSMA/CD (Carrier Sense Multiple Access with Collision Detection) – Множественный доступ с прослушиванием несущей и разрешением коллизий.

CWIS (Campus Wide Information System) – глобальная информационная система.

DAS (Double Attached Station) – станция сети FDDI с двойным подключением к магистральному кольцу или концентратор.

DBMS (DataBase Management System) – Система управления БД (СУБД).

DDC (Display Data Channel) – интерфейс обмена данными между компьютером и монитором.

DDE (Dynamic Date Exchange) – Динамический обмен данными.

DDP (Delivery Protocol – Протокол доставки дейтаграмм). Протокол передачи данных Apple, используемый в Apple Talk.

Demand packet – специальный пакет, посылаемый компьютером в сети 100VG-AnyLAN, информирующий управляющий концентратор о том, что у компьютера есть данные для отправки.

DHCP (Dynamic Host Configuration Protocol) – протокол динамической конфигурации хоста.

DLC (Dada Link Control) – протокол управления каналом передачи данных.

DLL (Dynamic Linked Library) – динамическая библиотека.

DMA (Direct Memory Access) – прямой доступ к памяти.

DNS (Domain Name System) – доменная система имен.

DRAM (Dynamic Random Access Memory) – динамическая память прямого доступа, память, схемотехнически выполненная в виде двумерной матрицы (строки и столбцы) конденсаторов.

SDH (Synchronous Digital Hierarchy) –синхронная дискретная иерархия. Европейский стандарт на использование оптических кабелей в качестве физической среды для скоростных сетей передачи на большие расстояния.

DVI (Digital Video Interactive) – система аппаратного сжатия движущихся видеоизображений.

DVD (Digital Versatile Disk) – цифровой универсальный диск, самый современный стандарт хранения информации на оптическом (лазерном) диске.

EBCDIC (Extended Binary Coded Decimal Interchange Code) – схема кодировки IBM. Используется мэйнфреймами и ПК.

ECC (Error Correction Code) – код коррекции ошибок.

EISA (Enhanced Industry Standard Architecture) – 32-разрядная архитектура системной шины для ПК на базе процессора Intel.

Ethernet – сетевая технология, подчиняется спецификации 802.3 IEEE.

FAG (Frequently Asked Questions) – часто задаваемые вопросы.

FDDI (Fiber Distributed Date Interface Station) – распределенный интерфейс передачи данных по волоконно-оптическому кабелю. Технология ЛВС, использующая скорость передачи 100 Мбит/с.

FDMA (Frequency Division Multiple Access) – множественный доступ с разделением частоты.

FDSE (Full Duplex Switched Ethernet) – полнодуплексная коммутируемая сеть Ethernet.

FTAM (File Transfer, Access, and Management) – протокол передачи, доступа и управления файлами.

FTP (File Transfer Protocol) – протокол передачи файлов. Позволяет обмениваться файлами по сети.

GDI (Graphics Device Interface) – интерфейс графического устройства.

GIF (Graphics Interchange Format) – файлы растровых изображений, в которых используется не более 256 индексированных цветов.

GUI (Graphics User Interface) – графический интерфейс пользователя.

HAL (Hardware Abstraction Layer) – уровень аппаратных абстракций.

HDL (Hardware Description Language) – язык описания технических средств.

HDLC (High Level Data Link Control) – протокол управления каналом передачи данных высокого уровня.

HP (Hewlett Packard) – Хьюлитт Паккард (корпорация HP).

HTML (Hyper Text Markup Language,) – язык гипертекстовой разметки.

HTTP (Hyper Text Transfer Protocol) – протокол передачи гипертекста.

IBM (International Business Machines) – международные бизнес-машины.

ICMP (Internet Control Message Protocol) – протокол управления сообщениями Интернета.

IDE (Integrated Device Electronic) – интерфейс жестких дисков.

IEEE (Institute of Electrical and Electronics Engineers) – институт инженеров по электротехнике и электроники.

IIS (Internet Information Server) – компонент Microsoft Back Office, который действует как Web-сервер в среде Windows NT.

IMAP (Internet Message Access Protocol) – протокол доступа к электронной почте. Разработан на смену SMTP.

IP (Internet Protocol) – протокол Internet, сетевой протокол стека TCP/IP, который предоставляет адресную и маршрутную информацию.

IPX (Internetwork Packet Exchange) – протокол межсетевого обмена пакетами, предназначенный для адресации и маршрутизации пакетов в сетях Novell.

IRQ (Interrupt Request) – запрос на прерывание.

ISA (Industry Standard Architecture) – системная шины IBM PC/IT. Позволяет подключить к системе различные адаптеры, установив дополнительную плату в гнездо расширения.

ISAPI (Microsoft API) – интерфейсы прикладного программирования фирмы Microsoft.

ISDN (Integrated Services Digital Network) – цифровая сеть с интеграцией услуг.

ISO (International Standard Organization) – организация стандартизации различных стран.

JPEG (Joint Photographic Expert Group) – файлы растровых изображений, в которых используется не более 16,7 млн. цветов (24-битовый цвет).

JTM (Job Transfer and Manipulation) – сетевая служба передача и управление заданиями.

LAN (Local-Area Network) – локальная сеть.

LAP (Link Access Procedure) – процедура доступа к каналу.

LAT (Local-Area Transport) – немаршрутизируемый протокол фирмы Digital Equipment Corporation.

LLC (Logical Link Control) – логический контроль связи.

MAC (Media Assess Control) – контроль доступа к среде.

MAPI (Messaging Application Program Interface) – интерфейс прикладных программ обработки сообщений.

MCA (Micro Channel Architecture) – 32-битная системная шина в ПК IBM PS/2.

MIB (Management Information Base) – базы управляющей информации.

MNP (Microcom Network Protocol) – серия стандартов, предназначенная для сжатия информации и исправления ошибок при асинхронной передачи данных по телефонным линиям.

NBP (Name Binding Protocol) – транспортный протокол связывания имен Apple Talk.

NCP (NetWare Core Protocol) – базовый протокол сетей NetWare.

NDIS (Network Device Interface Specification) – спецификация интерфейса сетевого устройства, программный интерфейс, обеспечивающий взаимодействие между драйверами транспортных протоколов и соответствующими драйверами сетевых интерфейсов. Позволяет использовать несколько протоколов даже если установлена только одна сетевая карта.

NetBEUI (NetBIOS Extended User Interface) – протокол ЛВС, поддерживаемый всеми СОС фирмы Microsoft, обеспечивает транспортные услуги для NetBIOS.

NetBIOS (Network Basis Input/Output System) – интерфейс прикладных программ, для ЛВС**.** Устанавливает соединение между компьютерами.

NFS (Network File System) – сетевая файловая система.

NIS (Network Information System) – сетевая информационная система. NIS обеспечивает способ доступа к данным, благодаря которому все узлы сети могут использовать единую БД, содержащую все учетные записи пользователей сети и имена всех сетевых узлов.

NLM (NetWare Loadable Module) – загружаемый модуль NetWare.

NLSP (NetWare Link Service Protocol) – протокол канального сервиса NetWare.

NOS (Network Operating System) – сетевая операционная система.

NRZ (Non-Return to Zero) – без возврата к нулю. Метод двоичного кодирования информации, при котором единичные биты представляются положительным значением, а нулевые отрицательным.

NSAPI (Netscape API) – интерфейсы прикладного программирования фирмы Netscape.

ODBC (Open Database Connectivity) – открытый доступ к базам данных.

OLE (Object Linking and Embedding) – связь и внедрение объектов.

OME (Open Messaging Environment) – среда открытых сообщений.

OSA (Open Scripting Architecture) – архитектура открытых сценариев.

OSPM (Operating System Directed Power Management) – непосредственное управление энергопотреблением операционной системой.

OSI (Open System Interconnection) – взаимодействие открытых систем.

PCI (Peripheral Component Interconnect) – соединение внешних устройств, шина PCI.

PDC (Primary Domain Controller) – первичный контролер доменов, ПК под управлением Windows NT Server, на котором хранятся БД учетных записей домена.

PnP (Plug-and-Play) – технология само настраиваемого оборудования.

PPP (Point to Point Protocol) – протокол «точка-точка». Протокол, предназначенный для работы на двухточечной линии (линии, соединяющей два устройства). Протокол канального уровня.

PTM (Packet Transfer Mode) – пакетный способ передачи.

RAID (Redundant Arrays of Inexpensive) – избыточный массив недорогих дисков.

RAM (Random Access Mammary) – память с произвольным доступом.

RARP (Reverse Address Resolution Protocol) – реверсивный протокол разрешения адреса.

RFS (Remote File System) – удалённая файловая система.

RIP (Routing Internet Protocol) –протокол взаимодействия маршрутизаторов в сети.

RPC (Remote Procedure Call) – вызов удаленных процедур.

RTOS (Real-Time Operating System) – операционная система реального времени.

RTP (Real-time Transport Protocol) – транспортный протокол передачи в реальном времени.

SAP (Service Access Point) – точка доступа к службе. Точка, в которой услуга какого-либо уровня OSI становиться доступной ближайшему вышележащему уровню. Точки доступа именуются в соответствии с уровнями, обеспечивающими сервис.

SAS (Single Attached Station) – станция сети FDDI с одинарным подключением.

SDLC (Synchronous Data Link Control) – протокол синхронной передачи данных.

SDN (Software-Defined Network) – сеть, определяемая программным обеспечением - Виртуальная сеть.

SID (Security Identification) – идентификатор безопасности.

SLIP (Serial Line IP) – IP для последовательных линий. Протокол последовательной посимвольной передачи данных. Позволяет компьютеру использовать IP (и, таким образом, становиться полноправным членом сети), осуществляя связь с миром через стандартные телефонные линии и модемы, а также непосредственно через RS-232 интерфейс.

SMTP (Simple Mail Transfer Protocol) – простой протокол электронной почты.

SNA (System Network Architecture) – архитектура систем связи, предназначенная для обмена данными между ПК различных типов.

SNMP (Simple Network Management Protocol) – простой протокол сетевого управления. Протокол сетевого администрирования SNMP очень широко используется в настоящее время. Управление сетью входит в стек протоколов TCP/IP.

SONET (Synchronous Optical Network) – синхронная оптическая сеть.

SPX (Sequenced Packet Exchange) – протокол, который осуществляет передачу сообщений с установлением соединений в сетях Novell.

SQL (Structured Query Language) – язык структурированных запросов.

SSL (Secure Socket Layer) – протокол, который обеспечивает секретный обмен сообщениями для протоколов прикладного уровня стека TCP/IP.

STP (Spanning Tree Protocol) – протокол связывающего (остового) дерева.

TCP (Transmission Control Protocol) – протокол управления передачей.

TDI – (Transport Driver Interface) – интерфейс транспортного драйвера.

TDMA (Time Division Multiple Access) – множественный доступ с разделением во времени.

TFTP (Trivial File Transfer Protocol) – простейший протокол передачи файлов.

TIFF (Tagged Image Format File) – спецификация формата файла изображения.

TLI (Transport Level Interface) – интерфейс транспортного уровня.

TP4 (Transmission Protocol) – протокол передачи класса 4.

TPMA (Token Passing Multiple Access) – множественный доступ с передачей полномочия или метод с передачей маркера.

UDP (User Datagram Protocol) – пользовательский протокол дейтаграмм.

UNI (User-to-Network Interface) – сетевой интерфейс пользователя. Набор правил, определяющий взаимодействие оконечного оборудования и сети ATM с физической и информационной точек зрения.

UNS (Universal Name Convention) – стандартный метод именования в сети, имеющий вид \\сервер\общий_ресурс.

UPS (Uninterruptible Power Supply) – источник бесперебойного питания.

URL (Uniform Resource Locator) – адрес универсального указателя ресурсов.

UTP (Unsealing Twist Pare) – неэкранированная витая пара.

UUCP (Unix-to-Unix Copy Protocol) – протокол копирования от Unix к Unix.

VESA (Video Electronics Standard Association) – ассоциация стандартов электронной графики.

VGA (Video Graphics Array) – видеографическая матрица.

VHDL (Very High-speed integrated circuit Hardware Description Language) – язык описания технических средств сверхскоростных интегральных схем.

WAIS (Wide Area Information Server) – протокол глобального информационного сервера.

WDMA (Wavelength Division Multiple Access) – множественный доступ с разделением длины волны.

WINS (Windows Internet Name Service) – сетевая служба Windows, используемая для определения IP-адреса по имени NetBIOS.

WWW (Word Wide Web) – всемирная паутина.

X.25 – международный стандарт для глобальных коммуникаций с коммутацией пакетов.