Министерство образования и науки Республики Казахстан

Павлодарский государственный университет им. С. Торайгырова

Кафедра Вычислительная техника и программирование

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к курсовой работе

по дисциплине Компьютерные системы

для студентов специальности 050704 Вычислительная техника и программное обеспечение

Павлодар

Лист
утверждения к
методическим
указаниям

Форма
Ф СО ПГУ
7.18.1/05

УТВЕРЖДАЮ
Декан факультета ФМиИТ
_____ Ж.К. Нурбекова
«___»_____ 2010 г.

Составитель: ст. преподаватель _____Балгабаева Г.С.

Кафедра Вычислительная техника и программирование

Методические указания

к курсовой работе

по дисциплине Компьютерные сети

для студентов специальности 050704 Вычислительная техника и программное обеспечение

Рекомендовано на заседании кафедры

«__»_____.2010 г., протокол № 1

Заведующий кафедрой _____ Потапенко О.Г.

Одобрено МС факультета ФМиИТ

«___»__ _____ 2010 г., протокол № 1

Председатель МС _____ Ж.Г.Муканова

Курсовая работа предназначена для закрепления знаний и умений по дисциплине и развития навыков самостоятельной работы обучающихся при построении и расчете локальных сетей.

Перечень тем:

1. Разработка проекта локальной сети офиса с заданным количеством рабочих мест.
2. Выбор аппаратных и программных средств локальной сети офиса, занимающегося обучением работе на компьютере.
3. Выбор аппаратных и программных средств локальной сети офиса, занимающегося WEB дизайном.
4. Разработка проекта локальной сети какого-либо офиса (предприятия, фирмы) для реализации технологии клиент-сервер.

ВВЕДЕНИЕ

Данное пособие предназначено для студентов, выполняющих курсовую работу по курсу «Компьютерные сети», но может быть полезным и практическим инженерам. Курсовая работа представляет собой разработку компьютерной сети небольшого предприятия и программы, работающей с сетевыми сокетами на уровне системных функций.

Не смотря на то, что локальные и корпоративные сети являются необходимым атрибутом современного предприятия, имеется существенный дефицит учебных материалов, охватывающих комплексно вопросы проектирования сети. Данное пособие призвано заполнить образовавшийся вакуум и дать читателю общую картину проблем, которые нужно решить при построении современной корпоративной сети. Пособие не претендует на полный охват всех аспектов в виду объема и жанра, а лишь задаёт основные направления, требующие внимания при построении корпоративной сети и даёт ссылки на более подробные источники информации.

ТРЕБОВАНИЯ К КУРСОВОЙ РАБОТЕ

Курсовой проект по курсу "Компьютерные сети" является частью квалификационной работы бакалавра, поэтому к данному курсовому проекту предъявляются требования, в большей части совпадающие с требованиями к дипломной работе, за исключением объема работы и некоторых не технических разделов.

ТРЕБОВАНИЯ К ПРОЕКТУ СЕТИ

В аппаратной части курсового проекта необходимо разработать проект локальной сети среднего предприятия. Сеть должна содержать не менее 50 хостов, диаметр локальной сети должен составлять не менее 800м. Сеть должна обязательно иметь защищенный выход в интернет. В сети должны быть системные сервисы, такие как сервис имён DNS, сервис конфигурирования при загрузке DHCP, WINS и файловый сервис для сетей на ОС Windows.

Кроме того, в сети должна быть организована связь с удалённым офисом либо в пределах города с использованием технологий "последней мили", либо с использованием сервисов, предоставляемых телефонными компаниями, таких как FrameRelay или других технологий, предоставляемых телекоммуникацимонными компаниями.

Исходным материалом для проектирования сети является поэтажный план зданий с обозначенным на нём размещением компьютеров и сетевого оборудования, размещением отделов предприятия, а так же подробное описание информационных потоков на предприятии.

По информационному описанию предприятия определяются основные информационные потоки, их можности, требования к безопасноти и т.д., то есть

в конечном итого — структура сети предприятия и сервисов, в ней размещенных.

По плану здания рассчитывается пассивное сетевое оборудование, как то: коммуникационные шкафы, короба, кабель, розетки, уголки и пр. На плане так же указывается размещение активного сетевого оборудования, такого как коммутаторы, маршрутизаторы, серверы.

Результат размещения оборудования отображается на плане здания и в сводных таблицах по этажам, зданиям и проекту в целом.

Выбор активного сетевого оборудования должен производится исходя из чётко сформулированных требований к сети на основе как минимум 3 альтернативных решений, т.е. в проекте должен быть приведен сравнительный анализ оборудования 3-х различных производителей по критерию качество/стоимость.

Не рекомендуется использование в проекте устаревших типов оборудования , такого как, например, концентраторы. Даже если проектирование производится на основе реального предприятия с существующей сетевой инфраструктурой, в проекте необходимо не констатировать текущее состояние, а разработать проект модификации сети с учётом современных решений.

Современная кабельная инфраструктура сети строится с учётом подведения гарантированного питания в критические участки сети, поэтому в проекте должны быть учтены источники бесперебойного питания основных серверов и активного сетевого оборудования. Кабельная система должна обеспечить подвод питания к ним. Кроме того, в современной структурированной кабельной системе (СКС) прокладываются коммуникации не только для компьютерной сети, но и для телефонной сети. Обычно корпоративная телефонная станция находится в серверной комнате и использует ту же систему гарантированного электропитания. Наиболее современные АТС могут так же интегрировать голосовые сервисы традиционных телефонных сетей и компьютерные голосовые сервисы. Эти моменты стоит учесть при создании проекта сети.

Логическая структура сети так же должна быть спроектирована в ходе работы. В случае применения управляемых коммутаторов с поддержкой функций VLAN необходимо привести таблицы виртуальных сетей. Обязательным есть использование протокола IPv4 в сети, следовательно, должно быть осуществлено планирование адресного пространства сети.

Важное место в проекте занимает обеспечение безопасности в сети. Ведущим моментом в разработке средств обеспечения безопасности является разработка политики безопасности (security policy) для сети в целом с последующей детализацией для отдельных сегментов сети и сетевых сервисов. Политика безопасности представляет собой обычный текст, описывающий

уровни безопасности тех или иных информационных ресурсов и права доступа к ним. Этот текст утверждается руководством или соответствующими режимными службами и является основой для проектирования технических средств защиты сети.

Для организации необходимого уровня безопасности необходимо разбивать сеть на сегменты маршрутизаторами с функциями фильтрации трафика. Например, финансовые службы предприятия должны находится в отдельном сегменте сети, доступ к ресурсам который не возможен из сегмента сети общего пользования.

Доступ в сеть Интернет должен так же осуществляться с использованием необходимых средств защиты. Для сетей масштаба предприятия необходимо строить доступ с учетом защиты внутренней сети от вторжений из Интернета, защиты сервисов, предоставляемых сетью в Интернет, а так же с учётом разграничения прав пользователей сети по доступу в Интернет.

В случае использования фильтрующих маршрутизаторов обязательным является описание функций фильтра. Желательным является написание текста фильтра на языке применённого оборудования.

Работа должна содержать раздел, описывающий физическую и логическую структуру спроектированной сети (описание схемы сети).

ТРЕБОВАНИЯ К ПРОГРАММНОЙ ЧАСТИ.

Программная часть курсового проекта представляет собой программы, работающие с сетевыми сокетами на системном уровне и имеющие графический пользовательский интерфейс. Для большинства случаев программы имеют архитектуру клиент-сервер.

Серверная часть, естественно, не обязана иметь графический интерфейс. Она представляет собой программу-демон (системный сервис), который считывает текстовый конфигурационный файл при старте или по сигналу SIGHUP. Серверная программа должна собираться и работать на POSIX-совместимых системах. Для поддержки подсистемы POSIX в ОС Windows обычно используют либо окружение CyGNUs, либо MINGW.

Клиентская программа должна разрабатываться с учётом переносимости на популярные платформы, как минимум Windows и Linux. При разработке программы рекомендуется использование кросс-платформенных библиотек, таких как QT, GTK. Для данных библиотек существуют визуальные конструкторы, облегчающие разработку полнофункциональных пользовательских интерфейсов.

Рекомендуемые языки разработки - C или C++.

В случае упрощённого варианта заданий возможно использование Java.

Поскольку данная работа позиционируется как часть квалификационной работы бакалавра, особое внимание следует уделять качеству проектирования и

структурированию программного проекта. Оценка работы производится не только на основе функциональности программы и ее интерфейса, а и на основе анализа исходных текстов. В работе должен быть показан надлежащий уровень программирования и умение оформлять текст программы.

Документированию исходных текстов следует так же уделить особое внимание. Скрупулёзное документирование исходных текстов при помощи тегов какой-либо системы авто-документирования, например DoxyGen или DOC++ существенно облегчает и упрощает написание отчета в части раздела разработки программ.

Примеры типовых заданий на разработку программной части:

1. **Разработать программу, позволяющую секретарю руководителя быстро отправлять SMS сообщения сотрудникам.**

Клиентская часть программы должна иметь удобный пользовательский интерфейс, обеспечивающий авторизацию, внесение пользователей и групп, поиск пользователей, редактирование пользователей, отправку сообщений с поддержкой архива отправленных сообщений. Клиентская программа не должна хранить никаких данных, кроме адреса сервера.

Серверная часть программы должна отправлять SMS по электронной почте, выбирая адрес почтового сервера по префиксу телефонного номера, хранить все необходимые данные и предоставлять клиентской части необходимый сервис черех TCP сокет. Программа должна обслуживать произвольное количество клиентов. Серверная и клиентская части программы так же должны обеспечивать необходимый уровень конфиденциальности путем шифрования данных.

2. **Разработать программу мониторинга работоспособности и уровня загрузки хостов в сети.**

Программа должна определять уровень загрузки процессоров, дисковой подсистемы, каналов ввода-вывода и сетевых устройств.

Быстродействие системы должно быть максимальным в пределах одного сегмента сети.

Клиентская программа, отображающая состояние хостов, не должна требовать никаких настроек, а обнаруживать хосты с установленной программой мониторинга автоматически. Отображение хостов должно быть упорядоченным по имени, адресу, уровню загрузки той или иной подсистемы. Уровень загрузки должен отображаться в виде графика.

3. **Написать программу для быстрого обмена сообщениями, упрощённый вариант ICQ для использования в корпоративной сети.**

Программа должна обеспечивать регистрацию пользователей, привязку к штатному расписанию организации, поиск пользователей.

Клиентская часть программы должна иметь удобный графический интерфейс. Все данные система должна хранить на сервере, возможно, в базе данных.

4. **Программа отслеживания присутствия пользователя на рабочем месте.**

Данная программа должна запускаться на любом рабочем месте (Windows, Linux) как апплет рабочего стола и отслеживать активность пользователя с компьютером. Программа так же должна иметь возможность регистрации пользователя на сервере и возможность настройки таймаутов на определённые события (движение мыши, клавиатурный ввод, специфические события системы).

Серверная часть программы должна вести протокол активности зарегестрированных пользователей и по каждому пользователю генерировать файл статистики в формате HTML. Файлы статистики должны складываться в директорию, доступную вэб-серверу для просмотра.

Студенты могут самостоятельно предлагать варианты заданий по программной части и согласовывать их с преподавателем.

В отчёте по проекту должны содержаться все разделы, определённые стандартами кафедры.

РЕКОМЕНДАЦИИ ПО ПРОЕКТИРОВАНИЮ СЕТИ МАСШТАБА ПРЕДПРИЯТИЯ.

ИСХОДНЫЕ ДАННЫЕ ДЛЯ РАЗРАБОТКИ.

Исходными данными для проектирования сети являются 2 документа: план зданий и результаты информационного обследования предприятия. Поэтажный план зданий рисуется в масштабе и на нём указывается размещение рабочих мест. В ходе разработки проекта сети на плане указываются также розетки, короба, в которые производится укладка кабеля, коммуникационные шкафы с активным сетевым оборудованием.

Информационное обследования предприятия производится по следующему шаблону.

1. Описание предприятия в целом, т.е. сфера деятельности предприятия (организации), внешние информационные потоки, необходимые для деятельности предприятия.

2. Для каждого отдела (подразделения, рабочей группы) предприятия описываются функции отдела, количество рабочих мест, используемое программное обеспечение, используемые общие ресурсы сети предприятия, выделяемые данным отделом ресурсы для других пользователей сети, требования к уровню безопасности сегмента сети данного отдела.

3. Общие ресурсы сети, необходимые для работы предприятия, такие как файловые серверы, серверы баз данных, серверы доступа в Интернет, серверы голосовых коммуникаций и т.д.

4. Требования к системе обеспечения безопасности сети, т.е. какие необходимы сервисы аутентификации, авторизации и учёта.

На основании плана здания и результатов информационного обследования предприятия выполняется эскизный проект сети.

СТРУКТУРИРОВАННАЯ КАБЕЛЬНАЯ СИСТЕМА И РАЗМЕЩЕНИЕ ОБОРУДОВАНИЯ.

Структурированная кабельная система (СКС) является "скелетом", на котором основывается вся коммуникационная инфраструктура предприятия, поэтому проектированию СКС необходимо уделять особое внимание.

В состав СКС входят кабельные системы для передачи данных, для передачи голоса и для подвода гарантированного питания.

Для передачи данных со скоростью 100 и 1000 Мбит необходим кабель витой пары категории 5е. Для передачи телефонного сигнала достаточно кабеля категории 2 или 3, но с целью взаимозаменяемости кабелей и использования резервных кабелей как для телефонных соединений, так и для сетевых соединений, все кабели прокладываются по высшей необходимой категории.

В СКС так же закладываются резервные кабеля в объёме не менее 15% от общего числа для обеспечения надёжности и для облегчения расширения сети. Короба, используемые для укладки кабелей, должны иметь сечение, позволяющее уложить требуемое количество кабелей плюс запас 20% на расширение сети.

Кабеля подвода гарантированного электропитания так же прокладываются в общем коробе с сигнальными кабелями, однако монтируются в специальную изолированную секцию короба. Силовой кабель имеет 3 провода - "фаза", "ноль" и "земля". Очень важно соблюдение фазировки кабелей и обеспечение надёжного контура заземления.

Розетки для телефонных, сетевых и силовых подключений выбираются обычно универсальные, с переходными элементами на требуемое сечение короба и необходимым количеством гнёзд для разъёмов. Телефонные сети обычно используют разъём RJ11, но для обеспечения взаимозаменяемости

кабелей в СКС рекомендуется и для телефонных, и для сетевых соединений использовать разъём RJ45.

Розетки в обязательном порядке маркируются наклейками с обозначением их назначения и с регистрационным номером кабеля, подключенного к ним.

Кабели в СКС обязательно маркируются специальными наклейками и составляется документ, специфицирующий маршрут каждого кабеля. Таблица кроссировки кабелей обычно содержит номер кабеля, точки кроссировки и примечания. Эта таблица является основным эксплуатационным документом на СКС.

Короба стыкуются при помощи специальных конструкционных элементов: уголков, крестовин, переходов на другое сечение и разветвителей.

Кабеля должны заводится в коммуникационные шкафы и распределяться не в оконечное оборудование, а в кроссировочные панели.

Применение кросс-панелей позволяет легко осуществить перекоммутацию кабелей при замене оборудования либо при выходе из строя какого-либо канала связи.

Изменения в кроссировке должны отражаться в специальном листе кроссировки, который либо находится в общем журнале эксплуатационных документов, либо в каждом коммуникационном шкафу.

Коммутация внутри шкафов между кросс-панелями и активным оборудованием осуществляется при помощи коротких кабелей с разъёмами RJ45, называемых патчкордами.

Магистральные кабели между коммуникационными шкафами могут содержать несколько комплектов пар (20 и более). Перекоммутация между магистральными и конечными кабелями так же производится на кросс-панели в коммуникационных шкафах.

Кроссировочные панели тоже нумеруются, маркируются и заносятся в таблицу кроссировки кабелей.

Оптоволоконные кабели прокладываются в тех же коробах. Поскольку оптоволоконный канал не предоставляет гальванической связи, нет особых требований по изоляции при укладке кабеля, однако есть требования на минимальный радиус закругления изгиба кабеля, поэтому оптический кабель на поворотах короба укладывается в специальные пластиковые «радиусы».

Перегиб кабеля может привести к его выходу из строя, а несоблюдение минимального радиуса - к появлению отражений и затуханий в кабеле, что повлечёт за собой нестабильную работу сети.

Коммутация оптический кабелей осуществляется при помощи специальных оптических концентраторов.

Оптические кабели необходимо применять там, где нужна гальваническая развязка между сетями. Гальваническая развязка позволяет избежать выхода из строя оборудования при скачках напряжения между питающими фазами, при пробое на корпус оборудования и при грозовых разрядах. Обычно посредством оптического кабеля подключают сервера, удалённые сегменты сети и сегменты, запитанные из разных электрических сетей.

Важной частью СКС является система гарантированного электропитания. В зависимости от требований к бесперебойной работе оборудования выбирается мощность источников бесперебойного питания, которые должны обеспечить работу сети на протяжении определённого промежутка времени. Обычно, при отсутствии специальных требований к электропитанию, мощность источников питания и ёмкость их батарей выбирается такой, что бы обеспечить безаварийное отключение оборудования. Источник питания должен быть подсоединён с серверу, рассылающему в сеть сообщения о переходе на автономное питание и о времени до отключения питания. На остальных узлах сети устанавливается ПО, принимающее эти сообщения и реагирующее заданным образом на события в сети электропитания.

Активное оборудование размещается в коммуникационных шкафах, в которые заводится кабельная система в пределах допустимого диаметра для данного типа сети. В большинстве случаев диаметр не должен превышать 200 метров. Коммуникационные шкафы обычно располагают на каждом этаже.

Коммуникационные шкафы должны иметь замки для предотвращения несанкционированного доступа к оборудованию.

Сервера и базовое сетевое оборудование, а так же АТС размещают в отдельном помещении - серверной комнате, доступ в которую ограничен.

В данной комнате должны быть расположены так же средства поддержки бесперебойного питания, по крайней мере для оборудования, размещённого здесь же.

ВЫБОР АКТИВНОГО ОБОРУДОВАНИЯ.

Для начала стоит очертить класс технологий, применяемых наиболее часто для построения локальных сетей.

Единственной, выжившей на сегодня технологией построения локальных сетей, является Ethernet в различных его модификациях. Наиболее распространённым на сегодня стандартом является 100BaseT, обеспечивающий передачу данных со скоростью 100 Мбит/с по медной витой паре 5-й категории. В последнее время всё большее распространение получают стандарты 1000 Мбит и выходят на рынок производители устройств 10Гбит.

Стандарт 1000 Мбит используется в 2-х вариантах - медный кабель и оптоволоконный кабель. Для стандарта 10Гбит используют только

оптоволоконный кабель.

Все большее распространение получают стандарты беспроводной связи IEEE 802.11 с различными скоростями от 2 до 50 Мбит. Наиболее распространенным на сегодня является стандарт IEEE 802.11g, или WiFi, обеспечивающий передачу данных со скоростью до 11 Мбит. Применение беспроводной технологии позволяет обеспечить доступ к сети для мобильных пользователей с такими устройствами, как, например, ноутбуки, наладонные компьютеры, сматрфоны.

Для доступа в сеть через WiFi устанавливаются радио-концентраторы, которые подключаются непосредственно в локальную сеть Ethernet. Обычно такие устройства содержат коммутатор на несколько портов и маршрутизатор с 1 портом, который позволяет выделить беспроводной сегмент в отдельную сеть.

Сети на основе других технологий не нашли распространения при построении локальных сетей.

Для глобальных сетей и для объединения удалённых сегментов корпоративных сетей используются другие технологии, которые описаны в отдельном разделе.

Активное оборудование локальных сетей можно разбить на следующие группы:

Концентраторы - это устройства , позволяющие соединить сетевое оборудование в один ФИЗИЧЕСКИЙ сегмент. Концентраторы не обрабатывают сетевые пакеты (кадры), а лишь обеспечивают необходимое согласование сигналов среды передачи и усиление слабого сигнала.

Концентраторы обеспечивают подключение к одной общей физической среде передачи всех устройств, следовательно трафик в этой среде будет общим для всех сетевых устройств, и, трафик между какими либо двумя устройствами будет мешать третьему устройству.

Концентраторы являются устройствами уровня 1 по модели взаимодействия открытых систем ISO.

Для сети Ethernet 100Мбит применение концентраторов не целесообразно, поскольку коммутаторы имеют приблизительно такую же стоимость, но обеспечивают разделение трафика между портами и пропускная способность сети значительно возрастает. Для оптических кабелей применение концентратора может оказаться оправдвнным.

Коммутаторы - это устройства второго уровня модели OSI, которые работают с пакетами (кадрами) сети. Каждый порт коммутатора имеет свою

буферную память и ассоциированную с портом память для хранения MAC адресов. Коммутация пакетов между портами осуществляется через коммутационную матрицу по MAC адресу. Пропускная способность коммутационной матрицы должна позволять обрабатывать пакеты "со скоростью провода", т.е., с той скоростью, с которой пакеты поступают по физической среде передачи. Пропускная способность коммутационной матрицы должна быть равна сумме пропускных способностей всех портов коммутатора, тогда любая пара потров коммутатора будет работать независимо и не будет оказывать влияния на работу другой пары. Через некоторое время после включения коммутатор накапливает информацию о том, какие MAC адреса находятся на каком порту, и пересылает пакеты только в нужный порт, а не на все порты, как происходит в случае использования концентратора. Широковещательные (broadcast) пакеты пересылаются, естественно, на все порты коммутатора.

Управляемые коммутаторы имеют дополнительные функции, основными из который является поддержка виртуальных сетей и жесткая привязка MAC адреса к порту. Эти функции позволяют повысить безопасность в сети одновременно с гибкостью настройки. Поскольку участники одной виртуальной сети "не видят" участников другой сети на уровне MAC адресов,возможно создание нескольких независимых сетей на основе одной сети Ethernet. Обмен данными между этими сетями будет возможен только на 3-м уровне, то есть через маршрутизатор, что позволяет более гибко контролировать трафик в сети. Привязка потра к конкретному MAC адресу не позволит пользователю несанкционированно попасть в другую виртуальную сеть путём замены MAC адреса. Ещё одной, удобной для провайдеров сетевых сервисов, функцией, является возможность подсчёта трафика по порту и по MAC адресу.

Коммутаторы с поддержой виртуальных сетей VLAN по стандарту IEEE 802.1q позволяют разделить одну физическую сеть на несколько изолированны логических сетей, используя либо группы портов, либо, в общем случае, дополнительнын поля (теги) в кадре Ethernet.

Коммутаторы с приоритизацией трафика позволяют более ефективно использовать имеющуюся полосу пропускания.

Коммутаторы с поддержкой аутентификации на уровне 2

Маршрутизаторы - это устройства 3-го уроня OSI, с некоторыми функциями 4-го уровня. Маршрутизаторы работают на уровне сетевого протокола, например, на уровне протоколов IP или IPX. Поскольку IPX потихоньку уходит в небытие, будем рассматривать только семейство протоколов TCP/IP. К основным функциям маршрутизаторов можно отнести следующие;

1. Маршрутизация. Собственно, вполне понятно, что это основная функция маршрутизатора, у которой есть 2 важных аспекта: динамическая маршрутизация обеспечивает живучесть сети за счёт использования альтернативных маршрутов; маршрутизация происходит на уровне сетевого протокола, а не на 2-м уровне, поэтому исключается зависимость от конкретной несущей сети и появляется возможность объединения сетей различной природы.

2. Управление трафиком. Важнейшим аспектом управления трафиком является приоритизацию трафика по различным признакам, как то по адресам, полю TOS, по используемым протоколам и т.д. Другим важным аспектом является фильтрация трафика по всевозможным критериям, основанным на разборе заголовков межсетевого и транспортного уровней, а иногда и уровня доступа к сети, в соответствии с моделью взаимодействия в сетях TCP/IP.

3. Маршрутизатор необходимо устанавливать в случае объединения сетей различной природы, в случае необходимости разделить сеть на сегменты с целью обеспечения безопасности и при необходимости обеспечения живучести сети за счёт использования альтернативных маршрутов.

Маршрутизирующие коммутаторы - устройства, объединяющие в себе функции коммутатора и маршрутизатора. Маршрутизатор - это специализированный компьютер с различными сетевыми интерфейсами, который производит операции над пакетами в ОЗУ с использованием своего процессора. Маршрутизирующий коммутатор имеет огромную коммутационную матрицу, в которой имеются аппаратные структуры не только для разбора заголовков уровня 2, но и для уровней 3 и 4. Коммутационная матрица программируется "на лету" процессором устройства для отображения текущей конфигурации, состояния таблиц маршрутизации и т.д. В отличие от маршрутизаторов, эти устройства обычно имеют гораздо большую пропускную способность, позволяющую вести обработку трафика "со скоростью провода", однако, могут работать только в сетях одной природы, например, в сетях Ethernet.

Маршрутизирующие коммутаторы применяют в случае необходимости динамической маршрутизации в больших сетях на основе технологии Ethernet. В виду их дороговизны другое применение не оправдано. Если необходимо разграничение доступа в сеть для виртуальных локальных сетей, имеет смысл использовать управляемый коммутатор в паре с маршрутизатором на основе ПК под управлением ОС Linux или FreeBSD и портом Ethernet 1000Мбит. Маршрутизатор включается во асе виртуальные сети и на него устанавливается маршрут по умолчанию (default route) всех хостов во всех виртуальных с сетях.

Таким образом, все пакеты, проходящие из одной сети в другую, будут попадать сначала на маршрутизатор, там обрабатываться соответствующими фильтрами, и затем попадать по назначению. Естественно, пропускная способность такого маршрутизатора будет определять скорость обмена между виртуальными сетями.

РЕКОМЕНДАЦИИ ПО ПРИМЕНЕНИЮ СЕТЕВОГО ОБОРУДОВАНИЯ

Исходя из изложенного, можно сформулировать следующие рекомендации по выбору типа и размещению активного сетевого оборудования.

1. Рабочие группы со стандартными требованиями к скорости включаются в порты 100 Мбит неуправляемого коммутатора. Для выхода в общий сегмент желательно использовать порт 1000 Мбит.

2. Рабочие группы с повышенными требованиями к пропускной способности сети включаются в неуправляемый коммутатор с портами 1000Мбит, при чём файловый сервер для таких групп необходимо размещать в этом же сегменте сети, т.е. включать в тот же коммутатор.

3. Рабочие группы без дополнительных требований к безопасности либо сегменты сети с одними и теми же логическими уровнями доступа объединяются в один сегмент сети Ethernet при помощи скоростного неуправляемого коммутатора.

4. Рабочие группы с дополнительными требованиями к сетевой безопасности включаются в отдельный сегмент сети, физический , либо логический (VLAN). Для разделения сети на логические сегменты (виртуальные локальные сети) используют управляемые коммутаторы.

5. Все сегменты сети объединяются при помощи маршрутизатора. Поскольку маршрутизатор обрабатывает пакеты в памяти, то далеко не всегда можно достичь нужной скорости передачи данных между сегментами сети ввиду низкого быстродействия маршрутизаторов. Для решения проблемы скорости обмена нужно размещать совместно используемые ресурсы в тех сегментах, где скорость доступа к ним наиболее критична и где происходит основная масса обращений к данным ресурсам. Если поступить так по каким-либо причинам не удаётся, то вместо маршрутизатора нужно использовать маршрутизирующий коммутатор.

Основной причиной объединения сегментов сети при помощи маршрутизатора является возможность дополнительного управления трафиком

с целью поддержки определённой политики безопасности. Например, хорошо известно, что работники финансовых служб предприятия зачастую являются простыми пользователями и не обладают достаточной квалификацией для обеспечения надлежащего уровня безопасности своих персональных компьютеров. Однако, именно их рабочие компьютеры могут содержать коммерческие и другие секреты, которы не должны случайно попасть в сегмент общего пользования. С другой стороны, эти сотрудники должны иметь полный доступ к информационным ресурсам сети.

Решить такую задачу можно, применив пакетные фильтры на маршрутизаторе, объединяющем локальную сеть финансовой службы с другими сегментами корпоративной сети.

Оборудование "последней мили".

Традиционно проблема "последней мили" - это проблема передачи сигнала от городской АТС до квартиры абонента. С развитием цифровых телекоммуникационных технологий это понятия приобрело более широкий смысл - передача сигнала в пределах небольших расстояний.

Для решения проблемы "последней мили", т.е. подачи сетевого трафика от телекоммуникационного провайдера к конечному потребителю либо для соединения сетей, расположенных в небольшом радиусе (до примерно 7 км) используется ряд технологий, однако мы остановимся только на оборудовании, предназначенном для передачи IP трафика без жёстких требований к низ лежащему уровню.

Очевидно, что потребителю удобнее всего принимать IP трафик в порт Ethernet в виду распространенности и, следовательно, дешевизны оборудования. Однако, в отдельных случаях приходится использовать порты с синхронными протоколами, такими как V.35/V.36, X.21 или E1. Синхронные порты поменяются для работы через глобальные сети провайдеров услуг традиционной телефонии или сети FrameRelay.

Оборудование для интерфейсирования компьютера с синхронным потоком в десятки и даже в сотни раз дороже, чем оборудование Ethernet.

Однако, какая бы технология не использовалась для глобальной сети, в конце концов IP трафик должен попасть в локальную сеть на базе Ethernet.

Сначала обсудим, что имеется в наличии в качестве физической среды передачи.

1. Эфир является наиболее удобным способом достичь соединения сетей в пределах прямой видимости. Сложность заключается в том, что в Украине для использования радиочастот необходимо наличие довольно дорогостоящей

лицензии, и даже для оборудования WiFi, работающего с шумоподобным сигналом на частоте микроволновых печей нет свободно используемого диапазона частот. По украинскому законодательству ГИЭ может конфисковать оборудование и наложить штраф, как только засечет использование оборудования WiFi за пределами здания. Следовательно, использование WiFi (IEEE 802.11) для решения проблемы "последней мили" возможно только в случае договора с лицензиатом.

2. Медные пары диаметром 0.4 мм используются для подачи телефонного сигнала от АТС до конечного абонента. Стоимость аренды одной пары в пределах кабельного хозяйства одной АТС составляет примерно 5$ в месяц. Оборудование имеет приемлемые цены. Скорость передачи данных в пределах 2 Мбит/с. Проблема в одном - в дефиците (как повеяло советской историей!) этих пар.

3. Оптоволоконные кабели - наиболее удобная среда для передачи данных. Стоимость кабелей и оконечного оборудования приемлема. Проблема заключается в том, что прокладка кабеля должна производится по колодцам, принадлежащим другим организациям либо в собственные траншеи, на что требуется довольно много официальных разрешений от муниципальных и других органов. Чужой оптоволоконной структурой воспользоваться практически не возможно, поскольку в аренду кабельную систему сдавать не выгодно, гораздо выгоднее предоставлять сервис по передаче данных.

На сегодняшний день практически нет необходимости использовать какие либо протоколы, кроме семейства TCP/IP по той простой причине, что данное семейство протоколов используется в сети Интернет и фактически вытеснило другие протоколы. Для доступа к сетевым службам, специфичным для сетей Windows применяется специальный вариант протокола NetBIOS, работающий поверх протоколов семейства TCP/IP. Применение «чистого» NetBIOS и IPX не оправдано с точки зрения безопасности и данные протоколы должны фильтроваться маршрутизаторами.

Использование NetBIOS в «чистом» виде, на первый взгляд, может облегчить администрирование небольших сетей, однако на практике приводит к возникновению существенной путаницы в сети, поскольку пользователи предоставлены сами себе и в вопросах назначения имён и в вопросах адресации. Это а конце концов приводит к хаосу в сети.

Использование протоколов семейства TCP/IP подразумевает планирование сети, централизованную схему выдачи адресов и присвоения имён, а так же определённую политику маршрутизации.

Рассмотрим пример планирования адресного пространства сети и размещения необходимых системных сетевых сервисов.

Для корпоративных сетей выделены следующие блоки адресов:

10.0.0.0/8
172.16.0.0/12
192.168.0.0/16

Приведенные блоки адресов не маршрутизируются в Интернете, администратор сети может брать любой блок для использования в своей сети.

Поскольку адресов более чем достаточно для создания сети масштаба корпорации, разбивать на мелкие блоки адреса нет необходимости. Однако, следует помнить, что "плоская" модель сети, без разбиения на иерархические сегменты, ущербна с точки зрения организации безопасности.

Оптимальным является использование маски 255.255.255.0 для сегментов сети, что позволит ввести дополнительную сегментацию при необходимости, с одной стороны, и является удобным блоком для маршрутизации, с другой стороны. Таким образом, в сегменте может быть до 254 хостов, при чем один и з них - это и интерфейс маршрутизатора, обеспечивающего выход наружу из данной подсети.

Маршруты по умолчанию для рабочих станций устанавливаются именно на адрес данного интерфейса (192.169.5.1).

В приведенном примере примере сети можно использовать статическую маршрутизацию, однако это сопряжено с трудностями при дальнейшем росте сети. Для локальных сетей вполне удобен протокол RIP, который почти не требует настроек и реализован в каждом маршрутизаторе. Для UNIX систем рекомендуется использовать демон ripd из пакета zebra.

Для сетей с множественными альтернативными маршрутами и удалёнными сегментами с небольшой пропускной способностью каналов рекомендуется использовать протокол OSPF,однако данный севрис более сложен в настройке.

Прежде, чем говорить о технических средствах подключения сети предприятия к Интернет, необходимо сформулировать и выписать в виде обычного текста политику предоставления сервисов Интернет во внутреннюю сеть и политику предоставления сервисов корпоративной сети в Интернет. На основе этой политики, согласованной с руководством, производится размещение сервисов для предоставления информации в сеть Интернет и для доступа пользователей корпоративной сети в интернет.

Пример такой политики приведен ниже. Данный пример будет пригоден

для большинства случаев.

Доступ к информационным ресурсам корпоративной сети.

Доступ к информационным ресурсам корпоративной сети пользователей сети Интернет осуществляется через информационный вэб-сайт предприятия, который должен быть виден для всей сети Интернет. Доступ фирм-партнёров к информационным ресурсам предприятия производится через другой вэб-сайт с возможностью контроля доступа при помощи пароля и криптографической защиты канала. Должна быть так же учтена возможность контроля электронных сертификатов пользователей.

Доступ сотрудников предприятия как мобильных пользователей ко внутренним ресурсам корпоративной сети должен осуществляться через сеть Интернет с использованием сервера виртуальных приватных сетей по протоколу PPTP с криптографическими расширениями.

Доступ сотрудников предприятия из внутренней сети предприятия в сеть Интернет должен осуществляться в зависимости от должности с определённых рабочих станций при введении учётного имени и пароля для доступа в сеть. Для некоторых рабочих станций и серверов доступ в сеть Интернет должен быть не возможен ни при каких обстоятельствах.

Использование программ моментальных сообщений разрешается неограниченно, за исключением отмеченных выше компьютеров.

Использование протокола удалённого доступа к UNIX-системам ssh разрешается только с определённых рабочих станций в нескольких отделах.

Естественно, слова *"некоторые", "определённые"* и т.п. должны быть конкретизированы в реальном документе.

После формирования такого документа можно говорить о технических средствах, необходимых для реализации описанной политики доступа.

Поскольку в приведенном примере имеются вэб-сервера и сервера виртуальных приватных сетей, то доступ в сеть интернет должен осуществляться по высоконадёжному выделенному каналу. Кроме того, указанные сервера должны иметь постоянный IP адрес и соответствующие записи в публично доступном сервере имён DNS.

Организация физического канала к провайдеру сетевых услуг в большинстве случаев зависит от провайдера, однако эти технические средства должны быть отражены в проекте сети.

Для подключения сети предприятия к Интеренет обычно используется схема, приведенная на рисунке. Пограничный маршрутизатор обеспечивает максимальную защиту сети при помощи пакетного фильтра, настроенного для блокировки всего трафика, кроме того, который поступает на гарантированно обслуживаемые сервисы в демилитаризованной зоне (DMZ) и определённого исходящего плюс соответствующего ему входящего трафика из внутренней сети в соответствии с политикой доступа.

Сам маршрутизатор практически не может быть взломан, поскольку не выполняет никаких программ, доступных во внешнюю сеть.

Таким образом, доступ из внешней сети возможен только к сервисам, расположенным в демилитаризованной зоне. и эти сервисы постоянно мониторятся и контролируются сетевыми администраторами. Остальная сеть не доступна извне без инициирования определённого трафика изнутри самой корпоративной сети.

Доступ из внутренней сети в сеть Интернет должен так же быть под контролем администратора. Для наиболее ресурсоемких протоколов, таких, как ftp и http, обычно используют прокси-сервер с контролем списков доступа. В простейшем случае контроль производится по логину и паролю, однако, современные прокси-сервера, такие как Squid, имеют широкий набор средств авторизации и аутентификации; nt-domain, RADIUS, LDAP, SQL-bsed и т.д. Выбирается обычно та система учёта, авторизации и аутентификации (AAA), которая применяется для других сервисов в корпоративной сети.

Доступ в сеть Интернет для остальных протоколов, таких как ICQ, ssh может производится через маршрутизатор с поддержкой трансляции сетевых адресов (NAT).

Протоколы, которые не используются, должны быть закрыты на пограничных маршрутизаторах, а так же должна быть настроена система журналирования пакетов, заблокированных пограничными маршрутизаторами.

Доступ мобильных пользователей в корпоративную сеть осуществляется через сервер виртуальных приватных сетей (VPN). В качестве сервера можно использовать сервер под управлением ОС Windows, имеющий сервис PPTP в качестве стандартного сервиса удалённого доступа, однако в таком случае слишком велик риск несанкционированного доступа в сеть путём взлома данного сервера. Дело скорее не в низкой защищённости данной ОС, а в её популярности в сочетании с закрытостью. Популярность делает данный сервис мишенью номер один для взломщиков, а закрытость затрудняет несвоевременное обновление системы с целью решения проблем безопасности. В качестве сервера VPN рекомендуется использовать либо специализированное устройство, либо UNIX-подобную свободно распространяемую ОС с соответствующим ПО поддержки PPTP сервиса и необходимых средств авторизации и аутентификации. На сервере VPN не должно выполняться больше никаких сервисов для исключения возможности взлома, а удалённый доступ по протоколу ssh должен быть открыт только с рабочих станций сетевых администраторов. Жёсткость требований данному серверу определяется его положением в сети: с одной стороны, он должен быть доступен из сети Интернет для мобильных пользователей, а с другой - он открывает путь во внутреннюю сеть предприятия. Именно потому, что взлом данного сервера открывает полный доступ к корпоративной сети, рекомендуется использовать операционные системы и приложения с безупречной репутацией, например такие как FreeBSD или Solaris.

Настройка фильтрующих маршрутизаторов.

Настройка пакетных фильтров является отдельной обширной темой, поэтому предварительно стоит ознакомится со следующим материалом:

Настройка пакетных фильтров производится на основе всё тех же писанных правил, определяющих политику доступа к тем или иным информационным ресурсам.

Если речь идёт о пограничном маршрутизаторе между корпоративной сетью и сетью интернет, то пакетный фильтр проектируется на основе приведенной выше политики доступа в Интернет. Если речь идёт о маршрутизаторах между различными сегментами корпоративной сети, то должна быть сформулирована политика, описывающая информационный обмен между сегментами сети.

Политика информационного обмена между сетями следующая:

Доступ из других сегментов сети в подсеть финансовых служб должен быть запрещён по всем протоколам. Мобильные пользователи могут получить доступ только пройдя авторизацию в отдельной группе пользователей с обязательным использованием средств криптозащиты. Доступ из финансовой подсети к информационным ресурсам корпоративной сети должен быть неограниченным по протоколам ssh, smb.

По протоколу http и ftp доступ возможен в Интернет и к корпоративным ресурсам. Доступ по протоколу ODBC для драйверов баз дынных PostgreSQL должен быть возможен к корпоративным серверам баз данных. Доступ к службам моментальных сообщений возможен только через корпоративный сервер Jabber. Все остальные протоколы должны блокироваться.

В соответствии с приведенной политикой спроектирован фильтр, приведенный ниже.

В заключение данной темы следует сказать, что наличие общей политики доступа к информационным ресурсам обязательно, поскольку это затрагивает настройки не только конкретных пакетных фильтров, но и настройки серверов доступа, авторизации, аутентификации и т.д. Должен так же быть писанный документ, определяющий, как технически реализован тот или иной пункт политики доступа к информационным ресурсам. Форма таких документов произвольная, однако документирование сети является залогом её безопасной эксплуатации, и, следовательно, является обязательным.

Интеграция голосовых сервисов локальной сети с телефонной сетью.

Современные сети передачи данных имеют достаточную полосу для передачи голосовых данных, а компьютеры и перифирия - достаточное быстродействие для обработки звука в реальном масштабе времени. С другой стороны, стоимость передачи данных по сетям IP в несколько раз, а иногда и в несколько десятков раз ниже, чем передача голоса по телефонным сетям общего

пользования. Очевидно, что указанные факторы ауктуализируют проблему интеграции голосовых сервисов телефонной сети и сети передачи данных.

Рассмотрим следующие аспекты данной проблемы: оборудование конечного пользователя, сопряжение телефонной сети предприятия с компьютерной сетью, использование внешних каналов передачи данных для телефонногго трафика.

Оборудование конечнгого пользователя для работы с телефонной сетью не требует никаких изменений, поскольку АТС пердприятия полностью определяет стандартны оборудования, допустимого для и спользования.

Единственный момент, требующий внимания - это использование одной и той же СКС для телефонной и компьютерной сети.

Оборудование для сетевых голосовых сервисов так же стандартное - гарнитура (микрофон плюс наушники) и дуплексная звуковая картра.

Внимание следует уделить программному обкспечению поддержки голосовых сервисов. В настоящкк время есть ряд стандартов, таких как

H.232, X., которые должны поддерживаться клиентским ПО для успешной интеграции с серверной частью голосовых служб. На сегодняшний день существует довольно много програм, реализующих данные стандарты. Наиболее популярными являются для платформы

NetMeeting Windows GnomeMeeting Linux.

Кроме того, существует ряд аппартных реализаций клиентского оборудования для голосовых сервисов, т.н. EthernetPhones.

Для сопряжения телефонной сети предприятия с голосовыми службами компьютерной сети необходимо оборудование, поддерживающее, с одной стороны, группу стандартов H.232, с другой стороны, интерфейсы к АТС. Такой класс оборудования называется голосовами шлюзами (voice gateways). Стандарты H.232 поддерживаются программно, а на интефейсах с АТС следует остановиться отдельно. В случае использования аналоговой АТС либо обычных аналоговых портов цифоровой АТС в голосовой шлюз добавляюься модули поддержки аналоговых линий, которые имитируют обычные аналоговые линии АТС.

Если устанавливается современная АТС, то наиболее удобным сопряжением ее с голосовым шлюзом является интерфейс ISDN BRI, обеспечивающий передачу данных в цифоровом виде для 30 голосовых каналов одновременно.

Естественно, для качественной передачи голоса по сети необходимо иметь достаточный запас полосы пропускания сети (как минимум 16 Кбит/с для одного сжатого канала) и минимальную задержку в канале. Использование ассиметричных спутниковых каналов практически неприемлемо из-за ассиметрии полос пропускания, а с симметричными спутниковыми каналами могут возникнуть проблемы из-за значительных (350 мс и более) задержек на

распространение сигнала. Поэтому для организации голосовых сетевых сервисов обычно используют наземные каналы.

Поскольку сети на основе протокола IP не предоставляют гарантий качества обслуживания(QoS), таких как фиксированная задержка и гарантированная полоса, необходимо так же не перегружать каналы, используемые для голосовых сервисов.

Для передачи голоса часто используют сети FrameRelay, имеющие средства обеспечения QoS, однако расценки на данный сервис не сильно уступают расценкам на передачу голоса, а оборудование достаточно дорого.

ВЫБОР СЕРВЕРНЫХ ОС.

Выбор серверной ОС должен удовлетворить целый ряд требований по ....

РЕКОМЕНДАЦИИ ПО ПРОГРАММНОЙ ЧАСТИ ПРОЕКТА.

РАЗРАБОТКА КЛИЕНТСКОЙ ЧАСТИ ПРОГРАММ.

Разработка клиентской части программ должна производитс с учётом переносимости программы на различные платформы. Естсетственно, что написание таких программ "с нуля" занятие очень трудоёмкое, особенно. если речь идёт о создании графического интерфейса. Поэтому для реализации клиентского приложения необходимо использовать специальные кроссплатформыне библиотеки. Из свободно распространаемых библиотек наиболее популярнвми являются wxWidjets, gtk2 для языка C и gtkmm, qt4 для языка C++. Отмеченные библиотеки позволяют один и тот же код скомпилировать как приложение для ОС Windows, так и для бошльшого количества систем, исполтьзующих X-Window system и другие графические системы.

Использование одного и того же кода для разных платформ позволяет разработчику сосредоточиться на разработке функциональности системы, а не на переносе кода, что существенно повышает качество программного продукта.

Примененение интерпретирующих систем является альтернативным путем решения проблемы переносимости кода, однако это требует установки интерпреиаиора на целевую систему. Кроме того, не все интерпретируемые языки обладают достаточной скоростью работы приложений и тем более не все имеют достаточно выразительных средств для объектного программирования. Из наиболее удобных средств данного класса стоит упомянуть язык Python.

Использование Java и компонетов swing является хорошим копромисом между первым и вторым вариантом, поскольку обеспечивает достаточно высокую скорость работы приложения за счёт механизма компиляции JIT, однако всё таки требует уствановки системы поддержки времени выполнения.

К недостаткам последних двух следует так же отнести медленный старт приложения.

Для реализации клиентской части приложения возможен выбор любого из упомянутых инструментов, однако требование к использованию одного и того же кода для разных платформ являтеся существенным.

РАЗРАБОТКА СЕРВЕРНОЙ ЧАСТИ ПРОГРАММ.

Серверная часть программы как правило не имеет пользовательского интерфейса, однако не смотря на наличие стандартов ISO на язык C и его стандартную библиотеку, проблема переносимости ПО стоит очень остро и требует от программиста знания нескольких операционных систем для написания импортируемого кода. Даже для POSIX-совместимых систем есть трудности импортирования ПО, связанные с различными интерфейсами к системным ресурсам. Можно выделить следующий набор рекомендаций, облегчающих импортирование вашей программы.

1. Отделяйте логику работы программы и интерфейс с системой. Наример, для работы с файловой системой нужно использовать свои интерфейсные функуии, преобразующие строку пути к виду, приемлемому для данной ОС.

2. Используйте по возможности не системные библиотеки, а кросс-платформные библиотеки или надстройки над системными функциями. Например, для работы с XML лучше пользоваться libxml2, а не интерфейсом, предоставляемым

Visual C++.

3. При необходимости использования специфичных для данной системы функций выносите код, вызывающий их, в отдельный модуль компиляции (*.h, *.c) с собственными интерфейсными функиями, одинаковыми для всех систем .

4. Не применяйте непереносимого кода нигде, кроме чётко оговоренных в п.1, 3 мест. Многочисленные макрооператоры "#idef OS ..." по тексту программы затрудняют ее восприятиё и ведут к логичесуким ошибкам.

5. Пользуйтесь общепринятыми стандартами для работы с подсистемами. Напрмер, для доступа к базам данных используйте SQL и ODBC.

6. Не используйте библиотек, предоставляемых каким-либо отдельным компилятором. Например, среды разработки Borland предоставляют на первый взгляд удобный набор интерфейсных функций, которые затрудняют перенос программ не то что на другую систему, а и на другой компилятор в той же ОС,

поскольку исходные тексты этих интерфейсных библиотек не доступны или используют специфические для данного компилятора директивы.

Если нужно написать сервреное приложение, но затратфы на тщательное порти рованние кода не оправданы, можно писать его под POSIX-совместимую ОС, а для переноса на MINGW.

СПРАВОЧНЫЙ МАТЕРИАЛ РАЗРАБОТЧИКА.

Наиболее полное руководство по функциям libc можно получить при помощи просмотрщика документации в формате GNU info. В браузере konqueror среды KDE можно получить доступ к этой инфориации, введя в поле URL следующую строку: info:libc. Аналогично можно получить доступ к справочнику в среде Gnome при помощи программы gnome-help-browser. В терминальном варианте навигация по справочной системе производится интерактивной командой info.

Руководство по программированию сокетов и примеры применения функций на языке С можно найти по адресу:

Для языка С++ наиболее удачными являются примеры из следующих источников:

ЗАКЛЮЧЕНИЕ.

Результатом данной курсовой работы является проект сетевой кабельной инфраструктуры предприятия и проект логической структура сети с размещёнными активными сетевыми устройствами и системными сетевыми сервисами. Результатом программной части проекта является набор программ (как минимум клиент и сервер) для предоставления какого-либо сетевого сервиса. Данная работа должна подтвердить квалификацию бакалавра в области проектирования сетей и сетевого программного обеспечения.

Список литературы:

Основная

1. Олифер В.Г., Олифер Н.А.. Компьтерные сети: принципы, технологии, протоколы. Учебник. СПб. "Питер", 2001.
2. Бройдо В. Вычислительные системы, сети и телекоммуникации – СПб. "Питер", 2004.
3. Оглтри Т. Модернизация и ремонт сетей, - 2-е изд.: Пер. с англ.: Учеб. пос. – М.: Издательский дом «Вильямс», 2000. – 928 с.
4. Гук М. Аппаратные интерфейсы ПК. Энциклопедия. СПб. "Питер", 2002.
5. Microsoft Corporation. Компьютерные сети + : Учеб. Курс: Официальное пособие для самостоятельной подготовки/пер. с англ. – М.:Русская Редакция, 2000. – 552.

Дополнительная

6. Андерсон К., Минаси М. Локальные сети. Полное руководство: Пер. с англ. – К.: ВЕК+, М.: ЭНТРОП, Спб: КОРОНАпринт, 1999.-624 с.
7. Назаров С. В. Администрирование локальных сетей Windows NT: Учеб. пособие. – М.: Финансы и статистика, 1999. – 336.