Курс «Корпоративные информационные системы»

Попов В. Б.
доцент кафедры информационных систем в экономике

Тема1. Анализ сетевых моделей корпоративных сетей.

Службы каталога Windows NT/2000 Server и UNIX реализуют доменную модель корпоративной сети, когда учетные записи пользователя хранятся и управляются централизованно через базу данных доменных учетных записей, а управление сетевыми ресурсами возлагается на владельца или администратора данного ресурса. Данное занятие знакомит с двумя возможными моделями сети на основе Windows NT/2000 — доменной моделью и моделью рабочей группы. Приводится обзор четырех типов доменной сети.

Определение корпоративной среды. В отличие от простой вычислительной среды, когда один или несколько серверов объединены в один локальный домен, корпоративная среда может включать в себя множество серверов в нескольких доменах, которые могут находиться в разных географических точках.

Сетевые модели. Основная цель сети — обеспечить совместное использование ресурсов. Хотя для достижения этой цели существуют различные способы структурирования сети, Windows NT/2000 поддерживает две разных модели: доменную и модель рабочей группы. Выбор зависит от требований предъявляемых к сети, но почти всегда, за исключением самых маленьких организаций, применяется доменная модель. Примером доменной модели может служит сеть в Таврическом (Симферопольском) национальном университете. Студентам рекомендуется ознакомиться с архитектурой сети, с ее доменами, с информационными возможностями сети, с используемым программным обеспечением для поддержки учебного процесса и научных экспериментов и разработок.

Модель рабочей группы. Модель рабочей группы, известная также как *одноранговая* сеть, предоставляет минимальные возможности централизованного управления. В этой модели все ресурсы предоставляются и управляются членами рабочей группы. Иными словами, управление учетными записями осуществляется локально на каждом компьютере, при этом на нем поддерживается своя база данных учетных записей. Эта модель приемлема только для очень небольших сетей, где пользователей незначительное количество: однако с увеличением сложности сети усложняется и управление. Кроме того, в рабочей группе необязательно наличие Windows NT/2000 Server. Пользователи могут совместно обращаться к ресурсам рабочих станций, не реализуя выделенный сервер файлов, печати или приложений.

Доменная модель. Доменная (корпоративная) модель разработана фирмой Microsoft, чтобы удовлетворить требования к управлению сетью, растущие с увеличением рабочей группы. *В этой модели поддерживается централизованная база данных учетных записей пользователя и группы.* Доступ к ресурсам осуществляется на основе *прав пользователя и группы*, задаваемых для каждого ресурса. Пользователи и группы являются членами домена и поэтому представлены в *базе данных учетных записей* домена. При каждом доступе к ресурсу информация о пользователе из этой базы сравнивается *с правами доступа*, назначенными данному ресурсу, после чего доступ разрешается или запрещается.

Такая модель обеспечивает *высокий уровень защиты*. В отличие от модели рабочей группы доменная модель подходит и для маленьких, и для больших организаций. Таким образом, в корпоративной сети на первый план выходят следующие важные понятия: централизованный сетевой администратор, администратор пользователей, единый идентификатор пользователя, универсальный доступ к ресурсам. В Windows NT/2000 Server поддержкой доменной структуры занимаются службы каталога. Доменная структура службы каталога Windows NT/2000 Server обеспечивает:

- поддержку однократного входа в сеть для доступа ко всем разделяемым доменным ресурсам;
- централизованное управление ресурсами и учетными записями;
- реализацию служб для обновления информации о защите и сетевых учетных записях;
- поддержку паролей и учетных записей пользователя в разных средах;
- подключение служб каталога BackOffice, таких как службы управления аутентификацией и однократного входа в сеть, во всех приложениях BackOffice.

Для выполнения этих требований предназначены службы каталога Windows NT/2000 Server. Они поддерживают защищенную распределенную базу данных каталога и предоставляют услуги, как конечным пользователям, так и сетевым администраторам. Службы аутентификации позволяют каждому пользователю иметь единый идентификатор и пароль, который можно ввести с любой рабочей станции в сети и получить доступ к службам, приложениям и ресурсам, расположенным в любом месте сети. Для администраторов имеются графические средства управления и защиты. Все это облегчает создание и поддержку сетевых пользователей и их прав от рабочей группы до организации в целом.

Единый вход в сеть. Корпоративная сетевая среда должна поддерживают концепцию «один пользователь — одна учетная запись», благодаря чему пользователи могут подключаться к множеству серверов в рамках единого входа в сеть. При этом они избавлены от необходимости запоминать пароли для нескольких учетных записей.

Централизованное администрирование. Централизованный просмотр всей сети с любой ее рабочей станции позволяет контролировать информацию о пользователях, группах и ресурсах в распределенной сети. Единые учетная запись и пароль – это все, что нужно пользователю для доступа к сетевым ресурсам. Информация о защите и учетных записях. Службы должны обеспечивать приложениям защиту.

Поддержка паролей и учетных записей пользователя в разных средах. Пользователи могут обращаться к ресурсам любого домена, имея соответствующие права. Это справедливо независимо от местонахождения учетной записи. С единой учетной записью служб каталога Windows NT/2000 Server пользователь может войти в сеть из любой точки среды с *доверительными отношениями*. При наличии нескольких доменов один домен может *доверять* другому домену. *Доверяющий домен* разрешает пользователям *доверяемого домена* доступ к своим ресурсам.

Тема 2. Домен Windows NT/2000 Server.

Домен – это логическая группа сетевых серверов и других компьютеров, использующих общую информацию о защите и учетных записях. Обычно в рамках домена администратор создает одну учетную запись для каждого пользователя.

После этого пользователи входят в домен только один раз и не регистрируются на отдельных серверах этого домена.

Термин «домен» не относится к конкретному местоположению или специфической сетевой конфигурации. Компьютеры одного домена могут стоять рядом, являясь членами локальной вычислительной сети (ЛВС), или находиться в разных концах света, взаимодействуя через глобальную вычислительную сеть (ГВС). Взаимодействие через ГВС может осуществляться различными физическими способами, включая удаленный доступ, соединения Integrated Services Digital Network (ISDN), оптоволоконные, Ethernet, Token Ring, frame relay, спутниковые и по выделенным линиям.

Контроллеры домена. Контроллеры домена - это компьютеры под правлением Windows NT/2000 Server, разделяющие общую базу данных каталогов для хранения доменной информации о защите и учетных записях пользователя. Контроллеры домена используют информацию из базы данных каталога для аутентификации пользователей, регистрирующихся в домене. Контроллер домена может быть главным и резервным.

Главный контроллер домена. Главный контроллер домена (Primary Domain Controller, PDC) отслеживает изменения доменных учетных записей. Когда администратор вносит изменения в доменную учетную запись, они сохраняются в базе данных каталога на PDC. PDC — это единственный сервер в домене, который получает эти изменения напрямую. В домене может быть только один PDC.

Резервный контроллер домена. Резервный контроллер домена (Backup Domain Controller, BDC) хранит копию базы данных каталога. Она периодически автоматически синхронизируется с базой на PDC. Обычно BDC занимаются аутентификацией пользователей, но их можно повысить до PDC. В домене может быть несколько BDC.

Тема 3. Доверительные отношения

Домены могут быть связаны друг с другом доверительными отношениями. Доверительные отношения — это защищенный канал связи между двумя доменами. При наличии таких отношений домен может принимать учетные записи, созданные в других доменах, и позволять их владельцам обращаться к локальным ресурсам. Доверительные отношения могут быть односторонними и двухсторонними.

Односторонние доверительные отношения. При односторонних доверительных отношениях один домен предоставляет пользователям другого домена доступ к своим ресурсам. Точнее, один домен разрешает контроллерам домена в другом домене проверять подлинность учетных записей пользователя из другого домена при обращении к своим ресурсам. Ресурсы находятся в доверяющем домене, а учетные записи, которым разрешен доступ к ним, — в доверяемом. Однако, если пользователям из доверяющего домена нужны ресурсы доверяемого, надо установить двухсторонние доверительные отношения.

Двухсторонние доверительные отношения. Двухсторонние доверительные отношения состоят из двух односторонних, когда каждый домен принимает учетные записи другого домена. Пользователи могут регистрироваться в домене, содержащем их учетные записи из любого домена. Каждый домен может содержать ресурсы и учётные записи. Глобальные учетные записи пользователя и глобальные группы могут применяться в обоих доменах для назначения прав доступа к ресурсам любого домена. Иначе говоря, оба домена являются

доверяемыми.

Вопросы планирования.

При установке доверительных отношений фирма MICROSOFT предлагает руководствоваться следующими соображениями.

- Доверительные отношения можно установить только между доменами Windows NT/2000 Server.
- Физическое местоположение доменов не имеет значения.
- Использовать доверительные отношения по минимуму: чем их меньше, тем проще управлять сетью.
- Определить количество односторонних доверительных отношений. Например, продумать, достаточно ли односторонних доверительных отношений двух доменов, один из которых используется для учетных записей, а другой — для предоставления ресурсов, или все же сеть требует установки двухсторонних доверительных отношений, чтобы каждый домен мог использоваться как для хранения учетных записей, так и для предоставления ресурсов.
- Физическое или логическое местоположение пользователей не важно. Благодаря сквозной аутентификации пользователь может входить в систему с любого компьютера сети.
- Местоположение учетных записей пользователя имеет значение. Если учетная запись хранится в доверяемом домене, пользователь может входить в систему с любого компьютера любого домена.

Тема 4. Доменные модели.

Существует четыре типа доменных моделей, и у каждой свои преимущества: однодоменная, с одним главным доменом, с несколькими главными доменами и модель полностью доверительных отношений.

Однодоменная модель. Самая простая: включает один PDC и один или более BDC. PDC и каждый BDC могут поддерживать до 2 000 учетных записей для проверки подлинности пользователей и обеспечивать отказоустойчивость. Обычно эта модель подходит организациям, которым одновременно требуется централизованное управление учетными записями и простота администрирования.

Модель с одним главным доменом. Если сеть надо разбить на несколько доменов, но общее число пользователей не превышает максимально допустимого для одного домена, скорее всего лучшим выбором будет модель с одним главным доменом. Она объединяет преимущества централизованного администрирования и выгоду от наличия нескольких доменов. В соответствии с этой моделью один домен – главный – является центральной административной единицей для учетных записей пользователя и группы. Главный домен хранит все учетные записи. Другие домены содержат ресурсы: принтеры, серверы приложений и рабочие станции. Главный домен является доверяемым по отношению к этим доменам, аутентифицируя учетные записи и, таким образом, разрешая пользователям доступ к ресурсам. Если в компании есть отдел управления информационной системой (ИС) предприятия, в ведении которого находится и ЛВС, имеет смысл передать функции администрирования главного домена этому отделу, так как именно в главном домене хранятся все учетные записи пользователей и групп. Все пользователи входят в сеть, применяя учетные записи из главного домена. Ресурсы, такие как принтеры и серверы файлов, расположены в ресурсных доменах. Каждый такой домен имеет односторонние доверительные отношения с главным доменом, благодаря чему

пользователи с учетными записями из главного домена могут обращаться к ресурсам во всех доменах. Сетевой администратор может управлять всей многодоменной сетью из одной точки. Преимущество модели с одним главным доменом заключается в гибкости администрирования.

Модель с несколькими главными доменами. Эта модель включает два и более главных домена и несколько ресурсных доменов, каждый из которых доверяет всем главным доменам. Как и в модели с одним главным доменом, каждый главный домен служит хранилищем учетных записей, все учетные записи пользователя и глобальные группы создаются в одном из главных доменов. Отделы управления ИС могут централизованно управлять доменами. Сходство с моделью с одним главным доменом также в том, что остальные домены в сети не содержат учетных записей пользователя, а только предоставляют сетевые ресурсы, такие как серверы файлов и принтеры, и поддерживают только учетные записи компьютера. В данной модели каждый главный домен связан со всеми другими главными доменами двухсторонними доверительными отношениями. Каждый ресурсный домен имеет со всеми главными доменами односторонние доверительные отношения. Одни ресурсные домены также могут иметь доверительные отношения с другими ресурсными доменами, но это не обязательно. Так как каждая учетная запись существует в одном из главных доменов, а каждый ресурсный домен доверяет всем главным, любая учетная запись может использоваться в любом домене сети. Пользователи входят в тот домен, где хранится их учетная запись. В каждом главном домене должен существовать PDC и минимум один BDC.

Модель полностью доверительных отношений. В ней организуются двухсторонние доверительные отношения между всеми доменами в сети. Данную модель применяют, если надо распределить управление пользователями и ресурсами по разным отделениям, а не делать его централизованным. Каждый домен при этом связан двухсторонними доверительными отношениями со всеми другими доменами, так что ни один не контролирует другие. Модель полностью доверительных отношений распределяет управление пользователями, группами, доменами и ресурсами по различным отделам, а не централизует его.

Модель полностью доверительных отношений может быстро стать неуправляемой, но она обеспечивает следующие преимущества:

- ее могут использовать компании без централизованного отдела управления ИС;
- модель масштабируется до любого числа пользователей;
- каждый отдел полностью контролирует свои ресурсы и учетные записи;
    - как ресурсы, так и учетные записи пользователей сгруппированы в единицы, соответствующие отделам компании.

Тема 5. Характеристики Интернета и интрасетей.

В теме рассматриваются основные вопросы организации Интернет и, в том числе, WWW (World Wide Web) как графической среды Интернета. Обсуждаются проблемы защиты, связанные с подключением интрасети к Интернету.

Основные вопросы темы:

- описание функции и возможности IIS(INTERNET INFORMATION SERVER) и PWS(PEER WEB SERVICES), компонентов, поддерживающих взаимодействие интрасети и интернета;
- установка и настройка IIS;

- безопасность подключения интрасети к Интернету

Интернет – это сеть, объединяющая множество сетей по всему миру. *Интрасеть – это Интернет* в миниатюре. Она состоит из компьютеров, связанных локальными сетями.

Интернет глобальная сеть, связывающая компьютеры, которые используют общие протоколы. Интернет появился в начале 70-х. Первые его серверы поддерживали протоколы File Transfer Protocol (FTP) и Virtual Terminal Protocol (VTP, в настоящее время Telnet). Эти протоколы обеспечивали передачу файлов, ввод команд и удаленный запуск программ. Все операции выполнялись через символьный интерфейс.

Интернет имеет графический интерфейс. Главной графической службой стал World Wide Web (WWW, или Web). Пользователи создают Web-страницы, связанные между собой через Hypertext Transfer Protocol (HTTP). Каждая Web-страница, включая домашнюю страницу, имеет уникальный адрес - универсальный локатор ресурса (Uniform Resource Locator, URL), например, http://www.terry.uga.edu/~rsteuer/egypt/index.htm (страничка международной конференции MCDM, may 27-30, 2001) или http://www.intel.ru/ (информация фирмы INTEL в России).

Web-страницы являются гипертекстовыми документами - файлами, содержащими **гиперссылки** и форматированными с помощью языка *Hypertext Markup Language (HTML)*. Гиперссылки содержат адреса других Web-страниц и оформляются в виде подчеркнутого или раскрашенного текста или картинки. Щелкнув гиперссылку, можно перейти в то место Интернета, которое задано адресом из данной гиперссылки.

Web-серверы автоматически передают пользователям Интернета форматированный текст, картинки, звуки и видео. Для подключения к Web-серверу нужна специальная программа просмотра Интернета - броузер - например, Microsoft Internet Explorer или Netscape.

Интрасеть - это внутренняя сеть организации, использующая технологии Интернета, например, Web-серверы и броузеры, для улучшения обмена информацией и разработки приложений. Очень часто под интрасетью понимается TCP/IP-сеть, использующая технологии Интернета, но не являющаяся его частью. Интрасети называют еще корпоративными сетями. Интрасети имеют ответвления, называемые *экстрасетями (extranets). Экстрасети* являются агентами одной корпоративной сети в других интрасетях и способствуют деловому сотрудничеству между двумя или больше компаниями. Примером служат сети, организованные для поддержки внешних торговых операций, обмена документами между потребителем и поставщиком. Получается гибрид - и не частная сеть, и не Internet. Internet и интрасети кажутся похожими с точки зрения используемых технологий и предоставляемых функциональных возможностей, однако у них имеется ряд существенных и специфических черт. Глобальная корпоративная сеть Internet не является безопасной. Она предполагает всеобщий неограниченный доступ со стороны любых пользователей и групп пользователей, а также компаний, правительственных и исследовательских институтов и др. Это является как преимуществом так и недостатком этой глобальной сети. Интрасети не могут позволить себе такую неограниченную доступность. Доступ к информационным сетевым ресурсам даже для служащих компании следует предоставлять только в случае необходимости. Обычно для ограничения доступа из Internet к ресурсам

интрасети используются брандмауэры, списки доступа, системы безопасности на уровне сервера и приложений и др. Экстрасеть предполагает селективное объединение двух или более интрасетей в целях содействия деловому сотрудничеству. Ключевым условием для организации эффективной **экстрасети** является возможность снижения риска потери или разглашения конфиденциальной информации до "приемлемого уровня".

Тема 6. Вопросы безопасности при подключении к Интернету.

Интернет, как и любая другая сеть, предоставляет двухсторонний канал связи. Если компьютер «видит» компьютеры Интернета, то и те «видят» его. По умолчанию Windows NT/2000 защищает компьютер от случайного вторжения извне. Прежде чем устанавливать и настраивать TCP/IP и компоненты удаленного доступа к сети, компьютер следует защитить.

Защита узла интрасети, подключенного к Интернету.

Можно интегрировать корпоративную интрасеть с Интернетом на базе одной сетевой ОС. При этом надо обеспечить невозможность доступа к интрасети из Интернета. Не рекомендуется предоставлять полный доступ к интрасети пользователям из Интернета. Windows NT/2000 снабжена компонентами, поддерживающими взаимодействие интрасети и Интернета, - Internet Information Server (IIS) и Peer Web Services (PWS).

Эти службы позволяют Windows NT/2000-компьютерам предоставлять свои ресурсы и услуги пользователям интрасетей и Интернета. IIS и PWS - серверы файлов и приложений, использующие службы HTTP, Gopher и FTP для публикации информации в Интернете и интрасеть. HTTP используется для перемещения по гипертекстовых Web-документам и приложениям. Gopher формирует иерархическую систему ссылок на компьютеры и службы и организует ее в виде меню, а также аннотирует файлы и каталоги. FTP используется для передачи файлов между компьютерами в сети TCP/IP.

IIS и PWS поддерживают Internet Server Application Programming Interface (ISAPI). ISAPI позволяет создавать интерфейсы для клиент-серверных программ. Например, используя его, можно создать приложение, предоставляющее клиенту доступ к Web-странице и ввод информации в нее.

Рекомендации по защите узла Интернета и интрасети

Необходимо реализовать следующую политику учетных записей:

- Запретить использование пустых паролей.
- Задать минимальную длину пароля.
- Рекомендовать пользователям часто менять свои пароли. Пользователи при смене должны применять пароль, отличный от предыдущих.
- Задать блокировку учетной записи при многократных неудачных попытках зарегистрироваться.
- Разрешить только администратору снимать блокировку с учетных записей.
- Задать автоматическое принудительное отключение от сервера пользователей с ограниченным временем нахождения в системе.

Тема 7. Сетевые протоколы.

Одним из важнейших отличий между Windows NT/2000 Server и другими ОС является наличие в Windows NT/2000 Server встроенных сетевых возможностей. Для эффективного планирования корпоративной ИС требуется знание и понимание преимуществ и недостатков всех протоколов, поддерживаемых WinNT/2000.

1. TCP/IP;

2. NET BEUI;
3. NWLINK(совместимый IPX/SPX).

Transmission Control Protocol /Internet Protocol. Это стандартный набор протоколов для построения Интернета и интрасетей. Появился в 1969 году в Агенстве перспективных исследований Министерства обороны США в рамках эксперимента ARPANET.

Цель - создание высокоскоростных сетей связи. Преимущество TCP/IP.

1. Возможность взаимодействия различных ОС и аппаратных платформ.
2. Взаимодействие с Интернетом.
3. Маршрутизируемость.
4. Динамическое назначение IP-адресов с помощью протокола динамической хоста (DHCP).
5. Поддержка службой Windows Internet Name Service (WINS) динамической базы данных соответствия IP-адресов NetBIOS-именам.

Каждый интерфейс узла сети TCP/IP идентифицируется уникальным IP-адресом, который также несет в себе информацию о маршрутизации в объединенной сети. IP-адрес состоит из 32 битов, разделенных на 4 поля и обычно записывается в десятичном виде с точками между октетами: *ТНУ Сервер DNS - 195.5.61.20.*

Или произвольный IP-адрес

130.5.4.200=10000010.00000101.00000100.11001000.

В 32 битном адресе проводится логическая граница между двумя частями - идентификатором сети и идентификатором узла. Первый обозначает физическую сеть, второй узел сети. Объединенные в IP-адрес, они используются для адресации конкретного узла TCP/TP в конкретной сети. Для подключения к Интернету нужно использовать уникальные IP-адреса.

Классы сетей в Internet WinNT/2000.

Класс	**Число сетей**	**Число узлов**	**Первый октет диапазона адресов**
A	126	16111214	1-126
B	16384	65534	128-191
C	2097152	254	191-223

Маска подсети. Используется для разделения IP-адреса на части: идентификатор сети и идентификатор хоста. При взаимодействии хостов TCP/IP маска подсети используется для определения, в какой сети находится хост - локальной или удаленной. Нестандартная маска подсети позволяет разбить один идентификатор сети на несколько подсетей.

Основной шлюз. Это промежуточный хост сети или подсети, знающий адреса для идентификаторов других подсетей данной сети. Если с помощью маски подсети, хост - отправитель определяет, что хост- получатель не является членом локальной подсети, он передает пакеты основному шлюзу. Основной шлюз может направлять их другим шлюзам, пока данные не будут доставлены по адресу. Хостам TCP/IP можно назначить только один основной шлюз.

Domain Name System (DNS). DNS(доменная система именования) занимается преобразованием (разрешением) имен известных ей хостов в IP-адреса. DNS облегчает пользователям доступ к серверам Интернета. Например, проще запомнить имя www.microsoft.com чем IP-адрес этого сервера или

http://ccssu.crimea.ua/ адрес университетского сервера ТНУ г. Симферополь. Чтобы использовать DNS. на рабочей станции должен быть задан адрес. по крайней мере. одного сервера DNS. Эти адреса задаются одним из двух способов:

- *Статически (при настройке TCP/IP) на рабочей станции;*
- *Динамически (назначается DHCP-сервером).*

Dynamic Host Configuration Protocol (DHCP). Динамический протокол конфигурации хоста устраняет множество проблем. связанных с настройкой TCP/IP и управляет выделением конфигурационной информации TCP/IP. автоматически назначает IP-адреса компьютерам-DHCP-клиентам. DHCP выделяет хостам IP-адреса. Кроме IP-адреса DHCP также задает маску подсети. адрес основного шлюза и IP-адреса серверов Wins.

Агент-ретранслятор DHCP. Позволяет компьютеру передавать сообщения DHCP из одной ЛВС в другую. Например. сеть состоит из двух ЛВС (ЛВС1 и ЛВС2). соединенных маршрутизатором. В ЛВС1 расположен DHCP-сервер. В обычных условиях, чтобы компьютеры из ЛВС2 автоматически получали адрес надо разместить DHCP-сервер и в этой сети. Вместо этого устанавливают агент-ретранслятор DHCP на любом компьютере ЛВС2. и он через маршрутизатор будет передавать сообщения DHCP -серверу. находящемуся в ЛВС1.

Windows Internet Naming Service (WINS).

DNS: имена хостов → в IP- адреса.

WINS: NETBIOS-имена в IP-адреса.

WINS является сервером имен NetBIOS. В локальных подсетях WINS снижает количество широко вещательных запросов по разрешению имен NetBIOS . а также разрешает NetBIOS - имя из других подсетей. При взаимодействии между собой клиентов WINS. расположенных в разных подсетях. они узнают IP-адреса друг друга у WINS -сервера. а не с помощью запросов.

Routiny Information Protocol (RIP). RIP служит для обмена информацией между маршрутизаторами RIP маршрутизатор - это компьютер или другое устройство. которое обеспечивает рассылку маршрутной информации (такой, как сетевые адреса) и ретранслирует пакеты IP в смежные сети. RIP позволяет соседним маршрутизаторам обмениваться маршрутной информацией. С помощью RIP WINDOWS NT/2000 Server обеспечивает динамическое управление таблицами IP маршрутизации. что позволяет не заниматься формированием статистических таблиц. Если RIP для IP устанавливается на PC с единственной сетевой платой. он работает в режиме Silent Mode . В этом случае компьютер только прослушивает сообщения RIP и обновляет свою таблицу маршрутизации.

Routing & Remote Access Service реализует дополнительные возможности маршрутизации, удаленного доступа и виртуальной частной сети.

Возможности RRAS:

1. Единая служба маршрутизации и удаленного доступа. интегрированная ОС.
2. Полный набор протоколов маршрутизации для IP и Internet Packet Exchange (IPX). включая разработанный Bay Networks протокол Open Shortest Path First (OSPF).
3. Простой интуитивный графический интерфейс.
4. API для функций управления.
5. Защита на основе протокола PPTP(Point-to-Point Tunneling Protocol).
6. Поддержка клиентов RADIUS (Remote Authentication Dial - In User Service).

NET BEUI (Net BIOS Enhanced User Interface) был создан как простой и эффективный протокол для небольших ЛВС в которых не требуется маршрутизация. Реализация NET BEUI в Win NT/2000 обеспечивает:

1. Применение интерфейса транспортного драйвера эмулирующего интерпретацию сетевых команд Net Bios.
2. Применение спецификации интерфейса сетевых устройств (NetWork Device Interface Specification NDIS) версии 3 с улучшенной поддержкой транспорта и полным 32-разрядным асинхронным интерфейсом.
3. Снятие ограничения на количество Net BIOS.
4. Динамическое использование памяти.
5. Поддержку клиентов удаленного доступа с помощью служб RAS.
6. Передачу данных как с установлением соединения, так и без него.

NWLInk. Это совместимый с IPX/SPX протокол сетевой архитектуры WINDOWS NT/2000 Server. NTLInk не выходит за рамки сетевого протокола и сам по себе не обеспечивает серверу WINDOWS NT/2000 доступ к общим файлам и принтерам сервера NETWare , и сам не является таким сервером для клиентов NETWare. Для доступа к ресурсам сервера NETWare необходим редиректор, например, Gateway Service Netware (GSNW) в Windows NT/2000 Server. NWLink полезен при наличии клиент - серверных приложений NetWare, использующих (sockets) или NetBIOS поверх IPX/SPX. Клиентская часть может работать под управлением WinDOWS NT/2000, обращаться к серверной части на NetWare - сервере и наоборот.

Data Link Control (DLC). Не используется как основной сетевой протокол. Используется для двух задач:

- Доступ к *мэйнфреймам* IBM.
- Печати на принтерах HP.

Тема 8. Работа с DNS.

Domain Name System, DNS (доменная система именования) представляет собой распределенную БД, которая реализует иерархическую систему именования, предназначенную для идентификации хостов в Интернете. DNS была разработана в начале 80 годов. DNS-имена компьютеров состоят из имени хоста и домена, которые, соединяясь образуют полное доменное имя (Fully Qualified Domain Name, FQDN).

Процедура разрешения имен:

1. Клиент передает запрос своему локальному серверу имен.
2. Если локальный сервис имен не имеет запрашиваемых данных, он посылает запрос на другие серверы имен.
3. Получив требуемый адрес, локальный сервер имен возвращает информацию клиенту.

Доменная система имен (DNS) - это иерархично распределенный метод организации пространства имен в Internet, который переводит ответственность за подмножество имен на разные группы пользователей. Пример: ux.cso.uiuc.edu

edu-образование в США.
|
uiuc-все учебные заведения штата Иллинойс
| |
cso-группа департамента
| |
ux-пользователь

Домен edu включает все компьютеры учебных заведений США.
Каждая группа может изменять и производить новые имена(ответственность возлагаются на них). Новое имя нужно добавить в мировую БД. Для США приводится ниже таблица.

Домен	Использование домена
com	коммерческие, предприятия
edu	университеты, средние школы
gov	государственные организации
mil	военные
net	системы базовой сети
int	международные организации
org	остальные организации и предприятия

При использовании имени, компьютер изменяет его на нужный адрес. И передает имя серверу DNS. Возможны три случая:
1. Локальный сервер знает, где находится нужная информация.
2. Помнит, т.к. уже отвечал.
3. Не знает. Передает узлам сети.

• **edu.→ .uiuc.→ .cso.→ .ux .→**

Служба DNS Server.

Это служба имен в составе Windows NT/2000 Server. Она отвечает за преобразование FQDN в IP-адреса, используемые в объединенной сети. В Microsoft Internet Explorer указывается имя **ccssu.crimea.ua**, которое затем преобразуется сервером DNS в правильный IP -адрес Интернета.

Пространство имен доменов. БД DNS - это древовидная структура, называемая также пространством имен доменов (domain name space). Имя домена определяет его расположение в БД относительно родительского домена. Каждая часть имени домена DNS отделяется точкой. Например, доменное имя csu.edu определяет субдомен csu и его родительский домен edu, а доменное имя microsoft.com определяет субдомен microsoft и родительский домен com. Корневой узел БД DNS имени не имеет (пустой символ). Корневой узел обозначается в именах DNS концевой точкой. Например, в имени "microsoft.com." точка после com ссылается на корневой узел DNS.

Домены верхнего уровня. Корень и домены верхнего уровня БД DNS управляются Inter NIC. Практически во всем мире имена доменов верхнего уровня являются двухбуквенным кодом страны, например, uk-U.Kingdom, ru-Russiau, ua - Ukraine. В USA многие домены верхнего уровня обозначают организации и состоят из трех букв, com, edu и т.д.

Полные доменные имена. Кроме корня, все узлы в БД DNS имеют до 63 символов. У каждого субдомена должно быть имя, уникальное в пределах родительского домена. Это гарантирует уникальность имен DNS. Имена доменов DNS формируются путем прохождения дерева DNS снизу вверх до его корня. Имена узлов объединяются, отделяясь друг от друга точками. В конце, имени может стоять обозначающая корень необязательная точка. Такие имена называются полными доменными именами. Любой работающий под управлением WINDOWS и использующий протокол TCP/IP компьютер имеет два имени: имя Net BIOS и имя хоста. Имя Net BIOS - это имя компьютера, которое задается при установке

сетевых служб. Имя хоста формируется на основе имени компьютера. Как правило Net BIOS и имя хоста совпадают, но не обязательно.

Работа с DHCP. Протокол динамической конфигурации хоста (Dynamic Host Configuration Protocol) представляет собой открытый промышленный стандарт, разработанный с целью упрощения администрирования сетей, работающих на базе протокола TCP/IP. DHCP определяет методы упрощенного динамического конфигурирования в сетях TCP/IP, которые позволяют сократить объем работы администратора по добавлению, перемещению и конфигурированию компьютеров в подсетях. Для работы службы DHCP необходимо наличие компьютеров двух типов: серверов DHCP и клиентов DHCP. Первые определяют конфигурационные параметры вторых, и управляют параметрами. Как минимум DHCP предоставляют клиентам IP-адреса, маску подсети и адрес шлюза по умолчанию. Также клиенты получают от сервера DHCP IP-адреса DNS и Net BIOS - серверов имен, а также имя DNS.

Тема 9. Построение распределенных корпоративных СУБД на базе продуктов ORACLE.

Продукты семейства ORACLE, лидирующие в настоящее время в области корпоративных технологий, используют архитектуру типа клиент-сервер. Концепция распределенной обработки данных ORACLE обеспечивает ряд преимуществ. Распределенная БД – это сеть баз данных, размещенных на нескольких ORACLE SERVER, которые представляются пользователю как логически единая БД. Можно одновременно иметь доступ к данным, хранящимся на различных серверах. Каждая БД управляется своим собственным локальным сервером. Одним из идеологов и последовательным сторонником технологии клиент-сервер является глава фирмы ORACLE Ларри Эллисон. По его словам, в настоящее время как раз происходит перенос приложений с персональных компьютеров на серверы, причем на настольных компьютерах остается ряд приложений, таких как броузер, пакет Office, мультимедийный проигрыватель MPEG, mp3, mp4 файлов и некоторые другие (например, игры), поэтому "сегодня создавать приложения для персональных компьютеров очень не дальновидно". По словам же руководителей фирмы Microsoft броузерная модель, на которую делался немалый упор в течение последних нескольких лет, полностью себя исчерпала. Предлагается новая оптимальная концепция, которую уже называют (Бил Гейтс) "взаимодействие программных средств" - "software-to-software". На наш взгляд это пока наиболее оптимальная технология поддержки информационных процессов в век корпоративных систем и технологий. Одна технология дополняет другую. В такой технологии клиент более свободен от поведения сервера и может сам принимать важные решения, связанные с информационными технологиями. Обе фирмы и ORACLE и MICROSOFT внесли и вносят существенный вклад в развитие и поддержку современных корпоративных технологий. Их продукты совместно используются для организации корпоративных информационных сетей. В курсе "Корпоративные информационные системы" студенты специальности Экономическая кибернетика изучают вопросы организации корпоративных сетей на базе операционных систем Windows NT/2000 Server и UNIX, а также вопросы организации распределенных баз данных на основе продуктов фирмы ORACLE.

Литература

1. Корпоративные технологии. MICROSOFT CERTIFIED PROFESSIONAL. Microsoft Press. Учебный курс.
2. Д. Васкевич. Стратегии клиент/сервер. Диалектика : Киев. 1996г. - 396 с.
3. Использование ORACLE 8. Que Corporation. Диалектика. Киев.- 1998 г. – 75[illegible] с.
4. Laura Leman. Electronic WEB Workshop. Teach yourself Web Publishing with HTML 3.2 in a week. Third Edition. Sams.net. Indianapolis, Indiana. 1996.-581 P with 2 CD.
5. Microsoft Corp. Компьютерные сети. Microsoft Press. 1998г. 696 с. with CD.