Операционные системы, среды и оболочки

Особенности операционных систем семейства Windows

История ОС Windows

- Предшественником ОС Windows является одноименная операционная оболочка, появившаяся как надстройка над ОС DOS.
- Наиболее популярной оболочкой стала Windows 3.11 for Workgroup, где были реализованы многозадачность, графический интерфейс, поддержка одноранговой сети.
- Полноценная операционная система MS Windows появилась в 1995 г., как однопользовательская 32-разрядная операционная система, поддерживающая вытесняющую многозадачность, работу в сети, использование длинных имен и ряд других новых и удобных функций.
- Развитием линии явились операционные системы Windows’98, Windows ME.

История ОС Windows

- Другая линейка ОС корпорации Microsoft была связана с развитием операционной системы OS/2. Сетевая оболочка LAN Manager послужила основой для создания ОС Windows NT.
- В Windows NT реализован ряд важных решений: возможность организации двухуровневой сети, использование данной ОС для организации файлового сервера, сервера приложений, поддержка различных сетевых протоколов и сервисов, поддержка более надежной файловой системы NTFS.
- Windows NT 4.0 явилась настоящей сетевой ОС.

Особенности Windows 2000

- ОС Windows 2000 поддерживает службу каталогов Active Directory и на ее основе службу безопасности Public Key Infrastructure (PKI) и протокол Kerberos, терминальные службы, службы IIS.
- Система поддерживает до 4 Гб оперативной памяти и многопроцессорную симметричную обработку (SMP) – Windows 2000 Prof (до 2 процессоров), Windows 2000 Server SE (до 4 процессоров), Windows 2000 Sever AE (до 8 процессоров).

Особенности Windows 2000

- Windows 2000 рассчитана на рабочие станции и серверы;
- Отказоустойчива;
- Защищенная ОС;
- Содержит богатый набор утилит для администрирования локального компьютера и сети;
- Ядро ОС написано на C и C++, что обеспечивает переносимость ОС;
- Поддержка Unicode, что обеспечивает поддержку различных языков;
- Высокоэффективная подсистему управления памятью;
- Поддержка структурной обработки исключений (SEH), что облегчает восстановление после сбоев;
- Поддержка динамически подключаемых библиотек (DLL);
- Поддержка многопоточной и многопроцессорной обработки;
- Поддержка файловых систем NTFS, FAT, FAT32.

Администрирование системы

- Для управления операционной системой используются **консоль управления** – MMC. Отдельные инструменты управления компьютером или сетью объединяются в оснастки (snap-in).
- **Групповые политики** – технология управления, предназначенная для конфигурирования групп компьютеров и пользователей. Групповые политики сохраняются в виде объектов групповых политик (GPO), связанные с объектами Active Directory – областями (sites), доменами (domains), организационными единицами (ou). Групповые политики могут включать в себя параметры безопасности, параметры установки и поддержки ПО, загрузку и завершение работы системы.

Терминальные службы

- Терминальные службы позволяют клиентам Windows выполнять приложения на стороне сервера под управлением Windows 2000.
- Со стороны клиентской машины работает «тонкий клиент», требующий небольшой объем оперативной памяти и дискового пространства.
- С помощью терминальных служб создается собственная сессия пользователя независимая от остальных.

Взаимодействие с другими ОС

- Средства сетевого взаимодействия Windows 2000 позволяют:
  - Взаимодействовать с компьютерами UNIX и NetWare используя TCP/IP протокол;
  - Предоставлять компьютерам на базе UNIX, NetWare, Macintosh службы доступа к файлам и принтерам;
  - Использовать программное обеспечение открытого программного интерфейса подключения к базам данных (ODBC), службы очередей сообщений, объектной модели компонентов системы (COM+), позволяет новым приложениям взаимодействовать с существующими данными и ПО.

Сетевая и системная безопасность

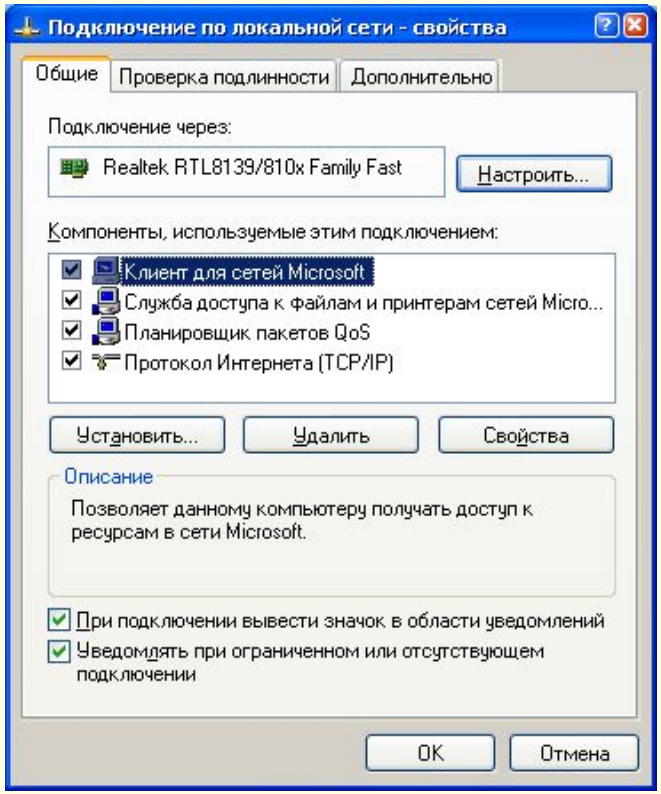
- Windows 2000 Server включает в себя средства, обеспечивающие полную поддержку протокола безопасности Kerberos 5, что позволяет обеспечить доступ к ресурсам предприятия, используя однократную регистрацию в системе.
- Сервер сертификатов с открытым ключом на основе X.509, интегрированный с Active Directory, использующий аутентификацию с открытым ключом;
- Поддержка защищенных смарт-карт для хранения личных паролей;
- Поддержка протокола IPSec (Internet Protocol Security).

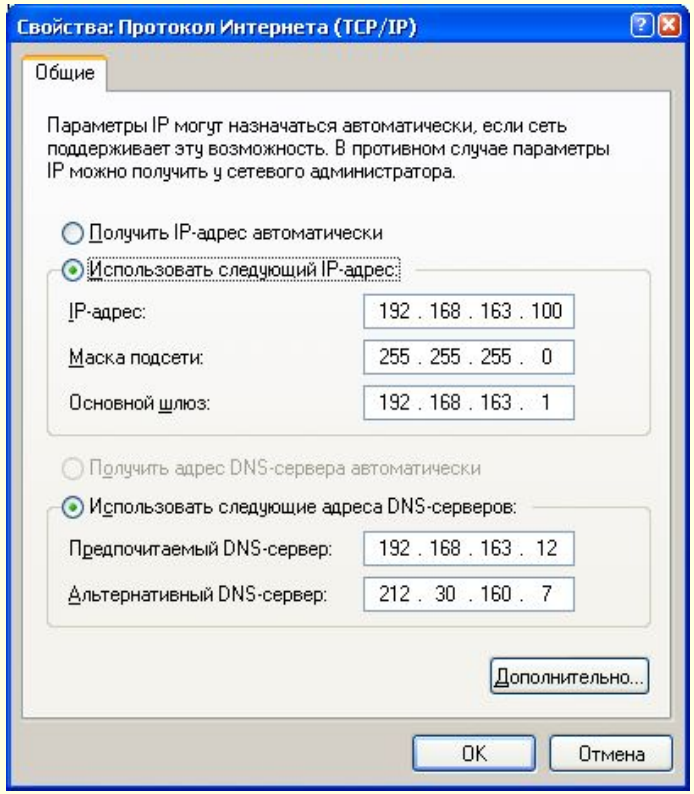
Поддержка аппаратного обеспечения

- В ОС Windows 2000 включена поддержка большого количества оборудования: принтеров, сканеров, модемов и др.
- Windows 2000 в полной мере поддерживает технологию Plug and Play (PnP);
- В операционной системе включена поддержка динамически подгружаемых драйверов.

Первоначальная настройка сети

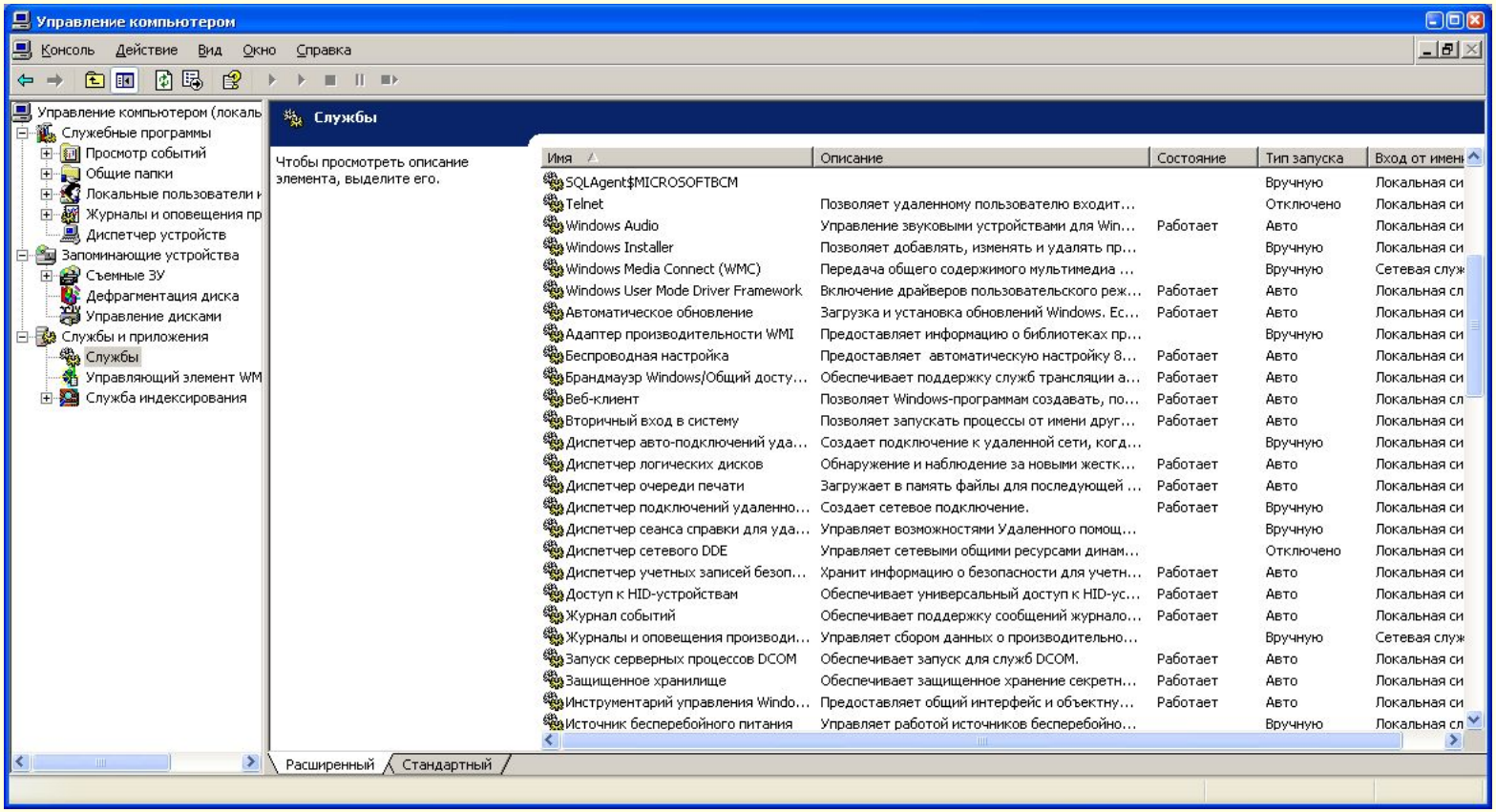
- При настройке сетевых интерфейсов необходимо установить протокол TCP/IP и выполнить конфигурирование системы





Управление службами

- Для управления службами можно использовать GUI интерфейс.



Команды обслуживания сети

- При работе с сетевым окружением администратору необходимо иметь инструменты управления и обслуживания сети. Команды работы с сетью разделяются на категории:
  - Диагностика
  - Устранение неполадок
  - Конфигурирование

Диагностика сети

- Команды диагностики в реальном времени предоставляют информацию о работе сети и сетевых подключений. К числу команд диагностики сети относятся команды
  - **netstat** (команда выводит статистику протокола и текущие сетевые подключения TCP/IP)
  - Синтаксис
    - **netstat** [**-a**] [**-e**] [**-n**] [**-o**] [**-p** *протокол*] [**-r**] [**-s**] [*интервал*]
  - **Параметры**
    - **-a** Вывод всех активных подключений TCP и прослушиваемых компьютером портов TCP и UDP.
    - **-e** Вывод статистики Ethernet, например количества отправленных и принятых байтов и пакетов. Этот параметр может комбинироваться с ключом **-s**.
    - **-n** Вывод активных подключений TCP с отображением адресов и номеров портов в числовом формате без попыток определения имен.
    - **-o** вывод активных подключений TCP и включение кода процесса (PID) для каждого подключения. Код процесса позволяет найти приложение на вкладке **Процессы** диспетчера задач Windows. Этот параметр может комбинироваться с ключами **-a**, **-n** и **-p**.
    - **-p** *протокол* Вывод подключений для протокола, указанного параметром *протокол*. В этом случае параметр *протокол* может принимать значения **tcp**, **udp**, **tcpv6** или **udpv6**. Если данный параметр используется с ключом **-s** для вывода статистики по протоколу, параметр *протокол* может иметь значение **tcp**, **udp**, **icmp**, **ip**, **tcpv6**, **udpv6**, **icmpv6** или **ipv6**.
    - **-s** Вывод статистики по протоколу. По умолчанию выводится статистика для протоколов TCP, UDP, ICMP и IP. Если установлен протокол IPv6 для Windows XP, отображается статистика для протоколов TCP через IPv6, UDP через IPv6, ICMPv6 и IPv6. Параметр **-p** может использоваться для указания набора протоколов.
    - **-r** Вывод содержимого таблицы маршрутизации IP. Эта команда эквивалентна команде **route print**.
    - *интервал* Обновление выбранных данных с интервалом, определенным параметром *интервал* (в секундах). Нажатие клавиш CTRL+C останавливает обновление. Если этот параметр пропущен, **netstat** выводит выбранные данные только один раз.
    - **/?** Отображение справки в командной строке.

Диагностика сети

- Команда netdiag позволяет выводить статистику и выполнять диагностику сетевого интерфейса.
  - Синтаксис: netdiag [/опции]
  - Опции:
    - /q - Quiet output (errors only)
    - /v - Verbose output
    - /l - Log output to NetDiag.log
    - /debug - Even more verbose.
    - /d:<DomainName> - Find a DC in the specified domain.
    - /fix - fix trivial problems.
    - /DcAccountEnum - Enumerate DC machine accounts.
    - /test:<test name>
    - /? вызов подсказки
  - netdiag /test:server выводит статистику и запускает диагностику сетевой карты

Конфигурирование сети

- Для просмотра конфигурации сетевых интерфейсов используется команда ipconfig
  - Синтаксис:
- ipconfig [/? | /all | /release [адаптер] | /renew [адаптер] |
- /flushdns | /displaydns /registerdns |
- /showclassid адаптер |
- /setclassid адаптер [устанавливаемый_код_класса_dhcp]]
  - ключи:
    - /? Отобразить это справочное сообщение.
    - /all Отобразить полную информацию о настройке параметров.
    - /release Освободить IP-адрес для указанного адаптера.
    - /renew Обновить IP-адрес для указанного адаптера.
    - /flushdns Очистить кэш разрешений DNS.
    - /registerdns Обновить все DHCP-аренды и перерегистрировать DNS-имена
    - /displaydns Отобразить содержимое кэша разрешений DNS.
    - /showclassid Отобразить все допустимые для этого адаптера коды (IDs) ыDHCP-классов.
    - /setclassid Изменить код (ID) DHCP-класса.

Конфигурирование сети

- Для конфигурирования сети может быть использована команда route. Данная команда управляет таблицами маршрутов.
  - ROUTE [-f] [-p] [команда [узел] [MASK маска] [шлюз] [METRIC метрика] [IF-интерфейс]
    - -f Очистка таблиц маршрутов от записей для всех шлюзов. При указании одной из команд, таблицы очищаются до выполнения команды.
    - -p При использовании с командой ADD задает сохранение маршрута при перезагрузке системы. По умолчанию маршруты не сохраняются при перезагрузке. Игнорируется для остальных команд изменяющих соответствующие постоянные маршруты.
    - команда:
      - PRINT Печать маршрута
      - ADD Добавление маршрута
      - DELETE Удаление маршрута
      - CHANGE Изменение существующего маршрута
    - узел Адресуемый узел.
    - MASK Если вводится ключевое слово MASK, то следующий параметр интерпретируется как параметр "маска".
    - маска Значение маски подсети, связываемое с записью для данного маршрута. Если этот параметр не задан, по умолчанию подразумевается 255.255.255.255.
    - шлюз Шлюз.
    - METRIC Определение параметра метрика/цена для адресуемого узла.

Сетевые службы

- В основе серверных функций операционной системы Windows лежат специальные службы. **Служба** – программа, выполняющая некоторую базовую задачу в фоновом режиме.
- Примеры служб Windows
  - Alerter (оповещатель)
  - Browser (обозреватель)
  - Clipbook (сервер папки обмена)
  - Dhcp client
  - Messenger
  - Netlogon
  - Server
  - Workstation
  - Spooler

Сетевые службы

- Служба Workstation позволяет организовать доступ компьютеров к информации и данным, расположенным на других компьютерах сети.
- Возможности службы workstation могут быть настроены с помощью команды net config workstation
- net config workstation /charwait:<sec> - задает время, которое должно пройти прежде, чем будет превышен лимит времени для устройства и оно не будет больше признаваться сетью.

Сетевые службы

- Служба Server другим системам, подключенным к сети, получать доступ к данным компьютера. Серверные платформы запускают данную службу автоматически, для операционных систем Windows 2000/XP Professional служба запускается, если установлена служба File and Printer Sharing.
- Конфигурирование службы выполняется с помощью команды net config server:
  - Net config server /autodisconnect:<min> - задает количество времени, в течение которого соединение может не использоваться, прежде чем прекратить текущий сеанс (по умолчанию 15 мин)
  - Net config server /hidden:yes|no – удаляет имя системы из списка сервера
  - Net config server /srvcomment:”text” – выводит текстовое сообщение или описание с именем компьютера

Мониторинг служб

- Для мониторинга служб Workstation и Server используются команды:
  - Net statistics workstation – выводит статистику соединений, работы в сети и сеансов для службы со времени ее последнего запуска
  - Net statistics server – выводит статистику сеансов, нарушения безопасности и информацию о доступе к устройствам сервера со времени ее последнего запуска
  - Net session – используется для определения соединений с текущим сервером, а также управления соединениями
    - Net session – отображает все текущие подключения к серверу
    - Net session \\<компьютер> /delete – завершает подключения между сервером и указанным компьютером
  - Net file – показывает список открытых файлов на сервере. Для принудительного закрытия файла используется команда
    - Net file <code file>\close

Просмотр сетевых компонентов

- Для просмотра содержимого в сети используется команда net view. Используя службу workstation данная команда обращается к главному браузеру сети и просматривает хранящийся на нем список компьютеров.
  - Net view – выводит список компьютеров, содержащих общие ресурсы
  - Net view /domain:<domain> - выводит список входящих в домен систем
  - Net view \\<компьютер> - выводит список общих ресурсов компьютера

Использование сетевых ресурсов

- Для подключения сетевого ресурса к системе и задания ему имени используется команда net use
  - **net use** [{*имя_устройства* | ***}] [*имя_компьютера**ресурс*[*том*]] [{*пароль* | ***}]] [**/user:**[*имя_домена*\]] [**/user:**[*имя_домена_с_точкой*\]*имя_пользователя*] [**/user:**[*имя_пользователя*@*имя_домена_с_точкой*] [**/savecred**] [**/smartcard**] [{**/delete** | **/persistent:**{**yes** | **no**}}]
  - **/savecred**
    - Сохраняет введенные учётные данные для дальнейшего использования.
  - **/smartcard**
    - Указывает необходимость считывания учетных данных со смарт-карты для сетевого подключения. При наличии нескольких смарт-карт появится запрос на указание одной из них.
  - **/delete**
    - Отменяет указанное сетевое подключение. Если подключение задано с символом звездочки (*), будут отменены все сетевые подключения.
  - **/persistent:{yes** | **no}**
    - Управляет постоянными сетевыми подключениями. По умолчанию берется последнее использованное значение. Подключения без устройства не являются постоянными. Выбор значения **Yes** приводит к сохранению всех существующих соединений и восстанавлению их при следующем подключении. При выборе значения **No** выполняемые и последующие подключения не сохраняются. Существующие подключения восстанавливаются при следующем входе в систему. Для удаления постоянных подключений используется ключ **/delete**.
  - **/home**
    - Подключает пользователя к его основному каталогу.

Службы каталогов

- Основная цель объединения компьютеров в вычислительную сеть – обеспечение совместного использования ресурсов.
- Одна из основных решаемых задач – реализация оптимального метода организации общих ресурсов.
- В крупной организации речь идет о множестве ресурсов и множестве потребителей данных ресурсов. Для эффективного управления такими списками применяются разные методы. Один из методов – развертывание *службы каталогов*.
- Служба каталогов – сетевая служба позволяющая пользователям получить доступ к ресурсу без знания точного месторасположения ресурса.
- При использовании службы каталогов вся информация об объектах сети объединяется в каталог (directory).
- Внутри каталога объекты организуются в соответствии с физической или логической структурой сети.

Службы каталогов

- Службы каталогов решают следующие задачи:
  - **Управление сетевыми ресурсами**. Служба каталогов облегчает пользователям поиск необходимых ресурсов, скрывая подробности реализации механизма поиска.
  - **Управление пользователями**. Каждый пользователь в сети идентифицируется набором реквизитов. Это позволяет осуществлять управление доступом к сетевым ресурсам.
  - **Управление приложениями**. В крупных вычислительных сетях возникает задача централизованного управления программным обеспечением, включая развертывание новых приложений и обновление существующих.
  - **Обеспечение функционирования сети**. Использование службы каталогов позволяет решить вопросы выделения IP-адресов, других параметров сети.
- **Сети Microsoft организуются с использованием службы каталогов Active Directory.**

Пространство имен X.500 и протокол LDAP

- Пространство имен (в соответствии со стандартом X.500) представляет собой иерархическую структуру имен, которая идентифицирует уникальный путь к контейнеру службы каталога.
- Это пространство имен определяется в числовой (точечной) нотации или в строковой.
- В строковой нотации пользовательский объект представляемый как:
  - cn=Dmitry, cn=Users, dc=Rosnou, dc=ru
  - Для удовлетворения требованию уникальности в пространстве имен X.500 в домене Rosnou.ru в контейнере Users может быть единственное имя Dmitry.

Протокол LDAP

- Протокол LDAP (облегченный протокол службы каталогов) является протоколом доступа. В данном протоколе для именования объектов используется система *характерных имен (Distinguish Name)*, предоставляющая информацию обо всех узлах дерева каталогов.
- Представление иерархии имен LDAP имеет вид:
  - LDAP: // cn=Dmitry, cn=Users, ou=faculty, dc=Rosnou, dc=ru
  - При записи характерного имени используются специальные ключевые слова:
    - DC – составная часть доменного имени;
    - OU – организационная единица;
    - CN – общее имя.
  - Имя, идентифицирующее сам объект, согласно терминологии LDAP, выступает в качестве относительного характерного имени. Относительное имя может быть не уникальным в рамках всего дерево, но должно быть уникальным в пределах контейнера.
  - *Каноническое имя* подобно характерному имени, за исключением того, что опускаются сокращения, обозначающие тип контейнера:
    - Rosnou.ru/faculty/Users/Dmitry

Использование имен объектов системы

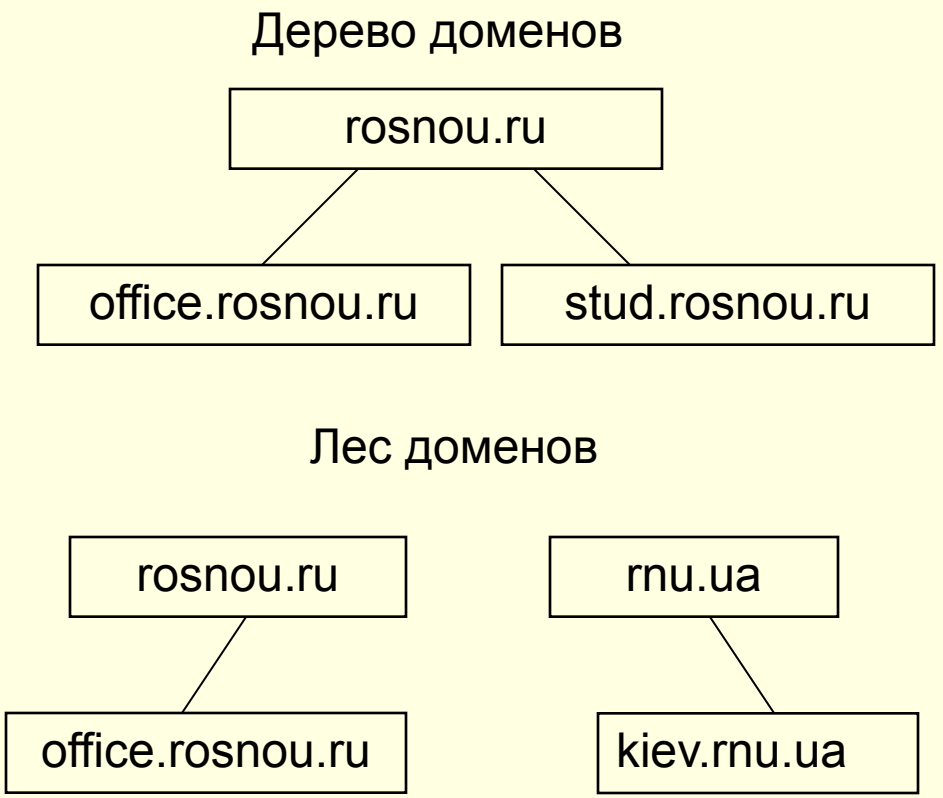
- Другой способ именования объектов – использование *основных имен* субъектов системы безопасности.
- Основное имя субъекта системы безопасности имеет вид:
  - <имя субъекта>@<суффикс основного имени>
  - В качестве суффикса основного имени выступает имя домена, которому принадлежит данный субъект
  - Пример основного имени пользователя:
    - dmitry@rosnou.ru
- Глобальные идентификаторы. Для обеспечения уникальности объектов и облегчения поиска, каждому объекту ставится в соответствие 128-разрядное число – *глобальный уникальный идентификатор.*
- Данный идентификатор является обязательным атрибутом любого объекта, который не изменяется ни при каких обстоятельствах.

Доменная модель службы каталогов

- В рамках каталога Active Directory одним из основных понятий является понятие **домена** – совокупность компьютеров, характеризующихся наличием общей базы учетных записей пользователей и единой политики безопасности.
- Использование доменов позволяет разделить пространство имен на несколько фрагментов. Каждый объект может принадлежать **только** одному домену.
- Цели создания доменов:
  - **Разграничение административных полномочий.**
  - **Создание единой политики безопасности.**
  - **Разделение доменного контекста имен.**
- Центральным компонентом домена выступают серверы, хранящие фрагменты каталогов. Такие серверы называются **контроллерами домена**.

Иерархия доменов

- Windows позволяет организовать разные типа иерархии доменов.
  - Отношение между доменами по схеме «родитель-потомок». Имя дочернего домена включает в себя имя родительского домена.
  - Отношения, включающие несколько связанных деревьев – лес доменов (forest).



Доверительные отношения

- Для объединения объектов, хранящихся в разных доменов должны существовать определенные связи – *доверительные отношения*.
- Механизм установленных доверительных отношений позволяет организовать процесс аутентификации объектов и субъектов системы.
- Выделяют два типа доверительных отношений:
  - **Односторонние доверительные отношения**
  - **Двусторонние доверительные отношения**

Контроллеры домена

- Контроллеры домена в доменах Windows отвечают за аутентификацию пользователей и содержат фрагмент каталога.
- Некоторые операции могут выполняться только одним контроллером. Эти операции называются *операции с одним исполнителем (flexible single-master operations – FSMO).*
- Контроллеры доменов могут выполнять специализированные роли:
  - **Роли, требующие уникальности в пределах всего леса доменов:**
    - **Исполнитель роли владельца доменных имен**
    - **Исполнитель роли владельца схемы**
  - **Роли, требующие уникальности в пределах домена:**
    - **Исполнитель роли владельца идентификаторов**
    - **Исполнитель роли эмулятора основного контроллера домена**
    - **Исполнитель роли владельца инфраструктуры каталога.**
- По умолчанию все данные роли возлагаются на первый контроллер домена, установленный в лесе.
- Процесс принудительной передачи функций специализированной роли другому контроллеру называется *захватом роли*.

Раздел глобального каталога

- *Глобальный каталог* – специализированная база данных, содержащая фрагменты всех доменных контекстов имен.
- Для исключения чрезмерного разрастания базы данных в нее включены значения только наиболее часто используемых атрибутов.
- Контроллер домена, выступающий в качестве носителя такой базы данных, называется *сервером глобального каталога*. Он выполняется следующие функции:
  - *Предоставление пользователям возможности поиска объектов в лесу доменов по атрибутам*
  - *Разрешение основного имени пользователя*
  - *Предоставление информации о членстве пользователя в различных группах с универсальной областью действия.*
- В лесу доменов присутствует по крайней мере один сервер глобального каталога. По умолчанию это первый контроллер созданный в домене.

Другие разделы

- **Раздел конфигурации** – используется для размещения сведений о структуре системы: список всех доменов и деревьев леса, перечень существующих контроллеров домена и серверов глобального каталога.
- **Доменный раздел** – используется для размещения объектов, являющихся непосредственно частью домена. Здесь хранятся объекты, ассоциированные с пользователями, компьютерами, общими ресурсами. Данный раздел передается в рамках домена.
- **Разделы приложений** – могут быть созданы для различных сетевых приложений. Разделы могут быть созданы администратором вручную или самими приложениями при помощи интерфейса программирования ADSI (Active Directory Service Interfaces). Создание таких разделов позволяет обращаться к приложениям используя общий подход доменных имен.

Организационные единицы

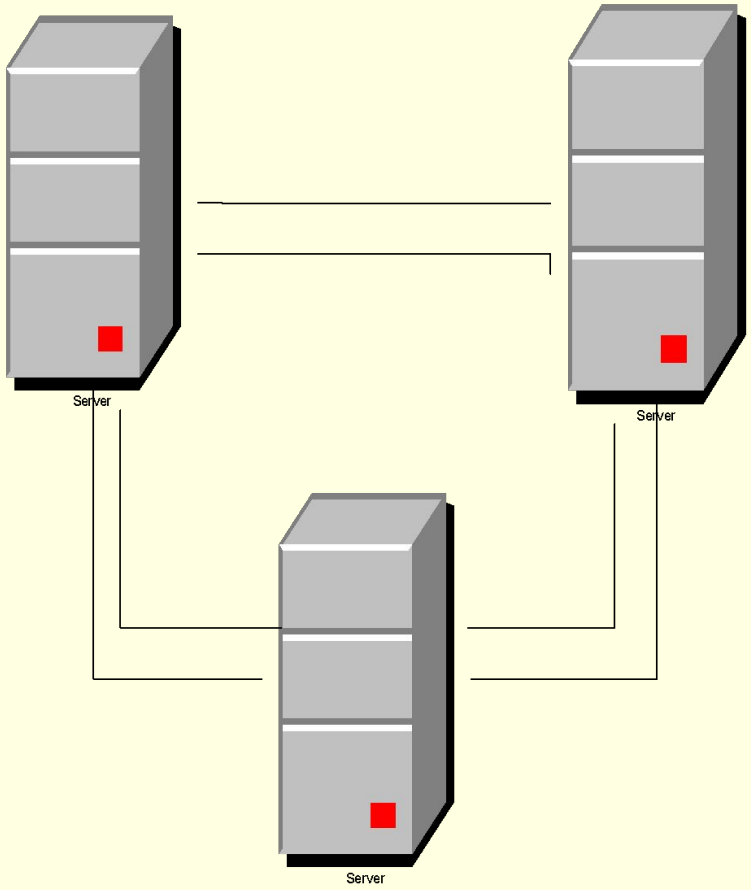
- В структуре службы каталога можно использовать специальные объекты контейнерного типа, позволяющие группировать объекты. Такими объектами являются *организационные единицы*, позволяющие объединять объекты в логическую структуру. Используются для упрощения управления входящими в них объектами.
- Иерархия организационных единиц образуется только в пределах домена. Организационные единицы принадлежащие разным доменам леса не связаны друг сдругом.

Физическая структура каталога. Репликация данных.

- Корпоративная сеть – совокупность подсетей, соединенных между собой линиями связи.
- Под узлом (site) в сетях Windows понимается совокупность подсетей объединенных высокоскоростными линиями связи.
- В структуре каталога существует специальный класс объектов, описывающий связи между узлами, - *соединение узлов.*
- Каждое соединение как объект каталога имеет следующие атрибуты:
  - Стоимость соединения
  - Расписание доступности соединения
  - Интервал репликации
  - Транспорт репликации
    - В качестве транспорта используются протоколы RPC и SMTP

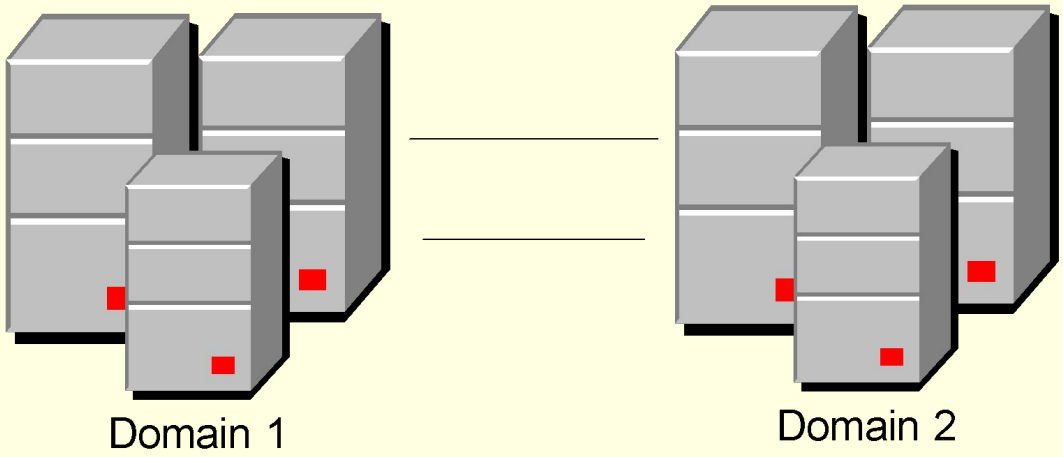
Репликация внутри узла

- При репликации баз данных каталога внутри узла осуществляется автоматически. В процессе репликации используется кольцевая топология (двунаправленное кольцо).
- В процессе репликации применяется протокол RPC. Используется *синхронное взаимодействие* – принимающий партнер, отправляя запрос, ожидает ответа от передающего партнера.



Репликации между узлами

- Одной из причин объединения подсетей в узлы – необходимость управления процессом репликации между контроллерами домена на медленных линиях связи.
- В процессе репликации между узлами передается только информация об изменениях в схеме и данных конфигурации. Для серверов глобального каталога – данные о подмножестве объектов всех доменов, образующих лес.
- При передаче используются два протоколы: RPC и SMTP – для асинхронного взаимодействия.
- При репликации между узлами существенную роль играют *мостовые серверы*.



Управление службой Active Directory

- Для управления службой каталогов Active Directory используются специальные средства администрирования.

- Утилиты администрирования службы каталогов:
  - . Active Directory – пользователи и компьютеры
  - Active Directory – домены и доверие
  - Active Directory – сайты и службы