Глава 8

Работа с сетью

- **Создание сетевого подключения**
- **Работа с удаленным помощником**
- **Терминальные службы**
- **Новые возможности программ командной строки**
- **Протокол iSCSI**
- **Создание общих папок**
- **Удаленное управление операционной системой**
- **Команды rundll32.exe для доступа к сетевым возможностям**
- **Стандартные классы репозитария CIM**

Немаловажной частью работы любого администратора (да и любого пользователя, имеющего несколько компьютеров) является настройка сетевых компонентов операционной системы и подключение компьютера к сети организации. Ранее в этой книге вообще не затрагивался вопрос настройки сетевых компонентов операционной системы Windows Vista. Этой теме будет посвящена восьмая глава.

8.1. Создание сетевого подключения

Настройка сетевого подключения в операционной системе Windows Vista выполняется немного сложнее, чем в предыдущих версиях. Это связано как с новыми механизмами защиты, реализованными в Windows Vista (NAP и новый стандартный брандмауэр), так и с другими проблемами работы сетевого подключения.

Использование сетевого кабеля

Как только вы соедините два компьютера сетевым кабелем, перед вами отобразится окно Настройка сетевого размещения (в книге рассматривается настройка сетевых соединений только в операционной системе Windows Vista). С его помощью можно определить, каким является устанавливаемое вами соединение: частным или публичным.

Типы сетей

Частным соединением в операционной системе Windows Vista считается локальное соединение нескольких компьютеров, которые не подключены к таким глобальным сетям, как Интернет. Ограничения, налагаемые операционной системой и стандартным брандмауэром на подобные сети, менее жестки, чем налагаемые на публичные сети.

Публичными же сетями считаются такие, доступ к которым можно получить удаленным пользователям по модемным или другим линиям через Интернет. Естественно, что публичные сети представляют большую угрозу вашему компьютеру, поэтому их использование ограничено в операционной системе Windows Vista сильнее, и, следовательно, настраивать их немного сложнее.

Именно поэтому, если вы создаете сетевые подключения впервые, лучше всего назначить их частными. Тем более что вы в любой момент сможете изменить категорию сетевого подключения, сделав его публичным.

После того как вы нажмете кнопку OK окна Настройка сетевого размещения, значок сетевого подключения, отображаемый в области уведомления, будет показывать, что сетевое соединение установлено. Однако пока что вы не сможете воспользоваться данным сетевым подключением, так как вашему компьютеру еще не были назначены IP-адрес и маска подсети.

Чтобы назначить IP-адрес вашему компьютеру, нужно в контекстном меню значка сетевого подключения, отображаемого в области уведомления, выбрать коман-

ду Центр управления сетями и общим доступом, после чего отобразится одноименный мастер (рис. 8.1). Его также можно вызвать с помощью значка Центр управления сетями и общим доступом папки Панель управления.

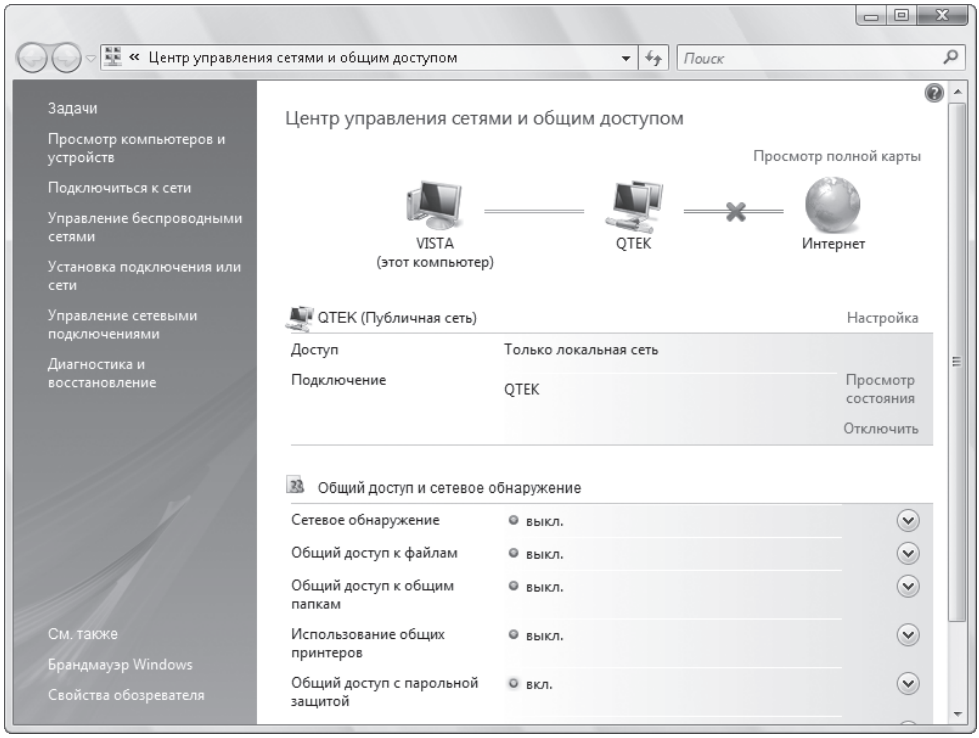

Рис. 8.1. Мастер Центр управления сетями и общим доступом

Мастер Центр управления сетями и общим доступом

Окно мастера состоит из нескольких частей.

Поле в верхней части мастера справа. Данное поле графически показывает состояние вашего сетевого подключения (карту сети). В центре рисунка отображается ваша сеть. Слева от нее ваш компьютер, а справа указывается, есть ли доступ к Интернету. Если сетевое подключение установлено, то оно отображается зеленой линией между значком сети и вашим компьютером или Интернетом. Если же сетевое подключение отсутствует, то линия перечеркнута красным крестиком.

Обратите внимание на ссылку Просмотр полной карты данного поля. После ее выбора перед вами отобразится мастер Карта сети, с помощью которого можно просмотреть карту сети для всех сетевых подключений. Для этого достаточно выбрать конкретное сетевое подключение из списка Карта сети. В нижней части мастера можно также увидеть список сетевых устройств, которые не участвуют в построении карты сети. Например, к таким устройствам по умолчанию относится соединение Общий доступ к сети Интернет.

ПРИМЕЧАНИЕ

Вы можете запретить использование ICS на компьютере домена с помощью групповой политики Запретить использование общего доступа к подключению Интернета в сети DNS-домена, расположенной в разделе Конфигурация компьютера ▸ Административные шаблоны ▸ Сеть ▸ Сетевые подключения. Данная политика изменяет значение параметра REG_DWORD-типа NC_ShowSharedAccessUI, расположенного в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Network Connections.

Поле с описанием сети в центре правой части мастера. Данное поле отображает дополнительные сведения о сети: название сетевого соединения, указание, является оно частным или публичным. Кроме того, данное поле имеет несколько ссылок, позволяющих настроить важные параметры работы сетевого соединения. К ним относятся следующие.

- Настройка — позволяет изменить тип данного сетевого подключения на публичный или частный.
- Просмотр состояния — отображает окно Состояние для данного сетевого адаптера. Именно с его помощью можно изменить IP-адрес компьютера, поэтому мы рассмотрим его отдельно немного дальше.

Поле Общий доступ и сетевое обнаружение в нижней части мастера справа. С помощью данного поля можно определить, будут ли разрешены создание и доступ к общим папками на данном компьютере, а также параметры доступа к общим папкам. Возможности данного поля будут описаны в разд. 8.6.

Панель ссылок в левой части мастера. Слева от основного поля мастера Центр управления сетями и общим доступом находится панель ссылок, которая позволяет отобразить другие мастера для настройки сетевого соединения. В ней содержатся следующие ссылки.

- Просмотр компьютеров и устройств — отображает папку Сеть. Она содержит список всех компьютеров и устройств, входящих в созданную вами сеть. Пока вы не настроите IP-адрес вашего компьютера и его рабочую группу, данная папка будет пуста.
- Подключиться к сети — открывает одноименный мастер, с помощью которого можно легко настроить любое сетевое соединение или просмотреть список уже созданных сетей. Чтобы создать сетевое соединение с помощью данного мастера, нужно выбрать ссылку Установка подключения или сети. После этого отобразится список сетевых соединений, которые вы можете создать с его помощью (рис. 8.2). Он содержит следующие элементы.
  - Настройка беспроводной сети компьютер–компьютер — позволяет создать непостоянное беспроводное соединение между двумя компьютерами (одноранговое соединение).
  - Подключение к беспроводной сети вручную — дает возможность создать беспроводное соединение с точкой доступа или между двумя беспроводными сетевыми адаптерами.

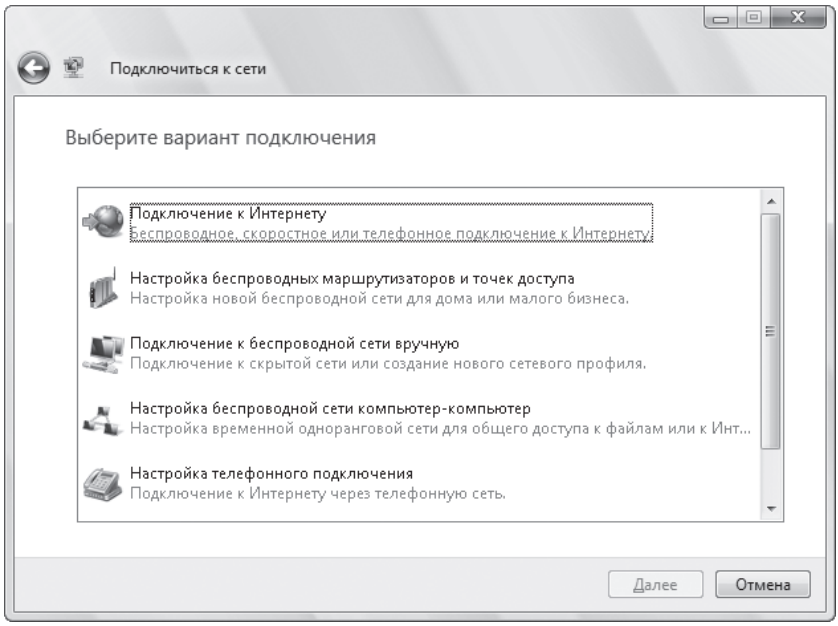

Рис. 8.2. Окно для выбора варианта подключения

- Подключение к Интернету — дает возможность создать подключение к Интернету с помощью модема, DSL или беспроводной сети.
- Настройка телефонного подключения — позволяет создать подключение к Интернету с помощью модема.
- Подключение к рабочему месту — дает возможность создать соединение с удаленной сетью с помощью модема или VPN. Технология VPN позволяет выполнить подключение к локальной сети через Интернет. Это достигается путем туннелирования (создания туннеля между двумя компьютерами через Интернет, по которому будут передаваться данные). После того как вы создадите VPN-подключение, его значок отобразится в папке Сетевые подключения (которая отображается с помощью ссылки Управление сетевыми подключениями мастера Центр управления сетями и общим доступом). С помощью команды Свойства контекстного меню данного значка можно изменить основные настройки подключения VPN. Если же нужно выполнить подключение, достаточно воспользоваться командой Подключить в контекстном меню значка.

ПРИМЕЧАНИЕ

Для работы VPN необходимо, чтобы на сервере был открыт порт 1723/TCP, а на клиенте — порты 1024–65535/TCP (они необходимы для работы протокола PPTP). Если же для создания VPN используется протокол L2TP, то на сервере должен быть открыт порт 1701. Также необходимо, чтобы на всех маршрутизаторах туннеля был открыт порт 500 (он используется протоколом IKE).

Для работы VPN между клиентом и сервером не должны находиться устройства преобразования сетевых адресов (NAT), так как после того как они выполнят замену адреса у зашифрованного пакета VPN, его целостность будет нарушена.

Для нормальной работы VPN также необходим достоверный сертификат компьютера.

- Подключение к сети — дает возможность создать сетевое соединение с использованием сетевого кабеля для отображения списка доступного сетевого оборудования.

- Диагностика и восстановление — выполняет диагностику сетевых подключений и пытается найти неисправности в них, после чего отображает список решений, которые могут пригодиться вам в устранении возникшей проблемы.
- Установка подключения или сети — отображается тот же шаг мастера Подключиться к сети, что и при выборе одноименной ссылки мастера Центр управления сетями и общим доступом.
- Управление беспроводными сетями — открывает список доступных беспроводных сетей, к которым вы можете подключиться. В этом списке отображаются беспроводные сети как между двумя компьютерами, так и между компьютерами и точкой доступа.
- Управление сетевыми подключениями — отображает папку Сетевые подключения, которая содержит список всех сетевых адаптеров, а также подключений удаленного доступа. С помощью контекстного меню определенного значка данной папки можно отключить или включить сетевое подключение или непосредственно сетевой адаптер, а также создать соединение типа мост между двумя сетевыми подключениями. Для этого нужно выделить два сетевых адаптера или подключения удаленного доступа и в контекстном меню одного из них выбрать команду Подключения типа мост.

ПРИМЕЧАНИЕ

Вы можете запретить создание мостов на компьютере домена DNS с помощью групповой политики Запретить установку и настройку сетевых мостов в вашей сети DNS-доменов, расположенной в разделе Конфигурация компьютера ▸ Административные шаблоны ▸ Сеть ▸ Сетевые подключения. Данная политика изменяет значение параметра REG_DWORD-типа NC_AllowNetBridge_NLA, расположенного в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Network Connections.

Кроме того, как и в предыдущих версиях операционной системы Windows, папка Сетевые подключения содержит меню Дополнительно, с помощью которого можно изменить дополнительные параметры работы сетевых возможностей операционной системы Windows Vista. Наиболее интересной командой данного меню является команда Дополнительные параметры, отображающая одноименное окно. С помощью этого окна можно настроить приоритет использования сетевых компонентов операционной системы для реализации доступа к сети.

Для этого в нем присутствуют списки сетевых компонентов, напротив которых отображены стрелки вверх и вниз. Чем выше находится сетевой компонент в списке, тем раньше операционная система использует его для попытки установления сетевого подключения.

Окно Дополнительные параметры содержит следующие списки.

- Подключения — содержит список всех доступных на компьютере сетевых подключений (сетевых адаптеров и подключений удаленного доступа). Обратите внимание, что по умолчанию операционная система пытается установить соединение с помощью беспроводной сети. Учитывая, что скорость беспроводных соединений, как правило, ниже, чем соединений на основе сетевого кабеля, лучше изменить порядок установления сетевых соединений в данном списке.
- Привязка для беспроводного сетевого соединения — показывает список всех протоколов, которые используются операционной системой для установления беспроводного сетевого соединения. По умолчанию сначала используется привязка Служба доступа к файлам и принтерам сетей Microsoft, а потом привязка Клиент для сетей Microsoft. При этом в обоих случаях сначала выполняется попытка установки соединения на основе протокола IPv4, а потом на основе протокола IPv6.
- Службы доступа к сети — содержит список провайдеров, которые используются операционной системой для установки сетевого соединения. По умолчанию сначала используется провайдер Microsoft Windows Network, потом провайдер терминальных служб и в последнюю очередь провайдер доступа к сети на основе веб-сервисов.

Настройка свойств сетевого соединения

Но вернемся к нашей задаче. Итак, нам нужно установить IP-адрес для сетевого адаптера, используемого создаваемым сетевым подключением. Для этого нужно воспользоваться окном Свойства (рис. 8.3), доступ к которому можно получить с помощью одноименной кнопки окна Состояние. Доступ же к этому окну можно получить с помощью ссылки Просмотр состояния мастера Центр управления сетями и общим доступом.

С помощью групповой политики Запрет доступа к свойствам подключений локальной сети, расположенной в разделе Конфигурация пользователя ▸ Административные шаблоны ▸ Сеть ▸ Сетевые подключения, можно запретить отображение окна свойств сети. Данная политика изменяет значение параметра REG_DWORD-типа NC_LanProperties, расположенного в ветви реестра HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Network Connections.

Вы можете воспользоваться еще одной групповой политикой данного раздела — Запретить подключение и отключение для подключений удаленного доступа. С ее помощью можно запретить конкретному пользователю подключение и отключение соединений удаленного доступа. Данная политика изменяет значение параметра REG_DWORD-типа NC_RasConnect, расположенного в ветви реестра HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Network Connections.

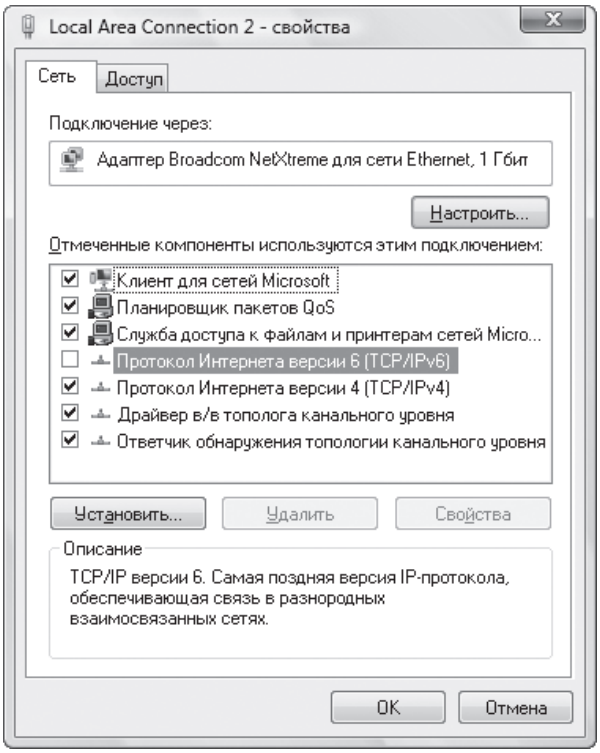

Рис. 8.3. Окно Свойства

И еще одна групповая политика данного раздела — Запрет изменения свойств частного подключения удаленного доступа. С ее помощью можно запретить конкретному пользователю настройку частного удаленного подключения (то есть подключения, доступного только для данного пользователя). Данная политика изменяет значение параметра `REG_DWORD`-типа `NC_RasMyProperties`, расположенного в ветви реестра `HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Network Connections`.

Кроме того, с помощью групповой политики Запретить переименование частных подключений удаленного доступа можно запретить конкретному пользователю переименование его частных удаленных соединений. Данная политика изменяет значение параметра `REG_DWORD`-типа `NC_RenameMyRasConnection`, расположенного в ветви реестра `HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Network Connections`.

Окно Свойства подключения на основе сетевого кабеля содержит две вкладки: Сеть и Доступ. С помощью вкладки Доступ можно включить механизм общего доступа к Интернету. А с помощью вкладки Сеть выполняется настройка работы сетевого адаптера. На этой вкладке расположено поле Отмеченные компоненты используются этим подключением, отображающее список протоколов и привязок, которые поддерживаются данным сетевым адаптером. Многие из используемых по умолчанию

элементов данного списка можно отключить для ускорения работы сети. Для этого нужно снять флажки рядом с их названиями.

По умолчанию это поле содержит следующие элементы.

- Клиент для сетей Microsoft — позволяет получить доступ к компьютерам с более ранней операционной системой, чем Windows Vista. Как вы уже знаете из окна Дополнительные параметры, сначала для установления соединения используется связка Служба доступа к файлам и принтерам сетей Microsoft и лишь потом Клиент для сетей Microsoft. Однако отключать этот элемент не рекомендуется, так как это может привести к проблемам получения доступа к компьютерам с операционной системой, отличной от Windows Vista.
- Планировщик пакетов QoS — дает возможность использовать механизм QoS для резервирования 20 % пропускной способности сети с целью использования этой части сети трафиком, нуждающимся в скоростном подключении. Механизм QoS может также уменьшать ширину окна передаваемого трафика с целью стабилизации скорости доступа к сети всех программ, которые в данный момент обращаются к ней (слишком большая ширина окна, используемого одной программой, может привести к задержкам в работе другой, только что запущенной программы).

  В локальных сетях механизм QoS практически не используется, поэтому данный элемент можно отключить.

  Тем не менее, отключение данной службы не приведет практически ни к каким положительным результатам. Дело в том, что, хоть служба QoS и резервирует до 20 % пропускной способности сети компьютера для передачи чувствительных к задержке данных, эта часть пропускной способности сети не простаивает — если в данный момент никаких чувствительных к задержке данных передавать не нужно, она используется для передачи обычных данных.

  Настроить параметры работы протокола QoS можно с помощью групповых политик операционной системы Windows Vista. Для этого применяются политики, расположенные в разделе Конфигурация компьютера ▸ Административные шаблоны ▸ Сеть ▸ Диспетчер пакетов QoS. Политики данного раздела изменяют значения параметров `REG_DWORD`-типа, расположенных в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Psched`.

  Например, в данном разделе можно встретить следующие политики.

  - Ограничение ожидающих обработки пакетов — изменяет значение параметра `MaxOutstandingSends`. Данная политика определяет максимальное количество пакетов, которые были переданы службой QoS для передачи по сетевому интерфейсу, но до сих пор еще не были посланы в сеть. После достижения значения, указанного данной групповой политикой, служба QoS должна прекратить передачу пакетов до тех пор, пока сетевой интерфейс не передаст пакеты, находящиеся в очереди.
  - Ограничить резервируемую пропускную способность — меняет значение параметра `NonBestEffortLimit`. Политика позволяет изменить процент пропускной способности сети, который будет резервироваться для нужд QoS.

  - Задать разрешение таймера — изменяет значение параметра `TimerResolution`. Она позволяет изменить интервал времени, с которым протокол QoS может передавать пакеты в сеть.

- Служба доступа к файлам и принтерам сетей Microsoft — позволяет получить доступ к общим папкам и принтерам компьютеров сети. Данный элемент отключать нельзя, если вы хотите, чтобы сетевое соединение работало.
- Протокол Интернета версии 6 (TCP/IPv6) — дает возможность использовать протокол IPv6 для установки сетевого соединения. В данный момент переход на эту версию протокола IP только начинается, поэтому этот элемент списка также можно отключить.
- Протокол Интернета версии 4 (TCP/IPv4) — позволяет использовать протокол IPv4 для установки сетевого соединения. Данная версия протокола IP используется по умолчанию для установки соединения, поэтому данный элемент списка отключать нельзя. Именно его мы будем использовать для установки IP-адреса компьютера.

ПРИМЕЧАНИЕ

В операционной системе Windows Vista стек протоколов TCP/IP был переделан полностью с нуля. Это позволило повысить стабильность и скорость работы данного стека.

- Драйвер в/в тополога канального уровня — используется устройствами и операционной системой для обнаружения сетевой топологии и построения карты сети (отображение того, как между собой подключены компьютеры и сетевые устройства). Отключение данного элемента приведет к отключению некоторых возможностей операционной системы Windows Vista, однако реальная пропускная способность сети может повыситься. Например, не будет строиться карта сети, отображаемая мастером Карта сети. Кроме того, могут возникнуть проблемы с подключением к сетевым компьютерам.
- Ответчик обнаружения топологии канального уровня — используется компьютером для обнаружения сетевой топологии и построения карты сети. Отключение данного элемента приведет к отключению некоторых возможностей операционной системы Windows Vista, однако реальная пропускная способность сети может повыситься. Например, не будет строиться карта сети, отображаемая мастером Карта сети. Кроме того, могут возникнуть проблемы с подключением к сетевым компьютерам.

ПРИМЕЧАНИЕ

Карта сети не будет отображать компьютеры с операционной системой Windows XP, находящиеся в вашей сети, пока на них не будет установлен компонент ответчика обнаружения топологии уровня связи (LLTD). Данный компонент можно установить в виде обновления операционной системы Windows XP.

Чтобы установить IP-адрес компьютера, нужно выделить элемент Протокол Интернета версии 4 (TCP/IPv4) и нажать кнопку Свойства. После этого отобразится окно Свойства: Протокол Интернета версии 4 (TCP/IPv4). Он содержит переключатель, который нужно установить в положение Использовать следующий IP-адрес, после чего активизируются два поля под ним: IP-адрес и Маска подсети. В поле IP-адрес вводится IP-адрес компьютера. А в поле Маска подсети — маска подсети (как правило, маску подсети вводить не нужно — достаточно ввести IP-адрес и перейти в поле Маска подсети, чтобы маска подсети появилась в нем автоматически).

Если ваш компьютер не подключен напрямую к Интернету и вы планируете использовать на нем механизм Internet Connection Sharing, то нужно использовать IP-адрес компьютера 192.168.0.1, так как именно такой IP-адрес по умолчанию требует ICS для своей работы.

После того как вы укажете IP-адрес компьютера, может потребоваться также изменить его сетевое имя или рабочую группу. Компьютеры одной сети должны входить в одну рабочую группу, чтобы можно было получить доступ к общим папкам сетевых компьютеров. Для этого нужно вызвать окно Система (нажатием комбинации клавиш Windows+Pause Break), после чего щелкнуть кнопкой мыши на ссылке Изменить параметры, чтобы отобразилось окно Свойства системы, открытое на вкладке Имя компьютера. На данной вкладке нужно нажать кнопку Изменить, после чего отобразится еще одно окно (Изменение имени компьютера). С помощью поля Имя компьютера данного окна можно указать новое имя компьютера, а с помощью поля, расположенного напротив переключателя Является членом, установленного в положение рабочей группы, можно изменить рабочую группу, в которую входит компьютер. Еще раз напомню, что компьютеры должны входить в одну и ту же рабочую группу, чтобы можно было получить доступ к их общим папкам.

После применения описанных выше настроек вы сможете успешно подключиться к другим компьютерам с установленной операционной системой Windows Vista. К вам также смогут подключаться компьютеры с установленными операционными системами семейства Windows. Однако если вы попробуете подключиться к операционным системам более ранних версий, например к Windows XP, скорее всего, это у вас не получится. Связано это с тем, что по умолчанию операционная система Windows Vista использует при аутентификации только пакеты NTLMv2, что может не соответствовать настройкам более ранних версий Windows. Чтобы это изменить, нужно воспользоваться оснасткой `gpedit.msc`. В разделе Конфигурация компьютера ▸ Конфигурация Windows ▸ Параметры безопасности ▸ Локальные политики ▸ Параметры безопасности данной оснастки нужно выбрать элемент Сетевая безопасность: уровень проверки подлинности LAN Manager и установить его значение в состояние Отправлять LM и NTLM — использовать сеансовую безопасность NTLMv2 при согласовании (по умолчанию используется значение Отправлять только NTLMv2 ответ).

Настройка с помощью команды netsh interface

Как и раньше, установить или просмотреть настройки работы определенного сетевого интерфейса можно с помощью команды программы командной строки `netsh interface`. Она поддерживает следующие возможности (далее будут описаны дочерние команды, которые реализуют эти возможности).

Работа с сетевыми интерфейсами

Программа позволяет просмотреть все сетевые интерфейсы, а также добавить новый интерфейс или удалить уже существующий (под сетевыми интерфейсами, как правило, понимаются сетевые карты, установленные в компьютере, а также различные модемные подключения). Для этого применяются дочерние команды `show interface`, `add interface`, `delete interface` (например, чтобы просмотреть список всех интерфейсов, нужно ввести команду `netsh interface show interface`).

Можно также воспользоваться дочерней командой `set interface`, чтобы изменить такие настройки сетевого интерфейса, как его имя, указания, включен ли он, подключен ли к сети. Например, с помощью команды `netsh interface set interface <имя интерфейса, например Wireless Network Connection> ENABLED` можно включить сетевой интерфейс.

Настройка протокола IP

Можно настроить работу протоколов IPv4 и IPv6. Для этого применяются, соответственно, дочерние команды `IPv4` и `IPv6`. Они, в свою очередь, поддерживают следующие команды, реализующие возможности настройки протоколов.

- Просмотреть или изменить статический IP-адрес и маску подсети, которые установлены для данного сетевого интерфейса. Для этого можно воспользоваться следующими дочерними командами: `add address`, `delete address`, `show addresses` и `set address`.
- Просмотреть или изменить статический адрес DNS-сервера. Для этого можно воспользоваться следующими дочерними командами: `add dnsserver`, `delete dnsserver`, `show dnsservers` и `set dnsserver`.
- Просмотреть или изменить список IP-адресов компьютеров, которые находятся в одной сети (содержимое ARP-кеша). Для этого можно воспользоваться следующими дочерними командами: `add neighbors`, `delete neighbors`, `show neighbors` и `set neighbors`. Можно также удалить ARP-кеш с помощью дочерней команды `delete arpcache`.
- Просмотреть или изменить таблицу маршрутизации. Для этого можно воспользоваться следующими дочерними командами: `add route`, `delete route`, `show route` и `set route`.
- Просмотреть или изменить список адресов WINS-серверов. Для этого можно воспользоваться следующими дочерними командами: `add winsserver`, `delete winsserver`, `show winsserver` и `set winsserver`.
- Просмотреть основную информацию о настройках сетевого интерфейса. Для этого применяется дочерняя команда `show config`. Можно также просмотреть список IP-адресов назначения (команда `show destinationcache`), диапазон динамических портов (команды `show dynamicportrange tcp` и `show dynamicportrange udp`), статистику получения и передачи пакетов ICMP разных типов (команда `show icmpstats`), список установленных соединений TCP и UDP (команды `show tcpconnections` и `show udpconnections`),

а также статистику работы протоколов TCP и UDP (команды `show tcpstats` и `show udpstats`).

- Просмотреть или изменить глобальные параметры работы сетевой части операционной системы Windows Vista. Для этого можно воспользоваться следующими дочерними командами: `show global` и `set global`. Например, с помощью данных команд можно изменить параметры реестра, расположенные в ветви `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters` и имеющие тип `REG_DWORD`.
  - Предел прыжков по умолчанию — изменяет значение параметра `DefaultTTL`. Он определяет время жизни передаваемого в сети пакета, то есть указывает количество маршрутизаторов, через которые передаваемый пакет может пройти, прежде чем достигнет пункта назначения. Каждый пройденный пакетом маршрутизатор уменьшает его значение TTL на единицу. Если в итоге значение TTL становится равным нулю, то следующий маршрутизатор, получивший пакет, удаляет его из сети.
  - Переадресовано ICMP — меняет значение параметра `EnableICMPRedirect`. Он позволяет определить, разрешено ли в сети использовать пакеты ICMP типа перенаправление.
  - Поведение маршрутизации источников — изменяет значение параметра `DisableIPSourceRouting`. Он дает возможность определить, будет ли разрешена передача пакетов с помощью флага маршрутизации от источника.
  - Разгрузка задач — меняет значение параметра `DisableTaskOffload`. Он позволяет включить или отключить работу сопроцессора, расположенного на сетевой карте (сопроцессор часто устанавливается на дорогих сетевых картах). Отдельный сопроцессор, который будет обрабатывать запросы сетевой карты, позволяет снизить нагрузку на центральный процессор компьютера при передаче сетевой платой пакетов.
  - Определение носителя Dhcp — изменяет значение параметра `DisableDHCPMediaSense`. Он дает возможность указать, будет ли операционная система пытаться определить события подключения и отключения устройств от сети. Эта функция может быть полезна владельцам ноутбуков, которые часто переходят между разными сетями.
  - Журнал определения носителя — меняет значение параметра `DisableMediaSenseEventLog`. Он позволяет определить, будут ли сведения о событиях подключения и отключения устройств от сети заноситься в стандартный журнал операционной системы.
  - Уровень MLD — меняет значение параметра `IGMPLevel`. Он дает возможность определить, может ли операционная система поддерживать многоадресную рассылку с помощью протокола IGMP. При этом существует несколько уровней работы протокола IGMP: `0` (система не поддерживает многоадресную рассылку), `1` (система может только посылать пакеты многоадресной рассылки), `2` (система может как посылать пакеты многоадресной рассылки, так и получать такие пакеты).

- Версия MLD — изменяет значение параметра `IGMPVersion`.
- Многоадресная пересылка — меняет значение параметра `EnableMulticastForwarding`. Он позволяет определить, может ли компьютер передавать широковещательные IP-пакеты.
- Ответы с маской адреса — изменяет значение параметра `EnableAddrMaskReply`. Он дает возможность определить, разрешено ли компьютеру отвечать на пакеты ICMP типа Ответы с маской адреса (тип 17).

- Установить или удалить протокол IPv4. Для этого применяются дочерние команды `install` и `uninstall`.
- Переустановить стек протоколов TCP/IP и параметры его настройки. Для этого применяется дочерняя команда `reset`.

Настройка прокси-сервера

Вы также можете просмотреть или настроить списки используемых прокси-серверов, воспользовавшись для этого дочерней командой `portproxy`. Она поддерживает следующие возможности.

- Просмотр списка прокси-серверов, которые взаимодействуют с сетями протоколов IPv4 и IPv4 (команда `v4tov4`), IPv6 и IPv6 (команда `v6tov6`), IPv4 и IPv6 (команда `v4tov6`), IPv6 и IPv4 (команда `v6tov4`), или списка всех прокси-серверов (команда `all`).
- Добавить или удалить прокси-сервер, который взаимодействует с определенным типом сетей (команды `add v4tov4`, `delete v4tov4`, `add v6tov6`, `delete v6tov6` и т. д.).

Настройка протокола TCP

Программа позволяет настроить работу протокола TCP, для чего применяется команда `TCP`. Она поддерживает следующие возможности.

- Просмотр или изменение списка приложений и портов таблицы TCP. Для этого применяются команды `add chimneyapplication`, `add chimneyport`, `delete chimneyapplication`, `delete chimneyport`, `show chimneyapplication`, `show chimneyport`.
- Просмотр или изменение глобальных параметров работы сетевой части операционной системы. Для этого применяются команды `show global` и `set global`. Например, с помощью данных команд можно изменить параметры реестра, расположенные в ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters` и имеющие тип `REG_DWORD`.

Настройка TEREDO

Можно также просмотреть или изменить параметры настройки TEREDO. Для этого применяются дочерние команды `teredo show state` и `teredo set state`.

ПРИМЕЧАНИЕ

Как и раньше, с помощью дочерних команд команды netsh winsock можно просмотреть каталог провайдеров winsock (команда show catalog), удалить провайдера или восстановить по умолчанию содержимое каталога провайдеров (команды remove и reset), а также просмотреть события аудита установки и удаления провайдеров LSP (команда audit trail).

Создание беспроводного соединения

Создание беспроводного соединения на первых шагах отличается от создания подключения с использованием сетевого кабеля. Это связано с тем, что после установки драйверов сетевой карты и включения этих сетевых карт ничего не произойдет (значок беспроводного сетевого соединения в области уведомления отображаться не будет, как не будет отображаться само беспроводное соединение в мастере Центр управления сетями и общим доступом).

Для создания беспроводного сетевого соединения необходимо воспользоваться мастером Подключиться к сети. Как мы уже знаем, его можно отобразить с помощью ссылки Подключиться к сети мастера Центр управления сетями и общим доступом. Однако его можно отобразить и с помощью команды Подключиться к сети контекстного меню значка сетевого подключения, отображаемого в области уведомления.

ПРИМЕЧАНИЕ

Значок сетевого подключения может не отображаться в области уведомления, если вы сняли флажок Сеть на вкладке Область уведомлений окна Свойства панели задач и меню "Пуск".

Мастер Подключиться к сети

После отображения этого мастера нужно щелкнуть кнопкой мыши на ссылке Создать новое подключение или на ссылке Установка подключения или сети, чтобы отобразить список соединений, которые можно создать с его помощью. Рассмотрим подробнее те из соединений, которые создаются с помощью беспроводных сетевых адаптеров.

Настройка беспроводной сети компьютер–компьютер

Как вы уже знаете, при выборе этого варианта будет создано непостоянное беспроводное соединение (однако с его помощью можно создать и постоянное беспроводное соединение). После того как вы выберете данный вариант, нужно будет установить определенные настройки нового беспроводного соединения.

В поле Имя сети можно указать имя сети, в которую войдет данное беспроводное соединение.

Раскрывающийся список Тип безопасности дает возможность указать тип аутентификации, используемый при установлении данного беспроводного соединения.

Список возможных типов аутентификации зависит от беспроводного сетевого адаптера, установленного на вашем компьютере. Однако на первых порах лучше попробовать создать беспроводное сетевое соединение без использования аутентификации. Для этого в этом раскрывающемся списке нужно выбрать элемент Нет проверки подлинности (Open).

ПРИМЕЧАНИЕ

Операционная система Windows Vista поддерживает новейшие протоколы безопасности. Например, протоколы Wi-Fi Protected Access (WPA) 2, PEAP-TLS и PEAP-MS-CHAP v2

В поле Ключ безопасности или парольная фраза вы можете указать строку, используемую для аутентификации подключаемых компьютеров.

С помощью переключателя Сохранить параметры этой сети можно выбрать, сохранится ли созданное вами беспроводное подключение. Если сохранится, то также можно указать, кто сможет получить к нему доступ. Если беспроводное подключение будет сохранено, то в будущем вы сможете воспользоваться создаваемым в данный момент подключением, так как оно будет отображаться в списке сетевых подключений мастера Подключиться к сети. Вам будет достаточно выбрать данное подключение из списка и нажать кнопку Подключиться.

После того как вы создадите беспроводное сетевое подключение, оно будет отображаться в мастере Подключиться к сети как локального компьютера, так и удаленного. При этом на локальном компьютере беспроводное соединение будет установлено, однако для полной установки соединения вам нужно будет выбрать его на удаленном компьютере и нажать кнопку Подключиться.

Кроме того, после создания беспроводного соединения и подключения удаленного компьютера данное соединение будет отображаться в поле мастера Центр управления сетями и общим доступом. Напротив этого соединения будет две ссылки: Просмотр состояния и Отключение. С помощью первой ссылки можно отобразить окно Состояние данного соединения. Не забудьте в этом окне указать IP-адрес вашего беспроводного сетевого адаптера, как мы это делали для сетевого подключения с использованием сетевого кабеля. С помощью же второй ссылки можно отключить данное беспроводное сетевое соединение. Также отключиться от беспроводного соединения можно с помощью контекстного меню значка сетевого соединения, отображаемого в области уведомления. Для этого в данном контекстном меню нужно выбрать команду Отключиться от и выбрать сеть, от которой вы хотите отключиться.

Подключение к беспроводной сети вручную

Позволяет вручную создать беспроводное сетевое подключение с точкой доступа. Данный способ позволяет настроить больше параметров, чем предыдущий.

После того как вы введете все данные, будет выполнена попытка создания беспроводного сетевого соединения. Если она пройдет успешно, то сетевое соединение будет создано.

Мастер Управление беспроводными сетями

Если вы уже создали данное беспроводное сетевое соединение, то, наверное, заметили, что оно не отображается в списке мастера Подключиться к сети. Для доступа к данному беспроводному соединению необходимо использовать мастер Управление беспроводными сетями (рис. 8.4), доступ к которому можно получить с помощью одноименной ссылки панели ссылок мастера Центр управления сетями и общим доступом. Использование мастера Управление беспроводными сетями является единственным способом не только для доступа к беспроводным сетям на основе точки доступа, но и для удаления созданных ранее беспроводных сетей. Панель инструментов данного мастера содержит следующие кнопки.

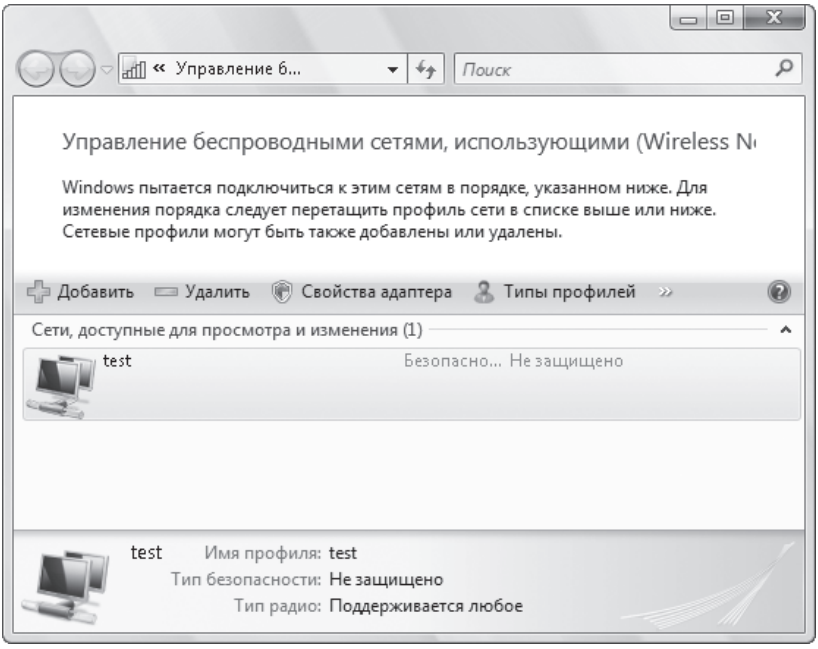

Рис. 8.4. Мастер, отображающий список всех беспроводных сетей

- Добавить — создать новую беспроводную сеть на основе точки доступа (кнопка Добавить сеть, находящуюся в зоне действия этого компьютера отображаемого после нажатия кнопки Добавить мастера) или непосредственно между двумя компьютерами (кнопка Создать сеть компьютер–компьютер отображаемого после нажатия кнопки Добавить мастера).
- Удалить — удалить созданную ранее беспроводную сеть.
- Переместить вниз и Переместить вверх — повысить или понизить приоритет использования беспроводных сетей. От приоритета зависит то, какая из беспроводных сетей, доступных в данный момент, будет использоваться. Чем выше приоритет сети (чем выше она находится в списке беспроводных сетей мастера Управление беспроводными сетями), тем больше вероятность того, что именно эта сеть будет использоваться при установлении соединения.

- Свойства адаптера — отображает окно Свойства беспроводного сетевого адаптера, используемого данной беспроводной сетью.
- Типы профилей — открывает окно Тип профиля беспроводной сети, с помощью которого можно выбрать, смогут ли другие пользователи увидеть данную беспроводную сеть и подключиться к ней.
- Центр управления сетями и общим доступом — отображает одноименный мастер.

Кроме того, с помощью команды Свойства контекстного меню беспроводной сети можно открыть окно свойств беспроводной сети, в котором изменяются все те настройки, которые вы указывали при создании данной беспроводной сети.

Независимо от того, с помощью какого способа вы настроите беспроводное сетевое соединение, вам самостоятельно придется указать IP-адрес и маску подсети, используемые беспроводными сетевыми адаптерами. Это выполняется тем же способом, что и настройка IP-адреса для сетевого соединения, использующего сетевой кабель.

Создание удаленного подключения с помощью модема

Рассмотрим процесс создания удаленного подключения к Интернету с помощью модема. Этот процесс начинается с установки и настройки модема (обычного либо модема мобильного телефона). Установку модема мы рассматривать не будем, настройка же, в основном, заключается в указании строки инициализации модема. Для этого нужно открыть окно Диспетчер устройств (`devmgmt.msc`) и выбрать в списке Модемы установленный вами модем, после чего вызвать его окно Свойства. После этого нужно перейти на вкладку Дополнительные параметры связи и в поле Дополнительные команды инициализации ввести строку инициализации. Как правило, строка инициализации имеет следующий формат: `AT+CGDCONT=1,"протокол","точка доступа"<cr>`. Например, для мобильного оператора UMC необходимо указать строку инициализации `AT+CGDCONT=1,"IP","www.umc.ua"<cr>`. А для оператора сотовой связи Life необходимо указать такую строку инициализации, как `AT+CGDCONT=1,"IP","internet"<cr>`.

Мастер Подключиться к сети

После этого необходимо воспользоваться уже знакомым нам окном Подключиться к сети, чтобы создать удаленное соединение на основе настроенного нами модема. Для этого нужно вызвать данный мастер (с помощью команды Подключиться к сети контекстного меню значка сетевого подключения, отображаемого в области уведомления), после чего щелкнуть кнопкой мыши на ссылке Установка подключения или сети и в появившемся списке выбрать элемент Настройка телефонного подключения. Это приведет к запуску мастера создания модемного подключения. Вам необходимо будет выполнить кое-какие установки.

- В поле Набираемый номер нужно ввести номер телефона, на который должен совершить звонок ваш модем, чтобы подключиться к провайдеру. Как правило, заполнение этого поля обязательно. Мобильные операторы очень часто используют номер телефона *99#.

- В поле Имя пользователя вводится имя пользователя, применяемое при аутентификации у оператора. Заполнение этого поля необязательно.
- В поле Пароль нужно ввести пароль пользователя, применяемый при аутентификации у оператора. Заполнение этого поля необязательно.
- После установки флажка Отображать вводимые знаки вводимый вами пароль не будет заменяться звездочками.
- После установки флажка Запомнить этот пароль вводимый вами пароль будет запомнен операционной системой, и вам больше не придется вводить его заново.
- В поле Имя подключения указывается имя создаваемого вами соединения. Это имя в дальнейшем будет отображаться в списке окна Подключиться к сети.
- Если установить флажок Разрешить использовать это подключение другим пользователям, то другие пользователи смогут пользоваться созданным вами модемным соединением.

Последним шагом мастера будет попытка установки связи с Интернетом. Если перед созданием модемного подключения вы правильно настроили модем, то эта попытка должна пройти успешно. В дальнейшем, чтобы воспользоваться созданным вами модемным подключением, будет достаточно вызвать окно Подключиться к сети, в списке доступных сетей (в поле Удаленный доступ и виртуальные частные сети) выбрать созданную вами ранее сеть и нажать кнопку Подключиться. После этого связь с Интернетом будет установлена. Заметьте, что при подключении к Интернету значок сетевого подключения в области уведомления изменится (на нем появится изображение земного шара).

ПРИМЕЧАНИЕ

С помощью групповой политики Запретить удаление подключений удаленного доступа, расположенной в разделе Конфигурация пользователя ▸ Административные шаблоны ▸ Сеть ▸ Сетевые подключения, можно запретить определенному пользователю удаление подключений удаленного доступа.

Данная политика изменяет значение параметра REG_DWORD-типа NC_DeleteConnection, расположенного в ветви реестра HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Network Connections.

Настройка браузера

Но это еще не все. К Интернету вы подключились, однако теперь нужно настроить используемый вами браузер, чтобы он пользовался созданным вами ранее модемным подключением. Поскольку в операционной системе Windows Vista по умолчанию установлен браузер Internet Explorer 7.0, мы рассмотрим именно его настройку. Для его настройки необходимо отобразить окно Свойства обозревателя (команда Свойства обозревателя меню Сервис) и перейти на вкладку Подключения. Она содержит список созданных вами ранее модемных подключений (Настройка удаленного доступа и виртуальных частных сетей), в котором нужно выбрать необходимое вам модемное подключение и установить переключатель в положение Всегда использовать принятое по умолчанию подключение.

ПРИМЕЧАНИЕ

Как правило, в настройке браузера Internet Explorer нет никакой необходимости: операционная система сама это сделает после того, как вы создадите удаленное подключение.

Теперь браузер будет по умолчанию использовать именно созданное вами модемное подключение и вы сможете выйти в Интернет. Однако, если вы используете прокси-сервер, этого будет недостаточно для подключения к Интернету. Вам также нужно будет указать IP-адрес и порт прокси-сервера. Для этого на вкладке Подключения окна Свойства обозревателя нужно выбрать используемое вами модемное подключение и нажать кнопку Настройка. После этого отобразится окно Параметры, в области Прокси-сервер которого нужно ввести настройки прокси-сервера.

8.2. Работа с удаленным помощником

Расположение: `%systemroot%\system32\msra.exe`.

ПРИМЕЧАНИЕ

Сведения об использовании удаленного помощника заносятся в журналы, расположенные в разделе Журналы приложений и служб ▸ Microsoft ▸ Windows ▸ Remote Assistance.

Как и в предыдущих версиях, в Windows Vista присутствует средство для доступа к удаленному компьютеру Удаленный помощник Windows. Однако перед его использованием необходимо сначала активировать данную возможность. Для этого нужно открыть окно Система (комбинацией клавиш Windows+Pause Break), после чего щелкнуть кнопкой мыши на ссылке Настройка удаленного доступа. После этого отобразится окно Свойства системы, открытое на вкладке Удаленное использование. Область Удаленный помощник данной вкладки содержит следующие элементы.

- Флажок Разрешить подключения удаленного помощника к этому компьютеру. Если он установлен, то операционная система разрешит взаимодействие пользователя с удаленным помощником.
- Кнопка Дополнительно. С ее помощью отображается окно Параметры удаленного помощника, поддерживающее следующие возможности: позволяет запретить или разрешить удаленное управление компьютером, а также указать определенный период времени, когда удаленное управление компьютером разрешено.

Мастер Удаленный помощник Windows

Чтобы воспользоваться возможностями удаленного помощника, нужно запустить программу `msra.exe`, что приведет к отображению мастера Удаленный помощник Windows. Основное окно данного мастера содержит две ссылки.

ПРИМЕЧАНИЕ

Механизм удаленного помощника основан на модели DCOM, поэтому он не будет работать в том случае, если параметру строкового типа EnableDCOM присвоено значение N. Этот параметр расположен в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole.

Отправка приглашения удаленному помощнику

Щелкнув кнопкой мыши на ссылке Пригласить того, кому вы доверяете, для оказания помощи, вы сможете послать приглашение удаленному помощнику. Вы можете либо послать приглашение в виде электронного сообщения (кнопка Пригласить по электронной почте), либо сохранить его в файле (кнопка Сохранить приглашение как файл). В любом случае также необходимо указать пароль, который должен ввести удаленный пользователь, чтобы подключиться к вашему компьютеру с помощью мастера Удаленный помощник Windows.

После того как вы создадите приглашение, нажав кнопку Готово мастера Удаленный помощник Windows, будет открыто окно, представленное на рис. 8.5. Оно свидетельствует о том, что операционная система ожидает ответа на приглашение, после которого удаленное управление Рабочим столом будет установлено. Чтобы отменить приглашение, нужно нажать кнопку Отмена. Открывшееся окно Удаленный помощник Windows содержит следующие кнопки.

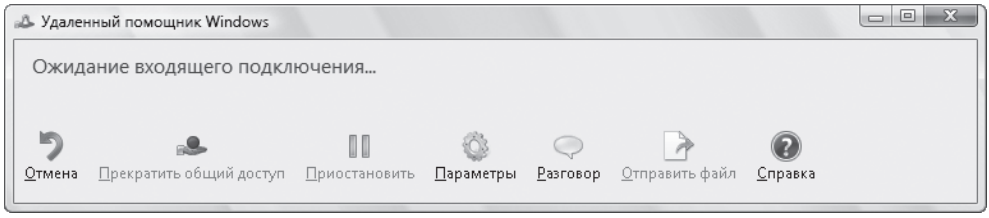

Рис. 8.5. Результат создания приглашения удаленного помощника

- Прекратить общий доступ — если удаленному пользователю было передано разрешение на удаленное управление компьютером (использование мыши и клавиатуры компьютера), то с помощью этой кнопки он сможет завершить удаленное управление компьютером. Вы и сами можете завершить удаленное управление компьютером, нажав клавишу Esc.

  Чтобы запросить удаленное управление компьютером, подключенный удаленный пользователь должен нажать кнопку Начать общий доступ.

- Приостановить — приостанавливает передачу удаленному помощнику сведений о текущем состоянии экрана.

- Параметры — позволяет определить процент пропускной способности сети, который разрешено использовать удаленному помощнику, а также определить, будут ли сохраняться сведения о работе удаленного помощника в файл журнала. С помощью данной кнопки можно также запретить использование клавиши Esc для завершения удаленного управления компьютером.

- Разговор — дает возможность вам и удаленному помощнику переговариваться в режиме чата.
- Отправить файл — позволяет отправить файл удаленному помощнику (или вам, если файл отправляется удаленным помощником).

Ответ на приглашение удаленного помощника

Если вы щелкнете кнопкой мыши на ссылке Предложить помощь кому-либо, то сможете ответить на приглашение удаленного помощника. При этом необходимо указать IP-адрес удаленного компьютера или выбрать файл, который был сформирован при создании приглашения удаленному помощнику. Если приглашение было послано с помощью файла, то нет смысла запускать мастер Удаленный помощник Windows — достаточно запустить данный файл, после чего необходимо ввести пароль, чтобы соединение с удаленным компьютером было установлено. Если пользователь, пославший приглашение, подтвердит установление связи, то перед вами отобразится окно, представленное на рис. 8.5, которое также будет отображать снимок с монитора удаленного пользователя.

Параметры программы msra.exe

Программа `msra.exe` поддерживает следующие параметры.

- `/email <пароль>` — отображает мастер Удаленный помощник Windows, открытый на шаге создания электронного сообщения, содержащего приглашение удаленному помощнику.
- `/RAConnectionString <компьютер>` — недокументированный параметр. Позволяет подключиться к удаленному компьютеру на основе знания пароля.
- `/offerra <компьютер>` — позволяет запустить мастер Удаленный помощник Windows для создания приглашения удаленному помощнику на удаленном компьютере, используя возможности DCOM.
- `/CreateRAConnectionString` — недокументированный параметр. Позволяет создать пароль для доступа к удаленному компьютеру.
- `/SolicitedIM` — также недокументированный параметр. Позволяет указать пароль для подключения удаленного помощника.
- `/OfferIM` — недокументированный параметр. Позволяет указать пароль для подключения удаленного помощника.
- `/openfile <путь к файлу>` — открывает файл приглашения удаленному помощнику и отвечает на него.
- `/saveasfile <путь к файлу> <пароль>` — сохраняет приглашение удаленному помощнику в файл, используя указанный пароль.
- `/history <приглашение>` — недокументированный параметр. Позволяет просмотреть историю сеанса удаленной помощи.
- `/novice` — отображает мастер Удаленный помощник Windows на шаге создания приглашения удаленному помощнику.
- `/expert` — открывает мастер Удаленный помощник Windows на шаге ответа на приглашение удаленному помощнику.

- /RecoverDesktop — недокументированный параметр. Присваивает параметру REG_DWORD-типа Altered Desktop, расположенному в ветви реестра HKEY_CURRENT_USER\Software\Microsoft\Remote Assistance, значение 0.

Настройка с помощью групповых политик

Настроить некоторые параметры работы удаленного помощника можно с помощью групповых политик операционной системы Windows Vista. Для этого применяются политики, расположенные в разделе Конфигурация компьютера ▸ Административные шаблоны ▸ Система ▸ Удаленный помощник.

Политики данного раздела изменяют значения следующих параметров REG_DWORD-типа, расположенных в ветви HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services.

- CreateEncryptedOnlyTickets — если значение данного параметра равно 1, то к компьютеру будет разрешено подключаться только удаленным помощникам, работающим в операционных системах Windows Vista. При этом будет повышен общий уровень безопасности удаленного подключения к компьютеру.
- UseCustomMessages — при установке значения этого параметра равным 1 текст стандартных сообщений будет переопределен параметрами ShareControlMessage и ViewMessage.
- ShareControlMessage — имеет строковый тип. Он определяет текст стандартного сообщения, отображаемого перед совместным использованием определенного элемента
- ViewMessage — параметр строкового типа. Он определяет текст стандартного сообщения, отображаемого перед подключением удаленного помощника.
- fAllowFullControl — если значение данного параметра равно 1, то удаленным помощникам будет разрешен полный доступ к управлению компьютером.
- fAllowToGetHelp — при установке значения этого параметра равным 1 запрошенная удаленная помощь будет разрешена.
- fUseMailto — если значение данного параметра равно 1, то запрос на удаленную помощь будет передаваться электронной почтой с помощью метода mailto. Если же значение данного параметра равно 0, то запрос будет передаваться с помощью метода Simple MAPI.
- MaxTicketExpiry — значение данного параметра определяет интервал, в течение которого переданный запрос на удаленную помощь будет работоспособен. При этом единицы, в которых указан этот интервал, определяются с помощью параметра MaxTicketExpiryUnits.
- MaxTicketExpiryUnits — если значение данного параметра равно 0, то интервал, определенный параметром MaxTicketExpiry, указан в минутах. Если значение равно 1, то интервал определен в часах. А если значение равно 2, то в днях.

- `fAllowUnsolicited` — при установке значения этого параметра равным `1` будет разрешена незапрошенная помощь удаленного помощника. С помощью параметров строкового типа ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services\RAUnsolicit` можно будет указать учетные записи конкретных пользователей, которым будет разрешено предлагать незапрошенную помощь.
- `fAllowUnsolicitedFullControl` — если значение данного параметра равно `1`, то удаленным помощникам, помощь которых была не запрошена, будет разрешен полный доступ к управлению компьютером.
- `UseBandwidthOptimization` — при установке значения этого параметра равным `1` будет включена возможность оптимизации сетевого подключения. При этом сам тип оптимизации будет указан в параметре `OptimizeBandwidth`.
- `OptimizeBandwidth` — значение данного параметра определяет различные эффекты интерфейса, которые будут отключены с целью оптимизации сетевого соединения, если значение параметра `UseBandwidthOptimization` равно `1`. Например, если значение данного параметра равно `0xC`, то содержимое окна при перетаскивании отображаться не будет. Если значение данного параметра равно `8`, то фон будет отключен и содержимое окна при перетаскивании отображаться не будет. А если значение данного параметра равно `0`, то будет выполняться полная оптимизация (фон отключен, содержимое окна при перетаскивании скрыто, используются восьмибитовые цвета).
- `LoggingEnabled` — если значение данного параметра равно `1`, то можно будет создать файл журнала работы удаленного помощника. Соответствующие файлы журнала будут храниться в папке Документы профиля пользователя.

8.3. Терминальные службы

Программы, работающие на основе терминальных служб операционных систем семейства Windows, позволяют получить доступ к удаленному компьютеру, как будто вы работаете непосредственно на нем. Примером такой программы может быть удаленный помощник, который мы рассмотрели выше. Сейчас же рассмотрим еще одну программу подобного рода.

ПРИМЕЧАНИЕ

С помощью класса Win32_TerminalService, принадлежащего пространству имен \\root\cimv2, можно просмотреть сведения о работе службы терминалов. Например, данный класс поддерживает следующие свойства: DisconnectedSessions (определяет количество отключенных сеансов), EstimatedSessionCapacity (указывает количество сеансов, которые способен обработать сервер), ResourceConstraint (определяет оборудование, из-за нехватки мощности которого нельзя увеличить количество подключенных сеансов), TotalSessions (указывает общее количество сеансов).

Сведения о работе терминальной службы хранятся в журналах, расположенных в разделе Журналы приложений и служб ▸ Microsoft ▸ Windows ▸ TerminalServices-RemoteConnectionManager.

Подключение к удаленному рабочему столу

Расположение: `%systemroot%\system32\mstsc.exe`.

Программа Подключение к удаленному рабочему столу позволяет удаленному пользователю подключиться к локальному компьютеру. При этом состояние экрана локального компьютера будет передаваться по сети на удаленный компьютер и отображаться на его мониторе. Кроме того, удаленный пользователь сможет пользоваться мышью и клавиатурой своего компьютера, как будто они принадлежат локальному компьютеру.

ПРИМЕЧАНИЕ

Подключиться к удаленному Рабочему столу можно и с помощью веб-сервера IIS. Для этого после установки IIS нужно воспользоваться адресом вида http://<имя сервера, к которому подключаемся>/tsweb. После этого на клиентский компьютер будут загружены дополнительные элементы управления ActiveX, и подключение будет установлено.

Как и при работе с удаленным помощником, перед тем как воспользоваться программой Подключение к удаленному рабочему столу, необходимо активировать возможность удаленного доступа к компьютеру. Для этого нужно открыть окно Система (комбинацией клавиш Windows+Pause Break), после чего щелкнуть кнопкой мыши на ссылке Настройка удаленного доступа. Появится окно Свойства системы, открытое на вкладке Удаленное использование. Область Удаленный рабочий стол данной вкладки содержит следующие элементы.

ПРИМЕЧАНИЕ

В операционной системе Windows Vista Home Basic присутствует только клиент подключения к удаленному Рабочему столу.

- Переключатель Выберите вариант и затем укажите, кому разрешено подключение, если нужно позволяет определить, могут ли пользователи получить удаленный доступ к данному компьютеру. Его можно установить в следующие положения.
  - Не разрешать подключения к этому компьютеру — запретить удаленный доступ к данному компьютеру. По умолчанию переключатель установлен в это положение.
  - Разрешать подключения от компьютеров с любой версией удаленного рабочего стола (опаснее) — разрешить удаленный доступ к данному компьютеру с помощью любых версий операционной системы Windows.
  - Разрешать подключения только от компьютеров с удаленным рабочим столом с сетевой проверкой подлинности (безопаснее) — позволить удаленный доступ к данному компьютеру, если операционная система поддерживает механизм сетевой проверки подлинности. По умолчанию его поддерживает только Windows Vista.

- Кнопка Выбрать пользователей — позволяет открыть окно Пользователи удаленного рабочего стола. С его помощью можно добавить пользователей, которые могут получить удаленный доступ к данному компьютеру. По умолчанию получить доступ к удаленному компьютеру может только тот пользователь, который в данный момент находится в системе.

Основное окно программы

После того как вы настроите параметры удаленного подключения к вашему компьютеру, можно запускать программу `mstsc.exe`. По сравнению с предыдущими версиями Windows, основное окно данной программы немного изменилось (рис. 8.6). Больше основное окно программы не содержит поля для ввода имени пользователя и пароля: теперь сначала нужно указать имя удаленного компьютера, нажать кнопку Подключить, и только после этого отобразится отдельное окно, в котором можно выбрать пользователя, от имени которого выполняется подключение к удаленному компьютеру.

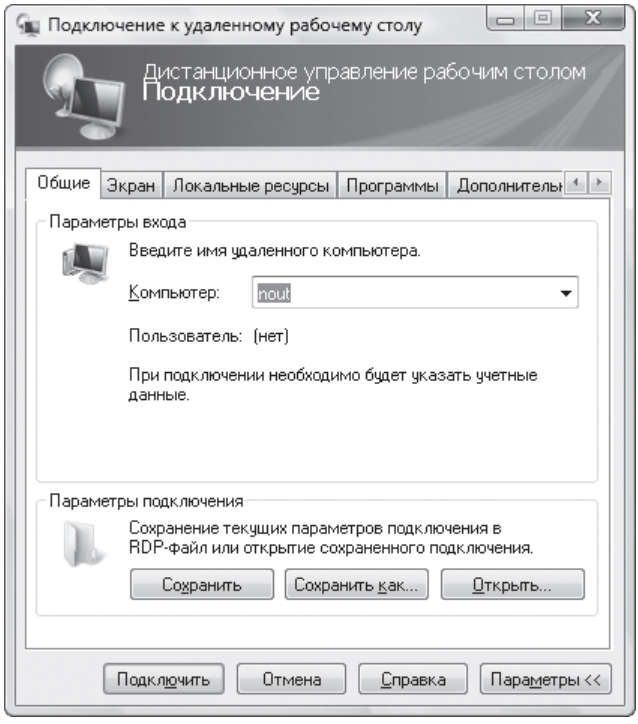

Рис. 8.6. Основное окно программы Подключение к удаленному рабочему столу

ПРИМЕЧАНИЕ

С помощью групповой политики Запретить сохранение паролей, расположенной в разделе Конфигурация компьютера ▸ Административные шаблоны ▸ Компоненты Windows ▸ Службы терминалов ▸ Клиент подключения к удаленному рабочему столу, можно запретить сохранение пароля подключения к удаленному компьютеру. Данная

политика изменяет значение параметра REG_DWORD-типа DisablePasswordSaving, расположенного в ветви системного реестра HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services.

Однако, если вы впервые используете программу `mstsc.exe`, сначала следует настроить ее с помощью вкладок главного окна. Оно содержит следующие вкладки.

- Экран — позволяет указать размер окна удаленного подключения, а также разрядность цвета.
- Локальные ресурсы — дает возможность указать устройства и компоненты операционной системы, которыми можно будет пользоваться удаленно. Например, с помощью данной вкладки можно определить, на каком из компьютеров (локальном или удаленном) будет воспроизводиться звук, будет ли вам разрешено получить доступ к буферу обмена, принтерам, устройствам удаленного компьютера, подключенным к последовательным портам.
- Программы — позволяет указать программу, которая автоматически запустится после вашего входа на удаленный компьютер.
- Дополнительно — дает возможность определить следующие параметры, влияющие на быстродействие вашей работы с удаленным компьютером: будут ли отображаться обои Рабочего стола удаленного компьютера, будет ли отображаться содержимое окна удаленного компьютера при перетаскивании, будут ли применяться эффекты анимации работы с окнами удаленного компьютера и т. д.
- Подключение — позволяет настроить параметры подключения к шлюзу удаленного доступа, если он используется, а также параметры подключения при неудачной аутентификации.

Файл настроек подключения

После того как вы настроите параметры подключения удаленного доступа, обратите внимание на кнопку Сохранить вкладки Общие. С ее помощью можно занести все указанные вами настройки в специальный файл с расширением RDP (`default.rdp`). Впоследствии с помощью кнопки Открыть вкладки Общие вы сможете выбрать созданный ранее файл, чтобы при подключении использовались настройки, хранящиеся в нем.

ПРИМЕЧАНИЕ

Настроить многие дополнительные параметры работы терминальных служб можно и с помощью групповых политик. Для этого нужно зайти в раздел Конфигурация компьютера ▸ Административные шаблоны ▸ Компоненты Windows ▸ Службы терминалов оснастки gpedit.msc.

RDP-файлы представляют собой обычные текстовые файлы, которые содержат строки вида `<настройка>:i:<значение>`. Например, вы можете добавить к контекстному меню файлов с данным расширением команду открытия с помощью Блокнота, чтобы просмотреть их содержимое. Для этого достаточно воспользоваться

ветвью реестра HKEY_CLASSES_ROOT\RDP.File\Shell. Например, присвоить параметру (По умолчанию), расположенному в ветви реестра HKEY_CLASSES_ROOT\RDP.File\shell\notepad\command, значение notepad.exe %1.

Файлы с расширением RDP могут содержать следующие строки.

- desktopwidth:i — определяет ширину Рабочего стола (операционная система Windows CE поддерживает только полноэкранный режим).
- desktopheight:i — указывает ширину Рабочего стола.
- session bpp:i — определяет используемую глубину цвета.
- winposstr:i — указывает положение окна подключения к удаленному Рабочему столу на экране компьютеров.
- full address:s — определяет компьютер, к которому необходимо выполнить подключение.
- compression:i — указывает, будет ли использоваться сжатие данных при передаче на клиентский компьютер.
- keyboardhook:i — определяет, на каком из компьютеров (локальном или удаленном) будут выполняться команды, выполняемые при нажатии вами комбинации клавиш.
- audiomode:i — указывает, на каком из компьютеров (локальном или удаленном) будет воспроизводиться звук.
- redirectdrives:i — определяет, будет ли использоваться автоматическое подключение дисков локального компьютера при входе на удаленный компьютер. Если данная возможность включена, то в окне папки Компьютер удаленного компьютера будут отображаться не только диски удаленного компьютера, но и диски вашего компьютера. Это позволяет облегчить передачу информации между двумя компьютерами.
- redirectprinters:i — указывает, будет ли использоваться автоматическое подключение принтеров при входе на удаленный компьютер. Если данная возможность установлена, то вы сможете работать с подключенными к удаленному компьютеру принтерами, как будто они установлены на вашем компьютере.
- redirectcomports:i — определяет, будет ли использоваться автоматическое подключение COM-портов при входе на удаленный компьютер.
- redirectsmartcards:i — указывает, будет ли использоваться автоматическое подключение смарт-карт при входе на удаленный компьютер.
- displayconnectionbar:i — определяет, будет ли отображаться панель подключений при входе на удаленный компьютер. С ее помощью можно легко управлять размером экрана удаленного подключения.
- username:s — указывает имя пользователя, от имени которого будет выполняться подключение к удаленному компьютеру.
- domain:s — определяет домен, к компьютеру которого будет выполняться удаленное подключение.

- `alternate shell:s` — указывает программу, которая будет автоматически запускаться при входе пользователя на удаленный компьютер.
- `shell working directory:s` — определяет рабочий каталог программы, которая будет автоматически запускаться при входе пользователя на удаленный компьютер.
- `disable wallpaper:i` — указывает, будет ли отображаться фоновый рисунок на удаленном компьютере.
- `disable full window drag:i` — определяет, будет ли отображаться содержимое папки при перетаскивании на удаленном компьютере.
- `disable menu anims:i` — указывает, будет ли выполняться анимация меню и окон на удаленном компьютере.
- `disable themes:i` — определяет, будет ли разрешено использование тем на удаленном компьютере.
- `bitmapcachepersistenable:i` — указывает, будет ли выполняться кеширование графики удаленного компьютера на локальном компьютере. Кеширование позволяет повысить быстродействие работы на удаленном компьютере.
- `autoreconnection enabled:i` — определяет, будет ли клиентский компьютер автоматически переустанавливать разорванное соединение с удаленным компьютером.

Параметры программы mstsc.exe

Программа `mstsc.exe` также поддерживает следующие параметры.

- `/CONSOLE` — выполняет подключение к удаленному компьютеру в консольном режиме, который может использоваться операционной системой Windows Server 2003.
- `/PUBLIC` — запускает программу Подключение к удаленному рабочему столу в публичном режиме.
- `/MIGRATE` — преобразует файлы настроек, созданные с помощью Диспетчера клиентских подключений, в новый формат RDP-файлов.
- `/EDIT <файл с настройками соединения>` — позволяет изменить настройки соединения, описанные в указанном файле с расширением RDP.
- `/FULLSCREEN` — запускает программу Подключение к удаленному рабочему столу в полноэкранном режиме. Можно также использовать параметр `/f`.
- `/V:<компьютер>:<порт>` — определяет удаленный компьютер, к которому вы хотите подключиться, а также порт.

ПРИМЕЧАНИЕ

Изменить номер порта, на котором ожидает удаленный Рабочий стол, можно с помощью параметра REG_DWORD-типа PortNumber, расположенного в ветви реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer\WinStations\RDP-Tcp.

- `/W:<ширина в пикселах>` — определяет ширину окна программы Подключение к удаленному рабочему столу в пикселах.
- `/H:<высота в пикселах>` — указывает высоту окна программы Подключение к удаленному рабочему столу в пикселах.
- `/SPAN` — устанавливает соответствие между шириной и высотой удаленного Рабочего стола и локального виртуального Рабочего стола.

Программа также поддерживает следующие недокументированные параметры: `/WEB`, `/WEBFILENAME`, `/S`, `/C`, `/CLXCMDLINE`, `/REMOTECMDLINE`, `/REMOTEFILE`.

Другие программы

Операционная система Windows Vista содержит множество программ командной строки, которые позволяют просматривать состояние параметров работы терминальных служб и даже управлять некоторыми аспектами ее работы.

change.exe

Расположение: `%systemroot%\system32\change.exe`.

Данная программа позволяет изменить некоторые настройки терминальных служб операционной системы. Она поддерживает следующие параметры.

- `Logon` — позволяет отключить или включить возможность сетевого доступа к операционной системе компьютера. Возможны следующие команды с использованием данного параметра.
  - `Change logon /query` — отображает текущее состояние настройки.
  - `Change logon /enable` — разрешает сетевой доступ. Данная команда присваивает параметру `REG_DWORD`-типа `WinStationsDisabled`, расположенному в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`, значение `0`.
  - `Change logon /disable` — запрещает сетевой доступ. Команда присваивает параметру `REG_DWORD`-типа `WinStationsDisabled`, расположенному в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`, значение `1`.
- `Port` — позволяет просмотреть или удалить COM-порты, которые используются приложениями MS-DOS. Возможны следующие команды с использованием данного параметра:
  - `Change port portX=portY` — отображает COM-порт X на COM-порт Y, где X и Y определяют номера портов;
  - `Change port /query` — выводит список портов;
  - `Change /D portX` — удаляет отображение данного COM-порта.
- `User` — позволяет изменить режим сетевой установки приложений. Возможны следующие команды с использованием данного параметра:
  - `Change user /query` — отображает текущий режим;
  - `Change user /install` — изменяет текущий режим на режим установки;

- `Change user /execute` — меняет текущий режим на режим выполнения.

Query.exe

Расположение: `%systemroot%\system32\query.exe`.

Благодаря этой программе можно просмотреть список объектов, которые подключены в данный момент к серверу терминалов или используются им. Она не является нововведением операционной системы Windows Vista, однако раньше она присутствовала только в специальных редакциях операционных систем, управляющих серверами терминалов.

С помощью данной программы можно выполнить следующие действия.

- **Просмотр процессов, работающих на сервере терминалов.** Для выполнения этого действия используется такая команда, как `query process <фильтр> /SERVER:<сервер>`.

  В качестве фильтра можно указать имя пользователя, чьи процессы будут отображены, имя сессии, идентификатор (идентификатор нужно указывать в формате `/ID:<идентификатор>`), PID процесса, имя процесса или значение `*`. Если вы укажете значение `*`, то отобразится список всех процессов, работающих на сервере терминалов. Кроме названия процесса, также отображаются все сведения, по которым можно выполнять фильтрацию: имя пользователя, который запустил процесс, имя сессии и т. д.

  Параметр `/SERVER` не является обязательным. Если вы его не укажете, то отобразится список процессов локального компьютера.

- **Просмотр сессий сервера терминалов.** Для выполнения этого действия используется команда `query session /SERVER:<сервер>`, после выполнения которой отображаются такие сведения об активных в данный момент сессиях сервера терминалов, как имя сессии, имя пользователя, ID сессии, состояние сессии, тип и устройство. Как обычно, параметр `/SERVER` необязателен.

  Можно также использовать дополнительные параметры, с помощью которых просматривается дополнительная информация о сессиях.

  - `/MODE` — отображает поля Бод четности, Данные стоп, но скрывает поля с именем пользователя и ID.
  - `/FLOW` — показывает поле Управление потоком, но скрывает поля с именем пользователя и ID.
  - `/CONNECT` — отображает поле Подключение, но скрывает поля с именем пользователя и ID.
  - `/COUNTERS` — показывает дополнительные сведения о работе сервера терминалов: общее количество созданных сессий, общее количество завершенных сессий, общее количество пересозданных сессий.

- **Просмотр сведений о доступных в домене серверов терминалов.** Для выполнения этого действия используется команда `query termserver`. Можно также использовать параметр `/DOMAIN:`, чтобы указать конкретный домен, серверы которого нужно отобразить.

- **Просмотр сведений о пользователях, работающих с сервером терминалов.** Для выполнения этого действия используется команда `query user <фильтр> /SERVER:<сервер>`. В качестве фильтра можно указать имя пользователя, имя сессии, идентификатор сессии или вообще ничего не указывать. Если фильтр не указан, то будут отображены сведения обо всех пользователях, работающих с сервером в данный момент.

  С помощью данной команды можно просмотреть следующие сведения о пользователях: имя пользователя, имя сессии, идентификатор сессии, состояние сессии, время простоя сессии, а также время входа пользователя на сервер терминала.

Помимо команды `query user`, те же сведения можно получить с помощью новой программы командной строки `quser.exe`. Она представляет собой аналог данной команды и поддерживает все ее возможности.

Logoff.exe

Расположение: `%systemroot%\system32\logoff.exe`.

Данная программа командной строки является стандартной программой большинства версий операционной системы Windows. С ее помощью можно завершить как текущий сеанс работы на локальном компьютере (выполнить программу без параметров), так и конкретный сеанс на сервере терминалов. Для этого применяется следующий синтаксис программы: `logoff <имя или идентификатор сессии> /SERVER:<имя сервера терминалов>`.

Reset.exe

Расположение: `%systemroot%\system32\reset.exe`.

Можно также завершить открытый в данный момент сеанс службы терминалов. Для этого применяется команда `reset session <имя или идентификатор сессии> /SERVER:<имя сервера терминалов>`, которая не является нововведением операционной системы Windows Vista.

Настройка с помощью групповых политик

Операционная система Windows Vista поддерживает множество групповых политик, позволяющих настроить практически все аспекты работы терминальных служб. Все они описаны в файле `TerminalServer.admx` и расположены в разделе Конфигурация компьютера ▸ Административные шаблоны ▸ Компоненты Windows ▸ Службы терминалов.

Политики данного подраздела изменяют параметры `REG_DWORD`-типа, расположенные в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services`.

Например, в данном подразделе можно найти следующие политики.

- Разрешить переподключения только от исходного клиента — изменяет значение параметра `fReconnectSame`. Политика позволяет запретить пользователям выпол-

нение повторного подключения к завершенному сеансу с помощью другого компьютера (не того, с помощью которого они подключались в прошлый раз).

- Разрешать удаленное подключение с использованием служб терминалов — меняет значение параметра `fDenyTSConnections`. Политика дает возможность запретить подключение к компьютеру с помощью службы удаленных терминалов.
- Автоматическое переподключение — изменяет значение параметра `fDisableAutoReconnect`. Политика позволяет определить, будет ли программа Подключение к удаленному рабочему столу автоматически переподключаться к утерянной сессии.
- Настроить интервал проверки активности подключений — меняет значение параметров `KeepAliveEnable` и `KeepAliveInterval`. Политика дает возможность разрешить использование пакетов проверки работоспособности соединения, а также настроить интервал их отправки.
- Запретить завершение консольного сеанса администратора — изменяет значение параметра `fDisableForcibleLogoff`. Политика позволяет запретить или разрешить завершение текущего удаленного подключения администратора, если к удаленному компьютеру пытается подключиться другой администратор.
- Ограничить количество подключений — меняет значение параметра `MaxInstanceCount`. Политика дает возможность изменить максимальное количество подключений к удаленному серверу.
- Ограничить пользователей службы терминалов одним удаленным сеансом — изменяет значение параметра `fSingleSessionPerUser`. Политика позволяет запретить открытие нескольких сессий удаленного подключения к серверу.
- Устанавливает правила удаленного управления для сеансов пользователей служб терминалов — меняет значение параметра `Shadow`. Политика позволяет изменить параметры работы сессий удаленного подключения.

8.4. Новые возможности программ командной строки

В этом разделе мы рассмотрим новые программы командной строки, появившиеся в операционной системе Windows Vista и предоставляющие сетевые функции. Также будут рассмотрены новые команды уже присутствовавших ранее программ командной строки.

Rpcping.exe — пингование серверов удаленного доступа

Расположение: `%systemroot%\system32\rpcping.exe`.

Данная программа предназначена для выполнения пингования серверов удаленного компьютера с помощью службы Подключение к удаленному рабочему столу. Она поддерживает следующие параметры (это не полный список; чтобы просмотреть весь список параметров, введите команду `rpcping /?`).

- `-t <протоколы>` — позволяет указать последовательность используемых для пингования протоколов. По умолчанию значение данного параметра равно `ncacn_ip_tcp`. Однако можно указать одну из следующих последовательностей: `ncacn_ip_tcp`, `ncacn_np`, `ncacn_http`.
- `-s <компьютер>` — определяет удаленный компьютер, серверы которого нужно пинговать. Если параметр не указан, то будет выполняться пингование локального компьютера.
- `-i <количество попыток>` — указывает количество попыток связи с сервером. По умолчанию значение данного параметра равно `1`.
- `-u <протокол аутентификации>` — определяет протокол аутентификации, который будет применяться при связи с сервером. По умолчанию протокол аутентификации не применяется, однако вы можете указать одно из следующих значений: `Negotiate`, `NTLM`, `SChannel` или `Kerberos`.
- `-a <уровень аутентификации>` — позволяет указать уровень аутентификации для указанного протокола аутентификации. По умолчанию значение данного параметра не применяется, однако вы можете указать одно из следующих значений: `connect`, `call`, `pkt`, `integrity` или `privacy`.
- `-l <путь к файлу журнала>` — определяет файл журнала, в который будет заноситься информация о пинговании сервера.
- `-v <уровень>` — определяет уровень протоколирования информации, возвращаемой программой. По умолчанию значение параметра равно `1`, но можно указать значения вплоть до `3`. Чем больше значение, тем больше информации будет отображено.
- `-M <уровень>` — указывает уровень заимствования прав программой при соединении с сервером. По умолчанию уровень заимствования прав равен `impersonate`, однако также можно указывать одно из следующих значений: `anonymous`, `identify`, `impersonate` или `delegate`. Описание уровней заимствования прав было приведено в подразд. «Другие компоненты операционной системы» разд. 5.2.
- `-P <имя пользователя, домен, пароль>` — указывает параметры аутентификации на прокси-сервере, необходимые для пингования сервера при использовании прокси.
- `-F <флаги>` — определяет флаги, указывающие параметры аутентификации RPC/HTTP. Например, можно указать флаг `ssl` (использование протокола защищенной передачи данных (ssl) при аутентификации) или `first` (использование указанной схемы). Если вы используете данный параметр, то также должны быть указаны параметры `-u` и `-a`.
- `-H <схема аутентификации RPC/HTTP>` — может содержать одно из следующих значений (или несколько значений, перечисленных через запятую): `Basic`, `NTLM`, `Cert`. Если вы используете данный параметр, то также должны быть указаны параметры `-u` и `-a`.
- `-c` — при использовании этого параметра аутентификация будет выполняться на основе смарт-карты.

- `-d` — запускает программу сетевой диагностики службы Удаленный вызов процедур (RPC).

ftp.exe — доступ к серверам FTP

Расположение: `%systemroot%\system32\ftp.exe`.

Программа `ftp.exe` представляет собой FTP-клиент, позволяющий получить доступ к содержимому серверов FTP. Данная программа не является нововведением операционной системы Windows Vista, однако она поддерживает несколько новых параметров.

- `-x:<размер буфера передачи>` — позволяет переопределить стандартный размер буфера передачи. По умолчанию используется значение `8192`.
- `-r:<размер буфера приема>` — дает возможность переопределить стандартный размер буфера приема. По умолчанию используется значение `8192`.
- `-b:<количество>` — определяет количество асинхронных потоков. По умолчанию используется значение `3`.

Ipconfig.exe — отображение сведений о протоколе IP

Расположение: `%systemroot%\system32\Ipconfig.exe`.

Данная программа также не является нововведением операционной системы Windows Vista, однако она поддерживает один новый параметр: `/allcompartments`. Программа с этим параметром отображает информацию обо всех режимах работы сетевых протоколов.

Netsh.exe — настройка сетевых подключений

Расположение: `%systemroot%\system32\Netsh.exe`.

Программа `Netsh.exe` позволяет настроить многие параметры работы сетевых компонентов операционной системы Windows Vista. Она не является нововведением данной операционной системы, однако поддерживает множество новых команд.

Вообще, данная программа представляет собой очень интересный вид программ — она построена по модульному принципу. Иными словами, поддерживаемые ею команды зависят от библиотек, которые были зарегистрированы для работы с данной программой. При этом вы можете управлять списком зарегистрированных библиотек с помощью специальных команд программы `netsh.exe`.

- `Show helper` — отображает список зарегистрированных библиотек, а также команды программы, которые описаны в этих библиотеках.
- `Add helper <имя библиотеки>` — регистрирует новую библиотеку для работы с программой `netsh.exe`. Библиотеку можно зарегистрировать, если она поддерживает функцию `InitHelperDll`.

- `Delete helper <имя библиотеки>` — запрещает использование программой `netsh.exe` команд, описанных в данной библиотеке.

Список всх библиотек, используемых программой `netsh.exe`, содержится в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NetSh`.

Команда advfirewall

Данная команда добавлена с помощью библиотеки `AUTHFWCFG.DLL`. С ее помощью вы можете управлять новым стандартным брандмауэром операционной системы Windows Vista (не возможностями, предоставляемыми окном Брандмауэр Windows, а возможностями, реализованными в оснастке Брандмауэр Windows в режиме повышенной безопасности). Данная команда поддерживает следующие дочерние команды (на страницах книги они будут описаны поверхностно, детальное описание можно просмотреть, если ввести команду `netsh advfirewall <команда> /?`).

ПРИМЕЧАНИЕ

Отменить все изменения, которые вы сделали с помощью команд программы netsh.exe в данный сеанс работы, можно с помощью команды netsh abort.

- `Consec` — предоставляет интерфейс для работы с правилами брандмауэра, хранящимися в подразделе Правила безопасности подключения оснастки Брандмауэр Windows в режиме повышенной безопасности. Эта команда также поддерживает дочерние команды: `add` (добавить правило), `delete` (удалить правило), `dump` (отображает конфигурационный сценарий), `set` (изменяет существующее правило), `show` (отображает правила). Более подробно их описание можно просмотреть с помощью команды `netsh advfirewall consec <команда> /?`.
- `Export <путь к файлу>` — сохраняет текущие настройки параметров, которые можно изменить с помощью команд программы `netsh.exe`, в файл (с расширением POL).
- `Import <путь к файлу>` — восстанавливает настройки параметров, которые можно изменить с помощью команд программы `netsh.exe`, из созданного ранее файла.
- `Inbound` — предоставляет интерфейс для работы с правилами брандмауэра, хранящимися в подразделе Правила для входящих подключений оснастки Брандмауэр Windows в режиме повышенной безопасности. Эта команда также поддерживает дочерние команды: `add` (добавить правило), `delete` (удалить правило), `dump` (отображает конфигурационный сценарий), `set` (изменяет существующее правило), `show` (отображает правила). Более подробно их описание можно просмотреть с помощью команды `netsh advfirewall consec <команда> /?`.
- `Monitor` — позволяет получить доступ к сведениям о сопоставлениях безопасности (SA), о которых известно вашей операционной системе (позволяет получить доступ к сведениям подраздела Наблюдение ▸ Сопоставления безопасности оснастки Брандмауэр Windows в режиме повышенной безопасности). Команда

Monitor поддерживает следующие дочерние команды: delete (позволяет удалить SA), dump (отображает настройки конфигурационного файла), show (позволяет просмотреть сведения о нужном SA).

- Outbound — предоставляет интерфейс для работы с правилами брандмауэра, хранящимися в подразделе Правила для исходящего подключения оснастки Брандмауэр Windows в режиме повышенной безопасности. Она также поддерживает дочерние команды, которые полностью аналогичны дочерним командам команд inbound и consec.
- Reset export filename="путь к файлу" — восстанавливает настройки по умолчанию стандартного брандмауэра Windows, сохраняя текущие настройки в указанном файле.
- Set allprofiles|currentprofile|domainprofile|global|privateprofile|publicprofile — позволяет изменить настройки одного из профилей стандартного брандмауэра Windows Vista. Например, с помощью ее дочерних команд можно отключить профиль (команда state), разрешить или запретить все входящие/исходящие подключения (команда firewallpolicy), определить параметры ведения файла журнала (команда logging) и многое другое. Более подробно их описание можно просмотреть с помощью команды netsh advfirewall set allprofiles|currentprofile|domainprofile|global|privateprofile|publicprofile /?.
- Show allprofiles|currentprofile|domainprofile|global|privateprofile|publicprofile — позволяет просмотреть настройки одного из профилей стандартного брандмауэра Windows Vista. Например, она поддерживает следующие дочерние команды: State (определяет, включен ли профиль брандмауэера), firewallpolicy (определяет, какие подключения разрешены), Settings (отображает состояние дополнительных настроек профиля), Logging (отображает сведения о файле журнала).

Команда http

Команда добавлена с помощью библиотеки NSHHTTP.DLL. Она позволяет получить доступ к параметрам работы службы http и поддерживает следующие дочерние команды.

- Add — позволяет добавить адрес к таблице прослушиваемых адресов. Она включает в себя дочерние команды. Например, команду iplisten ipaddress="IP-адрес", которая добавляет новый адрес к списку прослушиваемых. Или команду sslcert, которая добавляет SSL-сервер сертификации, который будет обслуживать конкретный IP-адрес.
- Delete cache|iplisten|sslcert|timeout|urlacl — удаляет содержимое кеша, IP-адрес из таблицы, SSL-сертификат, глобальный таймер и т. д.
- Flush logbuffer — заносит сведения из буфера, предназначенного для накопления записей файла журнала, в файл журнала.
- Show — отображает параметры работы службы HTTP. Она поддерживает следующие дочерние команды: cachestate (отображает содержимое кеша ответов службы HTTP), iplisten (выводит список прослушиваемых службой

HTTP IP-адресов), `servicestate` (отображает информацию о работе службы HTTP), `sslcert` (выводит список сертификатов SSL, которые удостоверяют прослушиваемые IP-адреса), `timeout` (отображает значения глобальных таймаутов), `urlacl` (выводит список зарезервированных пространств имен URL).

Команда ipsec

Данная команда добавлена с помощью библиотеки `NSHIPSEC.DLL`. Она позволяет изменить параметры работы протокола IPSec и поддерживает следующие дочерние команды.

- `Dynamic` — поддерживает следующие дочерние команды: `add` (позволяет добавить политику основного или быстрого режима или правило и фильтр SPD), `delete` (дает возможность удалить политики или правила и фильтры), `dump` (отображает конфигурационный сценарий), `set` (позволяет изменить политики или правила и фильтры), `show` (отображает политики, фильтры, настройки, статистику IPSec и IKE).
- `Static` — поддерживает те же дочерние команды, что и команда `Dynamic`. Но, кроме них, также поддерживаются команды `exportpolicy` и `importpolicy`, которые дают возможность экспортировать политики в файл или импортировать их из него.

Команда lan

Данная команда добавлена с помощью библиотеки `DOT3CFG.DLL`. Она позволяет получить доступ к настройкам сети и сетевых интерфейсов операционной системы и поддерживает следующие дочерние команды.

ПРИМЕЧАНИЕ

Если вы имеете беспроводную сетевую карту, то для доступа к настройкам сетевых интерфейсов на ее основе необходимо, чтобы Служба автонастройки WLAN была запущена.

- `Add profile filename="путь к файлу профиля и его имя" interface="интерфейс"` — добавляет новый сетевой профиль, настройки которого содержатся в указанном файле.
- `Delete profile interface="интерфейс"` — удаляет соответствующий сетевой профиль.
- `Export profile folder="путь к каталогу"` — сохраняет настройки сетевых профилей в указанную вами папку (в формате XML).
- `Reconnect interface="интерфейс"` — переподключает данный сетевой профиль.
- `Set` — позволяет установить некоторые параметры работы всех сетевых профилей. Например, с помощью дочерней команды формата `tracing enabled=yes|no mode=nonpersistent|persistent` можно включить|отключить постоянный|непостоянный режим трассировки. А с помощью дочерней команды фор-

мата `autoconfig enabled=yes|no interface="интерфейс"` можно включить|отключить режим автоматической конфигурации для определенного сетевого профиля.

- `Show interfaces|profiles|settings|tracing` — отображает сведения о существующих интерфейсах, сетевых профилях, сетевых настройках, а также о режиме трассировки.

Команда nap

Данная команда добавлена с помощью библиотеки `NAPMONTR.DLL`. Она позволяет управлять работой механизма NAP операционной системы Windows Vista и поддерживает следующие дочерние команды.

- `Client` — позволяет управлять клиентами NAP. Она поддерживает множество дочерних команд: `add` (добавляет доверенный сервер или группу серверов), `delete` (удаляет доверенный сервер или группу серверов), `dump` (отображает конфигурационный сценарий), `export filename="имя файла"` (экспортирует настройки клиента NAP в XML-файл), `import filename="имя файла"` (импортирует настройки клиента NAP из файла), `rename` (переименовывает доверенный сервер или группу серверов), `reset` (сбрасывает такую конфигурацию клиента NAP как CSP (Cryptographic service provider), доверенные серверы и группы, пользовательские интерфейсы и т. д.), `set` (изменяет параметры конфигурации клиента NAP), `show` (отображает текущие параметры конфигурации клиента NAP).
- `Reset configuration` — сбрасывает все настройки NAP.
- `Show configuration` — отображает текущие параметры конфигурации клиента NAP.

Команда netio

Данная команда добавлена с помощью библиотеки `NETIOHLP.DLL`. Она поддерживает следующие дочерние команды:

- `Add bindingfilter` — добавляет новый фильтр привязки;
- `Delete bindingfilter` — удаляет фильтр привязки;
- `Show bindingfilters store=active|persistent` — отображает список используемых в данный момент или постоянных фильтров.

Команда p2p

Данная команда добавлена с помощью библиотеки `P2PNETSH.DLL`. Она позволяет настроить параметры работы одноранговых сетей и поддерживает следующие дочерние команды.

- `Collab contact` — дает возможность управлять контактами апплета Соседние пользователи: экспортировать и импортировать их (дочерние команды `export` и `import`), изменять (команда `set`) или просматривать (команда `show`).
- `Group` — позволяет работать с группами одноранговых сетей.

- `Idmgr` — дает возможность получить доступ к менеджеру идентификации. Она поддерживает дочерние команды `delete` и `show`.
- `Pnrp` — позволяет управлять областями одноранговых сетей, а также работой одноранговой сети.

Команда rpc

Данная команда добавлена с помощью библиотеки `RPCNSH.DLL`. Она позволяет управлять настройками RPC и поддерживает следующие дочерние команды:

- `Add <подсети через пробел>` — создает список подсетей;
- `Delete <подсети через пробел>` — удаляет список подсетей;
- `Filter` — позволяет добавить (дочерняя команда `add`), удалить (дочерняя команда `delete`) или просмотреть (дочерняя команда `show filter`) список RPC-фильтров или правил стандартного брандмауэра Windows Vista;
- `Reset` — сбрасывает все настройки RPC;
- `Show` — отображает сведения о состоянии каждой подсети RPC.

Команда winhttp

Эта команда добавлена с помощью библиотеки `WHHELPER.DLL`. Она позволяет управлять настройками WinHTTP и поддерживает следующие дочерние команды.

- `Proxy` — позволяет просмотреть, изменить или импортировать настройки прокси-сервера для браузера Internet Explorer.
- `Tracing` — дает возможность настроить (дочерняя команда `config`), отключить (`disable`), включить (`enable`) или просмотреть конфигурацию трассировки WinHTTP (`show`).

Команда wlan

Данная команда добавлена с помощью библиотеки `WLANCFG.DLL`. Она позволяет работать с беспроводными сетями и поддерживает следующие дочерние команды.

- `Add filter|profile` — позволяет добавить новый сетевой профиль или фильтры стандартного брандмауэра Windows Vista.
- `Connect ssid="SSID сети" name="сетевой профиль" interface="интерфейс"` — выполняет подключение к указанной беспроводной сети.
- `Delete filter|profile` — дает возможность удалить сетевой профиль или фильтры стандартного брандмауэра Windows Vista.
- `Disconnect interface="интерфейс"` — отключается от указанной беспроводной сети.
- `Export profile folder="каталог"` — экспортирует настройки сетевых профилей в XML-файлы указанного каталога.
- `Set` — позволяет изменить настройки беспроводного подключения. Она поддерживает следующие дочерние команды: `AutoConfig enabled=yes|no`

`interface="интерфейс"` (устанавливает или отключает автоконфигурацию указанного беспроводного интерфейса), `blockednetworks display=show|hide` (позволяет определить, будут ли отображаться блокированные сети в списке сетей), `profileorder` (изменяет порядок использования профилей беспроводных сетей), `tracing` (позволяет включить или отключить трассировку работы беспроводного интерфейса).

- `Show all|autoconfig|blockednetworks|drivers|filters|interfaces|networks|profiles|settings|tracing` — отображает соответствующую информацию о работе беспроводной сети

Netstat.exe — сведения о работе сетевого соединения

Расположение: `%systemroot%\system32\Netstat.exe`.

Программа `netstat.exe` позволяет просмотреть список портов, которые в данный момент открыты или прослушиваются, а также определить IP-адрес компьютера, с которым ведется работа, и процесс (по PID процесса), который открыл соответствующий порт. Например, это можно сделать с помощью команды вида `Netstat -ano > c:\netstat.txt`. После выполнения этой команды на диске `C:` будет создан файл `netstat.txt`, содержащий список открытых в данный момент портов.

Программа иногда используется и для проверки корректности работы какого-нибудь удаленного подключения. Проверяются состояние используемого подключением порта и количество байт, которые находятся в очереди на передачу или прием.

Данная программа также не является нововведением операционной системы Windows Vista, однако она поддерживает несколько новых параметров:

- `-f` — отображать FQDN имя для неизвестных адресов;
- `-t` — показывать состояния текущих соединений.

Ping.exe — пингование удаленных компьютеров

Расположение: `%systemroot%\system32\Ping.exe`.

Программа `Ping.exe` предназначена для поиска удаленного компьютера с помощью ICMP-запросов. Она позволяет определить, может ли компьютер отправлять ICMP-пакеты другому компьютеру. Иначе говоря, данную команду можно применять при неполадках в работе сети, чтобы проверить, связаны они с сетевым оборудованием или настройками сети.

Программу `Ping.exe` часто используют для передачи пакетов на адрес 127.0.0.1 (то есть на свой же компьютер), чтобы проверить, корректно ли работает стек TCP/IP компьютера. Если пакеты доставить не удалось, значит, стек IP не отвечает, что может происходить вследствие повреждения драйвера TCP, неработающего сетевого адаптера или сторонней службы, которая мешает работе IP.

Ее также можно использовать для передачи пакетов на локальный IP-адрес. Это позволяет определить, содержит ли ошибки таблица маршрутизации драйвера сетевого адаптера (если содержит, то передача пакетов завершится неудачно).

Программа `Ping.exe` также применяется для передачи пакетов на IP-адрес маршрутизатора по умолчанию, чтобы проверить, работает ли он в данный момент.

Данная программа также не является нововведением операционной системы Windows Vista, однако поддерживает несколько новых параметров.

- `-R` — отображает информацию о пути передачи и подтверждения протокола IPv6.
- `-S <адрес источника>` — определяет адрес источника, который будет использоваться протоколом IPv6.
- `-4` — для работы программы использовать протокол IPv4.
- `-6` — для работы программы использовать протокол IPv6.

Route.exe — работа с функциями маршрутизации

Расположение: `%systemroot%\system32\Route.exe`.

Программа `route.exe` позволяет просмотреть таблицу маршрутизации для протоколов IPv4 и IPv6. Это может быть необходимо в том случае, если вы точно знаете, что удаленный компьютер работает, но связаться с ним не получается. При этом программа `ping.exe` корректно передает пакеты на локальный адрес и на адрес маршрутизатора по умолчанию. Для просмотра таблицы маршрутизации можно воспользоваться командой `route print`.

Данная программа также не является нововведением операционной системы Windows Vista, однако она поддерживает несколько новых параметров:

- `-4` — для работы программы использовать протокол IPv4;
- `-6` — для работы программы использовать протокол IPv6.

Tracert.exe — отображение пути до адресата

Расположение: `%systemroot%\system32\Tracert.exe`.

Программа `tracert.exe` позволяет просмотреть список маршрутизаторов, через которые проходит пакет перед тем, как попасть к пункту назначения. Это может быть необходимо в том случае, если вы точно знаете, что удаленный компьютер работает, но связаться с ним не получается. При этом программа `ping.exe` корректно передает пакеты на локальный адрес и на адрес маршрутизатора по умолчанию.

Принцип работы данной программы довольно прост: она отправляет сообщения ICMP с эхо-запросами, пока очередное сообщение не дойдет до узла-назначения, последовательно увеличивая значение поля TTL. При этом каждый маршрутиза-

тор, который получил сообщение со значением TTL, равным 0, удаляет такое сообщение и посылает программе tracert.exe пакет ICMP с сообщением о том, что сообщение было удалено. На основе этих пакетов программа строит список маршрутизаторов, через которые был передан пакет.

Программа tracert.exe также не является нововведением операционной системы Windows Vista, однако поддерживает несколько новых параметров:

- -R — отображает информацию о пути передачи и подтверждения протокола IPv6;
- -S <адрес источника> — определяет адрес источника, который будет использоваться протоколом IPv6;
- -4 — для работы программы использовать протокол IPv4;
- -6 — для работы программы использовать протокол IPv6.

Arp.exe — работа с таблицей ARP

Расположение: %systemroot%\system32\arp.exe.

С помощью данной программы можно просматривать и управлять таблицей ARP. Также одним из способов устранения неполадок в работе сети (если раньше сеть работала и если отправка сообщений на свой адрес с помощью программы ping.exe работает корректно) является очистка кеша ARP от записей. Для этого можно либо удалить все записи для конкретного IP-адреса (подключение к которому выполнить не удается), для чего нужно выполнить команду arp -d <IP-адрес>, либо удалить все содержимое таблицы ARP с помощью команды netsh interface ip delete arpcache.

Данная программа не является нововведением операционной системы Windows Vista, однако в этой операционной системе она стала поддерживать дополнительный параметр -v, с помощью которого можно отобразить расширенную информацию об элементах таблицы ARP.

8.5. Протокол iSCSI

iSCSI — это протокол для доступа и действий с системами хранения данных, серверами и клиентами, работа над которым началась в 2000 году. Работа данного протокола основана на стеке TCP/IP.

Протокол iSCSI описывает:

- новый транспортный протокол, работающий поверх TCP;
- механизм инкапсуляции команд iSCSI в сети IP;
- протокол, применяемый для новой генерации систем хранения данных, использующих родной TCP/IP.

Пакеты iSCSI канального уровня должны передаваться последовательно, без задержек и без нарушения порядка передачи (то есть совершенно противоположно IP-пакетам). Для этого к заголовку пакета будет добавлено новое поле.

Работа протокола iSCSI построена на основе модели клиент/сервер. Клиент инициирует запросы на считывание данных с сервера, который является системой хранения данных. В рамках данной модели клиента iSCSI также называют инициатором. Именно такое название используется в операционной системе Windows Vista.

iSCSI состоит из четырех компонентов: компонент управления именами и адресами (iSCSI Address and Naming Conventions), компонент управления сеансом (iSCSI Session Management), компонент обработки ошибок (iSCSI Error Handling), а также компонент, управляющий безопасностью (iSCSI Security). Компонент управления именами и адресами работает с сетевыми сущностями. Сетевая сущность — это один или несколько iSCSI-узлов или сетевых порталов, доступных через сеть. Компонент управления сеансом выполняет аутентификацию, обмен и завершение сеанса подключения к системе хранения данных. Компонент обработки ошибок буферизирует каждую команду iSCSI, чтобы при возникновении ошибки можно было эту команду достать из буфера и послать повторно. Он также выполняет восстановление поврежденного соединения, закрытие и повторную инициацию сессии.

Окно Свойства: Инициатор iSCSI

Чтобы настроить клиент iSCSI в операционной системе Windows Vista, нужно воспользоваться значком Инициатор iSCSI папки Панель управления. После щелчка кнопкой мыши на этом значке откроется окно Свойства: Инициатор iSCSI, имеющее следующие вкладки.

- Общие — с помощью данной вкладки можно переименовать инициатор iSCSI, установить пароль для CHAP-аутентификации, а также создать туннель IPSec.
- Обнаружение — позволяет просмотреть списки найденных порталов назначения, а также iSNS-серверов (отображается адрес, порт, сетевой адаптер портала или только имя iSNS-сервера). Кроме того, с помощью кнопки Добавить вы можете добавить новый портал или iSNS-сервер. А с помощью кнопки Удалить — удалить уже существующий.
- Конечные объекты — отображает сведения об устройствах хранения, к которым вы подключены.
- Избранные конечные объекты — выводит сведения об избранных устройствах хранения, к которым вы подключены.
- Тома и устройства — показывает список новых разделов вашего компьютера, которые были добавлены благодаря избранным устройствам хранения (подключенные системы хранения данных отображаются в вашем компьютере как новые жесткие диски).
- RADIUS — содержит описание серверов RADIUS, а также позволяет добавить или удалить сервер. С помощью кнопки RADIUS вы также можете установить новый пароль для аутентификации RADIUS.

Настройка с помощью групповых политик

Политики данного раздела изменяют значения следующих параметров REG_DWORD-типа, расположенных в ветви HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\iSCSI:

- RestrictAdditionalLogins — если значение данного параметра равно 1, то подключение с помощью непостоянных учетных данных будет запрещено;
- ChangeIQNName — при установке значения этого параметра равным 1 будет запрещено изменение iqn имени инициатора;
- ChangeCHAPSecret — если значение данного параметра равно 1, то изменение пароля CHAP будет запрещено;
- RequireIPSec — при установке значения этого параметра равным 1 будет запрещено создание сеанса iSCSI, если не используется протокол IPSec;
- RequireMutualCHAP — если значение данного параметра равно 1, то создание сеансов без взаимной проверки подлинности CHAP будет запрещено.
- RequireOneWayCHAP — при установке значения этого параметра равным 1 будут запрещены сеансы, не настроенные для односторонней проверки подлинности CHAP;
- NewStaticTargets — если значение данного параметра равно 1, то ручное изменение имени и портала для найденного объекта будет запрещено;
- ConfigureTargets — при установке значения этого параметра равным 1 будет запрещено ручное конфигурирование найденного объекта;
- ConfigureiSNSServers — если значение данного параметра равно 1, то новые серверы iSNS не могут быть добавлены, а уже существующие не могут быть удалены;
- ConfigureTargetPortals — при установке значения этого параметра равным 1 новые порталы не могут быть добавлены, а уже существующие не могут быть удалены.

Использование репозитария CIM

Пространство имен \\root\wmi операционной системы Windows Vista теперь хранит набор новых классов, свойства и методы которых предназначены для настройки протокола iSCSI и работы с ним. Рассмотрим эти классы.

Класс ISCSI_IP_Address

Он поддерживает следующие свойства, доступные как для чтения, так и для записи.

- IpV4Address, тип: uint32 — содержит IPv4-адрес, если он определен.
- IpV6Address, тип: массив значений uint8 — хранит IPv6-адрес, если он определен.
- IpV6FlowInfo, тип: uint32 — содержит информацию о потоке IPv6.

- `IpV6ScopeId`, тип: `uint32` — хранит идентификатор области IPv6.
- `TextAddress`, тип: `string` — значение данного свойства не может быть больше 256 символов. Содержит DNS-адрес или IP-адрес в виде строки.
- `Type`, тип: `uint32` — определяет тип адреса. Если значение свойства равно `0`, то используется текстовая строка адреса (DNS-имя или точечный адрес). Если значение равно `1`, то используется IPv4-адрес. Если значение свойства равно `2`, то используется IPv6-адрес. Если же значение равно `3`, то используется пустая строка адреса.

Класс ISCSI_TargetPortal

Данный класс описывает сетевой портал. Он поддерживает следующие свойства, доступные как для чтения, так и для записи:

- `Address`, тип: указатель на класс `ISCSI_IP_Address` — содержит сетевой адрес портала;
- `Socket`, тип: `uint16` — хранит номер порта.

Класс ISCSI_TargetPortalGroup

Содержит описание группы сетевых порталов. Данный класс поддерживает следующие свойства, доступные как для чтения, так и для записи:

- `PortalCount`, тип: `uint32` — определяет количество элементов в группе;
- `Portals`, тип: указатель на класс `ISCSI_TargetPortal` — содержит указатель на эти элементы группы.

Класс ISCSI_LoginOptions

Хранит настройки подключения к адресу назначения. Данный класс поддерживает следующие свойства, доступные как для чтения, так и для записи.

- `AuthType`, тип: `uint32` — определяет тип используемой при подключении аутентификации. Если значение данного свойства равно `0`, то аутентификация не требуется. Если значение равно `1`, то используется аутентификация с помощью метода CHAP. Если же значение свойства равно `2`, то используется аутентификация с помощью метода Mutual CHAP.
- `DataDigest`, тип: `uint32` — указывает способ создания контрольной суммы для данных при подключении. Если значение данного свойства равно `0`, то контрольная сумма не создается. Если же значение равно `1`, то используется контрольная сумма на основе метода CRC32C.
- `DefaultTime2Retain`, тип: `uint32` — определяет используемое по умолчанию время в секундах, которое должно пройти перед тем как сеанс окончательно завершится, если текущий сеанс неожиданно завершился или произошел сброс связи.
- `DefaultTime2Wait`, тип: `uint32` — указывает используемое по умолчанию время в секундах, которое должно пройти перед попыткой завершения сеанса после неожиданного завершения связи или сброса связи.

- HeaderDigest, тип: uint32 — определяет способ создания контрольной суммы для заголовка при подключении. Если значение данного свойства равно 0, то контрольная сумма не создается. Если же значение равно 1, то используется контрольная сумма на основе метода CRC32C.
- InformationSpecified, тип: uint32 — биты данного флага определяют используемые при подключении параметры. Данное свойство является битовой маской, содержащей следующие значащие биты, которые говорят о том, что будет использоваться значение свойства:
  - 0 — HeaderDigest;
  - 1 — DataDigest;
  - 2 — MaxConnections;
  - 3 — DefaultTime2Wait;
  - 4 — DefaultTime2Retain.
- LoginFlags, тип: uint32 — биты данного флага определяют возможности, которые можно использовать при подключении. Данное свойство является битовой маской, которая содержит следующие значащие биты:
  - 0 — определяет, поддерживается ли протокол IPSec;
  - 1 — указывает, поддерживаются ли множественные пути;
  - 3 — разрешает выполнять хопы через ворота.
- MaximumConnections, тип: uint32 — определяет максимально возможное количество соединений.

Класс ISCSI_LUNList

Данный класс описывает карту от OS LUN к адресу назначения устройства LUN. Он поддерживает следующие свойства, доступные как для чтения, так и для записи:

- OSLUN, тип: uint32 — содержит номер шины SCSI операционной системы;
- TargetLUN, тип: uint64 — определяет адрес назначения LUN.

Класс ISCSI_TargetMapping

Класс описывает карту от адреса назначения LUN до порта драйвера LUN операционной системы Windows. Он поддерживает следующие свойства, доступные только для чтения.

- FromPersistentLogin, тип: boolean — если сессия создана с помощью постоянной учетной записи, то свойство имеет значение true.
- LUNCount, тип: uint32 — определяет количество LUN карты.
- LUNList, тип: указатель на класс ISCSI_LUNList — содержит указатель на список LUN.
- OSBus, тип: uint32 — хранит номер шины SCSI операционной системы. Если значение свойства равно 0xffffffff, то номер шины SCSI определяется мини-портом.

- `OSTarget`, тип: `uint32` — содержит номер назначения SCSI операционной системы. Если значение свойства равно `0xffffffff`, то номер определяется мини-портом.
- `TargetName`, тип: `string` — хранит имя назначения.
- `UniqueSessionId`, тип: `uint64` — содержит уникальный идентификатор сессии.

Класс MSiSCSI_TCPIPConfig

Определяет конфигурацию TCP/IP для работы с iSCSI. Если не сказано об обратном, то свойства данного класса доступны как для чтения, так и для записи.

- `Active`, тип: `boolean` — указывает, активна ли данная конфигурация.
- `AlternateDNSServer`, тип: указатель на класс `ISCSI_IP_Address` — определяет имя альтернативного DNS-сервера.
- `DefaultGateway`, тип: указатель на класс `ISCSI_IP_Address` — указывает адрес шлюза, используемого по умолчанию.
- `EnableDHCP`, тип: `boolean` — определяет, разрешено ли использование сервера DHCP.
- `InstanceName`, тип: `string` — свойство является ключевым. Оно содержит имя экземпляра класса.
- `IpAddress`, тип: указатель на класс `ISCSI_IP_Address` — определяет IP-адрес.
- `IPVersions`, тип: `uint32` — доступно только для чтения. Указывает версию протокола IP.
- `PreferredDNSServer`, тип: указатель на класс `ISCSI_IP_Address` — определяет адрес предпочитаемого сервера DNS.
- `SubnetMask`, тип: указатель на класс `ISCSI_IP_Address` — указывает маску IP-адреса.
- `UseDHCPForDNS`, тип: `boolean` — определяет, будет ли использоваться DHCP для сервера DNS.
- `UseLinkLocalAddress`, тип: `boolean` — указывает, будет ли использоваться линия связи по локальному адресу.

Класс MSiSCSI_NICConfig

Определяет конфигурацию NIC. Если не сказано об обратном, то свойства данного класса доступны только для чтения.

- `Active`, тип: `boolean` — свойство доступно как для чтения, так и для записи. Оно определяет, активна ли данная конфигурация в текущий момент.
- `InstanceName`, тип: `string` — является ключевым.
- `LinkSpeed`, тип: `uint32` — указывает скорость сетевого подключения в мегабитах в секунду.
- `LinkState`, тип: `uint32` — определяет состояние линии связи. Если значение свойства равно `0`, то сетевое подключение разъединено. Если же значение данного свойства равно `1`, то сетевое соединение активно.

- MacAddress, тип: массив значений uint8 — указывает MAC-адрес сетевой карты.
- MaxFrameSize, тип: uint32 — определяет максимальный размер фрейма.
- MaxLinkSpeed, тип: uint32 — указывает максимальную скорость линии связи.

Класс MSiSCSI_BootConfiguration

Содержит настройки загрузочного устройства. Он поддерживает следующие свойства, доступные как для чтения, так и для записи.

- Active, тип: boolean — определяет, активна ли данная конфигурация.
- DiscoverBootDevice, тип: boolean — указывает, возможно ли динамическое обнаружение загрузочного устройства.
- InitiatorNode, тип: string — определяет название iSCSI узла инициатора, используемого для соединения. Если значение данного свойства пусто, то сетевой адаптер сам может выбрать название. Значение данного свойства не может быть больше 223 символов.
- InstanceName, тип: string — свойство является ключевым.
- LoginOptions, тип: указатель на класс ISCSI_LoginOptions — указывает параметры, используемые при подключении.
- LUN, тип: uint64 — определяет LUN, используемый загрузочным устройством.
- Password, тип: массив значений uint8 — указывает используемый при аутентификации пароль.
- PasswordSize, тип: uint32 — определяет длину пароля.
- SecurityFlags, тип: uint64 — содержит флаги безопасности. Например, битовая маска 0x00000040 говорит о предпочтении создания туннеля при подключении. Битовая маска 0x00000008 говорит о том, что агрессивный режим на данном подключении разрешен. Битовая маска же 0x00000002 говорит о том, что при подключении разрешено использовать протоколы IKE/IPSec.
- TargetName, тип: string — значение данного свойства не может быть больше 223 символов. Оно определяет имя адреса назначения iSCSI для загрузочного устройства.
- TargetPortal, тип: указатель на класс ISCSI_TargetPortal — указывает ворота, используемые при подключении.
- Username, тип: массив значений uint8 — определяет имя пользователя.
- UsernameSize, тип: uint32 — указывает размер имени пользователя.

Класс MSiSCSI_SecurityCapabilities

Содержит описание возможностей настройки безопасности. Если не сказано об обратном, то свойства данного класса доступны только для чтения.

- Active, тип: boolean — свойство доступно как для чтения, так и для записи. Оно определяет, активна ли данная конфигурация.

- `CertificatesSupported`, тип: `boolean` — указывает, поддерживает ли данный адаптер использование при подключении сертификатов.
- `EncryptionAvailable`, тип: массив значений `uint32` — определяет используемые подключением типы шифрования. Значение `0` говорит о том, что шифрование можно не выполнять. Значение `1` говорит о том, что для шифрования можно использовать алгоритмы 3DES HMAC/SHA1. Значение `2` говорит о том, что для шифрования можно использовать алгоритмы AES-CTR/CBC-MAC с XCBC.
- `EncryptionAvailableCount`, тип: `uint32` — указывает количество поддерживаемых типов шифрования.
- `InstanceName`, тип: `string` — свойство является ключевым.
- `ProtectiScsiTraffic`, тип: `boolean` — если значение данного свойства равно `true`, то адаптер может использовать протокол IPSec для трафика iSCSI.
- `ProtectiSNSTraffic`, тип: `boolean` — если значение свойства равно `true`, то адаптер может использовать протокол IPSec для трафика iSNS.

Класс MSiSCSI_DiscoveryConfig

Содержит настройки обнаружения iSNS-серверов, а также сетевых порталов. Он поддерживает следующие свойства, доступные как для чтения, так и для записи.

- `Active`, тип: `boolean` — определяет, активна ли данная конфигурация.
- `AutomaticiSNSDiscovery`, тип: `boolean` — если значение данного свойства равно `false`, то адаптер не может автоматически обнаруживать серверы iSNS.
- `InitiatorName`, тип: `string` — определяет имя, используемое для регистрации с iSNS. Значение данного свойства не может содержать больше чем 256 символов.
- `InstanceName`, тип: `string` — свойство является ключевым.
- `iSNSServer`, тип: указатель на класс `ISCSI_IP_Address` — содержит адрес сервера iSNS, если адаптер не может автоматически находить серверы iSNS.
- `PerformiSNSDiscovery`, тип: `boolean` — если значение данного свойства равно `false`, то адаптер не может обнаруживать компьютеры с помощью iSNS.
- `PerformSLPDiscovery`, тип: `boolean` — если значение свойства равно `false`, то адаптер не может обнаруживать компьютеры с помощью iSNS.

Класс MSiSCSI_RADIUSConfig

Определяет конфигурацию RADIUS. Он поддерживает следующие свойства, доступные как для чтения, так и для записи.

- `Active`, тип: `boolean` — указывает, активна ли данная конфигурация.
- `BackupRADIUSServer`, тип: указатель на класс `ISCSI_IP_Address` — определяет адрес для резервного сервера RADIUS.
- `InstanceName`, тип: `string` — свойство является ключевым.

- RADIUSServer, тип: указатель на класс ISCSI_IP_Address — определяет адрес для главного сервера RADIUS.
- SharedSecret, тип: массив значений uint8 — указывает пароль, используемый для взаимодействия главного севера RADIUS с резервным сервером.
- SharedSecretSizeInBytes, тип: uint32 — содержит размер общего секрета в байтах.
- UseRADIUSForCHAP, тип: boolean — если значение данного свойства равно false, то адаптер не может использовать сервер RADIUS для аутентификации CHAP.

Класс MSiSCSI_HBAInformation

Содержит информацию об адаптере HBA. Если не сказано об обратном, то свойства данного класса доступны только для чтения.

- Active, тип: boolean — свойство доступно как для чтения, так и для записи. Оно определяет, активна ли данная конфигурация.
- AsicVersion, тип: string — указывает версию Asic. Значение данного свойства не может содержать больше чем 255 символов.
- BiDiScsiCommands, тип: boolean — если интеллектуальные команды SCSI поддерживаются, то значение данного свойства равно true.
- CacheValid, тип: boolean — если значение данного свойства равно true, то кеш адаптера корректен.
- DriverName, тип: string — определяет название драйвера адаптера. Значение данного свойства не может содержать больше чем 255 символов.
- FirmwareVersion, тип: string — указывает версию программного обеспечения адаптера. Значение данного свойства не может содержать больше чем 255 символов.
- FunctionalitySupported, тип: uint32 — биты данной битовой маски определяют поддерживаемые HBA возможности. Например, битовая маска 0x00000008 определяет возможность аутентификации CHAP с помощью сервера RADIUS, а битовая маска 0x00000010 определяет возможность обнаружения с помощью iSNS. Битовая маска 0x00000020 определяет возможность обнаружения с помощью SLP.
- GenerationalGuid, тип: uint32 — указывает последний CLSID-номер, установленный методом SetGenerationalGuid класса MSiSCSI_Operations.
- InstanceName, тип: string — свойство является ключевым.
- IntegratedTCPIP, тип: boolean — доступно как для чтения, так и для записи. Если значение свойства равно true, то трафик TCP/IP объединен с сетевым стеком протокола TCP/IP операционной системы Windows только с помощью программного обеспечения инициатора.
- MaxCDBLength, тип: uint32 — определяет максимальную длину CDB, поддерживаемую адаптером.

- `MultifunctionDevice`, тип: `boolean` — если значение данного свойства равно `true`, то адаптер является многофункциональным устройством.
- `NumberOfPorts`, тип: `uint32` — определяет количество портов адаптера.
- `OptionRomVersion`, тип: `string` — указывает описание версии адаптера. Значение данного свойства не может содержать больше чем 255 символов.
- `RequiresBinaryIpAddresses`, тип: `boolean` — свойство доступно как для чтения, так и для записи. Если значение данного свойства равно `true`, то Служба инициатора Майкрософт iSCSI может выполнять поиск DNS и передавать IP-адреса на адаптер. Адаптер должен быть в той же сети стека TCP/IP. Если же значение данного свойства равно `false`, то сервер DNS должен находиться на адаптере.
- `SerialNumber`, тип: `string` — определяет серийный номер адаптера. Значение данного свойства не может содержать больше чем 255 символов.
- `Status`, тип: `uint32` — указывает статус работы адаптера. Если значение данного свойства равно `0`, то адаптер находится в рабочем состоянии. Если значение равно `1`, то состояние адаптера ухудшается. Если же значение данного свойства равно `2`, то адаптер находится в критическом состоянии. Ну, а если значение данного свойства равно `3`, то работа адаптера больше невозможна.
- `UniqueAdapterId`, тип: `uint32` — содержит уникальный адрес для всех инициаторов iSCSI, который может быть адресом расширения адаптера или другим адресом, принадлежащим драйверу устройства. Данное свойство доступно как для чтения, так и для записи.
- `VendorID`, тип: `string` — хранит идентификатор производителя адаптера. Значение данного свойства не может содержать больше чем 255 символов.
- `VendorModel`, тип: `string` — содержит описание модели адаптера. Значение данного свойства не может содержать больше чем 255 символов.
- `VendorVersion`, тип: `string` — хранит версию адаптера. Значение данного свойства не может содержать больше чем 255 символов.
- `VersionMax`, тип: `uint32` — содержит основную версию адаптера.
- `VersionMin`, тип: `uint32` — хранит дополнительную версию адаптера.

Класс MSiSCSI_HBASessionConfig

Содержит используемые по умолчанию настройки сессии адаптера HBA. Он поддерживает следующие свойства, доступные как для чтения, так и для записи.

- `Active`, тип: `boolean` — указывает, активна ли данная конфигурация.
- `FirstBurstLength`, тип: `uint32` — содержит максимальное количество байт, которые можно послать в незапрашиваемом пакете iSCSI инициатора при выполнении одной команды iSCSI.
- `ImmediateData`, тип: `boolean` — определяет, поддерживают ли компьютер назначения и инициатор непосредственно получаемые данные.

- InitialR2T, тип: boolean — указывает, возможно ли использование R2T. Отключение R2T позволяет инициатору посылать данные, как будто полученные от R2T со смещением буфера, равным 0, и минимальной длиной передаваемых данных.
- InstanceName, тип: string — свойство является ключевым.
- MaxBurstLength, тип: uint32 — определяет максимальный размер полезных данных (в байтах) в пакете SCSI.
- MaxOutstandingR2T, тип: uint32 — указывает максимальное количество просроченных R2T на процесс, исключая начальный R2T.
- MaxRecvDataSegmentLength, тип: uint32 — определяет максимальную длину полученного iSCSI сегмента данных в байтах.

Класс ISCSI_ConnectionStaticInfo

Содержит информацию о статическом соединении iSCSI. Данный класс поддерживает следующие свойства, доступные только для чтения.

- AuthType, тип: uint32 — указывает тип используемой при подключении аутентификации. Если значение данного свойства равно 0, то аутентификация не требуется. Если значение свойства равно 1, то используется аутентификация с помощью метода CHAP. Если же значение равно 2, то используется аутентификация с помощью метода Mutual CHAP.
- CID, тип: uint16 — определяет идентификатор соединения iSCSI.
- DataIntegrity, тип: uint8 — указывает способ создания контрольной суммы для данных iSCSI. Если значение свойства равно 0, то контрольная сумма не создается. Если же значение равно 1, то используется контрольная сумма на основе метода CRC32C.
- EstimatedThroughput, тип: uint64 — определяет предполагаемую пропускную способность данного соединения в байтах в секунду.
- HeaderIntegrity, тип: uint8 — указывает способ создания контрольной суммы для заголовка пакетов iSCSI. Если значение свойства равно 0, то контрольная сумма не создается. Если же значение равно 1, то используется контрольная сумма на основе метода CRC32C.
- LocalAddr, тип: указатель на класс ISCSI_IP_Address — содержит локальный сетевой адрес данного соединения.
- LocalPort, тип: uint32 — хранит локальный порт данного соединения.
- MaxDatagramSize, тип: uint32 — содержит максимальную длину датаграммы в байтах.
- MaxRecvDataSegmentLength, тип: uint32 — определяет максимальную длину полученного iSCSI сегмента данных или команды в байтах.
- Protocol, тип: uint8 — указывает транспортный протокол, используемый соединением. Если значение свойства равно 6, то используется протокол TCP.

- `RemoteAddr`, тип: указатель на класс `ISCSI_IP_Address` — содержит удаленный сетевой адрес данного соединения.
- `RemotePort`, тип: `uint32` — хранит удаленный порт данного соединения.
- `State`, тип: `uint8` — определяет текущее состояние работы соединения. Если значение свойства равно `0`, то выполняется установление сеанса. Если значение равно `1`, то соединение используется. Если же значение равно `2`, то работа сеанса завершена.
- `UniqueConnectionId`, тип: `uint64` — указывает уникальный идентификатор соединения.

Класс ISCSI_SessionStaticInfo

Содержит информацию об установленной сессии. Данный класс поддерживает следующие свойства, доступные только для чтения.

- `ConnectionCount`, тип: `uint16` — содержит количество соединений в сессии.
- `ConnectionsList`, тип: указатель на класс `ISCSI_ConnectionStaticInfo` — хранит список соединений в сессии.
- `DataPduInOrder`, тип: `boolean` — если значение свойства равно `false`, то данные PDU в пределах последовательности могут находиться в любом порядке. Если же значение равно `true`, то данные PDU в пределах последовательности должны иметь постоянно увеличивающиеся адреса.
- `DataSequenceInOrder`, тип: `boolean` — если значение свойства равно `false`, то данные последовательности PDU могут находиться в любом порядке. Если же значение равно `true`, то данные последовательности PDU должны иметь постоянно увеличивающиеся смещения.
- `ErrorRecoveryLevel`, тип: `uint8` — содержит уровень восстановления при возникновении ошибки между инициатором и компьютером назначения.
- `FirstBurstLength`, тип: `uint32` — определяет максимальную длину отправляемых в сессии данных.
- `ImmediateData`, тип: `boolean` — указывает, поддерживают ли компьютер назначения и инициатор непосредственно получаемые данные.
- `InitialR2t`, тип: `boolean` — если значение свойства равно `true`, то инициатор должен ждать R2T перед посылкой данных компьютеру назначения. Если же значение равно `false`, то инициатор может послать данные немедленно, если количество уже посланных данных не больше значения свойства `FirstBurstSize`.
- `InitiatoriSCSIName`, тип: `string` — определяет имя инициатора iSCSI в сессии. Значение данного свойства не может содержать больше 223 символов.
- `ISID`, тип: массив значений `uint8` — указывает идентификатор сессии iSCSI.
- `MaxBurstLength`, тип: `uint32` — определяет максимальное количество байт, которые можно послать в пределах единственной последовательности данных.

- MaxConnections, тип: uint32 — указывает максимальное количество соединений в сессии.
- MaxOutstandingR2t, тип: uint32 — определяет максимальное количество просроченных R2T на процесс сессии.
- TargetiSCSIName, тип: string — содержит iSCSI-имя компьютера назначения. Значение данного свойства не может содержать больше 223 символов.
- TSID, тип: uint16 — определяет идентификатор iSCSI компьютера назначения.
- Type, тип: uint8 — указывает тип сессии iSCSI. Если значение свойства равно 0, то установлена сессия обнаружения. Если значение равно 1, то установлена информационная сессия. Если же значение свойства равно 2, то установлена сессия передачи данных. Ну, а если значение равно 3, то установлена загрузочная сессия.
- UniqueSessionId, тип: uint64 — определяет уникальный идентификатор сессии. Значение данного свойства можно получить с помощью метода LoginToTarget.

Класс ISCSI_PortalInfo

Содержит информацию о воротах iSCSI. Данный класс поддерживает следующие свойства, доступные только для чтения.

- Index, тип: uint32 — содержит уникальный идентификатор порта.
- IPAddr, тип: указатель на класс ISCSI_IP_Address — хранит IP-адрес.
- Port, тип: uint32 — содержит номер порта.
- PortalTag, тип: uint16 — хранит агрегированный тег, используемый механизмом COM.
- PortalType, тип: uint8 — определяет тип ворот. Если значение свойства равно 0, то ворота являются инициатором. Если же значение равно 1, то компьютером назначения.
- Protocol, тип: uint8 — указывает транспортный протокол, используемый сессией. Если значение свойства равно 6, то используется протокол TCP.

Класс MSiSCSI_PortalInfoClass

Содержит информацию о классе портала iSCSI. Он поддерживает следующие свойства, доступные только для чтения.

- Active, тип: boolean — указывает, активна ли данная конфигурация.
- InstanceName, тип: string — свойство является ключевым.
- PortalInfoCount, тип: uint32 — определяет количество порталов, описанных в свойстве PortalInformation.
- PortalInformation, тип: указатель на класс ISCSI_PortalInfo — содержит описание используемых порталов.

Класс MSiSCSI_InitiatorSessionInfo

Содержит информацию об инициаторах iSCSI. Данный класс поддерживает следующие свойства, доступные только для чтения.

- `Active`, тип: `boolean` — указывает, активна ли данная конфигурация.
- `InstanceName`, тип: `string` — свойство является ключевым.
- `SessionCount`, тип: `uint32` — определяет количество элементов в массиве свойства `SessionsList`.
- `SessionsList`, тип: указатель на класс `ISCSI_SessionStaticInfo` — указывает список установленных сессий.
- `UniqueAdapterId`, тип: `uint64` — определяет уникальный идентификатор адаптера.

Класс MSiSCSI_InitiatorNodeFailureEvent

Содержит описание ошибки в работе инициатора iSCSI. Если не сказано об обратном, то свойства данного класса доступны только для чтения.

- `Active`, тип: `boolean` — указывает, активна ли данная конфигурация.
- `FailureTime`, тип: `uint64` — определяет время обнаружения ошибки.
- `FailureType`, тип: `uint8` — указывает тип ошибки. Например, если значение свойства равно `1`, то ошибка произошла во время аутентификации при установлении сеанса. Если значение равно `3`, то ошибка произошла во время переговоров при установлении сеанса. А если значение свойства равно `4`, то ошибка произошла во время завершения сеанса.
- `InstanceName`, тип: `string` — свойство является ключевым.
- `SECURITY_DESCRIPTOR`, тип: массив значений `uint8` — доступно как для чтения, так и для записи. Оно определяет идентификатор безопасности.
- `TargetFailureAddr`, тип: указатель на класс `ISCSI_IP_Address` — указывает адрес компьютера назначения, при работе с которым произошла ошибка.
- `TargetFailureName`, тип: `string` — определяет имя компьютера назначения, при работе с которым произошла ошибка. Значение данного свойства не может содержать больше 223 символов.
- `TIME_CREATED`, тип: `uint64` — содержит время создания данного экземпляра класса (то есть время возникновения ошибки).

Класс MSiSCSI_InitiatorInstanceFailureEvent

Содержит описание ошибки в запросе инициатора iSCSI. Если не сказано об обратном, то свойства данного класса доступны только для чтения.

- `Active`, тип: `boolean` — указывает, активна ли данная конфигурация.
- `FailureType`, тип: `uint8` — определяет тип ошибки. Например, если значение свойства равно `0`, то ошибка состоит в несовпадении контрольной суммы. Если значение равно `2`, то ошибка в формате сообщения.
- `InstanceName`, тип: `string` — свойство является ключевым.

- RemoteNodeName, тип: string — значение данного свойства не может содержать больше 223 символов. Оно определяет имя компьютера назначения, при работе с которым произошла ошибка.
- SECURITY_DESCRIPTOR, тип: массив значений uint8 — свойство доступно как для чтения, так и для записи. Оно определяет идентификатор безопасности.
- TIME_CREATED, тип: uint64 — содержит время создания.

Класс ISCSI_Path

Данный класс описывает соединение инициатора iSCSI с системой хранения данных. Он поддерживает следующие свойства, доступные как для чтения, так и для записи.

- ConnectionStatus, тип: uint32 — определяет статус соединения. Если значение свойства равно 1, то соединение установлено. Если значение равно 2, то соединение разъединено. Если же значение равно 3, то выполняется переподключение.
- EstimatedLinkSpeed, тип: uint64 — указывает приблизительную скорость соединения в мегабитах в секунду.
- PathWeight, тип: uint32 — определяет длину пути данного соединения.
- PrimaryPath, тип: uint32 — если данный путь является основным, то значение этого свойства равно 1.
- TCPOffLoadAvailable, тип: uint32 — если значение свойства равно 1, то разгрузка TCP поддерживается данным соединением.
- UniqueConnectionId, тип: uint64 — указывает уникальный идентификатор iSCSI-соединения.

Класс ISCSI_Supported_LB_Policies

Содержит настройки политики балансировки загрузки. Свойства данного класса поддерживают как чтение, так и запись.

- iSCSI_PathCount, тип: uint32 — содержит количество элементов в значении свойства iSCSI_Paths.
- iSCSI_Paths, тип: указатель на класс ISCSI_Path — описывает соединения iSCSI.
- LoadBalancePolicy, тип: uint32 — определяет политики балансировки нагрузки для данных соединений. Свойство может содержать следующие значения:
  - 1 — на основе количества ошибок;
  - 2 — Round Robin;
  - 3 — Round Robin с подмножеством;
  - 4 — на основе наименьшей глубины очереди;
  - 5 — на основе длины пути соединения;
  - 6 — определены производителем.
- UniqueSessionId, тип: uint64 — указывает уникальный идентификатор данной сессии с использованием соответствующего адаптера.

Класс MSiSCSI_LB_Operations

Определяет новые параметры балансировки нагрузки. Свойства данного класса доступны только для чтения.

- `Active`, тип: `boolean` — указывает, активна ли данная конфигурация.
- `InstanceName`, тип: `string` — свойство является ключевым.

Класс также поддерживает метод `SetLoadBalancePolicy`, который устанавливает новую политику балансировки загрузки для инициатора iSCSI.

Входящий параметр: указатель на класс `LoadBalancePolicies`.

Возвращаемый параметр: определяет статус. Данный параметр имеет тип `uint32`.

Класс MSiSCSI_QueryLBPolicy

Содержит информацию о текущей политике балансировки загрузки для данного инициатора iSCSI. Свойства данного класса поддерживают как чтение, так и запись.

- `Active`, тип: `boolean` — указывает, активна ли данная конфигурация.
- `InstanceName`, тип: `string` — свойство является ключевым.
- `LoadBalancePolicies`, тип: указатель на класс `ISCSI_Supported_LB_Policies` — определяет политику балансировки нагрузки.
- `SessionCount`, тип: `uint32` — содержит количество элементов свойства `LoadBalancePolicies`.
- `UniqueAdapterId`, тип: `uint64` — указывает уникальный идентификатор адаптера.

Класс MSiSCSI_Eventlog

Содержит параметры записи событий в журнал iSCSI. Свойства данного класса поддерживают как чтение, так и запись.

- `Active`, тип: `boolean` — указывает, активна ли данная конфигурация.
- `AdditionalData`, тип: массив значений `uint8` — определяет дополнительные данные, помещаемые в журнал при описании возникшего события.
- `InstanceName`, тип: `string` — свойство является ключевым.
- `LogToEventlog`, тип: `uint32` — если значение свойства равно `0`, то события не записываются в системный журнал Windows.
- `SECURITY_DESCRIPTOR`, тип: массив значений `uint8` — определяет дескриптор безопасности.
- `Size`, тип: `uint32` — указывает размер дополнительных данных.
- `TIME_CREATED`, тип: `uint64` — определяет дату создания.
- `Type`, тип: `uint32` — указывает тип записываемого в журнал события.

Класс ISCSI_RedirectPortalInfo

Содержит информацию о порталах перенаправления iSCSI.

- `OriginalIPAddr`, тип: указатель на класс `ISCSI_IP_Address` — содержит IP-адрес компьютера назначения, используемый при подключении.
- `OriginalPort`, тип: `uint32` — хранит номер порта компьютера назначения, используемый при подключении.
- `Redirected`, тип: `uint8` — если значение свойства равно `true`, то подключение было перенаправлено.
- `RedirectedIPAddr`, тип: указатель на класс `ISCSI_IP_Address` — указывает IP-адрес, на который было перенаправлено подключение.
- `RedirectedPort`, тип: `uint32` — определяет номер порта, на который подключение было перенаправлено.
- `TemporaryRedirect`, тип: `uint8` — если значение свойства равно `true`, то перенаправление было временным.
- `UniqueConnectionId`, тип: `uint64` — содержит уникальный идентификатор соединения.

Класс ISCSI_RedirectSessionInfo

Содержит информацию о перенаправленной сессии iSCSI.

- `ConnectionCount`, тип: `uint32` — определяет количество элементов в свойстве `RedirectPortalList`.
- `RedirectPortalList`, тип: указатель на класс `ISCSI_RedirectPortalInfo` — содержит список всех перенаправлений.
- `TargetPortalGroupTag`, тип: `uint32` — хранит тег группы для данной сессии.
- `UniqueSessionId`, тип: `uint64` — содержит уникальный идентификатор сессии.

Класс MSiSCSI_RedirectPortalInfoClass

Содержит информацию о классе перенаправлений iSCSI.

- `Active`, тип: `boolean` — указывает, активна ли данная конфигурация.
- `InstanceName`, тип: `string` — свойство является ключевым.
- `RedirectSessionList`, тип: указатель на класс `ISCSI_RedirectSessionInfo` — содержит список перенаправленных сессий.
- `SessionCount`, тип: `uint32` — определяет количество элементов свойства `RedirectSessionList`.
- `UniqueAdapterId`, тип: `uint64` — указывает уникальный идентификатор адаптера.

Класс MSiSCSI_ManagementOperations

Содержит описание операций управления iSCSI. Свойства данного класса доступны как для чтения, так и для записи.

- `Active`, тип: `boolean` — указывает, активна ли данная конфигурация.
- `InstanceName`, тип: `string` — свойство является ключевым.

Класс также поддерживает метод `PingIPAddress`, который выполняет пингование IP-адреса с помощью протокола ICMP.

Входящие параметры:

- указатель на класс `ISCSI_IP_Address`;
- количество отправленных запросов, имеет тип `uint32`;
- размер отправленных запросов, имеет тип `uint32`;
- таймаут между отправлениями запросов, имеет тип `uint32`.

Возвращаемые параметры:

- содержит ответы на ICMP-запросы пингования, имеет тип `uint32`;
- определяет статус, имеет тип `uint32`.

Класс MSiSCSI_MMIPSECStats

Содержит статистику работы протокола IPSec в основном режиме. Данный класс поддерживает следующие свойства, доступные только для чтения.

- `AcquireFailures`, тип: `uint64` — определяет количество времени, потраченного на обработку ошибок.
- `AcquireHeapSize`, тип: `uint64` — указывает количество записей в куче. Чем больше загрузка сети, тем больше количество записей.
- `Active`, тип: `boolean` — указывает, активна ли данная конфигурация.
- `ActiveAcquire`, тип: `uint64` — определяет количество запросов драйвера IPSec, которые выполняют задачи IKE.
- `ActiveReceive`, тип: `uint64` — указывает количество полученных от очереди для обработки сообщений IKE.
- `AuthenticationFailures`, тип: `uint64` — содержит общее количество ошибок, возникших при проверке подлинности.
- `Caption`, тип: `string` — значение данного свойства не может содержать больше 64 символов.
- `ConnectionListSize`, тип: `uint64` — определяет количество соединений в быстром режиме.
- `GetSPIFailures`, тип: `uint64` — общее количество ошибочных запросов IKE, содержащих уникальный индекс параметров безопасности SPI.

- `InstanceName`, тип: `string` — свойство является ключевым.
- `InvalidCookiesReceived`, тип: `uint64` — указывает количество cookies в полученных сообщениях IKE, которые недействительны в основном режиме.
- `InvalidPackets`, тип: `uint64` — определяет количество полученных некорректных пакетов IKE.
- `KeyAdditionFailures`, тип: `uint64` — указывает количество некорректных исходящих пакетов быстрого режима SA, подчиненных IKE.
- `KeyAdditions`, тип: `uint64` — определяет количество исходящих пакетов быстрого режима SA, добавленных к IKE.
- `KeyUpdateFailures`, тип: `uint64` — указывает количество некорректных входящих пакетов быстрого режима SA, добавленных к IKE.
- `KeyUpdates`, тип: `uint64` — определяет количество входящих пакетов быстрого режима SA, добавленных к IKE.
- `Name`, тип: `string` — значение данного свойства не может содержать больше 256 символов.
- `NegotiationFailures`, тип: `uint64` — определяет общее количество отказов в переговорах, произошедших как в основном, так и в быстром режиме.
- `OakleyMainMode`, тип: `uint64` — указывает общее количество успешных режимов SAs, созданных во время переговоров основного режима.
- `OakleyQuickMode`, тип: `uint64` — определяет общее количество успешных режимов SAs, созданных во время переговоров быстрого режима.
- `ReceiveFailures`, тип: `uint64` — указывает количество времени, которое стек TCP получал ошибочные сообщения IKE.
- `ReceiveHeapSize`, тип: `uint64` — определяет количество буферов IKE для входящих сообщений.
- `SendFailures`, тип: `uint64` — указывает количество времени, которое стек TCP отправлял ошибочные сообщения IKE.
- `SoftAssociations`, тип: `uint64` — определяет общее количество переговоров, которые привели к использованию режима SAs. Режим SAs обычно используется в том случае, если компьютер не может работать в основном режиме.
- `TotalGetSPI`, тип: `uint64` — указывает общее количество запросов к IKE на получение SPI.

Класс MSiSCSI_QMIPSECStats

Содержит статистику работы протокола IPSec в быстром режиме. Данный класс поддерживает следующие свойства, доступные только для чтения.

- `Active`, тип: `boolean` — указывает, активна ли данная конфигурация.
- `ActiveSA`, тип: `uint64` — определяет количество активных IPSEC SAs.
- `ActiveTunnels`, тип: `uint64` — указывает количество активных туннелей IPSec.

- `AuthenticatedBytesReceived`, тип: `uint64` — определяет количество байт, полученных при использовании протокола AH.
- `AuthenticatedBytesSent`, тип: `uint64` — указывает количество байт, отправленных при использовании протокола AH.
- `BadSPIPackets`, тип: `uint64` — определяет количество некорректных пакетов с SPI.
- `Caption`, тип: `string` — значение свойства не может содержать более 64 символов.
- `ConfidentialBytesReceived`, тип: `uint64` — определяет количество байт, полученных при использовании протокола ESP.
- `ConfidentialBytesSent`, тип: `uint64` — указывает количество байт, отправленных при использовании протокола ESP.
- `InstanceName`, тип: `string` — свойство является ключевым.
- `KeyAdditions`, тип: `uint64` — определяет общее количество успешных переговоров IPSec SA.
- `KeyDeletions`, тип: `uint64` — указывает общее количество удаленных ключей IPSec SA.
- `Name`, тип: `string` — значение данного свойства не может содержать более 256 символов.
- `PacketsNotAuthenticated`, тип: `uint64` — определяет общее количество пакетов без аутентификации данных.
- `PacketsNotDecrypted`, тип: `uint64` — указывает общее количество некорректно расшифрованных пакетов.
- `PacketsWithReplayDetection`, тип: `uint64` — определяет общее количество пакетов, которые содержат корректное поле Порядковый номер.
- `PendingKeyOperations`, тип: `uint64` — указывает количество незавершенных операций с ключами IPSec.
- `ReKeys`, тип: `uint64` — определяет количество операций повторного получения ключа для IPSec SAs.
- `TransportBytesReceived`, тип: `uint64` — указывает количество байт, полученных при использовании протокола IPSec.
- `TransportBytesSent`, тип: `uint64` — определяет количество байт, отправленных при использовании протокола IPSec.
- `TunnelBytesReceived`, тип: `uint64` — указывает количество байт, полученных при использовании туннельного режима протокола IPSec.
- `TunnelBytesSent`, тип: `uint64` — определяет количество байт, отправленных при использовании туннельного режима протокола IPSec.

Класс MSiSCSI_ConnectionStatistics

Содержит статистику по соединению IPSec. Данный класс поддерживает следующие свойства, доступные только для чтения.

- Active, тип: boolean — указывает, активна ли данная конфигурация.
- BytesReceived, тип: uint64 — определяет количество полученных по данному соединению байт.
- BytesSent, тип: uint64 — указывает количество отправленных по данному соединению байт.
- Caption, тип: string — значение данного свойства не может содержать более 64 символов.
- CID, тип: uint16 — содержит идентификатор соединения iSCSI.
- InstanceName, тип: string — свойство является ключевым.
- iSCSIName, тип: string — указывает имя компьютера назначения iSCSI. Значение данного свойства не может содержать более 223 символов.
- Name, тип: string — значение данного свойства не может содержать более 256 символов.
- PDUCommandsSent, тип: uint64 — определяет количество отправленных по данному соединению PDU.
- PDUResponsesReceived, тип: uint64 — указывает количество полученных по данному соединению PDU.
- UniqueAdapterId, тип: uint64 — содержит уникальный идентификатор адаптера.
- USID, тип: uint64 — хранит уникальный идентификатор сессии, используемый только внутри самой сессии. Данный идентификатор возвращается методом LoginToTarget.

Класс MSiSCSI_SessionStatistics

Содержит статистику по сессии IPSec. Данный класс поддерживает следующие свойства, доступные только для чтения.

- Active, тип: boolean — указывает, активна ли данная конфигурация.
- BytesReceived, тип: uint64 — определяет количество полученных по данной сессии байт.
- BytesSent, тип: uint64 — указывает количество отправленных по данной сессии байт.
- Caption, тип: string — значение данного свойства не может содержать более 64 символов.
- ConnectionTimeoutErrors, тип: uint64 — определяет количество ошибок преувеличения таймаута, произошедших за данную сессию.
- DigestErrors, тип: uint64 — указывает количество ошибок в контрольной сумме пакетов.
- FormatErrors, тип: uint64 — определяет количество ошибок в формате пакета.
- InstanceName, тип: string — свойство является ключевым.

- `iSCSIName`, тип: `string` — указывает имя компьютера назначения iSCSI. Значение свойства не может содержать более 223 символов.
- `Name`, тип: `string` — значение данного свойства не может содержать более 256 символов.
- `PDUCommandsSent`, тип: `uint64` — определяет количество отправленных в данной сессии PDU.
- `PDUResponsesReceived`, тип: `uint64` — указывает количество полученных в данной сессии PDU.
- `UniqueAdapterId`, тип: `uint64` — содержит уникальный идентификатор адаптера.
- `USID`, тип: `uint64` — хранит уникальный идентификатор сессии, используемый только внутри самой сессии. Данный идентификатор возвращается методом `LoginToTarget`.

Класс MSiSCSI_InitiatorLoginStatistics

Содержит статистику подключений к инициатору iSCSI. Данный класс поддерживает следующие свойства, доступные только для чтения.

- `Active`, тип: `boolean` — указывает, активна ли данная конфигурация.
- `Caption`, тип: `string` — значение свойства не может содержать более 64 символов.
- `InstanceName`, тип: `string` — свойство является ключевым.
- `LoginAcceptRsps`, тип: `uint32` — определяет количество принятых ответов.
- `LoginAuthenticateFails`, тип: `uint32` — указывает количество времени, затраченного на подключения с ошибочной аутентификацией.
- `LoginAuthFailRsps`, тип: `uint32` — определяет количество подключений, которые не состоялись из-за ошибочного отклика.
- `LoginFailures`, тип: `uint32` — указывает количество времени, потраченного на неудачные попытки подключения.
- `LoginNegotiateFails`, тип: `uint32` — определяет количество времени, потраченного на неудачные переговоры с компьютером назначения.
- `LoginOtherFailRsps`, тип: `uint32` — указывает количество других ошибок, из-за которых не удалось установить сеанс.
- `LoginRedirectRsps`, тип: `uint32` — определяет количество перенаправленных откликов установки сеанса.
- `LogoutNormals`, тип: `uint32` — указывает количество нормальных завершений сеанса (с кодом причины завершения 0).
- `LogoutOtherCodes`, тип: `uint32` — определяет количество завершений сеанса с ненулевым кодом причины завершения.
- `Name`, тип: `string` — значение данного свойства не может содержать более 256 символов.

- UniqueAdapterId, тип: uint64 — содержит уникальный идентификатор адаптера.

Класс MSiSCSI_InitiatorInstanceStatistics

Содержит статистику запросов инициатора iSCSI. Данный класс поддерживает следующие свойства, доступные только для чтения.

- Active, тип: boolean — указывает, активна ли данная конфигурация.
- Caption, тип: string — значение данного свойства не может содержать более 64 символов.
- InstanceName, тип: string — свойство является ключевым.
- Name, тип: string — значение свойства не может содержать более 256 символов.
- SessionConnectionTimeoutErrorCount, тип: uint32 — определяет количество ошибок преувеличения таймаута сессии.
- SessionDigestErrorCount, тип: uint32 — указывает количество ошибок в контрольной сумме пакетов сессий.
- SessionFailureCount, тип: uint32 — определяет количество ошибочных сессий, принадлежащих данному запросу.
- SessionFormatErrorCount, тип: uint32 — указывает количество ошибок в формате пакетов сессий.
- UniqueAdapterId, тип: uint64 — содержит уникальный идентификатор адаптера.

Класс MSiSCSI_NICPerformance

Представляет собой базовый абстрактный класс провайдера. Он поддерживает следующие свойства, доступные только для чтения.

- Active, тип: boolean — указывает, активна ли данная конфигурация.
- BytesReceived, тип: uint32 — определяет количество байт, полученных с помощью порта Ethernet.
- BytesTransmitted, тип: uint32 — указывает количество байт, переданных с помощью порта Ethernet.
- Caption, тип: string — значение данного свойства не может содержать более 64 символов.
- InstanceName, тип: string — свойство является ключевым.
- Name, тип: string — значение данного свойства не может содержать более 64 символов.
- PDUReceived, тип: uint32 — определяет количество PDU, полученных с помощью порта Ethernet.
- PDUTransmitted, тип: uint32 — указывает количество PDU, переданных с помощью порта Ethernet.

Класс MSiSCSI_RequestTimeStatistics

Определяет статистику по времени запросов iSCSI.

- `Active`, тип: `boolean` — указывает, активна ли данная конфигурация.
- `AverageProcessingTime`, тип: `uint32` — определяет среднее время, потраченное процессом на запросы по данному соединению.
- `Caption`, тип: `string` — значение данного свойства не может содержать более 64 символов.
- `CID`, тип: `uint16` — содержит идентификатор соединения.
- `InstanceName`, тип: `string` — свойство является ключевым.
- `iSCSIName`, тип: `string` — определяет имя компьютера назначения iSCSI. Значение свойства не может содержать более 223 символов.
- `MaximumProcessingTime`, тип: `uint32` — указывает максимальное время, потраченное процессом на запросы по данному соединению.
- `Name`, тип: `string` — значение свойства не может содержать более 256 символов.
- `UniqueAdapterId`, тип: `uint64` — содержит уникальный идентификатор адаптера.
- `USID`, тип: `uint64` — хранит уникальный идентификатор сессии, используемый только внутри самой сессии. Данный идентификатор возвращается методом `LoginToTarget`.

8.6. Создание общих папок

Механизм создания общих папок в операционной системе Windows Vista практически такой же, что и в предыдущих версиях этой операционной системы, однако имеет несколько особенностей, на которых будет сделан акцент.

ПРИМЕЧАНИЕ

Просмотреть список общих папок, созданных в операционной системе, можно с помощью экземпляров стандартного класса репозитария CIM Win32_Share. Данный класс содержится в пространстве имен \\root\cimv2 и позволяет обращаться к следующим основным свойствам: AllowMaximum (указывает, ограничено ли количество одновременно подключенных пользователей), Name (определяет название общей папки), Description (указывает описание общей папки), Path (определяет путь к общей папке), Type (определяет типа общего ресурса, который может принимать значения от 0 до 7 (соответственно Дисковый накопитель, Очередь печати, Устройство, IPC, Администратор диска, Администратор очереди печати, Администратор устройств, Администратор IPC)).

Класс также поддерживает следующие методы: Create (позволяет создать общую папку), Delete (удаляет общий ресурс), GetAccessMask (возвращает права доступа к общему ресурсу), SetShareInfo (изменяет настройки для общей папки).

Но перед тем как рассматривать создание общих папок в операционной системе Windows Vista, нужно обратить внимание на несколько параметров мастера Центр управления сетями и общим доступом. Его можно отобразить с помощью одноименного значка папки Панель управления или контекстного меню значка сети в области уведомлений.

Параметры мастера Центр управления сетями и общим доступом

Полностью возможности данного мастера мы уже рассматривали ранее в этой книге, однако тогда мы умышленно упустили область Общий доступ и сетевое обнаружение. Сейчас же мы рассмотрим переключатели данной области (чтобы просмотреть описание определенного переключателя и изменить его положение, его нужно сначала раскрыть с помощью стрелки вниз, расположенной справа от элемента).

- Сетевое обнаружение — определяет, будет ли виден ваш компьютер в сети и сможете ли вы увидеть другие компьютеры сети. Установка данного переключателя в положение вкл. приводит к тому, что вы сможете увидеть другие компьютеры сети.

  С помощью данного переключателя, если его раскрыть, можно изменить название рабочей группы, в которую входит ваш компьютер. Для этого нужно нажать кнопку Изменить параметры. Это приведет к открытию окна Свойства системы.

- Общий доступ к файлам — указывает, можно ли будет получить доступ к общим папкам вашего компьютера и будут ли они видны в сети. Установка данного переключателя в положение вкл. приводит к тому, что к общим папкам вашего компьютера можно будет получить доступ. На уровне же реестра это изменяет некоторые правила стандартного брандмауэра Windows Vista, описанные в ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules`.

- Общий доступ к общим папкам — определяет, будет ли папка Общие общей. При этом данный переключатель можно установить в следующие положения.

  - Включить общий доступ, чтобы сетевые пользователи могли открывать файлы — разрешить пользователям сети получать доступ только на чтение к папке Общие. Установка в это положение приводит к созданию общей папки с именем Общие.
  - Включить общий доступ, чтобы сетевые пользователи могли открывать, изменять и создавать файлы — позволить пользователям сети получать полный доступ к папке Общие. Установка в это положение приводит к созданию общей папки с именем Общие.
  - Отключить общий доступ (пользователи, выполнившие вход на этот компьютер, будут иметь доступ к общим папкам) — запретить общий доступ к папке Общие. Установка в это положение удаляет параметр `Public` из ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Shares`.

- Использование общих принтеров — указывает, будут ли общими принтеры, подключенные к вашему компьютеру (если установить переключатель в положение вкл., то будут). Установка переключателя приводит к созданию общего скрытого ресурса `print$`, а также общих ресурсов для каждого подключенного к вашему компьютеру принтера и для стандартного принтера Microsoft Office Document Image Writer.
- Общий доступ с парольной защитой — определяет, смогут ли пользователи, не имеющие учетных записей на данном компьютере, получить доступ к общим папкам. Установка данного переключателя в положение вкл. приводит к тому, что пользователи, не имеющие учетных записей, не смогут получить доступ к общим папкам вашего компьютера.
- Общий доступ к медиафайлам — указывает, будет ли ваша музыкальная библиотека общей. Чтобы сделать библиотеку общей, нужно нажать кнопку Изменить и в появившемся окне Общий доступ к файлам мультимедиа установить флажок Открыть общий доступ к моим файлам мультимедиа.

Использование вкладки Доступ

После того как вы изменили параметры доступа к общим ресурсам с помощью мастера Центр управления сетями и общим доступом, можно приступать к созданию своей общей папки. Для этого нужно открыть окно Свойства папки (в ее контекстном меню выбрать команду Свойства) и перейти на вкладку Доступ. Вид данной вкладки представлен на рис. 8.7.

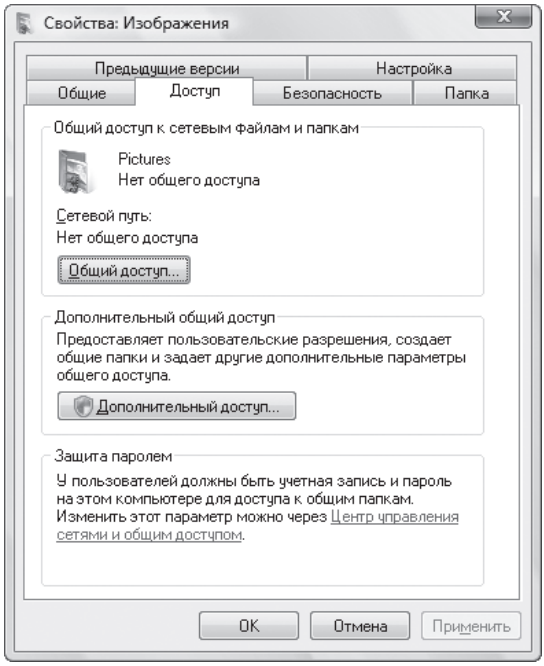

Рис. 8.7. Вкладка Доступ, предназначенная для создания общих папок

Вкладка Доступ состоит из трех областей.

- Общий доступ к сетевым файлам и папкам — с помощью кнопки Общий доступ данной области можно запустить новый мастер операционной системы Windows Vista Общий доступ к файлу, предназначенный для создания общей папки. Его также можно было запустить с помощью команды Общий доступ контекстного меню файла.

  Заметьте, что мастер можно использовать только в том случае, если флажок Использовать мастер общего доступа (рекомендуется), расположенный на вкладке Вид окна Свойства папки, установлен. В противном случае кнопка Общий доступ вкладки Доступ будет неактивна, а команда Общий доступ контекстного меню файла будет отображать окно Свойства, открытое на вкладке Доступ.

  Мастер Общий доступ к файлу состоит всего из одного шага. На нем вы указываете пользователей, которые смогут получить доступ к общей папке, и разрешения для них. После того как вы нажмете кнопку Общий доступ, операционная система попытается сделать папку общей.

  Если же папка уже общая, то после нажатия кнопки Общий доступ перед вами отобразится мастер Общий доступ к файлу, содержащий следующие ссылки:

  - Изменить разрешения на общий доступ — отображает основное окно мастера Общий доступ к файлу, позволяющее изменить права пользователей, которым разрешен доступ к общей папке;
  - Прекратить доступ — отключает общий доступ к папке.

- Дополнительный общий доступ — с помощью кнопки Дополнительный доступ данной области можно запустить новое окно операционной системы Windows Vista Дополнительный общий доступ (рис. 8.8), предназначенное для создания общей папки и имеющее больше настроек, чем мастер Общий доступ к файлу.

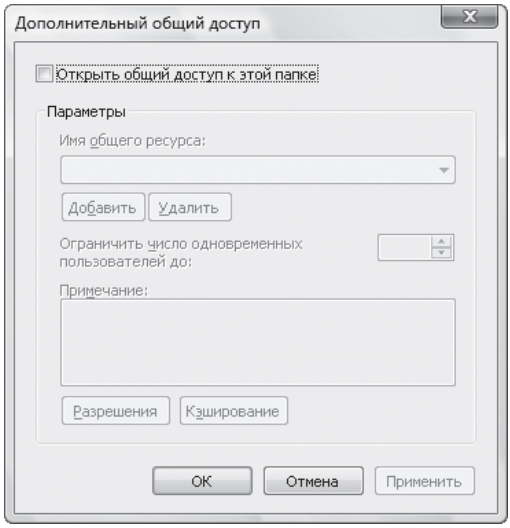

Рис. 8.8. Окно Дополнительный общий доступ

Окно содержит следующие элементы.

- Флажок Открыть общий доступ к этой папке. Его необходимо установить для того, чтобы остальные элементы окна стали активными.
- Поле Имя общего ресурса — позволяет указать общее имя для папки. По умолчанию общим именем папки является ее название.
- Счетчик Ограничить число одновременных пользователей до — дает возможность указать максимальное количество пользователей, которые могут одновременно подключиться к вашей общей папке. Чем больше пользователей подключатся одновременно, тем больше будет нагрузка на ваш компьютер.
- Поле Примечание — позволяет указать комментарий к общей папке, который будет отображаться при удержании указателя мыши над ней.
- Кнопка Разрешения — отображает стандартное окно Разрешения всех операционных систем семейства Windows NT. С его помощью можно определить пользователей, которые могут получить доступ к общей папке, и их права доступа к ней.
- Кнопка Кэширование — позволяет определить параметры автономного доступа к данной общей папке. После нажатия этой кнопки откроется окно Настройка автономного режима, которое определяет, будет данная общая папка автоматически становиться автономной для удаленных пользователей или они вручную должны сделать ее таковой. Можно также указать, будет ли запрещен автономный доступ к данной общей папке.

- Защита паролем — с помощью ссылки Центр управления сетями и общим доступом можно отобразить соответствующий мастер, настройки которого мы рассмотрели выше.

Использование оснастки Общие папки

Не забывайте также, что общие папки можно создавать и удалять с помощью консоли управления Microsoft. Для этого достаточно воспользоваться оснасткой Общие папки (входит в стандартную консоль `fsmgmt.msc`).

Чтобы создать общую папку, достаточно в контекстном меню раздела Общие ресурсы оснастки выбрать команду Новый общий ресурс. После этого будет запущен мастер Мастер создания общих ресурсов, первым шагом которого будет указание пути к папке, которую нужно сделать общей. На следующем шаге мастера указывается общее имя папки, ее описание, а также параметры автономного доступа. На последнем шаге мастера определяются права доступа пользователей к создаваемой папке.

ПРИМЕЧАНИЕ

Рассмотренный мастер является отдельной программой shrpubw.exe, расположенной в каталоге %systemroot%\System32, поэтому запустить его можно и отдельно от оснастки с помощью данной программы. Кроме того, с помощью параметра /s <компьютер> данной программы можно создать общую папку на любом компьютере сети, а не только на локальном компьютере.

Если же вы хотите удалить общую папку или изменить настройки уже созданной общей папки, то при переходе в раздел Общие ресурсы обратите внимание на основное окно оснастки. Оно содержит список всех общих папок компьютера. С помощью контекстного меню нужного вам элемента этого списка как раз и выполняются такие операции, как удаление или редактирование настроек соответствующей общей папки.

8.7. Удаленное управление операционной системой

В операционной системе Windows Vista присутствуют две программы командной строки, позволяющие настраивать командную строку удаленного компьютера и получать доступ к ней. Это программы `winrm.cmd` и `winrs.exe`.

ПРИМЕЧАНИЕ

Сведения об использовании удаленного управления хранятся в журналах, расположенных в разделе Журналы приложений и служб ▸ Microsoft ▸ Windows ▸ WinRM.

Как вы, наверное, уже поняли, возможность получения удаленного доступа реализована на основе службы Служба удаленного управления Windows (WS-Management) операционной системы Windows Vista. Поэтому перед тем как пользоваться программой удаленного доступа `winrs.exe`, необходимо запустить данную службу.

Настройка удаленного доступа

Для настройки удаленного доступа применяется командный файл `winrm.cmd`, который является лишь оболочкой для запуска сценария `winrm.vbs` (оба этих файла расположены в каталоге `%systemroot%\system32`). Собственно, сценарий `winrm.vbs` также является оболочкой для функций изменения параметров реестра, управляющих работой удаленного доступа.

Нужно признать, что использовать сценарий `winrm.vbs` намного сложнее, чем изменять настройки удаленного доступа с помощью реестра, поэтому в данном разделе будут приведены как возможности сценария `winrm.vbs`, так и параметры реестра, которые этим сценарием изменяются.

Примеры использования файла winrm.cmd

Сценарий `winrm.vbs` поддерживает следующие параметры (следовательно, также их поддерживает и командный файл `winrm.cmd`).

- `G` — отображает сведения о настройках удаленного доступа к командной строке операционной системы Windows Vista, а также позволяет выполнять запросы к репозитарию CIM. Рассмотрим несколько примеров использования этого параметра.
  - `WinRM g winrm/config` — выводит сведения о настройках клиента службы Служба удаленного управления Windows (WS-Management), настройках

службы и настройках программы `winrs.exe`. Также вместо параметра `winrm/config` можно воспользоваться параметрами `winrm/config/config`, `winrm/service` или `winrm/winrs`, чтобы получить только информацию о настройках клиента, службы или программы `winrs.exe`.

- `WinRM g <пространство имен и класс>?<ключевое свойство класса=значение>` — позволяет просмотреть значения экземпляра указанного класса, для которого указанное ключевое свойство соответствует указанному значению. Например, можно воспользоваться командой `WinRM g cimv2/Win32_Service?Name=WinRM`, чтобы просмотреть сведения о службе Служба удаленного управления Windows (WS-Management) локального компьютера.

- `S` — позволяет изменить настройки удаленного доступа к командной строке операционной системы Windows Vista. Рассмотрим несколько примеров использования этого параметра, которые приведены в описании программы `winrm`.

  - `Winrm s winrm/config/client @{TrustedHost="<local>, 192.168.0.2"}` — создает два доверенных хоста, которые могут подключаться к службе Служба удаленного управления Windows (WS-Management) без использования протокола Kerberos.

    Все дело в том, что по умолчанию подключиться к службе Служба удаленного управления Windows (WS-Management) можно только по протоколу Kerberos, который используется в домене Active Directory. Если компьютер, который не входит в домен, попытается подключиться к данной службе удаленного компьютера, то его запрос будет отвергнут. Чтобы запрос от такого компьютера был принят, необходимо, чтобы адрес компьютера, от которого пришел запрос, был занесен в раздел доверенных адресов. Поэтому, если в вашей сети не развернут домен Active Directory, вы не сможете подключиться к удаленному компьютеру, пока не укажете на нем, что адрес компьютера, с помощью которого вы подключаетесь к службе, является доверенным.

  - `Winrm s winrm/config/listener?Address=IP:1.2.3.4+Transport=HTTP @{Enabled="false"}` — удаляет запрос на прослушивание IP-адреса 1.2.3.4 для получения запросов удаленного управления от других компьютеров.

    Таким способом можно изменить все параметры конфигурации WinRM, однако эти параметры будут описаны чуть позже — при рассмотрении ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WSMAN`.

- `C` — создает запрос на прослушивание определенных адресов для получения запросов удаленного управления от других компьютеров. Например, можно воспользоваться следующими командами.

  - `Winrm c winrm/config/listener?Address=IP:3dd3:83dd:ffff:f2da::5e61+Transport=HTTP` — создает запрос на прослушивание адреса IPv6 3dd3:83dd:ffff:f2da по протоколу HTTP.

  - `Winrm c winrm/config/listener?Address=IP:1.2.3.4+Transport=HTTP` — формирует запрос на прослушивание адреса IPv4 1.2.3.4 по протоколу HTTP.

  - `Winrm c winrm/config/listener?Address=*+Transport=HTTP` — создает запрос на прослушивание любых IP-дресов по протоколу HTTP. Вместо протокола HTTP можно использовать и протокол HTTPS.

- `D` — удаляет созданный ранее запрос на прослушивание определенных адресов. Например, чтобы удалить предыдущий запрос на прослушивание любых IP-адресов по протоколу HTTP, нужно воспользоваться командой `Winrm d winrm/config/listener?Address=*+Transport=HTTP`.
- `E` — выводит список всех созданных запросов на прослушивание определенных адресов. С помощью этой команды можно также просмотреть содержимое репозитария CIM. Например, можно использовать следующие разновидности данной команды:
  - `Winrm e winrm/config/listener` — отображает список запросов локального компьютера;
  - `Winrm e cimv2/Win32_Service` — выводит сведения обо всех экземплярах класса `Win32_Service` репозитария CIM;
  - `Winrm e shell -remote:<IP или URL-адрес удаленного компьютера>` — отображает список запросов удаленного компьютера.
- `I` — выполняет указанный в параметрах данной команды запрос к репозитарию CIM. Например, с помощью команды `Winrm I StartService cimv2/Win32_Service?Name=WinRM` можно запустить на локальном компьютере остановленную службу Служба удаленного управления Windows (WS-Management). А с помощью разновидности данной команды `Winrm I StartService cimv2/Win32_Service?Name=WinRM -remote:<IP или URL-адрес удаленного компьютера>` это можно сделать на удаленном компьютере.
- `Id` — позволяет проверить, запущена ли служба Служба удаленного управления Windows (WS-Management) на удаленном компьютере. Примером использования данного параметра является команда `winrm id -remote:<IP или URL-адрес удаленного компьютера>`. Если служба Служба удаленного управления Windows (WS-Management) на удаленном компьютере запущена, то после вызова данной команды отобразятся следующие сведения о ней: версия протокола, а также версия и производитель службы.
- `Quickconfig` — вызов командного файла с данным параметром позволяет выполнить быструю настройку службы Служба удаленного управления Windows (WS-Management). Данная настройка состоит из следующих шагов: запуск служб, установка автоматического запуска службы при входе пользователей в систему, создание запроса на прослушивание любых адресов для получения запросов удаленного управления от других компьютеров, а также создание исключения для брандмауэра операционной системы.

Настройки удаленного доступа в реестре

Как вы, наверное, заметили, использование команды `winrm s` для конфигурации удаленного доступа представляет довольно сложную задачу. Поэтому теперь попробуем изменить настройки удаленного доступа с помощью реестра. Для этого предназначены три ветви реестра.

В ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WSMAN\Client хранятся параметры, которые можно настроить с помощью параметра winrm/config/client команды winrm s. Среди них можно найти такие.

- auth_basic — если значение данного параметра REG_DWORD-типа равно 1, то данный вид аутентификации пользователя разрешен. По умолчанию данный вид аутентификации запрещен.
- auth_digest — при установке значения этого параметра REG_DWORD-типа равным 1 разрешен данный вид аутентификации пользователя. По умолчанию данный вид аутентификации разрешен.
- auth_kerberos — если значение данного параметра REG_DWORD-типа равно 1, то данный вид аутентификации пользователя разрешен. По умолчанию данный вид аутентификации разрешен.
- auth_windows_integrated — при установке значения этого параметра REG_DWORD-типа равным 1 разрешен данный вид аутентификации пользователя. По умолчанию данный вид аутентификации разрешен.
- trusted_hosts — этот параметр строкового типа содержит список доверенных узлов, которым разрешен доступ к службе не только по протоколу Kerberos. Адреса доверенных узлов пишутся через запятую. По умолчанию доверенных адресов не существует.
- defaultports_https — имеет тип REG_DWORD и определяет порт, используемый по умолчанию при подключении по протоколу HTTPS. По умолчанию используется порт 443.
- defaultports_http — этот параметр REG_DWORD-типа определяет порт, используемый по умолчанию при подключении по протоколу HTTP. По умолчанию используется порт 80.
- allow_unencrypted — если значение данного параметра REG_DWORD-типа равно 1, то будет разрешено подключение к службе Служба удаленного управления Windows без использования шифрования передаваемых пакетов. По умолчанию незашифрованные сообщения запрещены.
- uriprefix — этот параметр строкового типа определяет uri-префикс, используемый по умолчанию. Параметр по умолчанию равен wsman.
- network_delay — имеет тип REG_DWORD и определяет допустимую задержу в миллисекундах при ожидании ответа от службы Служба удаленного управления Windows. По умолчанию задержка равна 5000 мс.
- batch_maxItems — этот параметр REG_DWORD-типа определяет значение параметра MaxBatchItems параметра winrm/config команды winrm s. По умолчанию значение данного параметра равно 20.
- maxEnvelopeSize — имеет тип REG_DWORD и определяет значение параметра MaxEnvelopeSizeKb параметра winrm/config команды winrm s. По умолчанию значение данного параметра равно 150 Кбайт.

- timeout — этот параметр REG_DWORD-типа определяет значение параметра MaxTimeout параметра winrm/config команды winrm s. По умолчанию значение данного параметра равно 60 000.
- Provider_maxrequests — имеет тип REG_DWORD и определяет значение параметра MaxProviderRequests параметра winrm/config команды winrm s. По умолчанию значение данного параметра равно 25.
- soapTraceEnabled — этот параметр REG_DWORD-типа определяет значение параметра SoapTraceEnabled параметра winrm/config команды winrm s. По умолчанию значение данного параметра равно false.

В ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WSMAN\Listener хранятся подразделы, соответствующие созданным с помощью параметра winrm/config/listener команды winrm l запросам. Каждый из этих запросов содержит параметры Port (тип REG_DWORD) и uniprefix (строковый параметр), с помощью которых можно изменить используемый данным запросом порт и uni-префикс.

В ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WSMAN\Service хранятся параметры реестра, которые можно настроить с помощью параметра winrm/config/service команды winrm s. Среди них можно найти такие.

- rootSDDL — имеет строковый тип и определяет значение параметра rootSDDL параметра winrm/config/service команды winrm s.
- maxConcurrentOperations — имеет тип REG_DWORD и определяет значение параметра maxConcurrentOperations параметра winrm/config/service команды winrm s. По умолчанию значение равно 100.
- continuedOpTimeoutms — имеет тип REG_DWORD и определяет значение параметра EnumerationTimeouts параметра winrm/config/service команды winrm s. По умолчанию значение равно 60 000.
- Maxconnections — имеет тип REG_DWORD и определяет значение параметра Maxconnections параметра winrm/config/service команды winrm s. По умолчанию значение равно 5.
- allow_unencrypted — если значение этого параметра REG_DWORD-типа равно 1, то будет разрешено подключение к службе Служба удаленного управления Windows без использования шифрования передаваемых пакетов. По умолчанию незашифрованные сообщения запрещены.
- auth_basic — при установке значения этого параметра REG_DWORD-типа равным 1 разрешен данный вид аутентификации пользователя. По умолчанию данный вид аутентификации запрещен.
- auth_kerberos — если значение этого параметра REG_DWORD-типа равно 1, то данный вид аутентификации пользователя разрешен. По умолчанию данный вид аутентификации разрешен.

- `auth_windows_integrated` — при установке значения этого параметра `REG_DWORD`-типа равным `1` разрешен данный вид аутентификации пользователя. По умолчанию данный вид аутентификации разрешен.
- `defaultports_http` — этот параметр `REG_DWORD`-типа определяет порт, используемый по умолчанию при подключении к службе по протоколу HTTP. По умолчанию используется порт 80.
- `defaultports_https` — имеет тип `REG_DWORD` и определяет порт, используемый по умолчанию при подключении к службе по протоколу HTTPS. По умолчанию используется порт 443.
- `IPv4Filter` — имеет строковый тип и определяет значение параметра `IPv4Filter` параметра `winrm/config/service` команды `winrm s`. По умолчанию значение равно `*`.
- `IPv6Filter` — имеет строковый тип и определяет значение параметра `IPv6Filter` параметра `winrm/config/service` команды `winrm s`. По умолчанию значение равно `*`.
- `AllowRemoteShellAccess` — имеет тип `REG_DWORD` и определяет значение параметра `AllowRemoteShellAccess` параметра `winrm/config/winrs` команды `winrm s`. По умолчанию значение равно `true`.
- `IdleTimeout` — имеет тип `REG_DWORD` и определяет значение параметра `IdleTimeout` параметра `winrm/config/winrs` команды `winrm s`. По умолчанию значение равно `4 294 967 295`.
- `MaxConcurrentUsers` — имеет тип `REG_DWORD` и определяет значение параметра `MaxConcurrentUsers` параметра `winrm/config/winrs` команды `winrm s`. По умолчанию значение равно `5`.
- `MaxShellRunTime` — имеет тип `REG_DWORD` и определяет значение параметра `MaxShellRunTime` параметра `winrm/config/winrs` команды `winrm s`. По умолчанию значение равно `4 294 967 295`.
- `MaxProcessesPerShell` — имеет тип `REG_DWORD` и определяет значение параметра `MaxProcessesPerShell` параметра `winrm/config/winrs` команды `winrm s`. По умолчанию значение равно `10`.
- `MaxMemoryPerShell` — имеет тип `REG_DWORD` и определяет значение параметра `MaxMemoryPerShell` параметра `winrm/config/winrs` команды `winrm s`. По умолчанию значение равно `83 886 080`.
- `MaxShellsPerUser` — имеет тип `REG_DWORD` и определяет значение параметра `MaxShellsPerUser` параметра `winrm/config/winrs` команды `winrm s`. По умолчанию значение равно `5`.

ПРИМЕЧАНИЕ

Настроить параметры работы протокола WinRM можно и с помощью групповых политик. Для этого нужно зайти в раздел Конфигурация компьютера ▸ Административные шаблоны ▸ Компоненты Windows ▸ Удаленное управление Windows оснастки gpedit.msc. С помощью политик данного раздела можно настроить те же возможности, что были описаны ранее в этой главе.

Программа winrs.exe

После того как вы настроите работу клиента удаленного доступа и запустите службу Служба удаленного управления Windows, нужно воспользоваться программой `winrs.exe` для подключения к удаленной службе. Использование данной программы намного проще, чем командного файла `winrm.cmd`, поэтому ее мы рассмотрим лишь поверхностно. Описание всех параметров программы `winrs.exe` можно вывести, введя команду `winrs.exe /?`.

Работа с программой winrs.exe

Основной синтаксис данной программы следующий: `winrs.exe <параметры подключения к удаленной службе> <команда, которая будет выполнена на удаленном компьютере>`. Например, самым простым способом подключения является команда `winrs.exe -r:<адрес удаленного компьютера> -u:<имя пользователя> -p:<пароль> cmd.exe`. После ввода данной команды будет запущена консоль `cmd.exe` удаленного компьютера от имени указанного пользователя (если, конечно, пароль для его учетной записи был верен).

Если же вместо запуска командной строки (заметьте, что она запускается не как отдельный процесс, а в текущей командной строке, поэтому, чтобы завершить с ней работу, нужно нажать комбинацию клавиш Ctrl+C) перед вами отобразилась информация о том, что подключиться к удаленному компьютеру можно только протоколу Kerberos, то вы забыли добавить данный адрес в список доверенных. Может также отобразиться сообщение о том, что соединение установить не удается. В этом случае убедитесь, что Служба удаленного управления Windows запущена как на локальном, так и на удаленном компьютере.

Настройка удаленной оболочки с помощью групповых политик

Настроить параметры удаленной оболочки можно с помощью групповых политик, описанных в файле `WindowsRemoteShell.admx` и расположенных в разделе Конфигурация компьютера ▸ Административные шаблоны ▸ Компоненты Windows ▸ Удаленная оболочка Windows.

Политики данного раздела изменяют параметры `REG_DWORD`-типа, расположенные в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WinRM\Service\WinRS`. О большинстве возможностей описанных ниже политик было рассказано в предыдущей главе книги (при описании параметров реестра, изменяемых файлом `winrm.cmd`), поэтому будет приведен лишь список групповых политик и параметров реестра, которые они изменяют:

- Разрешить доступ к удаленной оболочке — изменяет значение параметра `AllowRemoteShellAccess`;
- MaxConcurrentUsers — изменяет значение параметра `MaxConcurrentUsers`;
- Таймаут простоя — изменяет значение параметра `IdleTimeout`;
- Максимальный объем памяти в мегабайтах для одной оболочки — изменяет значение параметра `MaxMemoryPerShellMB`;
- Максимальное количество процессов для одной оболочки — изменяет значение параметра `MaxProcessesPerShell`;

- Максимальное число удаленных оболочек для одного пользователя — изменяет значение параметра `MaxShellsPerUser`;
- Таймаут оболочки — изменяет значение параметра `ShellTimeOut`.

8.8. Команды rundll32.exe для доступа к сетевым возможностям

Отдельно стоит описать команды `rundll32.exe`, с помощью которых можно получить доступ к сетевым возможностям операционной системы Windows Vista. Их много, но большая часть отображает сетевые мастера с помощью возможностей новой библиотеки `XWizards.dll`, поэтому их мы рассмотрим отдельно от остальных команд.

Основные команды rundll32.exe

Следующие команды `rundll32.exe` являются основными для настройки сетевых возможностей.

- `rundll32 ndfapi.dll,NdfRunDllDuplicateIPOffendingSystem` — открывает окно Сетевая ошибка с сообщением о том, что операционная система Windows Vista обнаружила конфликты в IP-адресах компьютеров сети. С помощью кнопки Диагностика данного окна можно выполнить диагностику конфликтов в IP-адресах.

  Данная команда используется назначенным заданием `IpAddressConflict1`, расположенным в разделе Библиотека планировщика заданий ▸ Microsoft ▸ Windows ▸ Tcpip.

- `rundll32 ndfapi.dll,NdfRunDllDuplicateIPDefendingSystem` — также открывает окно об обнаружении конфликта в IP-адресах. Но на этот раз оно не содержит кнопки Диагностика.

  Данная команда используется назначенным заданием `IpAddressConflict2`, расположенным в разделе Библиотека планировщика заданий ▸ Microsoft ▸ Windows ▸ Tcpip.

- `rundll32 ndfapi.dll,NdfRunDllDiagnoseIncident` — выполняет диагностику работы сети.

- `rundll32.exe SHWEBSVC.dll, AddNetPlaceRunDll` — вызывает окно Добавление сетевого размещения. С его помощью можно создать ссылку на сайт или FTP-сервер.

- `rundll32.exe SHWEBSVC.dll, PublishRunDll` — вызывает окно Заказ отпечатков. С его помощью можно опубликовать в Интернете ваши фотографии и рисунки.

- `rundll32.exe VAN.dll, RunVANW` — вызывает мастер Подключиться к сети. На страницах этой книги он часто упоминался при описании создания беспроводного или удаленного соединения.

- `rundll32.exe VAN.dll, RunVANW /disablediagnostics` — отключает механизм диагностики работы сети и вызывает мастер Подключиться к сети.
- `rundll32.exe wzcdlg.dll, FlashConfigCreateNetwork <файл настроек>` — вызывает окно настройки защищенной беспроводной сети.
- `rundll32.exe wlanmm.dll, StartDiagnostics MediaManagerHelperClass -mediatype NdisPhysicalMediumWirelessLan` — выполняет диагностику работы беспроводной сети. Для работы данной команды необходимо, чтобы Служба политики диагностики работала. Если служба определяет, что на вашем компьютере не установлен беспроводной адаптер или его драйверы, то она предлагает их установить.

Доступ к мастерам с помощью библиотеки XWizards

В операционной системе Windows Vista появилась специальная библиотека `xwizards.dll`, которая реализует доступ ко многим мастерам операционной системы. Основной синтаксис ее использования следующий: `rundll32.exe xwizards.dll, RunWizard <CLSID-номер>`. Однако вы можете просмотреть список дополнительных параметров данной функции с помощью команды `rundll32.exe xwizards.dll, RunWizard /?`.

Список CLSID-номеров, которые можно использовать с этой командой, будет приведен далее. Сейчас же рассмотрим еще один вопрос использования данной команды. Список CLSID-номеров, которые определяют мастера или части мастеров, вызываемых с помощью библиотеки `xwizards.dll`, содержится в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\XWizards\Components`. Каждый CLSID-номер имеет свой собственный подраздел в данной ветви реестра, и если вы удалите этот подраздел, то соответствующий мастер нельзя будет запускать.

Вот список некоторых CLSID-номеров, которые можно использовать в команде `rundll32.exe xwizards.dll, RunWizard <CLSID-номер>`, вызывающей определенный мастер:

- `{DB4F3FA7-5A08-4100-95DE-B46DF509B902}` — Подключиться к сети;
- `{d1a42999-0adf-11da-b070-0011856571de}` — Настройка беспроводных маршрутизаторов и точек доступа;
- `{d1a4299a-0adf-11da-b070-0011856571de}` — Добавить беспроводное устройство в сеть;
- `{C03E8586-781E-49a1-8190-CE902D0B2CE7}` — Разрешить подключение к этому компьютеру;
- `{C03E8585-781E-49a1-8190-CE902D0B2CE7}` — Set up a new broadband connection;
- `{C03E8584-781E-49a1-8190-CE902D0B2CE7}` — Set up a new dialup connection (Internet);
- `{C03E8583-781E-49a1-8190-CE902D0B2CE7}` — Set up a new dialup connection;

- {C03E8582-781E-49a1-8190-CE902D0B2CE7} — Set up a new virtual network connection (VPN);
- {C03E8581-781E-49a1-8190-CE902D0B2CE7} — Set up a new connection;
- {854CB94F-2279-4F7F-AC62-31E22E4D8899} — Подключение к беспроводной сети вручную;
- {7071ECA0-663B-4bc1-A1FA-B97F3B917C55} — Подключение к Интернету;
- {7071ECE0-663B-4bc1-A1FA-B97F3B917C55} — Установка подключения или сети;
- {7071ECB0-663B-4bc1-A1FA-B97F3B917C55} — Подключиться к рабочему месту;
- {7071EC75-663B-4bc1-A1FA-B97F3B917C55} — Создать подключение виртуальной частной сети;
- {7071EC71-663B-4bc1-A1FA-B97F3B917C55} — Создать телефонное подключение;
- {6db29a9b-10d0-4b93-b86a-188fc998eff8} — Подключение к беспроводной сети вручную;
- {34c219bd-85c1-4338-95e8-788a36901dc2} — Настройка сети для переносных устройств;
- {0cbb5030-f2b2-4b38-8cbc-895cec57db03} — Настройка сети компьютер-компьютер.

8.9. Стандартные классы репозитария CIM

Репозитарий CIM операционных систем семейства Windows содержит набор классов, которые позволяют не только просматривать сведения о сетевых компонентах компьютера, но и управлять ими, что бывает довольно полезно при создании сценариев, заменяющих выполнение одних и тех же действий.

Все эти классы хранятся в пространстве имен \\root\cimv2. Рассмотрим свойства и методы этих классов.

Win32_LogonSession

Данный класс содержит сведения об установленных сетевых сеансах.

- AuthenticationPackage — определяет механизм, используемый для проверки подлинности при подключении. Например, NTLM.
- LogonId — ключевое свойство, определяющее идентификатор сетевого сеанса.
- LogonType — указывает тип сетевого сеанса. Например, данное свойство может возвращать следующие значения:
  - 2 — пользователь подключен к компьютеру интерактивно;
  - 4 — вход выполнен пакетным заданием;

  - 5 — вход выполнен от имени учетной записи службы;
  - 9 —вход выполнен на основе клонированного маркера текущего клиента.
- Name — определяет название сетевого сеанса.
- StartTime — указывает время начала сетевого сеанса.

Win32_ServerSession

Данный класс позволяет просмотреть список сетевых сеансов, созданных удаленными пользователями (службой терминалов):

- ActiveTime — определяет длительность сетевого сеанса в секундах;
- ClientType — указывает тип клиента;
- ComputerName — ключевое свойство, определяющее имя компьютера, который установил сетевой сеанс;
- IdleTime — определяет длительность бездействия сетевого сеанса в секундах;
- ResourcesOpened — указывает количество файлов, устройств и именованных каналов, открытых пользователем во время сетевого сеанса;
- TransportName — определяет транспортный протокол, используемый клиентом для взаимодействия с сервером;
- UserName — ключевое свойство, определяющее имя пользователя, создавшего сетевой сеанс.

Win32_ServerConnection

Данный класс содержит описание общих ресурсов компьютера, к которым выполнен доступ в контексте одного сетевого подключения:

- ActiveTime — указывает длительность подключения в секундах;
- ComputerName — ключевое свойство, определяющее имя компьютера, который установил подключение;
- ConnectionID — указывает уникальный идентификатор сетевого подключения;
- NumberOfFiles — определяет количество файлов, открытых сетевым подключением;
- NumberOfUsers — указывает количество пользователей, использующих данное сетевое подключение;
- ShareName — ключевое свойство, определяющее общий ресурс, к которому установлено сетевое подключение;
- UserName — ключевое свойство, определяющее имя пользователя, который установил сетевое подключение.

Win32_NetworkConnection

Экземпляры данного класса определяют установленные сетевые подключения:

- `Comment` — определяет описание сетевого подключения;
- `ConnectionState` — указывает состояние сетевого подключения и может возвращать следующие значения: `connected`, `error`, `paused`, `disconnected`, `connecting`, `reconnecting`;
- `ConnectionType` — определяет тип сетевого подключения (постоянное или временное);
- `Name` — ключевое свойство, определяющее название сетевого подключения;
- `Persistent` — указывает, является ли сетевое подключение постоянным;
- `RemoteName` — определяет имя общего ресурса, к которому установлено подключение;
- `RemotePath` — указывает полный путь к общему ресурсу (в формате UNC), к которому установлено подключение;
- `ResourceType` — определяет тип ресурса, к которому установлено подключение, и может принимать следующие значения: `disk`, `print`, `any`;
- `UserName` — указывает имя пользователя, создавшего сетевое подключение.

Win32_NetworkProtocol

Экземпляры данного класса определяют сетевые протоколы, которые установлены в операционной системе.

- `ConnectionlessService` — указывает, поддерживает ли сетевой протокол использование UDP-пакетов.
- `Description` — определяет описание сетевого протокола.
- `GuaranteesDelivery` — указывает, может ли протокол гарантировать, что все отправляемые пакеты дойдут до пункта назначения.
- `GuaranteesSequencing` — определяет, может ли протокол гарантировать, что все отправляемые пакеты дойдут до пункта назначения в том же порядке, в котором они были отправлены.
- `MaximumAddressSize` — указывает максимальную длину адреса, которую поддерживает протокол.
- `MaximumMessageSize` — определяет максимальный размер сообщения, которое можно доставить с помощью данного протокола. Если значение данного свойства равно `0`, то протокол оперирует потоком, а не сообщением.
- `MessageOriented` — указывает, ориентирован данный протокол на сообщения или на поток.
- `MinimumAddressSize` — определяет минимальную длину адреса, которую поддерживает протокол.

- Name — ключевое свойство, определяющее название протокола.
- SupportsBroadcasting — указывает, поддерживает ли протокол широковещательную передачу в сети.
- SupportsEncryption — определяет, поддерживает ли протокол шифрование данных.
- SupportsExpeditedData — указывает, поддерживает ли протокол срочные данные.
- SupportsGuaranteedBandwidth — определяет, поддерживает ли протокол механизм гарантированной пропускной способности.
- SupportsMulticasting — указывает, поддерживает ли протокол многоадресную рассылку.
- SupportsQualityofService — определяет, поддерживает ли протокол механизм QOS.

Win32_NetworkLoginProfile

Экземпляры данного класса определяют учетные записи, с помощью которых можно выполнить сетевое подключение к данному компьютеру.

- BadPasswordCount — определяет количество неудачных попыток ввода пароля, по истечении которых учетная запись будет заблокирована.
- CodePage — указывает кодовую страницу языка, которая используется данным пользователем.
- Flags — определяет флаги настройки данной учетной записи. Например, возможны следующие значения свойства: 1 (учетная запись заблокирована), 4 (учетная запись отключена), 6 (пользователь не может изменять пароль), 23 (срок действия пароля истек).
- LastLogon — указывает дату последнего входа в систему с помощью данной учетной записи.
- LogonHours — определяет дни недели, когда можно входить в систему с помощью данной сетевой учетной записи.
- MaximumStorage — указывает максимальный размер дискового пространства, доступного данной учетной записи.
- Name — ключевое свойство, определяющее имя учетной записи и компьютера.
- PasswordAge — указывает время, истекшее после последней смены пароля для данной учетной записи.
- PasswordExpires — определяет время окончания действия пароля для данной учетной записи.
- Privileges — указывает группу, к которой принадлежит данная учетная запись. Например, свойство может принимать следующие значения: 0 (гость), 1 (пользователь), 2 (администратор).

- `ScriptPath` — определяет путь к сценарию входа в систему для данной учетной записи.
- `Workstations` — указывает имена компьютеров, с которых данный пользователь может войти в систему.

Win32_NetworkClient

Экземпляры данного класса определяют сетевые клиенты, которые доступны в операционной системе:

- `Manufacturer` — указывает создателя сетевого клиента;
- `Name` — определяет имя сетевого клиента.

Win32_NetworkAdapter

Экземпляры данного класса определяют сетевые адаптеры, которые установлены в операционной системе.

- `AdapterType` — указывает тип сети, для которой предназначен сетевой адаптер. Например, «Ethernet 802.3».
- `DeviceID` — ключевое свойство, определяющее порядковый номер сетевого адаптера.
- `Installed` — указывает, установлен ли сетевой адаптер.
- `MACAddress` — определяет MAC-адрес сетевого адаптера.
- `MaxNumberControlled` — указывает количество портов, к которым может напрямую адресоваться сетевой адаптер.
- `Name` — определяет имя сетевого адаптера.

Win32_NetworkAdapterConfiguration

Экземпляры данного класса определяют настройки сетевых адаптеров, которые установлены в операционной системе.

- `DHCPEnabled` — указывает, разрешено ли использование DHCP.
- `Index` — ключевое свойство, определяющее порядковый номер сетевого адаптера.
- `IPEnabled` — указывает, разрешено ли использование протокола TCP/IP.
- `IPXEnabled` — определяет, разрешено ли использование протокола IPX.
- `SettingID` — указывает GUID-номер сетевого адаптера.

Класс также поддерживает следующие методы.

- `DisableIPSec` — отключить использование протокола IPSec для данного сетевого адаптера.

- `EnableDHCP` — разрешить использование DHCP для данного сетевого адаптера.
- `EnableDNS <имя сервера DNS>, <домен DNS>, <массив IP-адресов для запроса DNS>, <массив DNS-суффиксов, используемых хостом>` — позволить использование DNS для данного сетевого адаптера.
- `EnableIPFilterSec <флаг установки безопасности для всех сетевых адаптеров, использующих IP>` — разрешить использование протокола IPSec.
- `EnableIPSec <массив портов, которые будут доступны по TCP>, <массив портов, которые будут доступны по UDP>, <массив протоколов, которые будут использоваться поверх IP>` — позволить использование IPSec.
- `EnableStatic <массив сетевых адресов>, <маска сети>` — включить статическую TCP\IP-адресацию для сетевого адаптера.
- `EnableWINS <флаг использования разрешений адресов DNS с помощью WINS>, <флаг использования файлов просмотра>, <имя файла просмотра (например, hosts)>, <идентификатор области>` — разрешить использование WINS.
- `ReleaseDHCPLease` — освободить IP-адрес, привязанный к данному сетевому адаптеру.
- `ReleaseDHCPLeaseAll` — освободить все IP-адреса, привязанные ко всем сетевым адаптерам.
- `RenewDHCPLease` — обновить IP-адрес сетевого адаптера с помощью сервера DHCP.
- `RenewDHCPLeaseAll` — обновить все IP-адреса сетевых адаптеров с помощью сервера DHCP.
- `SetArpAlwaysSourceRoute <флаг передачи ARP-запросов с включенной маршрутизацией источников в сетях Token Ring>` — разрешить передачу ARP-запросов с помощью протокола TCP\IP.
- `SetArpUseEtherSNAP <флаг передачи пакетов SNAP 802.3>` — позволить использование формата пакета SNAP 802.3.
- `SetDatabasePath <новый путь>` — изменить путь к каталогу `%SystemRoot%\system32\drivers\etc`.
- `SetDeadGWDetect <флаг включения проверки>` — установить проверку недоступных маршрутизаторов.
- `SetDefaultTOS <значение TOS>` — установить тип службы в IP-пакетах.
- `SetDefaultTTL <новое значение>` — изменить используемое по умолчанию время жизни пакета.
- `SetDNSDomain <домен DNS>` — установить новый домен DNS.
- `SetDNSServerSearchOrder <массив адресов>` — установить массив адресов, используемых при поиске DNS.

- `SetDNSSuffixSearchOrder <массив суффиксов>` — установить массив суффиксов, добавляемых к имени компьютера при поиске в DNS.
- `SetForwardBufferMemory <размер очереди пакетов>` — определяет размер буфера, используемого для хранения на маршрутизаторе данных пакета.
- `SetGateways <маршрутизатор>, <метрика>` — установить маршрутизатор.
- `SetIGMPLevel <уровень>` — установить уровень поддержки IGMP. Возможны следующие уровни: `0` (система не поддерживает многоадресную рассылку), `1` (операционной системе разрешено лишь посылать пакеты IGMP), `2` (операционной системе разрешено как посылать, так и получать IGMP-пакеты).
- `SetIPConnectionMetric <метрика>` — установить новую метрику маршрутизации.
- `SetIPUseZeroBroadcast <флаг использования широковещания 0.0.0.0>` — использовать широковещание с помощью адреса 0.0.0.0.
- `SetIPXFrameTypeNetworkPairs <номер сети>, <тип IPX>` — изменить номер сети для IPX-соединения.
- `SetIPXVirtualNetworkNumber <номер сети>` — изменить виртуальный номер сети для IPX-соединения.
- `SetKeepAliveInterval <интервал отправки пакетов проверки активности>` — изменить интервал отправки пакетов активности сетевого соединения.
- `SetKeepAliveTime <интервал проверки работоспособности неактивного подключения>` — изменить интервал проверки неактивного сетевого соединения.
- `SetMTU <новый размер MTU>` — изменить размер MTU.
- `SetNumForwardPackets <размер очереди пакетов маршрутизатора>` — изменить размер очереди пакетов маршрутизатора.
- `SetPMTUBHDetect <флаг включения определения маршрутизаторов типа черная дыра>` — определяет, будет ли перед передачей данных выполняться проверка маршрутизаторов типа «черная дыра».
- `SetPMTUDiscovery <флаг разрешения изменения максимального размера MTU>` — разрешить изменение максимального размера MTU перед передачей данных.
- `SetTcpipNetbios <флаг использования NetBios>` — позволить или запретить работу NetBios через TCP\IP.
- `SetTcpMaxConnectRetransmissions <количество попыток передачи пакетов>` — установить количество неудачных попыток передачи пакета, по истечении которого соединение будет разорвано.
- `SetTcpMaxDataRetransmissions <количество попыток передачи сегмента данных>` — установить количество неудачных попыток передачи сегмента данных, по истечении которого соединение будет разорвано.

- SetTcpNumConnections <максимальное количество поддерживаемых по TCP соединений> — изменить максимальное количество поддерживаемых TCP соединений, установленных одновременно.
- SetTcpUseRFC1122UrgentPointer <флаг использования спецификации RFC 1122> — разрешить использование спецификации RFC 1122 для передачи данных срочности.
- SetTcpWindowSize <новая ширина окна> — изменить ширину окна передачи данных.
- SetWINSServer <IP-адрес основного WINS-сервера>, <IP-адрес дополнительного WINS-сервера> — установить WINS-сервер для данного сетевого адаптера.

Win32_IP4RouteTable

Экземпляры данного класса определяют записи таблицы маршрутизации, используемой операционной системой:

- Age — определяет время в секундах, которое прошло с момента последнего обновления информации о маршруте;
- Destination — указывает конечный адрес маршрута;
- InterfaceIndex — определяет индекс локального интерфейса, используемого при следующей ретрансляции пакетов;
- Mask — указывает маску адреса;
- Metric1 — определяет основную метрику маршрута;
- NextHop — указывает адрес для следующей маршрутизации пакетов;
- Protocol — определяет тип протокола маршрутизации, создавшего данный элемент таблицы маршрутизации.

Win32_IP4PersistedRouteTable

Экземпляры данного класса определяют описание всех постоянных маршрутов таблицы маршрутизации:

- Mask — указывает маску адреса;
- Metric1 — определяет основную метрику маршрута;
- NextHop — указывает адрес для следующей маршрутизации пакетов.

На этом закончим рассмотрение параметров работы с сетью в Windows Vista.

Глава 9

Установка и удаление компонентов операционной системы

- **Компоненты Windows**
- **Установка и удаление сетевых компонентов с помощью программы netcfg.exe**
- **Мастер Установка или удаление языков отображения**
- **Установка пакетов обновлений операционной системы**

Одной из задач администратора является удаление ненужных или установка дополнительных компонентов операционной системы. Именно о дополнительных компонентах операционной системы Windows Vista и работе с ними пойдет речь в этой главе.

Особенно актуально вопрос удаления ненужных компонентов стоит перед пользователями Windows Vista Ultimate, которым приходится жертвовать почти 10 Гбайт объема жесткого диска на нужды операционной системы.

9.1. Компоненты Windows

Расположение: `%systemroot%\system32\optionalfeatures.exe`.

Самым простым способом установки и удаления компонентов операционной системы является использование окна Компоненты Windows (рис. 9.1). Это окно можно вызвать либо из папки Панель управления (значок Программы и компоненты, ссылка Включение или отключение компонентов Windows), либо с помощью исполняемого файла `optionalfeatures.exe`.

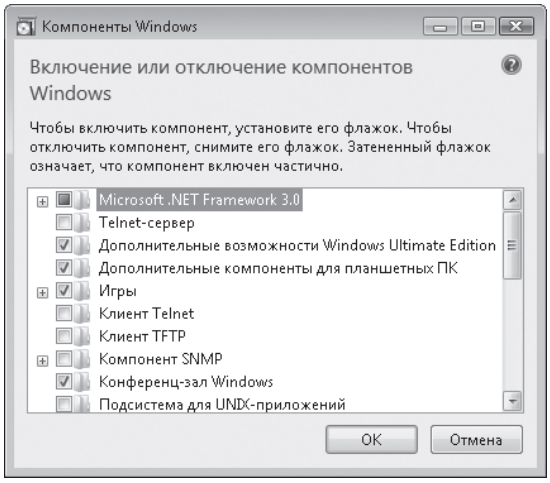

Рис. 9.1. Окно Компоненты Windows

Надо заметить, что при работе с данным окном операционная система никогда не просит вставить загрузочный диск для копирования с него файлов устанавливаемого компонента. Это говорит о том, что все компоненты операционной системы устанавливаются вместе с ней и расположены на диске в сжатом виде (в каталоге `%systemroot%\winsxs`).

Компоненты операционной системы

В Windows Vista Ultimate окно Компоненты Windows содержит различные компоненты операционной системы, которые можно установить или удалить. Заметьте, что для каждого элемента окна Компоненты Windows приводится название компонента

операционной системы, который устанавливается или удаляется с его помощью. Эти сведения могут понадобиться в будущем.

Рассмотрим компоненты операционной системы, которые можно установить или удалить с помощью окна Компоненты Windows.

Microsoft .NET Framework 3.0

Название компонента: `NetFx3`.

Microsoft .NET Framework 3.0, также называемый WinFX, представляет собой набор API, который включает в себя подсистему презентаций Windows Presentation Foundation (бывшую Avalon), платформу для веб-сервисов (бывшую Indigo), а также Windows Workflow Foundation и Windows CardSpace (вспомните одноименный значок папки Панель управления). Все это является фундаментом для приложений следующего поколения, разрабатываемых специально для Windows Vista.

Данный компонент состоит, в свою очередь, из трех компонентов: Windows Communication Foundation HTTP Activation (название компонента: `WCF-HTTP-Activation`), Windows Communication Foundation Non-HTTP Activation (название компонента: `WCF-NonHTTP-Activation`) и XPS Viewer (название компонента: `XPS-Viewer`).

Первые два по умолчанию не установлены, а третий установлен. Ранее, при описании работы с принтерами в операционной системе Windows Vista, мы обсуждали основы нового формата XPS и стандартного принтера операционной системы Microsoft XPS Document Writer.

Данный принтер позволял создавать файлы в XPS-формате, которые потом можно было просмотреть с помощью компонента XPS Viewer. Этот компонент является частью браузера Internet Explorer 7.0.

Если вы удалите компонент XPS Viewer, то не сможете просматривать файлы в XPS-формате, хотя по-прежнему сможете создавать их с помощью стандартного принтера Microsoft XPS Document Writer.

Telnet-сервер

Название компонента: `TelnetServer`.

По умолчанию данный компонент не установлен. Он создает службу Telnet (файл `tlntsvr.exe`), которая позволяет удаленному пользователю подключаться к данному компьютеру и управлять им с помощью программы `telnet.exe`. Служба расположена в подразделе реестра `TlntSvr`, запускается от имени локальной службы, но с дополнительными привилегиями SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeChangeNotifyPrivilege, SeCreateGlobalPrivilege, SeImpersonatePrivilege, SeIncreaseQuotaPrivilege.

ПРИМЕЧАНИЕ

Для сетевого взаимодействия службы при установке данного компонента также создается несколько правил стандартного брандмауэра.

Параметры настройки службы Telnet хранятся в ветви HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\TelnetServer\Defaults. Например, данная ветвь реестра хранит следующие параметры.

- DefaultShell — этот параметр строкового типа определяет оболочку, к которой будет выполняться подключение удаленного пользователя. По умолчанию значение этого параметра равно %systemroot%\system32\cmd.exe.
- DisconnectKillAllApps — имеет тип REG_DWORD и определяет, будут ли автоматически завершаться все запущенные пользователем задачи при завершении его сеанса. По умолчанию значение параметра равно 1.
- LogFile — этот параметр строкового типа определяет путь к файлу, в который будут заноситься сведения о работе службы Telnet. По умолчанию файл журнала не используется.
- LoginScript — имеет строковый тип и указывает путь к файлу сценария, который будет выполняться для всех пользователей, которые подключаются к компьютеру. По умолчанию значение данного параметра равно %WINDIR%\system32\login.cmd.
- MaxConnections — этот параметр REG_DWORD-типа определяет максимальное количество разрешенных одновременных подключений к данному компьютеру. По умолчанию значение данного параметра равно 2.
- TelnetPort — имеет тип REG_DWORD и определяет номер порта, используемый службой Telnet для работы с удаленными пользователями. По умолчанию значение данного параметра равно 17.
- MaxFailedLogins — этот параметр REG_DWORD-типа определяет количество неудачных подключений к компьютеру, после преувеличения которого попытки подключения удаленного пользователя будут блокироваться. По умолчанию значение данного параметра равно 3.

Кроме того, этот компонент создает такие файлы: tlntsvr.exe, tlntsess.exe, tlntadmn.exe, termcap, login.cmd.

Файл tlntadmn.exe представляет собой программу командной строки, с помощью которой можно настроить работу сервера Telnet либо управлять ею (запускать, останавливать и т. д.). Есть несколько основных синтаксисов данной программы. Во всех из них для аутентификации пользователя можно также указывать следующие параметры: <имя компьютера> -u <имя пользователя> -p <пароль>.

- tlntadmn.exe -s|-k|-m <идентификатор сессии> — соответственно, отображает список активных сессий, прекращает одну из них, посылает сообщение пользователю, инициировавшему сессию.
- tlntadmn.exe start|stop|pause|continue — управляет работой сервера Telnet.
- tlntadmn.exe <параметры настройки> — настраивает параметры работы сервера Telnet. Описание данных параметров можно просмотреть, введя команду tlntadmn.exe /?.

Файл termcap представляет собой обычный текстовый файл, содержащий набор команд, заканчивающих сессию.

Файл login.cmd представляет собой обычный текстовый файл, в котором содержится только одна основная команда: cd /d %HOMEDRIVE%\%HOMEPATH%.

Дополнительные возможности Windows Ultimate Edition

Название компонента: Windows-Ultimate-Extras.

По умолчанию установлен.

Дополнительные компоненты для планшетных ПК

Название компонента: TabletPCOC.

По умолчанию установлен. Данный компонент представляет собой набор файлов для работы с пером и другими элементами планшетных компьютеров. Например, такими файлами являются программы StikyNot.exe, SnippingTool.exe, а также большинство программ из раздела %ProgramFiles%\Common Files\microsoft shared\ink. Общий размер данных файлов составляет примерно 170 Мбайт.

Игры

Название компонента: InboxGames.

По умолчанию установлен. Данный компонент представляет собой набор игр из каталога %programfiles%\Microsoft Games, а также библиотеку CardGames.dll. Он занимает примерно 111 Мбайт свободного места на жестком диске.

При этом можно удалить как все стандартные игры операционной системы, так и только некоторые из них. Игры также считаются компонентами операционной системы и имеют следующие названия: Solitaire, SpiderSolitaire, Hearts, FreeCell, Minesweeper, PurblePlace, CardGames, Chess, Shanghai, Inkball.

Клиент Telnet

Название компонента: TelnetClient.

По умолчанию не установлен. Данный компонент устанавливает файл telnet.exe и библиотеку telnetcr.dll.

Программа telnet.exe позволяет подключиться к службам удаленного компьютера, на котором установлен сервер Telnet, для управления их работой. Основной синтаксис программы следующий: telnet.exe <IP-адрес компьютера> <порт>. При подключении можно также использовать дополнительные параметры:

- -a -l <имя пользователя> — при подключении к службе автоматически на ней регистрироваться;

- `-f <путь к файлу журнала и его имя>` — имя файла, в который будут заноситься сведения о работе с сервером Telnet.

Клиент TFTP

Название компонента: `TFTP`.

По умолчанию данный компонент не установлен. Он представляет собой единственный исполняемый файл — `TFTP.EXE`. Этот файл должен быть вам знаком по операционной системе Windows XP. Если в ней он присутствовал по умолчанию, то в Windows Vista его нужно устанавливать отдельно.

Данная программа предназначена для передачи файлов на удаленный компьютер (или наоборот). Ее основной синтаксис следующий: `tftp <IP-адрес удаленного компьютера> GET|PUT <имя передаваемого файла>`. Если используется параметр `GET`, то файл передается на удаленный компьютер. Если же используется параметр `PUT`, то файл передается на локальный компьютер.

Компонент SNMP

Название компонента: `SNMP`.

По умолчанию не установлен. С помощью данного компонента можно установить файлы, предназначенные для работы со службой SNMP и агентами SNMP.

Добавляемые службы

Установка данного компонента приводит к созданию служб SNMP Service (файл `snmp.exe`) и SNMP Trap Service (файл `snmptrap.exe`). Первая из этих служб предназначена для обработки запросов SNMP на локальном компьютере. Вторая же позволяет собирать сведения от агентов SNMP и передавать их программам, которые ожидают данные сведения.

Служба SNMP Service определяется в подразделе `snmp`, запускается автоматически, с правами локальной системы и без дополнительных привилегий.

ПРИМЕЧАНИЕ

При установке компонента создаются несколько правил стандартного брандмауэра Windows, разрешающих доступ к сети службе SNMP Service.

Вы можете настроить работу данной службы довольно экстравагантным способом — с помощью консоли `services.msc`. Как вы уже знаете, данная консоль отображает список всех служб, зарегистрированных в операционной системе. При этом, если в контекстном меню определенной службы вы выберете команду Свойства, то откроется окно, описывающее настройки службы. Это окно для всех служб содержит четыре вкладки: Общие, Вход в систему, Восстановление и Зависимости. Но только не для службы SNMP Service. Окно данной службы содержит дополнительные

вкладки, описанные далее. Эти вкладки добавляются с помощью расширения, устанавливаемого вместе с компонентом Компонент SNMP.

- Agent — хранит сведения об агентах SNMP.
- Traps — содержит сведения об элементах, собирающих данные от агентов SNMP.

  Данная вкладка редактирует параметры подразделов ветви системного реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\TrapConfiguration.
- Безопасность — с помощью данной вкладки можно добавить новые сообщества, указав их права доступа, а также указать компьютеры, от которых можно получать SNMP-пакеты.

  Новые сообщества описываются в виде строковых параметров ветви реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ValidCommunities.

  Компьютеры, от которых можно получать SNMP-пакеты, хранятся как параметры строкового типа ветви реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\PermittedManagers.

Другим способом настройки работы SNMP является применение групповых политик. Все они описаны в файле Snmp.admx и расположены в подразделе Конфигурация компьютера ▸ Административные шаблоны ▸ Сеть ▸ SNMP.

- Сообщества — эта групповая политика позволяет определить сообщества SNMP. Все сообщества, определяемые ею, заносятся в ветвь реестра HKEY_LOCAL_MACHINE\SOFTWARE\Policies\SNMP\Parameters\ValidCommunities.
- Разрешенные диспетчеры — дает возможность указать компьютеры, от которых можно получать SNMP-пакеты. Все компьютеры, определяемые ею, заносятся в ветвь реестра HKEY_LOCAL_MACHINE\SOFTWARE\Policies\SNMP\Parameters\PermittedManagers.
- Ловушки только для публичного сообщества — позволяет определить ловушки, собирающие данные от агентов SNMP для публичного сообщества. Все ловушки, определяемые ею, заносятся в ветвь реестра HKEY_LOCAL_MACHINE\SOFTWARE\Policies\SNMP\Parameters\TrapConfiguration\public.

Служба SNMP Trap Service определяется в подразделе SNMPTRAP, запускается вручную, с правами локальной службы и дополнительной привилегией SeChangeNotifyPrivilege.

Добавляемые файлы

Данный компонент также устанавливает следующие библиотеки.

- evntagnt.dll — определяется в параметре строкового типа Pathname, расположенном в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SNMP_EVENTS\CurrentVersion.
- hostmib.dll — указывается в параметре строкового типа Pathname, расположенном в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\HostMIB\CurrentVersion.

- lmmib2.dll — определяется в параметре строкового типа Pathname, расположенном в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\LANManagerMIB2Agent\CurrentVersion.
- snmpmib.dll — указывается в параметре строкового типа Pathname, расположенном в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SNMPMIB\CurrentVersion.
- inetmib1.dll — определяется в параметре строкового типа Pathname, расположенном в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\RFC1156Agent\CurrentVersion.

Все библиотеки представляют собой агенты SNMP. При этом настройки этих агентов хранятся в отдельных файлах, которые называются соответственно hostmib.mib, lmmib2.mib, snmpmib.mib и т. д.

Кроме того, компонент устанавливает следующие исполняемые файлы: snmp.exe, evntwin.exe, evntcmd.exe.

Программа evntcmd.exe позволяет выполнить конфигурацию работы службы SNMP Trap Service с помощью командной строки. Чтобы просмотреть параметры данной программы, нужно воспользоваться командой evntcmd.exe /?.

Программа evntwin.exe является аналогом evntcmd.exe, но, в отличие от нее, предоставляет графический интерфейс настройки службы SNMP Trap Service.

Программа snmp.exe представляет собой службу SNMP Service. При этом данная служба поддерживает следующие параметры запуска: /Wow64TrapEvent:, /Wow64Event64:, /Wow64Event32:, /Wow64TrapQMutex:, /Wow64Mutex:, /TrapQSharedMemory:, /SharedMemory:, /Debug, /logtype:, /loglevel:.

Конференц-зал Windows

Название компонента: WAS-WindowsActivationService.

По умолчанию установлен. Данный компонент работает на основе одноранговых сетей и позволяет множеству пользователей вести одновременную совместную деятельность. Более подробно об одноранговых сетях в целом и данном компоненте в частности описано в гл. 8.

Подсистема для UNIX-приложений

Название компонента: SUA.

По умолчанию не установлен. С помощью данного компонента можно инсталлировать и запускать программы, написанные для операционных систем семейства UNIX. Он устанавливает подсистему POSIX (переносимый интерфейс операционной системы на основе UNIX) на ваш компьютер (в предыдущих версиях операционной системы Windows данная подсистема устанавливалась автоматически).

Нововведением подсистемы POSIX в операционной системе Windows Vista является поддержка 64-разрядных вычислений, возможность подключения к базам данных Oracle и Microsoft SQL Server с помощью интерфейсов Oracle Call Interface (OCI)

и Open Database Connectivity (ODBC), а также поддержка двух сред операционной системы UNIX (SVR-5 и BSD).

Но, кроме подсистемы POSIX, в SUA входит большинство стандартных программ операционных систем семейства UNIX. Фактически SUA представляет собой дополнительную операционную систему, в которой без перекомпиляции (или с незначительными изменениями) смогут исполняться многие программы, написанные для UNIX.

ПРИМЕЧАНИЕ

Настроить интерфейс ODBC можно с помощью стандартных программ операционной системы odbcad32.exe и odbcconf.exe.

При своей инсталляции данный компонент создает следующие библиотеки: `posixsscom.dll`, `psxdll.dll`, `psxdllsvr.dll`, `suares.dll`.

Кроме того, создается исполняемый файл `psxss.exe` (исполняемый файл подсистемы POSIX), а также каталог `SUA` (в подразделе `%systemroot%`). Данный каталог является корневым разделом для файловой системы UNIX и содержит основную структуру данной файловой системы (подразделы и конфигурационные файлы).

ПРИМЕЧАНИЕ

Список всех подсистем (исполняемых файлов, которые их представляют), поддерживающихся операционной системой Windows, содержится в ветви системного реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems.

При установке данного компонента также регистрируется драйвер `psxdrv.sys`, описываемый в подразделе реестра `PsxDrv`.

Но и это еще не все. Если вы впервые установили подсистему POSIX, никогда раньше ею не пользовавшись, то обязательно загляните в меню Пуск ▸ Подсистема для UNIX-приложений. В нем вы сможете найти ссылку на сайт, с которого можно загрузить программы, работающие в подсистеме POSIX, а также ссылку на файл помощи, подробно описывающий все возможности данной подсистемы и ее назначение.

Прослушиватель RIP

Название компонента: `RasRip`.

По умолчанию не установлен. Данный компонент устанавливает библиотеку `iprip.dll`, которая реализует работу новой службы RIP Listener. Она предназначена для поддержки обновления таблиц маршрутизации (между маршрутизаторами сети) на основе протокола RIPv1.

Данная служба запускается автоматически, с правами локальной службы и дополнительной привилегией SeChangeNotifyPrivilege.

При установке данного компонента также создается новое правило брандмауэра, которое описывается в параметре строкового типа Rip-Listener-1, расположенном в ветви реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices\Configurable\System.

Простые службы TCPIP (такие как echo, daytime и т. п.)

Название компонента: SimpleTCP или SimpleTCP-Update.

По умолчанию не установлен. Данный компонент инсталлирует службу Simple TCP/IP Services (файл tcpsvcs.exe), позволяющую компьютеру работать со следующими протоколами:

- Character Generator — генерирует ответный непрерывный поток символов при получении пакета на порт 19;
- Daytime — возвращает дату и время при получении запроса на порт 13;
- Discard — отвергает любой пакет, полученный на порт 9;
- Echo — посылает ответы на все TCP- или UDP-запросы, полученные на порт 7;
- Quote of the Day — посылает строку текста в ответ на запрос, полученный на порт 17.

Данная служба описывается в подразделе реестра simptcp, запускается автоматически, с правами локальной службы и дополнительными привилегиями SeCreateGlobalPrivilege и SeAuditPrivilege.

Настройка компонента. Вы можете самостоятельно определить те из протоколов, которые будут поддерживаться службой Simple TCP/IP Services. Для этого нужно отредактировать следующие параметры REG_DWORD-типа ветви реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\simptcp\Parameters: EnableUdpDaytime, EnableTcpDaytime, EnableUdpQotd, EnableTcpQotd, EnableUdpChargen, EnableUdpDiscard, EnableTcpChargen, EnableTcpDiscard, EnableUdpEcho, EnableTcpEcho. Названия этих параметров говорят сами за себя.

Можно также воспользоваться параметром строкового типа QotdFileName данной ветви реестра, чтобы указать путь к файлу, который содержит цитаты, отправляемые службой Quote of the Day при получении запроса. По умолчанию значение данного параметра равно %SystemRoot%\system32\drivers\etc\quotes.

И еще несколько параметров REG_DWORD-типа, которые могут находиться в данной ветви реестра.

- IoBufferSize — определяет размер используемого службой буфера.
- MaxTcpClients — указывает максимальное количество клиентов, которые могут подключиться к службам с помощью протокола TCP. По умолчанию разрешено до 16 клиентов.

Этот компонент также устанавливает библиотеку simptcp.dll.

Сервер очереди сообщений (MSMQ)

Название компонента: `MSMQ-Server`.

По умолчанию не установлен. Он содержит набор вложенных компонентов, которые представляют собой сервер Microsoft Message Queue (MSMQ) и файлы для работы с ним.

Microsoft Message Queue позволяет клиенту обратиться к службе из серверного приложения COM+, даже если серверное приложение временно недоступно. В этом случае запрос клиента помещается в очередь MSMQ и обрабатывается, когда серверное приложение станет доступным. Иначе говоря, компонент MSMQ представляет собой некий инструмент промежуточного хранения (стек) самих запросов, адресов, по которым эти запросы нужно доставить в случае обнаружения доступности серверного приложения, а также последовательности, в которой эти запросы были получены и в которой их нужно передать серверному приложению.

MSMQ для создания приложений, работающих с очередями, содержит как специальные API-функции, так и набор ActiveX-объектов, дублирующих возможности API-функций и позволяющих работать с очередями MSMQ с помощью Microsoft Visual Basic, Microsoft Visual Java, Borland Delphi.

Возможность работы с очередями установлена в операционной системе Windows Vista по умолчанию. А с помощью данного компонента можно управлять работой очередей MSMQ.

Данный компонент содержит вложенные дочерние компоненты.

Основные компоненты сервера очереди сообщений (MSMQ)

Компонент содержит в себе следующие дочерние компоненты.

- MSMQ Active Directory Integration, название компонента: `MSMQ-ADIntegration` — позволяет выполнить интеграцию очереди MSMQ в домен Active Directory.

  Он добавляют следующие библиотеки: `mqqm.dll`, `mqrt.dll`, `mqsnap.dll`, `mqsec.dll`, `mqad.dll`, `mqcertui.dll`, `mqutil.dll`, `mqcmiplugin.dll`, `mqoa.dll`, `mqlogmgr.dll`, `mqmigplugin.dll`.

  Также добавляются исполняемые файлы `mqsvc.exe` и `mqbkup.exe` и несколько MOF-файлов (`msmqpub.mof`, `msmqtrc.mof`, `msmqtrcRemove.mof`) для работы с MSMQ с помощью инструментария управления Windows.

  Кроме того, в разделе `%systemroot%\system32` создается каталог msmq, хранящий файлы, необходимые для работы MSMQ. Однако на этом установка не заканчивается. После этого в ветвь реестра, предназначенную для автоматического запуска программ при входе пользователей в систему, заносится команда `regsvr32 /s mqrt.dll`.

- MSMQ HTTP Support, название компонента: `MSMQ-HTTP` — позволяет работать с очередями MSMQ через протокол HTTP. При установке данного компо-

нента также устанавливаются следующие компоненты сервера IIS: IIS-ManagementConsole, IIS-Metabase, IIS-CommonHttpFeatures, IIS-NetFxExtensibility, IIS-ISAPIExtensions и многие другие. Кроме множества устанавливаемых библиотек и MOF-файлов, также устанавливаются несколько исполняемых файлов: mqsvc.exe, iisreset.exe, mqbkup.exe. Кроме того, в операционной системе регистрируется оснастка Internet Information Services.

- MSMQ Triggers, название компонента: MSMQ-Triggers — устанавливает триггеры для работы с очередью MSMQ.

Прокси MSMQ DCOM

Название компонента: MSMQ-DCOMProxy.

По умолчанию не установлен. Данный компонент устанавливает четыре файла с описаниями новых свойств и методов для работы с DCOM: mqoa.tlb, mqoa10.tlb, mqoa20.tlb и mqoa30.tlb.

Служба активации Windows

Название компонента: WAS-WindowsActivationService.

По умолчанию не установлен. Он включает в себя набор вложенных компонентов, с помощью которых выполняется установка службы активации программ и файлы для ее работы.

Интерфейсы API настройки

Название компонента: WAS-ConfigurationAPI.

Устанавливает дополнительные API-функции для работы со службой Windows Activation Service.

Модель процесса

Название компонента: WAS-ProcessModel.

Данный компонент устанавливается вместе с компонентом .NET Environment, а также некоторыми компонентами службы IIS. Все, что сказано об установке компонента .NET Environment, касается и данного компонента.

Среда .NET Environment

Название компонента: WAS-NetFxEnvironment.

Он устанавливается вместе с компонентом Process Model, а также некоторыми компонентами службы IIS. Компонент состоит из библиотек admwprox.dll, iisrstap.dll, iisRtl.dll, wamregps.dll и файла iisreset.exe.

После установки данного компонента будет создана служба Windows Activation Service, которая управляет процессом активации приложений и компонентов операционной системы.

Служба индексирования

Название компонента: `Indexing-Service-Package`.

По умолчанию не установлен. Данный компонент состоит из следующих библиотек: `webhits.dll`, `ciadmin.dll`, `ciodm.dll`, `ixsso.dll` и `idq.dll`. В его состав также входят исполняемые файлы `cisvc.exe` и `cidaemon.exe` и оснастка `ciadv.msc`.

Пользователь, знакомый с операционной системой Windows XP, уже, наверное, понял, что представляет собой данный компонент операционной системы. Он содержит службу индексации и оснастку Служба индексирования, которые входили в стандартную поставку операционной системы Windows XP Professional. С их помощью можно было выполнять индексирование содержимого файлов для ускорения поиска по нему. Поиск проводился с помощью оснастки Служба индексирования.

Нельзя однозначно сказать, нужен ли данный компонент операционной системы Windows Vista, ведь она по умолчанию содержит службу, которая выполняет индексирование содержимого файлов для ускоренного поиска. Хотя нужно признать, что работа данной службы очень сильно влияет на производительность операционной системы.

Служба репликации DFS

Название компонента: `DFSR-Infrastructure-ClientEdition`.

По умолчанию установлен. Данный компонент состоит из исполняемого файла `dfsr.exe`, а также библиотек `dfsrres.dll` и `dfsrperf.dll`.

Эти файлы необходимы для работы службы Репликация DFS (соответственно, первый файл является службой, второй содержит ресурсы службы, а третий описывает счетчики производительности службы), предназначенной для равноправной репликации измененных файлов среди всех компьютеров файловой системы DFS. При этом для повышения производительности работы DFS используется алгоритм сжатия Remote Differential Compression, который позволяет передавать по сети лишь измененные части файлов.

Данная служба расположена в подразделе реестра `DFSR`, запускается вручную с правами локальной системы и множеством дополнительных привилегий.

Служба Репликация DFS позволяет объединить расположенные на разных компьютерах файлы и каталоги в одно общее пространство (файловую систему).

Служба установщика ActiveX

Название компонента: `AxInstallService`.

По умолчанию не установлен. Служба установщика ActiveX войдет в следующие версии операционной системы Windows Vista: Ultimate, Business и Enterprise. Это компонент, позволяющий выполнять инсталляцию ActiveX-объектов не только администраторам компьютера, но и другим пользователям.

После установки данного компонента в операционной системе будет зарегистрирована новая служба ActiveX Installer (AxInstSV), подразделом которой (в реестре) является AxInstSV. Она запускается вручную, работает от имени операционной системы, а также использует многие дополнительные привилегии, среди которых есть привилегии архивирования, восстановления, создания начального маркера доступа.

Управлять же работой службы Служба установки ActiveX можно с помощью групповой политики Веб-узлы, разрешенные для установки элементов управления ActiveX, расположенной в подразделе Конфигурация компьютера ▸ Административные шаблоны ▸ Компоненты Windows ▸ Служба установки ActiveX и описанной в файле ActiveXInstallService.admx. С помощью данной политики можно указать отдельные сайты, с которых пользователям будет разрешено или запрещено устанавливать ActiveX-объекты. Эти сайты и само поведение заносятся в параметры строкового типа ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\AxInstaller\ApprovedActiveXInstallSites. Названия параметров определяют название сайта, а значения указывают, можно или нет с этого сайта устанавливать ActiveX-объекты. Политика также устанавливает значение параметра REG_DWORD-типа ApprovedList, расположенного в ветви системного реестра HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\AxInstaller, равным 1.

При инсталляции данного компонента также устанавливается такое приложение, как AxInstUI.exe.

Службы IIS

Название компонента: IIS-WebServerRole.

По умолчанию не установлен. С помощью данного компонента можно установить веб-сервер IIS и программы, предназначенные для работы с ним. Данный компонент содержит множество вложенных компонентов, поэтому вы можете самостоятельно выбрать те из них, которые вам нужны. Хотя размер устанавливаемых файлов от этого существенно не изменится.

Данный компонент включает в себя следующие вложенные компоненты.

Служба FTP-публикации

Название компонента: IIS-FTPPublishingService.

Содержит файлы службы FTP, а также консоль для управления работой данной службы. Файлы службы FTP и консоль выполнены в виде отдельных компонентов, поэтому вы можете установить как оба компонента сразу, так и только один из них.

- FTP Management Console, название компонента: IIS-FTPManagement — устанавливает консоль для управления службой File Transfer Protocol (FTP).
- FTP Server, название компонента: IIS-FTPServer — устанавливает службу FTP.

Службы Интернета

Название компонента: `IIS-WebServer`.

Данный компонент собственно и представляет собой службу IIS 7.0. Он состоит из множества следующих вложенных компонентов.

- Application Development Features, название: `IIS-ApplicationDevelopment` — содержит компоненты, которые устанавливают файлы, необходимые для облегчения разработки сайтов с применением возможностей, поддерживаемых IIS. Среди них находятся следующие компоненты:
  - .NET Extensibility, название компонента: `IIS-NetFxExtensibility` — устанавливает приложения .NET Framework;
  - ASP, название компонента: `IIS-ASP` — устанавливает приложения для работы с ASP;
  - ASP.NET, название компонента: `IIS-ASPNET` — устанавливает приложения для работы с ASP.NET;
  - CGI, название компонента: `IIS-CGI` — устанавливает приложения для поддержки CGI;
  - ISAPI Extensions, название компонента: `IIS-ISAPIExtensions` — устанавливает файлы для поддержки расширений ISAPI;
  - ISAPI Filters, название компонента: `IIS-ISAPIFilter` — устанавливает файлы для изменения поведения веб-сервера с помощью фильтров ISAPI;
  - Server-Side Includes, название компонента: `IIS-ServerSideIncludes` — устанавливает файлы для поддержки расширений STM, SHTM и SHTML.
- Common Http Features, название компонента: `IIS-CommonHttpFeatures` — устанавливает поддержку веб-сервером дополнительных расширений файлов. Для этого используются следующие компоненты:
  - Default Document, название компонента: `IIS-DefaultDocument` — устанавливает используемые по умолчанию файлы, которые загружаются на запросы URL;
  - Directory Browsing, название компонента: `IIS-DirectoryBrowsing` — устанавливает возможность просмотра клиентами содержимого каталога веб-сервера;
  - HTTP Errors, название компонента: `IIS-HttpErrors` — устанавливает возможность изменения содержимого страниц, возвращаемых клиенту веб-сервером при возникновении ошибки;
  - HTTP Redirection, название компонента: `IIS-HttpRedirect` — устанавливает возможность перенаправления запросов клиента на другой адрес назначения;
  - Static Content, название компонента: `IIS-StaticContent` — устанавливает поддержку веб-сервером файлов с расширениями HTM, HTML и файлов изображений.

- Health and Diagnostics, название компонента: `IIS-HealthAndDiagnostics` — позволяет устанавливать мониторинг состояния сервера, сайта и других приложений IIS. Он состоит из следующих дочерних компонентов:
  - Custom Logging, название компонента: `IIS-CustomLogging` — устанавливает поддержку ведения файлов журналов работы сервера, сайта и других приложений IIS;
  - HTTP Logging, название компонента: `IIS-HttpLogging` — устанавливает поддержку ведения файлов журналов по активности сайтов данного сервера;
  - Logging Tools, название компонента: `IIS-LoggingLibraries` — устанавливает дополнительные сценарии и приложения веб-сервера IIS, предназначенные для слежения за работой компонентов IIS;
  - ODBC Logging, название компонента: `IIS-ODBCLogging` — устанавливает поддержку ведения файлов журналов работы базы данных ODBC;
  - Request Monitor, название компонента: `IIS-RequestMonitor` — устанавливает поддержку ведения мониторинга состояния работы сервера, сайта и других приложений IIS;
  - Tracing, название компонента: `IIS-HttpTracing` — устанавливает поддержку возможностей трассировки приложений ASP.NET и неудачных запросов.
- Performance Features, название компонента: `IIS-Performance` — содержит несколько компонентов, предназначенных для настройки производительности работы веб-сервера:
  - Http Compression Dynamic, название: `IIS-HttpCompressionDynamic` — устанавливает поддержку возможности выполнения компрессии динамического содержимого;
  - Static Content Compression, название: `IIS-HttpCompressionStatic` — устанавливает поддержку возможности выполнения компрессии HTM-, HTML-файлов и файлов изображений перед отправкой их клиенту.
- Security, название компонента: `IIS-Security` — включает в себя вложенные компоненты, предоставляющие дополнительные возможности по настройке безопасности веб-сервера IIS. К ним относятся следующие компоненты:
  - Basic Authentication, название компонента: `IIS-BasicAuthentication` — устанавливает возможность запроса логина и пароля пользователя при подключении к веб-серверу;
  - Client Certificate Mapping Authentication, название компонента: `IIS-ClientCertificateMappingAuthentication` — устанавливает возможность аутентификации пользователя на основе сертификата учетной записи пользователя домена Active Directory;
  - Digest Authentication, название компонента: `IIS-DigestAuthentication` — устанавливает возможность аутентификации пользователя на основе отправленного хеша контроллеру домена Active Directory;

- IIS Client Certificate Mapping Authentication, название компонента: `IIS-IISCertificateMappingAuthentication` — устанавливает возможность аутентификации пользователя на основе сертификатов при подключении к веб-серверу;
- IP Security, название компонента: `IIS-IPSecurity` — устанавливает возможность разрешения или запрета доступа к содержимому на основе IP-адреса или DNS-имени клиента;
- Request Filtering, название компонента: `IIS-RequestFiltering` — устанавливает возможность настройки правил на блокировку определенных клиентских запросов;
- URL Authorization, название компонента: `URL Authorization` — устанавливает возможность авторизации клиентов, которые пытаются получить доступ к веб-приложениям;
- Windows Authentication, название: `IIS-WindowsAuthentication` — устанавливает возможность аутентификации клиента на основе протоколов NTLM или Kerberos.

Средства управления веб-узлом

Название компонента: `IIS-WebServerManagementTools`.

Хранит набор компонентов, предназначенных для установки дополнительных программ и консолей, используемых для управления веб-сервером IIS. Среди вложенных компонентов можно встретить следующие.

- IIS 6 Management Compatibility, название: `IIS-IIS6ManagementCompatibility` — позволяет установить консоль управления IIS, а также дополнительные API-функции и сценарии, которые могут понадобиться при работе с веб-сервером. Этот компонент также содержит вложенные компоненты.
- IIS 6 Management Console, название компонента: `IIS-LegacySnapIn` — дает возможность установить консоль управления IIS.
- IIS 6 Scripting Tools, название компонента: `IIS-LegacyScripts` — позволяет установить набор конфигурационных сценариев для IIS.
- IIS 6 WMI Compatibility, название компонента: `IIS-WMICompatibility` — дает возможность установить дополнительные классы для работы с веб-сервером IIS с помощью инструментария управления Windows.
- IIS Metabase and IID 6 configuration compatibility, название компонента: `IIS-Metabase` — позволяет установить дополнительные функции для взаимодействия с хранилищем более новой версии IIS, а также метабазу IIS.
- IIS Management Console, название компонента: `IIS-ManagementConsole` — устанавливает консоль Web server Management Console, предназначенную для управления локальными или удаленными веб-серверами.
- IIS Management Scripts and Tools, название: `IIS-ManagementScriptingTools` — устанавливает сценарии для работы с локальным веб-сервером.

- IIS Management Service, название компонента: `IIS-ManagementService` — позволяет удаленно управлять локальным веб-сервером с помощью консоли Web server Management Console.

Службы для NFS

Название компонента: `ServicesForNFS-ClientOnly`.

По умолчанию не установлен. Данный компонент позволяет вам создать однородную среду из компьютеров, на которых установлены операционные системы семейства Windows или UNIX. После установки данного компонента пользователи этих операционных систем смогут обращаться к общим папкам компьютеров с любой операционной системой с помощью протокола NFS.

Компонент Службы для NFS содержит несколько дочерних компонентов, предназначенных для работы со службой NFS (Network File System). Описание данных компонентов приведено далее.

Администрирование

Название компонента: `NFS-Administration`.

Данный компонент устанавливает файлы для работы со службой NFS. К этим файлам, в первую очередь, относится консоль `nfsmgmt.msc` (Services for Network File System) и исполняемые файлы `nfsadmin.exe`, `rpcinfo.exe`, `showmount.exe`. Также устанавливаются библиотеки `nfscligrps.dll`, `nfsclilocks.dll`, `nfscommgmt.dll` и `nfsrc.dll`.

Оснастка Services for Network File System. Консоль `nfsmgmt.msc` предоставляет интерфейс для управления работой таких служб, как Клиент и сервер для сетей NFS.

С помощью этой консоли вы не сможете примонтировать (или размонтировать) каталоги к файловой системе NFS — это выполняется посредством программ, входящих в компонент Клиент для NFS. Но с ее помощью можно настроить работу служб NFS.

Для этого достаточно запустить данную оснастку, выбрать нужную службу из списка и в ее контекстном меню выбрать команду Свойства. Например, с помощью окна Свойства службы Клиент для NFS можно настроить следующие параметры работы файловой системы NFS (все эти настройки изменяют параметры `REG_DWORD`-типа ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Client for NFS\CurrentVersion\Default`).

- Используемые для соединения протоколы. Можно использовать либо протоколы TCP и UDP, либо один из них. Эта настройка изменяет значение параметра `Protocols`.
- Используемый по умолчанию тип монтирования каталога к файловой системе NFS. Эта настройка изменяет значение параметра `MountType`.
- Интервал поиска общих каталогов файловой системы NFS. Эта настройка изменяет значение параметра `Timeout`.

- Используемые по умолчанию разрешения доступа к каталогам файловой системы NFS.

Благодаря данной оснастке можно определить имя домена Active Directory, а также имя сервера User Name Mapping. Для этого достаточно воспользоваться командой Свойства контекстного меню корневого раздела оснастки.

Исполняемые файлы. Кроме оснастки Services for Network File System, данный компонент добавляет набор программ командной строки, которые позволяют управлять работой файловой системы NFS.

Программа `nfsadmin.exe` позволяет управлять клиентом, сервером или картой файловой системы NFS. Для этого применяются специальные разновидности данной программы (также с каждой командой можно указывать параметр `\\<IP-адрес>`, чтобы удаленно управлять компонентами файловой системы NFS).

- `nfsadmin.exe server <параметры>` — позволяет управлять службой `NfsSvc`. Параметры данной команды позволяют изменить те же настройки, что и окно Свойства раздела Server for NFS оснастки Services for Network File System.
- `nfsadmin.exe client <параметры>` — позволяет управлять службой `NfsClnt`. Параметры данной команды позволяют изменить те же настройки, что и окно Свойства раздела Client for NFS оснастки Services for Network File System.
- `nfsadmin.exe mapping <параметры>` — параметры данной команды позволяют изменить те же настройки, что и окно Свойства корневого раздела оснастки Services for Network File System.

Программа `showmount.exe` позволяет просматривать общие каталоги, примонтированные к файловой системе NFS. Список параметров данной программы можно просмотреть с помощью команды `showmount.exe /?`.

Программа `rpcinfo.exe` позволяет просматривать информацию о протоколе RPC и использующих его программах. Список параметров данной программы можно просмотреть с помощью команды `rpcinfo.exe /?`.

Клиент для NFS

Название компонента: `ClientForNFS-Infrastructure`.

Добавляемые службы. Устанавливает службу Client for NFS (файл `nfsclnt.exe`), позволяющую данному компьютеру получать доступ к общим каталогам файловой системы NFS. Служба запускается автоматически, с правами сетевой службы и дополнительными привилегиями SeAuditPrivilege, SeChangeNotifyPrivilege и SeImpersonatePrivilege.

Настройки службы Client for NFS хранятся в параметрах ветви системного реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NfsClnt\NFS LANs\Default LAN`.

Компонент также устанавливает драйвер Server for NFS Open RPC (ONCRPC), который представлен файлом `rpcxdr.sys` и запускается вручную. Именно он и является

клиентом службы NFS и выполняет взаимодействие с драйвером nfsrdr.sys, который является сервером службы NFS. Драйвер nfsrdr.sys получает запросы от драйверов rpcxdr.sys и передает их драйверу локальной файловой системы ntfs.sys на обработку.

Поведение данного драйвера также можно настроить. Для этого применяются параметры REG_DWORD-типа ветви реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RpcXdr\Parameters.

- DefaultNumberOfWorkerThreads — определяет количество рабочих потоков, используемых по умолчанию входящими запросами NFS. Значение данного параметра не может быть больше 64 потоков.
- DefaultWorkerThreadPriority — указывает используемый по умолчанию приоритет рабочих потоков.
- MaxWorkItems — определяет максимальное количество рабочих элементов, которые могут использоваться драйвером для обработки запросов.

Добавляемые файлы. Данный компонент также устанавливает исполняемые файлы mount.exe, nfsadmin.exe, nfsclnt.exe, rpcinfo.exe, showmount.exe и umount.exe. Большинство из них устанавливаются и компонентом Administrative Tools. Новыми же для нас являются только два файла: mount.exe и umount.exe. С их помощью можно добавить (удалить) общий каталог к файловой системе NFS.

Кроме того, устанавливаются библиотеки nfscligrps.dll, nfsclilocks.dll, nfscprop.dll, nfsnp.dll и nfsrc.dll.

Службы печати

Название компонента: Printing-Foundation-Features.

Содержит вложенные компоненты, позволяющие выполнять печать по сети или на компьютерах с операционными системами UNIX. Среди содержимого данного раздела можно встретить следующие компоненты.

Клиент интернет-печати

Название компонента: Printing-Foundation-InternetPrinting-Client.

По умолчанию установлен. Позволяет использовать принтер, подключаясь к нему по протоколу TCP/IP. Данный компонент состоит из исполняемого файла wpnpinst.exe и библиотек inetppui.dll и inetpp.dll.

Монитор LPR-портов

Название компонента: Printing-Foundation-LPRPortMonitor.

По умолчанию не установлен. Данный компонент позволяет работать с серверами печати UNIX (или VAX), для чего устанавливаются библиотеки lprhelp.dll, lprmon.dll, lprmonui.dll и SetupLpr.dll.

Библиотека lprmon.dll представляет собой порт LPR, который добавляется к списку портов ветви реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\

Control\Print\Monitors. Иначе говоря, после установки данного компонента в списке Порты принтера (отображается после нажатия кнопки Добавить порт, расположенной на вкладке Порты окна Свойства: Сервер печати) появится новый элемент LPR Port.

Этот компонент также устанавливает два исполняемых файла командной строки: lpq.exe и lpr.exe.

С помощью программы lpq.exe можно просмотреть очередь удаленного принтера, установленного на компьютере с операционной системой семейства UNIX. Для этого достаточно воспользоваться данной программой, применив следующий синтаксис: lpq.exe -s<имя сервера> -p<имя принтера>.

Если же вам нужно распечатать файл на удаленном принтере, то достаточно воспользоваться программой lpr.exe. Она имеет следующий основной синтаксис: lpr.exe -s<имя сервера> -p<имя принтера> <путь к файлу, который нужно распечатать, и его имя>. Вы также можете использовать дополнительные параметры:

- -C <класс> — класс нового задания;
- -J <имя> — название задания;
- -o <тип> — определяет тип распечатываемого файла (по умолчанию считается, что распечатываемый файл текстовый);
- -d — говорит о том, что перед печатью распечатываемый файл нужно скопировать на сервер печати.

Служба печати LPD

Название компонента: Printing-Foundation-LPDPrintService.

По умолчанию не установлен. Данный компонент устанавливает библиотеку lpdsvc.dll, необходимую для работы с LPD (Line Printer Daemon) и Remote Line Printer в качестве клиента.

После установки данного компонента в операционной системе будет зарегистрирована новая служба TCP/IP Print Server, подразделом которой (в реестре) является подраздел LPDSVC. Служба запускается автоматически, работает от имени операционной системы, но никаких дополнительных системных привилегий не использует.

Настройки данной службы хранятся в параметрах ветви системного реестраWindows HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LPDSVC\Parameters, имеющих тип REG_DWORD.

- AllowJobRemoval — определяет, разрешено ли принтеру выполнять удаленные задания. По умолчанию разрешено.
- AllowPrinterResume — указывает, разрешено ли пользователям возобновлять работу принтера. По умолчанию разрешено.

- MaxConcurrentUsers — определяет максимальное количество пользователей, которые могут пользоваться данным принтером одновременно. По умолчанию значение параметра равно 100.

Удаленное разностное сжатие

Название компонента: MSRDC-Infrastructure.

По умолчанию установлен. Данный компонент представлен библиотекой msrdc.dll. Именно этот способ сжатия используется некоторыми службами операционной системы Windows Vista для повышения скорости работы в сети.

Управление съемными носителями

Название компонента: Microsoft-Windows-RemovableStorageManagement.

По умолчанию не установлен. Данный компонент устанавливает следующие библиотеки: mll_hp.dll, mll_mtf.dll, mll_qic.dll, ntmsapi.dll, ntmsdba.dll, ntmsevt.dll, ntmsmgr.dll, ntmssvc.dll, rsmps.dll. Кроме того, устанавливаются следующие исполняемые файлы: rsm.exe, rsmmllsv.exe, rsmsink.exe, rsmui.exe.

Файл rsm.exe представляет собой программу командной строки, позволяющую управлять съемными устройствами. Чтобы просмотреть возможности данной программы, достаточно воспользоваться командой rsm.exe /?.

В процессе инсталляции данного компонента также устанавливаются консоли ntmsmgr.msc (Съемные ЗУ) и ntmsoprq.msc (Запросы операторов съемных ЗУ).

Библиотеки и исполняемые файлы, которые устанавливаются данным компонентом, необходимы не только для работы устанавливаемых консолей, но и для работы новой службы Съемные ЗУ (для своей работы она использует библиотеку ntmssvc.dll). Данная служба запускается вручную, работает от имени локальной системы, а также использует множество дополнительных привилегий.

Фактически данный компонент не является нововведением операционной системы Windows Vista, так как он присутствовал и в операционной системе Windows XP. Он позволяет управлять и каталогизировать подключенные к компьютеру съемные устройства, что может повысить скорость доступа к ним.

Факсы и сканирование Windows

Название компонента: FaxServicesUltimate.

По умолчанию установлен. Данный компонент состоит из исполняемых файлов wfs.exe, fxsunatd.exe, fxssvc.exe и fxscover.exe, а также библиотек winfax.dll, wfsr.dll, fxsxp32.dll, fxsutility.dll, fxstiff.dll, fxst30.dll, fxsst.dll, fxsroute.dll, fxsresm.dll, fxsmon.dll, fxsext32.dll, fxsevent.dll, fxscomposeres.dll, fxscompose.dll, fxscomex.dll, fxscom.dll и fxsapi.dll.

Все эти файлы необходимы не только для работы программы Факсы и сканирование Windows, но и для работы службы Факс. Данная служба запускается вручную с правами сетевой службы и множеством дополнительных привилегий.

Работа с компонентами

После того как вы выберете устанавливаемый/удаляемый компонент операционной системы и нажмете кнопку OK, начнется процесс установки/удаления выбранного компонента. Он выполняется автоматически и не требует от вас никаких действий. Если в процессе установки/удаления компонента программа установки обнаружит, что не может выполнить какое-либо действие, то будет выведено окно о необходимости перезагрузки компьютера и данное действие будет выполнено при следующем запуске. При этом сведения об отложенных действиях записываются в файл `pending.xml`, расположенный в каталоге `%systemroot%\WinSxS`, а в параметр `REG_MULTI_SZ`-типа `SetupExecute`, расположенный в ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager`, заносится значение `poqexec.exe \SystemRoot\WinSxS\pending.xml`.

Сведения о том, как прошел процесс удаления или установки компонентов, можно просмотреть в файле `CBS.log`, расположенном в каталоге `%systemroot%\logs`.

СОВЕТ

Перед установкой или удалением компонента операционной системы всегда выполняется создание точки восстановления, поэтому, если при выполнении операции произошел сбой, просто вернитесь к созданной точке восстановления с помощью Восстановления системы.

Этот совет вам может пригодиться, так как иногда процесс установки/удаления компонента может зависнуть (особенно если в это время работает множество других программ), и если вы перезагрузите компьютер, не дождавшись завершения установки/удаления компонента, то, скорее всего, при следующем запуске операционной системы окно Компоненты Windows будет пустым. Это говорит о том, что данные, на основе которых строится данное окно, повреждены или некорректны. В этом случае достаточно воспользоваться точкой восстановления, чтобы все вернулось на свои места.

Конечно, в окне Компоненты Windows показаны не все компоненты операционной системы Windows Vista. Однако теперь отобразить скрытые компоненты не так-то просто. Если раньше сведения о тех компонентах, которые будут отображаться, хранились в файле `sysoc.inf` раздела `%systemroot%\inf`, то теперь данный файл отсутствует.

Сведения обо всех компонентах операционной системы Windows Vista хранятся в каталоге `%systemroot%\servicing\packages`. Каждый компонент представлен в нем двумя или более файлами. Первый из них имеет расширение CAT

и содержит информацию о подписи компонента. Остальные же имеют расширение MUM и представляют собой текстовые файлы в XML-формате, которые описывают название компонента, а также его поведение в операционной системе или дополнительные языковые настройки.

Сведения о компонентах операционной системы, которые отображаются в окне Компоненты Windows, можно найти и в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Component Based Servicing. Она включает в себя два вложенных подраздела PackageDetect и Packages. С помощью подраздела PackageDetect можно удалить из окна Компоненты Windows некоторые элементы. Для этого достаточно удалить или присвоить значение 1 параметру, названному в честь файла компонента и расположенному в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Component Based Servicing\PackageDetect\x86_microsoft-windows-foundation-package_31bf3856ad364e35_0.0.0.0_none_1bcadd73a6fabe3b.

Сами же программы и компоненты, которые можно установить в операционной системе Windows Vista, хранятся в подразделах каталога %systemroot%\winsxs. Именно поэтому при установке и удалении компонентов операционной системы больше не нужно предоставлять загрузочный диск Windows.

Установка необязательного компонента Windows

Расположение: %systemroot%\system32\ocsetup.exe.

Мы рассмотрели окно Компоненты Windows, с помощью которого можно удалить или установить тот или иной компонент операционной системы. Однако это не единственный способ установки и удаления компонентов Windows. Для этого также можно воспользоваться программой командной строки ocsetup.exe. Основной синтаксис данной программы следующий: ocsetup <название компонента> <параметры>. Список названий компонентов операционной системы Windows Vista был приведен в подразд. «Компоненты операционной системы»» этого раздела. Параметры, которые можно использовать при работе с данной программой, представлены далее.

- /uninstall — удалить данный компонент операционной системы. Если не указывать данный параметр, то соответствующий компонент операционной системы будет установлен.
- /passive — не отображать информацию об установке или удалении компонента операционной системы.
- /unattendfile:<путь к файлу> — указывает путь к файлу ответов.
- /quiet — подавлять все запросы к пользователю, которые по умолчанию необходимо выполнить для корректной установки. Данные для корректной установки должны быть взяты из файла ответов.
- /norestart — не выполнять перезагрузку компьютера после установки или удаления компонента операционной системы.

- /log:<путь к файлу> — указывает путь к файлу, в который будут заноситься сведения о процессе удаления или установки компонента.
- /x:<дополнительные параметры> — дополнительные параметры работы базового установщика данного компонента.

Диспетчер пакетов Windows

Расположение: %systemroot%\system32\PkgMgr.exe.

Для установки или удаления компонентов операционной системы можно также использовать программу командной строки PkgMgr.exe. Список параметров данной программы можно просмотреть, воспользовавшись командой PkgMgr.exe /?. В остальном же использование данной программы похоже на использование программы ocsetup.exe, описанной выше (более того, программа ocsetup.exe при своей работе вызывает программу PkgMgr.exe).

Использование репозитария CIM

Работать с компонентами операционной системы можно и с помощью класса Win32_OsBaseline, принадлежащего пространству имен \\root\cimv2. Данный класс содержит методы для описания компонентов, из которых состоит операционная система.

- EnumBaselineComponents — перечисляет компоненты.

  Входящий параметр: строковый параметр, определяющий путь к компоненту.

  Возвращаемые параметры: массив параметров строкового типа, определяющих подлинность компонента.
- EnumOutOfDateComponents — перечисляет информацию о подлинности компонентов.

  Входящий параметр: строковый параметр, определяющий путь к компоненту.

  Возвращаемые параметры: массив параметров строкового типа, определяющих подлинность компонента.
- GetBaselineComponentInfo. Возвращает информацию о компоненте.

  Входящие параметры:

  - строковый параметр, определяющий путь к компоненту;
  - параметр строкового типа, определяющий подлинность компонента.

  Возвращаемые параметры:

  - строковый параметр, определяющий имя компонента;
  - строковый параметр, определяющий версию компонента;
  - определяет тип компонента, имеет тип uint32.
- GetBaselinePath — возвращает путь к компоненту.

  Входящий параметр: определяет версию пакета обновлений, имеет тип uint32.

  Возвращаемый параметр: строковый параметр, определяющий путь к компоненту.

- `GetInstalledComponentInfo` — определяет информацию об установленном компоненте.

  Входящие параметры:

  - параметр строкового типа, определяющий подлинность компонента;
  - строковый параметр, указывающий имя компонента;
  - строковый параметр, определяющий версию компонента.

  Возвращаемый параметр: определяет тип компонента, имеет тип `uint32`.

- `GetLatestBaselineServicePack` — возвращает версию установленного пакета обновлений компонента.

  Входящие параметры: нет.

  Возвращаемый параметр: отображает версию установленного в операционной системе пакета обновлений, имеет тип `uint32`.

9.2. Установка и удаление сетевых компонентов с помощью программы netcfg.exe

Расположение: `%systemroot%\system32\netcfg.exe`.

В поставку операционной системы Windows Vista входит специальная программа командной строки, позволяющая просмотреть, установить или удалить такие сетевые компоненты операционной системы, как протоколы NetBIOS, TCP/IPv6, IPX и т. д., сетевые службы QoS, Служба доступа к файлам и принтерам сетей Microsoft и т. д. Чтобы просмотреть описание работы программы `netcfg.exe`, введите команду `netcfg /?`.

Работа с программой

Работать с программой `netcfg.exe` довольно просто. Однако для этого нужно знать названия сетевых компонентов, которые с ее помощью можно установить или удалить.

Просмотр установленных сетевых компонентов

Как уже было сказано, данная программа позволяет просмотреть список установленных сетевых компонентов. Для этого применяется команда `netcfg -s n`. После ее ввода перед вами отобразится список установленных сетевых адаптеров, протоколов, служб и клиентов. Обратите внимание на левый столбец выводимых данных (в правом столбце отображается описание сетевого компонента). В нем содержится сокращенное имя компонента, которое применяется во всех командах программы `netcfg`.

Можно также просмотреть список установленных адаптеров, для чего применяется команда `netcfg -s a`. Или список привязок для определенного сетевого компонента, для чего применяется команда `netcfg -b <сокращенное имя сетевого компонента>`. Например, `netcfg -b ms_tcpip`.

Кроме того, вы можете просмотреть состояние только определенного сетевого компонента. Для этого применяется команда `netcfg -q <сокращенное имя сетевого компонента>`. Например, чтобы просмотреть, установлен ли компонент NetBIOS, нужно воспользоваться командой `netcfg -q ms_netbios`.

Установка сетевых компонентов

Для установки определенного сетевого компонента нужно знать его сокращенное имя или название INF-файла. Ниже будет приведет список всех возможных сокращенных имен.

Чтобы установить сетевой компонент, используя сокращенное имя, нужно воспользоваться командой `netcfg -c <класс компонента> -I <сокращенное имя компонента>`. Здесь `класс компонента` может принимать следующие значения: `p` для сетевого протокола, `s` для сетевой службы и `c` для сетевого клиента.

Чтобы установить сетевой компонент, используя его INF-файл, нужно воспользоваться немного отличной командой: `netcfg -l <путь к INF-файлу> -c <класс компонента> -I <сокращенное имя компонента, которое будет применяться для его идентификации>`.

Можно также воспользоваться командой `netcfg -winpe`, которая при инсталляции операционной системы используется для установки TCP/IP, NetBIOS и клиента для сетей Microsoft.

Сведения об установке сетевого компонента заносятся в файл журнала `setupapi.app.log`, расположенный в каталоге `%windows%\inf`.

Удаление сетевых компонентов

Для удаления сетевых компонентов используется команда `netcfg -u <сокращенное имя компонента>`. Например, чтобы удалить клиент для сетей Microsoft, нужно воспользоваться командой `netcfg -u MS_MSCLIENT`.

Стандартные сетевые компоненты

Теперь рассмотрим список стандартных сетевых компонентов, которые вы можете добавлять или удалять. Все INF-файлы, описанные ниже, расположены в каталоге `%systemroot%\INF`.

Для удобства разобьем его на сетевые протоколы, службы и клиенты.

Сетевые протоколы

Сначала будут описаны сетевые протоколы.

- `ms_pppoe` — по умолчанию установлен. Определяет протокол Протокол точка–точка по Ethernet, добавляя в систему драйвер Remote Access PPPOE. Данный протокол позволяет передавать кадры PPP через локальную сеть Ethernet,

используя туннели. Данный протокол, как и протокол PPTP, поддерживает авторизацию, шифрование и сжатие.

INF-файл: `netrast.inf`, секция `Ndi-PppoeProtocol`.

- `ms_tcpip6` — по умолчанию установлен. Определяет протокол Протокол Интернета версии 6 (TCP/IPv6). Основным новшеством данной версии IP-протокола является расширенное до 128 бит адресное пространство. Кроме того, протокол IPv6 обеспечивает упрощенный механизм автоконфигурирования адресов, а также масштабируемость групповых адресов.

  INF-файл: `netip6.inf`, секция `MS_TCPIP6.Install`.

- `MS_TCPIP6_TUNNEL` — по умолчанию установлен. Определяет протокол Microsoft TCP/IP версия 6 — туннели. Позволяет создавать туннели на основе протокола TCP/IP версии 6.

  INF-файл: `netip6.inf`, секция `MS_TCPIP6.Tunnel.Install`.

- `MS_NDISWAN` — по умолчанию установлен. Определяет драйвер NDIS-драйвер WAN удаленного доступа.

  INF-файл: `netrast.inf`, секция `Ndi-NdisWan`.

- `MS_wanarp` — по умолчанию установлен. Определяет драйвер Драйвер удаленного доступа IP ARP.

  INF-файл: `netrast.inf`, секция `Ndi-Wanarp`.

- `ms_netbt_smb` — по умолчанию установлен. Определяет протокол Протокол сообщений TCP/IP (сеанс SMB). Он является протоколом прикладного уровня, предназначенным для совместного использования файлов. Он работает поверх протоколов NBT или NetBEUI, но также может работать на основе протоколов IPX/SPX.

  INF-файл: `nettcpip.inf`, секция `MS_NETBT_SMB.PrimaryInstall`.

- `ms_netbt` — по умолчанию установлен. Определяет протокол Протокол клиента WINS (TCP/IP). Основным назначением службы WINS является организация процесса разрешения имен NetBIOS в соответствующие IP-адреса. Для этого и используется протокол, определенный данным сетевым компонентом.

  INF-файл: `nettcpip.inf`, секция `MS_WINS.PrimaryInstall`.

- `MS_RSPNDR` — по умолчанию установлен. Определяет протокол Ответчик обнаружения топологии канального уровня. Он используется сетевым модулем операционной системы Windows Vista для отображения графического представления сети. Например, графическое представление сети можно увидеть в мастере Центр управления сетями и общим доступом. Если операционная система не будет поддерживать данный протокол, то соответствующий компьютер не будет отображаться в графическом представлении сети.

  INF-файл: `rspndr.inf`, секция `Install`.

- `MS_SMB` — по умолчанию установлен. Определяет глобальное устройство Microsoft NetbiosSmb. На основе данного устройства работают экземпляры NetBT_Tcpip.

  INF-файл: `nettcpip.inf`, секция `MS_SMB.Install`.

- `MS_TCPIP` — по умолчанию установлен. Определяет протокол Протокол Интернета версии 4 (TCP/IPv4). Он является стандартным протоколом, используемым операционной системой для сетевого взаимодействия.

  INF-файл: `nettcpip.inf`, секция `MS_TCPIP.PrimaryInstall`.

- `ms_pptp` — по умолчанию установлен. Определяет протокол Туннельный протокол точка–точка. Он позволяет создавать туннели, которые будут передавать кадры PPP через сети на базе протокола TCP/IP. При этом протокол поддерживает шифрование кадров с помощью механизма MPPE (Microsoft Point-to-Point Encryption), основанного на алгоритме RSA.

  INF-файл: `netrast.inf`, секция `Ndi-PptpProtocol`.

- `ms_l2tp` — по умолчанию установлен. Определяет протокол Туннельный протокол уровня 2. Протокол туннелирования второго уровня, функционирующий на канальном уровне, представляет собой промышленный стандарт, впервые реализованный в операционной системе Windows 2000 и используемый как передающая среда в VPN (виртуальная частная сеть). В отличие от такого протокола, как PPTP (протокол L2TP является дальнейшим развитием протокола PPTP), протокол L2TP использует для шифрования протокол IPSec. Еще одним отличием протокола L2TP является то, что для передачи управляющих сообщений он использует дейтаграммный протокол UDP (PPTP в управляющем канале использует протокол TCP).

  INF-файл: `netrast.inf`, секция `Ndi-L2tpProtocol`.

- `MS_LLTDIO` — по умолчанию установлен. Определяет драйвер Драйвер в/в тополога канального уровня. Данный драйвер используется для создания графического представления сети (карты сети).

  INF-файл: `lltdio.inf`, секция `Install`.

- `MS_NDISUIO` — по умолчанию установлен. Определяет протокол NDIS-протокол ввода-вывода пользовательского режима.

  INF-файл: `ndisuio.inf`, секция `Install`.

- `MS_wanarpv6` — по умолчанию установлен. Определяет драйвер Драйвер удаленного доступа IPv6 ARP.

  INF-файл: `netrast.inf`, секция `Ndi-Wanarpv6`.

- `MS_TCPIP_TUNNEL` — по умолчанию установлен. Определяет протокол Протокол Интернета (TCP/IP) — туннели. Позволяет создавать туннели на основе протокола TCP/IP версии 4.

  INF-файл: `nettcpip.inf`, секция `MS_TCPIP.Tunnel.PrimaryInstall`.

- `ms_Bridge` — по умолчанию установлен. Определяет протокол MAC Bridge. Он используется во время маршрутизации с помощью стандартных средств операционной системы.

  INF-файл: `netbrdgs.inf`, секция `Bridge.ndi`.

- MS_IrDA — по умолчанию установлен. Определяет протокол IrDA Protocol. Он предназначен для выполнения подключения между двумя компьютерами с помощью инфракрасной связи. Нужно признать, что на сегодняшний день инфракрасная связь практически не используется, вытесненная беспроводной связью и Bluetooth.

  INF-файл: netirda.inf, секция IrDA.Install.

- MS_RMCAST — по умолчанию не установлен. Определяет протокол Reliable Multicast Protocol. Он представляет собой протокол транспортного уровня, поддерживающий широковещательную рассылку.

  INF-файл: netpgm.inf, секция MS_RMCAST.PrimaryInstall.

Сетевые службы

Теперь рассмотрим сетевые службы.

- MS_RASSRV — по умолчанию установлена. Определяет службу Сервер удаленного доступа. Она обрабатывает запросы от удаленных клиентов, подключаемых к серверу с помощью модема.

  INF-файл: netrass.inf, секция Ndi-RasSrv.

- MS_SERVER — по умолчанию установлена. Определяет службу Служба доступа к файлам и принтерам сетей Microsoft. Она является основной службой операционной системы, используемой при доступе к общим папкам и принтерам.

  INF-файл: netserv.inf, секция Install.ndi.

- MS_STEELHEAD — по умолчанию установлена. Определяет службу Сервер маршрутизации и удаленного доступа. Она представляет собой надстройку над локальной сетью, предназначенную для маршрутизации глобальных сетей (для этого используется Windows Sockets). Она не сможет заменить собой аппаратные маршрутизаторы, например маршрутизаторы Cisco, однако может превратить сервер в маршрутизатор низкого уровня. Данная служба поддерживает протоколы IP, RIP, OSPF и т. д.

  INF-файл: netrass.inf, секция Ndi-Steelhead.

- MS_PACER — по умолчанию установлена. Определяет службу Планировщик пакетов QoS. Эта служба, основанная на протоколах прикладного уровня, позволяет выделить определенную часть пропускной способности сети для передаваемых данных, которые чувствительны к задержкам.

  INF-файл: netpacer.inf, секция Install.

- MS_RASMAN — по умолчанию установлена. Определяет службу Диспетчер подключений удаленного доступа. Она позволяет удаленно подключиться к компьютеру (как правило, с помощью модема).

  INF-файл: netrass.inf, секция Ndi-RasMan.

- MS_NETBIOS — по умолчанию установлена. Определяет интерфейс NetBIOS Interface.

  INF-файл: netnb.inf, секция NetBIOS.ndi.

- MS_NATIVEWIFIP — по умолчанию установлена. Определяет фильтр Фильтр NativeWiFi.

  INF-файл: netnwifi.inf, секция MS_NWIFI.Install.

- MS_RASCLI — по умолчанию не установлена. Определяет службу Клиент удаленного доступа. Она выполняет подключение к серверу удаленного доступа с помощью модемного соединения.

  INF-файл: netrass.inf, секция Ndi-RasCli.

- MS_ALG — по умолчанию не установлена. Определяет службу Application Layer Gateway. Она является основой стандартного брандмауэра операционной системы и компонента ICS.

  INF-файл: netrass.inf, секция Ndi-ALG.

Сетевые клиенты

Последним, что мы рассмотрим, являются сетевые клиенты.

- MS_MSCLIENT — по умолчанию установлен. Определяет клиент для сетей Microsoft.

  INF-файл: netmscli.inf, секция MSClient.ndi.

Принцип работы программы netcfg.exe

И напоследок вкратце рассмотрим принцип работы программы netcfg.exe. При удалении сетевых компонентов данная программа не удаляет никаких файлов или ветвей, принадлежащих сетевым компонентам. Единственной ветвью, которую она использует, является HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Network. Эта ветвь включает в себя следующие подразделы:

- {4D36E972-E325-11CE-BFC1-08002BE10318} — определяет список сетевых адаптеров, которые установлены в системе;
- {4d36e973-e325-11ce-bfc1-08002be10318} — указывает список сетевых клиентов, установленных в операционной системе;
- {4d36e974-e325-11ce-bfc1-08002be10318} — определяет список сетевых служб, установленных в операционной системе;
- {4d36e975-e325-11ce-bfc1-08002be10318} — указывает список сетевых протоколов, установленных в операционной системе.

Каждый из них содержит вложенные подразделы, которые описывают один установленный сетевой компонент. При удалении сетевого компонента с помощью программы netcfg.exe она удаляет соответствующий компоненту подраздел данной ветви реестра.

Фактически действие программы командной строки netcfg.exe аналогично удалению или установке сетевых компонентов с помощью кнопок Установить и Уда-

лить окна свойств определенного сетевого подключения. Это окно можно вызвать с помощью ссылки Просмотр состояния напротив нужного сетевого подключения в папке Центр управления сетями и общим доступом. После выбора данной ссылки перед вами отобразится окно состояния данного сетевого подключения, в котором нужно нажать кнопку Свойства.

9.3. Мастер Установка или удаление языков отображения

Расположение: `%systemroot%\system32\lpksetup.exe`.

Нововведением операционной системы Windows Vista является новый способ изменения языка операционной системы. Если у вас имеется англоязычная версия операционной системы, то для ее, допустим, русифицирования вам не нужно устанавливать новую операционную систему. Достаточно установить новый языковой пакет. При этом предыдущий пакет по умолчанию также остается в системе, поэтому вы можете оперативно переходить от одного языкового пакета к другому.

Для изменения языкового пакета достаточно воспользоваться такой программой, как `lpksetup.exe`. После ее вызова отобразится мастер, позволяющий либо установить новый языковой пакет (кнопка Установить языки), либо удалить один из уже установленных (кнопка Удалить языки).

При установке пакета операционная система попросит указать путь к нему. Если же вы хотите удалить языковой пакет, то мастер выведет список установленных пакетов.

Для удаления недавно установленного языкового пакета можно воспользоваться программой `lpremove.exe`. Если она запущена без параметров, то создает задание на удаление языковых пакетов. Если же запустить программу с параметром `/c`, то задание будет отменено.

9.4. Установка пакетов обновлений операционной системы

Расположение: `%systemroot%\system32\wusa.exe`.

Пакеты обновлений операционной системы Windows Vista имеют расширение MSU и устанавливаются с помощью программы `wusa.exe`. Вряд ли вам когда-нибудь придется самостоятельно пользоваться этой программой, так как такие же пакеты обновлений можно установить и с помощью двойного щелчка кнопкой мыши на них. В этом случае команда установки записана в параметре `(По умолчанию)` ветви реестра `HKEY_CLASSES_ROOT\Microsoft.System.Update\shell\open\command`.

Однако программа `wusa.exe` имеет несколько параметров, которые по умолчанию не используются при установке с помощью оболочки. К ним относятся такие.

- `/quiet` — выполняется автоматическая установка без задания вопросов установки пользователю. Если необходимо, то после установки будет выполнена автоматическая перезагрузка компьютера.
- `/norestart` — используется вместе с предыдущим параметром и говорит о том, что после автоматической установки не будет выполнена перезагрузка компьютера, даже если это нужно для обновленных компонентов операционной системы.

На этом закончим рассмотрение параметров работы с компонентами операционной системы.

Приложения

- **Приложение 1. Команды rundll32**
- **Приложение 2. Работа с WMI**
- **Приложение 3. Новые программы командной строки**
- **Приложение 4. Использование ActiveX-объектов**

Приложение 1. Команды rundll32

Программа `rundll32.exe` входит в стандартную поставку всех операционных систем семейства Windows и позволяет выполнять различные функции, описанные в библиотеках, драйверах или ActiveX-объектах, как будто они выполняются из программы. Она также входит в состав новой операционной системы Windows Vista, поэтому обзор новой операционной системы, предназначенный для опытных пользователей, никак нельзя назвать законченным, если он не будет содержать описание команд `rundll32.exe`, доступных в Windows Vista.

Многие команды `rundll32.exe` уже были рассмотрены на страницах этой книги. Другие же команды, которые не подошли ни к одной главе, будут описаны в этом приложении.

Синтаксис использования программы `rundll32.exe` следующий: `rundll32.exe <библиотека>, <функция> <параметры>`. При этом очень важно понимать, что название функции, хранящейся в библиотеке, зависит от регистра, которым вы ее написали. Иначе говоря, например, функции `MessageBox` и `messageBox` в понимании программы `rundll32.exe` являются различными функциями, поэтому если в названии функции вы напишете вместо прописной буквы строчную, программа `rundll32.exe` выдаст ошибку. Название же самой программы `rundll32.exe` и название библиотеки можно указывать как строчными, так и прописными символами.

По сравнению с операционной системой Windows XP система Windows Vista поддерживает меньше команд `rundll32.exe`. Это связано с тем, что Windows Vista больше не использует многие библиотеки, доступные в Windows XP.

- `rundll32.exe shell32.dll, SHHelpShortcuts_RunDLL Connect` — вызвать мастер подключения сетевых дисков.
- `rundll32.exe shell32.dll, ShellAboutA` — вызвать окно, отображающее версию операционной системы Windows. Его же можно открыть, выполнив команду `winver.exe`.
- `rundll32.exe IEAKENG.dll, BrowseForFileA` — отображает дерево файловой системы жесткого диска компьютера.
- `rundll32.exe ndfapi.dll, NdfRunDllHelpTopic <html-страница>` — вызывает окно Справка и поддержка на указанной странице. Например, в качестве HTML-страницы можно использовать вызов `mshelp://Windows/?id=33307acf-0698-41ba-b014-ea0a2eb8d0a8`.
- `rundll32.exe shell32.dll, OpenAs_RunDLL "путь и имя файла"` — вызывает окно Выбор программы для открытия данного файла.
- `rundll32.exe shell32.dll, Control_RunDLL Cliconfg.dll` — открывает окно Программа сетевого клиента SQL Server.

- `rundll32.exe shell32.dll, Control_RunDLL Hotplug.dll` — отображает окно удаления съемного устройства.
- `rundll32.exe admparse.dll, CheckDuplicateKeysA "путь и имя файла"` — переписывает содержимое данного файла.
- `rundll32.exe IEAKENG.dll, BToolbar_SaveA "путь к папке"` — создает папку. Если данная папка уже существует, то все ее содержимое будет удалено.
- `rundll32.exe appwiz.cpl, GetProgramsOnline` — запускает браузер Internet Explorer и загружает страницу http://g.msn.com/WMHFUSEN/101724.
- `rundll32.exe shell32.dll, ShellExec_RunDLL "команда"` — выполняет указанную команду.
- `rundll32.exe url.dll, FileProtocolHandler "каталог"` — открывает папку. Если вы не укажете папки, то будет открыта папка вашего профиля.
- `rundll32.exe WININET.dll, RunOnceUrlCache "путь к папке"` — удаляет все файлы, содержащиеся в указанной папке и имеющие такой атрибут, как `FILEATTRIBUTETAGINFORMATION`.
- `rundll32.exe xwizards.dll, ProcessXMLFile "путь и имя XML-файла"` — выполняет XML-файл.
- `rundll32.exe user32.dll, mouse_event` — выполняет нажатие правой кнопки мыши.
- `rundll32.exe user32.dll, SetCursorPos` — устанавливает указатель мыши в правый нижний угол экрана.
- `rundll32.exe dfshim.dll, KillService` — останавливает работу службы фонового обновления `dfsvc.exe`
- `rundll32.exe IERNONCE.dll, RunOnceExProcess` — выполняет команды, описанные в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx` (или в ветви корневого раздела `HKEY_CURRENT_USER`).

Приложение 2. Работа с WMI

Если вы не боитесь таких слов, как «сервер сценариев Windows (WSH)» или «инструментарий управления Windows (WMI)», то вам, возможно, будет интересно узнать о новых классах, свойствах и методах, которые появились в репозитарии CIM операционной системы Windows Vista. Именно поэтому новые классы (а также некоторые из старых) были описаны на протяжении всей этой книги.

Настройка WMI

В этом примечании будут описаны способы работы с репозитарием CIM. Однако, перед тем как начать описание работы с репозитарием, рассмотрим настройки WMI и способы их просмотра.

Использование репозитария CIM

Одним из способов просмотра сведений о настройках WMI является использование класса `Win32_WMISetting`, принадлежащего пространству имен `\\root\cimv2`. Он поддерживает следующие свойства, большинство из которых доступно как для чтения, так и для записи.

- `ASPScriptDefaultNamespace` — определяет пространство имен, которое подразумевается по умолчанию при получении доступа к репозитарию CIM из сценариев, если пространство имен в сценарии не указано. По умолчанию данное свойство содержит значение `root\cimv2`. Данному свойству соответствует параметр реестра строкового типа `Default Namespace`.
- `ASPScriptEnabled` — указывает, разрешено ли использование возможностей WMI в сценариях на страницах ASP. Данному свойству соответствует параметр реестра `REG_DWORD`-типа `Enable for ASP`.
- `AutorecoverMofs` — определяет список MOF-файлов, которые загружены в репозитарий CIM. Также MOF-файлы, описанные в данном свойстве, используются при восстановлении репозитария CIM. Данному свойству соответствует параметр реестра `REG_MULTI_SZ`-типа `Autorecover MOFs`.
- `BackupInterval` — указывает интервал создания резервной копии репозитария CIM. Данному свойству соответствует параметр реестра строкового типа `Backup Interval Threshold`.
- `BackupLastTime` — определяет дату создания резервной копии репозитария CIM.
- `BuildVersion` — указывает номер версии WMI, установленной в операционной системе. Например, в Windows Vista используется WMI версии 6000.16386, а в Windows XP — версии 2600.0000. Данному свойству соответствует параметр строкового типа `Build`.

- DatabaseDirectory — определяет путь к репозитарию CIM. Данному свойству соответствует параметр реестра строкового типа Repository Directory.
- DatabaseMaxSize — указывает максимальный размер репозитария CIM. Данному свойству соответствует параметр реестра REG_DWORD-типа Max DB Size.
- EnableEvents — определяет, разрешена ли подсистема событий WMI. Данному свойству соответствует параметр реестра строкового типа EnableEvents.
- EnableStartupHeapPreallocation — указывает, будет ли куча (часть оперативной памяти, используемая для хранения объектов) выделяться сразу при запуске службы WMI. Данному свойству соответствует параметр реестра REG_DWORD-типа EnableStartupHeapPreallocation.
- HighThresholdOnClientObjects — определяет верхнее пороговое значение очереди объектов от поставщиков. Достижение данного порогового значения приводит к прекращению приема объектов от поставщиков и возвращению поставщикам кода WBEM_E_OUT_OF_MEMORY. Данному свойству соответствует параметр реестра REG_DWORD-типа High Threshold On Client Objects (b).
- HighThresholdOnEvents — указывает верхнее пороговое значение очереди событий от поставщиков. Достижение данного порогового значения приводит к прекращению приема событий от поставщиков и возвращению поставщикам кода WBEM_E_OUT_OF_MEMORY. Данному свойству соответствует параметр реестра REG_DWORD-типа High Threshold On Events (b).
- InstallationDirectory — определяет путь к каталогу, содержащему файлы WMI. Данный каталог хранит файлы службы WMI, MOF-файлы, файлы журнала, репозитарий CIM и основные программы командной строки, предназначенные для работы с репозитарием CIM. Свойству соответствует параметр реестра строкового типа Installation Directory.
- LastStartupHeapPreallocation — указывает размер выделяемой кучи, если свойство EnableStartupHeapPreallocation равно true.
- LoggingDirectory — определяет путь к каталогу, содержащему файлы журналов WMI. Данному свойству соответствует параметр реестра строкового типа Logging Directory.
- LoggingLevel — указывает уровень протоколирования ошибок, который может принимать следующие значения: 0 (отключить протоколирование), 1 (краткое протоколирование ошибок), 2 (полное протоколирование ошибок). Данному свойству соответствует параметр реестра строкового типа Logging.
- LowThresholdOnClientObjects — определяет нижнее пороговое значение очереди объектов от поставщиков, по достижении которого скорость создания объектов замедлится. Данному свойству соответствует параметр реестра REG_DWORD-типа Low Threshold On Client Objects (b).
- LowThresholdOnEvents — указывает нижнее пороговое значение очереди событий от поставщиков, по достижении которого скорость создания объектов замедлится. Данному свойству соответствует параметр реестра REG_DWORD-типа Low Threshold On Events (b).
- MaxLogFileSize — определяет максимальный размер журналов WMI. Данному свойству соответствует параметр реестра строкового типа Log File Max Size.

- MaxWaitOnClientObjects — указывает время в миллисекундах, в течение которого объект может находиться в очереди. Данному свойству соответствует параметр реестра строкового типа Max Wait On Client Objects (ms).
- MaxWaitOnEvents — определяет время в миллисекундах, в течение которого событие может находиться в очереди. Данному свойству соответствует параметр реестра строкового типа Max Wait On Events (ms).
- MofSelfInstallDirectory — указывает путь к каталогу, в который будут помещаться MOF-файлы, предназначенные для автоматического добавления новых поставщиков WMI, свойств и методов. Данному свойству соответствует параметр реестра строкового типа MOF Self-Install Directory.

Использование реестра

В предыдущем разделе мы рассмотрели свойства класса Win32_WMISetting, которые определяют настройки базы данных WMI. При этом при описании каждого свойства также указывался параметр реестра, который изменяется данным свойством. Сейчас же рассмотрим ветви реестра, в которых содержатся описанные выше параметры, а также несколько параметров, значения которых нельзя изменить с помощью свойств класса Win32_WMISetting.

Настройки репозитария. Параметры реестра BUILD, Installation Directory и MOF Self-Install Directory содержатся в ветви HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM.

Настройки сценариев. Параметры реестра Default Namespace, Enable for ASP и MOF Self-Install Directory хранятся в ветви HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Scripting.

В ней также может находиться параметр REG_DWORD-типа Default Impersonation Level. Он определяет используемый по умолчанию (если не указан в сценарии) уровень заимствования прав доступа. По умолчанию значение данного параметра равно 3.

Настройки WMI. Остальные параметры реестра содержатся в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM.

Кроме параметров, данная ветвь реестра хранит вложенный подраздел CIMOM, содержащий сведения о CIM-совместимой базе данных WMI. Данный подраздел включает в себя следующие параметры.

- DefaultRPCStackSize — имеет строковый тип. Он определяет используемый по умолчанию размер буфера для хранения запросов RPC.
- EnablePrivateObjectHeap — этот параметр REG_DWORD-типа указывает, будет ли использоваться куча для хранения объектов от поставщиков.
- EnableObjectValidation — имеет тип REG_DWORD. Если его значение равно 1, то будет выполняться проверка целостности объектов от поставщиков.
- Sink Transmit Buffer Size — этот параметр строкового типа определяет размер буфера, используемого при передаче ответа на асинхронный запрос.

Использование программы winmgmt.exe

Программа `winmgmt.exe`, которая расположена в каталоге `%systemroot%\system32\wbem`, является службой инструментария управления Windows (WMI). При этом она поддерживает набор параметров, с помощью которых можно управлять работой репозитария CIM и WMI в целом.

- `/backup <путь и имя файла с расширением REP>` — выполняет архивирование репозитария CIM.
- `/restore <путь и имя файла с расширением REP>` — восстанавливает содержимое репозитария CIM из указанного файла-архива.
- `/standalonehost <уровень аутентификации процесса svchost.exe>` — перемещает службу инструментария управления Windows в отдельный процесс `svchost.exe`. Если уровень аутентификации не задан, используется уровень `4`.
- `/sharedhost` — перемещает службу инструментария управления Windows в общий процесс `svchost.exe`.
- `/salvagerepository` — проверяет репозитарий CIM на корректность и в случае обнаружения неполадок восстанавливает его на основе стандартных MOF-файлов.
- `/verifyrepository <путь к репозитарию CIM>` — проверяет репозитарий CIM на корректность. Если не указывать путь к репозитарию CIM (или его копии), то будет выполнена проверка текущего репозитария CIM.
- `/resetrepository` — восстанавливает репозитарий CIM к состоянию, в котором он был на момент установки операционной системы.
- `/resyncperf <PID службы WMI>` — заново регистрирует в инструментарии управления Windows системные библиотеки производительности.
- `/clearadap` — удаляет из разделов реестра, принадлежащих службам, все параметры, связанные с инструментарием управления Windows.

Использование классов репозитария CIM

Перед тем как описать способы работы с репозитарием CIM с помощью сервера сценариев Windows, рассмотрим несколько простых способов работы с инструментарием управления Windows, чтобы вы смогли вспомнить, что это такое.

Программа WMIC

В стандартную поставку операционной системы Windows Vista входит программа командной строки `wmic.exe`, расположенная в каталоге `%systemroot%\SYSTEM32\wbem`. С ее помощью можно получить доступ к репозитарию CIM, даже не зная основ работы с инструментарием управления Windows.

Параметры программы

При первом запуске программы выполняется ее установка в системе, после чего будет выведена командная строка `wmic`. Программа `wmic.exe` поддерживает

множество параметров, но мы рассмотрим лишь некоторые из них. Весь же список команд можно просмотреть с помощью команды `wmic /?`.

- `/NAMESPACE:<пространство имен>` — определяет пространство имен, в котором будет выполнен поиск псевдонима.
- `/NODE:<компьютер>` — указывает компьютер, к репозитарию которого будет отправлен запрос WQL.
- `/USER:<пользователь>` — определяет пользователя, от имени которого будет выполнен запрос. Если вы выполняете запрос на локальном компьютере, то указывать пользователя нельзя (можно выполнять запрос только от текущего пользователя).
- `/PASSWORD:<пароль>` — указывает пароль для учетной записи пользователя, от имени которого будет выполняться запрос к репозитарию.
- `/ROLE:<пространство имен>` — определяет пространство имен, содержащее описание доступных псевдонимов. По умолчанию значение данного параметра равно `\\root\cli`.
- `/LOCALE:<язык>` — указывает идентификатор языка, к пространству имен которого будет выполнен запрос.
- `CONTEXT` — параметр указывается без косой черты (и без псевдонима). Он отображает список значений всех параметров, используемых в программе `wmic.exe`.

Доступные в программе псевдонимы

Кроме параметров, программа `wmic.exe` также поддерживает набор псевдонимов (ключевые слова, ассоциированные с конкретным запросом WQL). Список доступных программе псевдонимов можно просмотреть с помощью команды `wmic.exe /?`. Наиболее интересны из них следующие параметры, которые возвращают сведения.

- `BASEBOARD` — о материнской плате, установленной на компьютере: модель, производителя, описание. Эти сведения хранятся в классе `Win32_BaseBoard`.
- `BIOS` — о версии BIOS материнской платы: основную и дополнительную версию, производителя, название, язык, описание, дату установки, указание, является ли данная версия BIOS основной. Эти сведения хранятся в классе `Win32_BIOS`.
- `BOOTCONFIG` — о настройках загрузочного меню компьютера.
- `COMPUTERSYSTEM` — об операционной системе компьютера. Они хранятся в классе `Win32_ComputerSystem` репозитария CIM.
- `GROUP` — о группах учетных записей, зарегистрированных в системе: SID, присвоенный группе, название группы, ее описание. Эти сведения хранятся в классе `Win32_Group`.
- `LOGICALDISK` — о логических дисках компьютера: метке диска, букве, серийном номере, описании, размере, указания, включена ли квота, используется ли программное сжатие. Эти сведения хранятся в классе `Win32_LogicalDisk`.
- `OS` — об операционной системе, установленной на компьютере: системный каталог, версию, пакет обновлений, язык операционной системы, размер виртуаль-

ной памяти, размер оперативной памяти, количество процессоров, количество запущенных в данный момент процессов, регистрационные данные пользователя. Эти сведения хранятся в классе `Win32_OperatingSystem`.

- `PAGEFILESET` — о конфигурации файла подкачки: путь к нему, максимальный размер, используемый в данный момент размер. Эти сведения хранятся в классе `Win32_PageFileSetting`.
- `PARTITION` — о партициях, имеющихся на жестком диске: является ли активной, размер кластера партиции, общее количество блоков, описание партиции. Эти сведения хранятся в классе `Win32_DiskPartition`.
- `PRINTER` — о настройках принтеров, установленных на компьютере: название принтера, производителя, приоритет, номер порта, поддерживаемая бумага. Эти сведения хранятся в классе `Win32_Printer`.
- `PROCESS` — о запущенных на компьютере в данный момент процессах: название процесса, PID, командную строку, вызвавшую процесс, учетную запись, от имени которой работает процесс, размер используемой оперативной памяти, виртуальной памяти. Эти сведения хранятся в классе `Win32_Process`.
- `SHARE` — о папках общего доступа Windows: название, описание, тип. Эти сведения хранятся в классе `Win32_Share`.
- `STARTUP` — обо всех программах, запускаемых вместе с операционной системой, а также о файлах, которые они, в свою очередь, запускают. Эти сведения хранятся в классе `Win32_StartupCommand`.

Таким образом, программа `wmic.exe` имеет следующий синтаксис: `wmic.exe <параметры> <псевдоним>`. Если же вы вошли в оболочку программы, то достаточно указывать только параметры и псевдоним, без названия программы.

Примеры работы с программой

Напоследок рассмотрим несколько примеров работы с данной программой:

- `wmic OS Get DataExecutionPrevention_Available` — показывает, используется ли на данный момент в операционной системе механизм DEP;
- `wmic /OUTPUT:C:\cpu_settings.txt CPU GET /VALUE` — создает на диске `C:\` файл `cpu_settings.txt`, который будет содержать описание процессора, установленного на вашем компьютере;
- `wmic PROCESS WHERE Name="cmd.exe" CALL Terminate` — завершает работу процесса с именем `cmd.exe`;
- `wmic PROCESS CALL Create calc.exe` — запускает процесс `calc.exe`;
- `wmic SERVICE WHERE Name="browser" LIST` — отображает сведения о настройках службы обозревателя компьютеров.

Программа WBEMTEST.exe

Получить доступ к репозитарию CIM можно также с помощью приложения `wbemtest.exe`, имеющего графический интерфейс. Она также расположена в каталоге `%systemroot%\SYSTEM32\wbem`.

Программа `wbemtest.exe` позволяет перечислять, открывать и создавать классы или экземпляры этих классов, а также выполнять WQL-запросы к репозитарию CIM (представляют собой разновидность SQL-запросов) либо методы классов.

Для работы с данной программой необходимо знать названия классов, свойств и методов, реализуемых в этих классах. Названия новых классов и свойств, доступных в операционной системе Windows Vista, а также перечень основных свойств некоторых из уже существовавших в предыдущих операционных системах классов были описаны ранее на страницах данной книги.

Подключаемся к пространству имен

Перед тем как начать работу с программой `wbemtest.exe`, необходимо подключиться к нужному вам пространству имен. Для этого в окне программы нужно нажать кнопку Подключить. После этого перед вами отобразится окно. В этом окне нужно указать пространство имен, к которому выполняется подключение, а также логин пользователя и пароль (если логин пользователя и пароль не указаны, то будет выполнено подключение от имени текущего пользователя).

После того как вы введете необходимые данные, перед вами опять отобразится начальное окно программы, но теперь все ее кнопки будут активны.

Использование запросов WQL для получения экземпляров классов

Обратите внимание на кнопку Запрос основного окна программы `wbemtest.exe`. С помощью данной кнопки можно отобразить окно, позволяющее вводить WQL-запросы к репозитарию CIM и получать экземпляры классов, хранящиеся в нем.

После того как вы введете WQL-запрос, перед вами отобразится окно, содержащее список всех найденных экземпляров, удовлетворяющих введенному вами запросу. Если вы дважды щелкнете кнопкой мыши на каком-нибудь из экземпляров, то перед вами отобразится список всех доступных в этом экземпляре свойств, а также их значения.

Запросы WQL делятся на три типа: запросы данных, запросы схем и запросы событий. На страницах данной книги мы рассмотрим только синтаксис запросов данных. Они предназначены для получения экземпляров класса, а также их ассоциаций.

Самым простым запросом данных является запрос `Select * From <класс>`. С его помощью можно отобразить список всех экземпляров указанного класса, доступных на компьютере. Например, попробуйте ввести запрос для вывода экземпляров класса `Win32_OperatingSystem`.

Если же вам необходимо просмотреть значения не всех свойств класса, а лишь некоторых из них, то можно воспользоваться более конкретным запросом: `Select <список свойств, значения которых нужно вывести> From <класс>`. Например, если вы введете запрос `select SystemDevice, LargeSystemCache, EncryptionLevel from Win32_OperatingSystem`, то сможете просмотреть значения только этих свойств класса.

Можно также воспользоваться запросом вида `select <свойства> from <класс> where <свойство>=<значение>`. Он применяется в том случае, когда нужно отобразить только те экземпляры класса, свойства которых имеют указанные в запросе значения. При этом можно использовать операторы `AND`, `NOT` или `OR`, чтобы указать значения сразу нескольких свойств. Например, `select SystemDevice, EncryptionLevel from Win32_OperatingSystem where Primary="TRUE" AND EncryptionLevel>40`.

Ключевое слово `where` может содержать ключевое слово `__CLASS`. С его помощью можно ограничить вывод WQL-запроса только одним классом. Например, чтобы ограничить список выводимых экземпляров только классом `Win32_Service`, нужно воспользоваться запросом вида `select * from Win32_BaseService where __CLASS=" Win32_Service "`.

Обобщим схему запроса данных WQL: `select <свойства>|* from <класс> [where [__CLASS="класс"] [AND|OR] [<свойство>=<значение>]]`.

Выполнение методов классов

Если же вам нужно выполнить метод, который описан в одном из классов соответствующего пространства имен, то необходимо воспользоваться кнопкой Выполнить метод. После нажатия этой кнопки программа попросит вас ввести название класса, в котором находится нужный вам метод. После того как вы это сделаете, перед вами отобразится список методов данного класса, среди которых вы должны выбрать нужный метод.

Если метод, который вы хотите вызвать, не требует ввода никаких входящих параметров, то после его выбора просто нажмите кнопку Выполнить. В противном случае перед нажатием этой кнопки также нужно нажать кнопку Входные параметры. После этого в появившемся окне Редактор объекта _PARAMETERS нужно дважды щелкнуть кнопкой мыши на каждом параметре, значение которого нужно изменить (вызвав тем самым окно Редактор свойств), потом изменить значение параметра и нажать кнопку Сохранить.

Если метод, который вы выполнили, возвращает какие-либо значения, их можно просмотреть после его выполнения, просто нажав кнопку Выходные параметры.

Сервер сценариев Windows

Теперь рассмотрим несколько простых примеров использования инструментария управления Windows в сервере сценариев WSH.

Первый пример будет очень простым. В нем мы попробуем отредактировать параметр реестра с помощью одного из методов класса WMI. Например, изменим параметр строкового типа `Auto` из ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug` (листинг П2.1).

Листинг П2.1. Вызов методов инструментария управления Windows

```
Set WMIReg = GetObject("winmgmts:{impersonationLevel=impersonate}!root/
Default:StdRegProv")
'если метод возвращает значение, отличное от 0, значит,
'произошла ошибка и изменение параметра не произошло
if WMIReg.SetStringValue (&H80000002,"SOFTWARE\Microsoft\Windows NT\
CurrentVersion\AeDebug","Auto", 0) then MsgBox "Произошла ошибка", vbCritical
```

Рассмотрим данный пример детально.

Моникер

С помощью первой строки примера мы подключаемся к репозитарию CIM и получаем указатель на объект WMI, определенный моникером, являющимся атрибутом метода `GetObject`.

ПРИМЕЧАНИЕ

Моникером называется объект, предназначенный для доступа к другому объекту.

Наиболее простой синтаксис моникера следующий: `Winmgmts::<класс>[.<ключевое свойство>=<значение>]`. С его помощью мы подключаемся к классу или экземпляру класса (если указывается ключевое свойство и значение) пространства имен `root\cimv2` (именно оно используется по умолчанию). В качестве примера можно привести следующий моникер: `winmgmts::Win32_Service.Name="DHCP"`.

Если же вам нужно изменить пространство имен, к которому вы подключаетесь, а также компьютер, то нужно воспользоваться следующим синтаксисом моникера: `Winmgmts:\\[<компьютер>]\<пространство имен>:<класс>[.<ключевое свойство>=<значение>]`. Если вместо названия компьютера поставить точку, то подключение будет выполнено к локальному компьютеру. Например, `winmgmts:\\.\Root\Cimv2:Win32_Service.Name="DHCP"` или `winmgmts://NOUT/Root/Cimv2:Win32_Service.Name="DHCP"`. Заметьте, что в первом случае для указания пространства имен и подключаемого компьютера мы используем символ «\», а во втором случае — символ «/». Эти символы равнозначны.

Уровень заимствования прав

Следующий пример моникера: `Winmgmts:[{impersonationLevel=<уровень заимствования прав>}!]\\[<компьютер>]\<пространство имен>:<класс>[.<ключевое свойство>=<значение>]`. В нем мы используем новое ключевое слово `impersonationLevel`, которое определяет уровень заимствования прав пользователя. Возможны следующие уровни заимствования.

- `Anonymous` — использовать минимальные привилегии.
- `Identify` — запросить привилегии пользователя, если будет нужно. По умолчанию же использовать минимальные привилегии.
- `Impersonate` — использовать привилегии пользователя.

Уровень аутентификации

Еще один пример моникера: `Winmgmts:[{impersonationLevel=<уровень заимствования прав>, AuthenticationLevel=<уровень аутентификации>}!]\\[<компьютер>]\<пространство имен>:<класс>[.<ключевое свойство>=<значение>]`. В нем мы используем ключевое слово `AuthenticationLevel`, которое определяет уровень аутентификации и может принимать следующие значения.

- `Default` — использовать настройки аутентификации Windows. Данный уровень используется по умолчанию.
- `None` — не производить аутентификацию.
- `Connect` — выполнять аутентификацию клиента только при соединении с сервером.
- `Call` — выполнять аутентификацию клиента при получении любого запроса от сервера.
- `Pkt` — проверять все данные, получаемые от клиента.
- `PktIntegrity` — проверять любые данные, переданные как сервером, так и клиентом.
- `PktPrivacy` — проверять любые данные, переданные как сервером, так и клиентом, а также выполнять шифрование аргументов удаленных вызовов процедур.

Привилегии

Еще один пример синтаксиса моникера: `Winmgmts:[{impersonationLevel=<уровень заимствования прав>, AuthenticationLevel=<уровень аутентификации>}, (привилегия, привилегия и т.д.)!]\\[<компьютер>]\<пространство имен>:<класс>[.<ключевое свойство>=<значение>]`. В нем мы указываем дополнительные привилегии (если перед привилегией поставить восклицательный знак, то ее использование будет запрещено). Например, возможны следующие привилегии.

- `Audit` — разрешить создание записей в стандартном журнале Безопасность (`eventvwr.msc`).
- `ChangeNotify` — по умолчанию привилегия установлена. Разрешает не проходить все проверки прав доступа пользователя.
- `CreatePageFile` — позволить создание файла подкачки.
- `CreatePermanent` — разрешить создание постоянного объекта.
- `CreateToken` — позволить создание первичного маркера.
- `Backup` — разрешить выполнение операций архивирования.
- `Debug` — позволить отладку процесса.
- `EnableDelegation` — разрешить делегирование для учетных записей.
- `IncreaseBasePriority` — позволить увеличение приоритета процесса.
- `IncreaseQuota` — разрешить увеличение квоты, назначенной процессу.

- LoadDriver — позволить загрузку и выгрузку драйверов устройств.
- LockMemory — разрешить блокировку страниц памяти.
- MachineAccount — позволить создание привилегированной учетной записи.
- PrimaryToken — разрешить назначение первичного маркера процесса.
- ProfileSingleProcess — позволить сбор информации о профилях для одиночного процесса.
- RemoteShutdown — разрешить выключение удаленного компьютера.
- Restore — позволить операции восстановления.
- Security — повышает подключение к репозитарию до оператора системы безопасности.
- Shutdown — разрешить выключение локального компьютера.
- SyncAgent — позволить синхронизацию данных службы каталогов.
- SystemEnvironment — разрешить изменение энергонезависимой памяти.
- SystemProfile — позволить сбор информации о профилях.
- SystemTime — разрешить изменение системного времени.
- TakeOwnership — позволяет получать права владельца на объект (тем не менее, это не дает полного доступа к объекту).
- Tcb — повышает общие права сценария на работу в системе.
- Undock — разрешить отстыковку портативных компьютеров.

Например, чтобы разрешить выполнение перезагрузки компьютера, нужно использовать моникер `winmgmts:{impersonationLevel = Impersonate, (Shutdown)}!\\.\root\cimv2:Win32_OperatingSystem`.

Вызов методов WMI

С помощью второй строки примера мы вызываем метод класса, позволяющий изменить значение параметра строкового типа. Как правило, каждый метод после своей работы возвращает код выполнения, который определяет либо ошибку, произошедшую при работе метода, либо то, что метод выполнен без ошибок (в этом случае всегда возвращается значение `0`).

Использование WQL-запросов

Еще одним способом работы с репозитарием CIM является выполнение запросов WQL (листинг П2.2).

Листинг П2.2. Использование WQL-запроса

```
'Подключаемся к пространству root\cimv2 репозитария
'указанного компьютера
Set WMIReg = GetObject("winmgmts:{impersonationLevel=impersonate}!//" &
InputBox("Введите название компьютера, к которому будем подключаться (введите точку,
если нужно подключиться к локальному компьютеру).", "Connect...") & "/root/CimV2")
'Выполняем запрос данных WQL, возвращающий все экземпляры
'данного класса
```

```
'После этого отображаем содержимое свойств всех найденных
'экземплров в цикле For Each...Next
Set WMI = WMIReg.ExecQuery ("select * from Win32_Registry")
For Each i in WMI
MsgBox "Подключились к " & i.Name & " : " & i.Status & vbCrLf & "Текущий размер
реестра: " & i.CurrentSize & " Mb" & vbCrLf & "Максимальный размер реестра: " &
i.MaximumSize & " Mb"
Next
```

WQL-запрос к репозитарию CIM выполняется с помощью метода `ExecQuery` объекта `SWbemServices` объектной модели WMI. Заметьте, как именно возвращается результат запроса: в виде массива. Мы же с помощью цикла `for each in` выполняем перечисление каждого из элементов массива.

Редактирование значений свойств

Следующий листинг приводит пример изменения значения свойства экземпляра класса (листинг П2.3).

Листинг П2.3. Запись в свойство инструментария WMI

```
Set WMIReg = GetObject("winmgmts:{impersonationLevel=impersonate}!//" &
InputBox("Введите название компьютера, к которому будем подключаться (введите точку,
если нужно подключиться к локальному компьютеру).", "Connect...") & "/root/CimV2")
Set WMI = WMIReg.ExecQuery ("select * from Win32_Registry")
For Each i in WMI
MsgBox "Подключились к " & i.Name & " : " & i.Status & vbCrLf & "Текущий размер
реестра: " & i.CurrentSize & " Mb" & vbCrLf & "Максимальный размер реестра: " &
i.MaximumSize & " Mb" & vbCrLf & "Желаемый размер реестра: " & i.ProposedSize & " Mb"
Temp = InputBox ("Введите новый желаемый раздел реестра", "Только не перестарайтесь")

'Конечно, размер реестра в виде строки — это ваше дело,
'но мы такие значения все-таки отфильтруем
if NOT IsNumeric(Temp) then WScript.Quit
if Temp = "" then WScript.Quit

'Следующие две строки записывают в свойство, обратите на них внимание
i.ProposedSize = temp
i.Put_
MsgBox "Подключились к " & i.Name & " : " & i.Status & vbCrLf & "Текущий размер
реестра: " & i.CurrentSize & " Mb" & vbCrLf & "Максимальный размер реестра: " &
i.MaximumSize & " Mb" & vbCrLf & "Желаемый размер реестра: " & i.ProposedSize & " Mb"
Next
```

Обратите внимание, что после записи в свойство с помощью строки вида `<объект>.<свойство>=<значение>` необходимо использовать метод `Put_` данного объекта. С его помощью новое значение сохраняется в репозитарии CIM (если его не использовать, то свойство будет изменяться только на момент работы сценария, после чего опять примет свое исходное значение).

Приложение 3. Новые программы командной строки

Данное приложение содержит перечень всех программ командной строки, впервые появившихся в операционной системе Windows Vista (точнее, тех, которых не было в операционной системе Windows XP, хотя, возможно, они уже существовали в Windows Server 2003 или как отдельные программы, которые можно скачать с сайта Microsoft).

В приложении не описаны стандартные команды командной строки `cmd.exe`, которые являются ее частью, а не отдельными программами. Например, к таким командам относятся следующие.

- `CHCP <кодовая страница>` — изменяет кодовую страницу, используемую командной строкой. Если не указывать номер кодовой страницы, то отобразится номер текущей кодовой страницы.
- `DATE` — отображает текущую и предлагает ввести новую дату.
- `PATH <каталог;каталог…>` — позволяет указать каталоги, исполняемые файлы из которых можно выполнять из окна Запуск программы, не указывая при этом путь к файлу. Если в данной команде не указать каталог, то отобразится текущий список каталогов.
- `PROMPT <строка>` — дает возможность изменить приглашительную строку, отображаемую в `cmd.exe`. При этом вы можете указать как произвольный текст, так и, если использовать специальные символы, различные переменные. Список возможных переменных можно просмотреть, введя команду `prompt /?`. По умолчанию используется приглашительная строка, отображающая путь к текущему каталогу.
- `SET <переменная>=<значение>` — позволяет изменить значения переменных среды.
- `TIME` — отображает текущее и предлагает ввести новое время.
- `VER` — выводит версию операционной системы.
- `VOL <буква диска>` — отображает метку диска и серийный номер.
- `PAUSE` — приостанавливает работу командной строки `cmd.exe`.

Большинство новых программ Windows Vista уже были описаны в предыдущих главах данной книги, поэтому здесь их описывать не будем. Это такие программы, как: `auditpol.exe`, `icacls.exe`, `wbadmin.exe`, `where.exe`, `bitsadmin.exe`, `msfeedssync.exe`, `netcfg.exe`, `query.exe`, `quser.exe`, `RpcPing.exe`, `winrm.exe`, `winrs.exe`, `certreq.exe`, `certutil.exe`, `fveupdate.exe`,

TpmInit.exe, ocsetup.exe, PkgMgr.exe, wusa.exe, wevtutil.exe, WinSAT.exe, takeown.exe.

Описание остальных программ, о которых в книге еще не упоминалось, также будет включать в себя примеры работы с параметрами этих программ командной строки.

Работа с файлами

forfiles.exe

Данная программа предназначена для обработки файлов, хранящихся в одном каталоге, и позволяет выполнить определенную команду для этих файлов. Основной синтаксис данной программы следующий: forfiles /p <путь к каталогу> /m <маска файлов> /c <команда>. При этом в значении параметра /c можно использовать следующие константы программы.

- @file — при выполнении команды данная константа заменяется именем текущего файла, удовлетворяющего указанной в параметре /m маске.
- @fname — константа заменяется именем текущего файла (но без расширения), удовлетворяющего указанной в параметре /m маске.
- @ext — константа заменяется расширением текущего файла, удовлетворяющего указанной в параметре /m маске.
- @path — при выполнении команды данная константа заменяется полным путем к текущему файлу, удовлетворяющему указанной в параметре /m маске.
- @relpath — константа заменяется относительным путем к текущему файлу, удовлетворяющему указанной в параметре /m маске.
- @isdir — при выполнении команды данная константа заменяется значением true, если текущий, удовлетворяющий маске, файл является каталогом. В противном случае константа заменяется значением false.
- @fsize — константа заменяется размером текущего файла, удовлетворяющего указанной в параметре /m маске.
- @fdate — константа заменяется датой последнего изменения текущего файла, удовлетворяющего указанной в параметре /m маске.
- @ftime — при выполнении команды данная константа заменяется временем последнего изменения текущего файла, удовлетворяющего указанной в параметре /m маске.

Например, чтобы открыть в Блокноте все файлы с расширением VBS, расположенные в каталоге %systemroot%\system32, нужно воспользоваться следующей командой: forfiles /p c:\windows\system32 /m *.vbs /C "notepad.exe /c @path". Заметьте, что в значении параметра /C после названия программы notepad.exe и перед константой идет параметр /c. Если его не указать, то просто будет открыта программа notepad.exe, а не удовлетворяющие маске файлы в ней. Параметр /c нужно указывать и для других программ, если константы являются их аргументами.

В программе forfiles.exe также можно использовать параметр /D. Его значением должна быть дата в формате dd.MM.yyyy, перед которой может находиться знак + или –.

Если перед данной датой стоит знак +, то команда из параметра /C будет применяться для всех файлов, дата создания которых больше, чем указано в параметре /D. Если же перед датой стоит знак –, то команда будет применяться для всех файлов с датой создания меньше, чем дата параметра /D.

О других параметрах данной программы вы можете узнать, введя в командной строке команду forfiles /?.

Robocopy.exe

Данная программа предназначена для выполнения копирования одного или множества файлов, расположенных в определенном каталоге и его подкаталогах. При этом каталоги могут находиться как на локальном компьютере, так и на удаленном.

После копирования программа отображает таблицу, описывающую каждый скопированный файл: имя файла, процент копирования, размер файла. Она также строит таблицу, отображающую количество скопированных или пропущенных файлов, папок, байт, а также время копирования.

Основной синтаксис программы следующий: ROBOCOPY <каталог-источник> <каталог назначения> <список копируемых файлов> <параметры>. Если список файлов не указан, то будет выполнено копирование всех файлов (по умолчанию установлена маска файлов *.*). Можно использовать следующие параметры.

Копирование файлов и каталогов

Чтобы копировать все файлы и каталоги, включая пустые файлы, нужно использовать параметр /E. Если же пустые каталоги копировать не нужно, то необходимо указать параметр /S. Можно также указать параметр /LEN:<уровень>, чтобы определить максимальный уровень вложения папок, содержимое которого будет копироваться. Параметр /LEN:<уровень> должен использоваться с одним из предыдущих параметров, иначе копирование будет выполняться только в указанном каталоге, но не в каталогах, вложенных в него.

Например, для копирования файлов можно воспользоваться командой robocopy d:\windows c:\users\1\desktop\testing *as* /S /LEV:3, которая будет просматривать содержимое каталога d:\windows вплоть до третьего уровня вложения папок.

Копирование только файлов

Чтобы копировать только файлы, которые не открыты в монопольном режиме другими программами, нужно воспользоваться параметром/Z. Можно также воспользоваться параметром /B, чтобы выполнялось копирование даже тех файлов, которые открыты в монопольном режиме (теневое копирование). Теневое копирование проходит дольше, чем обычное.

Кроме того, можно использовать комбинацию данных параметров (/ZB), чтобы теневое копирование применялось только к тем файлам, доступ к которым при нормальном копировании был заблокирован.

Можно также указать параметр /EFSRAW, чтобы выполнялось копирование в режиме EFS RAW всех зашифрованных с помощью EFS файлов.

Определение копируемых сведений

Следующим набором параметров, которые можно указывать в программе, являются те, которые указывают атрибуты и метаданные файлов, копируемые от файлов и каталогов источников. Например, с помощью параметра /COPY:<флаги> можно указать флаги копируемой у файлов источника информации (также можно использовать параметр /DCOPY:<флаги>, чтобы указать флаги для копируемых каталогов). По умолчанию значение данного параметра равно DAT. Существуют следующие флаги, позволяющие копировать:

- D — содержимое файлов;
- A — атрибуты файлов;
- T — временные метки файлов;
- S — информацию об ACL-файла;
- O — информацию о владельце файла;
- U — сведения аудита для файла.

Можно также указать один из следующих параметров, которые заменяют собой параметр /COPY:<флаги> с его флагами.

- /SEC — заменяет собой параметр /COPY:DATS.
- /COPYALL — заменяет собой параметр /COPY:DATSOU.
- /NOCOPY — не копировать информацию о файлах. В этом случае не будет скопировано ни одного файла, однако в командной строке будет построено дерево каталогов и файлов каталога-источника.

Можно самостоятельно указать атрибуты, которые будут добавляться к копируемым файлам или удаляться из них. Для этого применяются соответственно команды /A+:<атрибуты> и /A-:<атрибуты>. В качестве атрибутов могут указываться стандартные флаги атрибутов, применяемые к программе attrib.exe.

- R — только чтение.
- A — архивный.
- S — системный.
- H — скрытый.
- C — сжимать файл. Не может устанавливаться вместе с атрибутом E.
- E — шифровать файл. Не может устанавливаться вместе с атрибутом C.

Определение копируемых файлов

Можно также указать параметры, определяющие файлы, которые будут копироваться. Например, чтобы указать копирование файлов, имеющих только определенные атрибуты, нужно воспользоваться одним из следующих параметров.

- /A — копировать только файлы с установленным атрибутом Архивный.
- /M — копировать только файлы с установленным атрибутом Архивный, после чего снимать данный атрибут.
- /IA:<атрибуты> — копировать только файлы с указанными атрибутами.
- /XA:<атрибуты> — копировать только файлы, не имеющие данных атрибутов.
- /XF <файлы> — не копировать файлы с указанными именами.
- /XD <каталоги> — не копировать каталоги с указанными именами.
- /MAX:<размер в байтах> — не копировать файлы, размер которых больше, чем указан в параметре.
- /MIN:<размер в байтах> — не копировать файлы, размер которых меньше, чем указан в параметре.
- /MAXLAD:<время последнего доступа> — не копировать файлы, время последнего доступа к которым больше, чем указано в атрибуте. Время можно указывать в днях (не больше, чем 1900) или в формате даты: yyyymmdd.
- /MINLAD:<время последнего доступа> — не копировать файлы, время последнего доступа к которым меньше, чем указано в атрибуте. Время можно указывать как в днях, так и в виде даты.
- /MAXAGE:<время создания> — не копировать файлы, время создания которых больше, чем указано в атрибуте. Время можно указывать как в днях, так и в виде даты.
- /MINAGE:<время создания> — не копировать файлы, время создания которых меньше, чем указано в атрибуте. Время можно указывать как в днях, так и в виде даты.

Дополнительные атрибуты

Можно также указывать следующие специфические атрибуты.

- /MOV — вместо копирования перемещать файлы.
- /MOVE — вместо копирования перемещать как файлы, так и каталоги.
- /CREATE — в каталоге назначения создает только дерево каталога-источника: содержащиеся в нем папки, а также все файлы, однако их размер будет равен нулю.
- /MON:<количество минут> — копирует файлы в режиме мониторинга. Иначе говоря, программа через указанное количество минут проверяет содержимое каталога-источника и, если находит в нем новые файлы, копирует их в каталог назначения.

Об остальных параметрах программы вы сможете узнать, если введете команду `robocopy /?`.

Работа в сети

iscsicli.exe

Управляет работой клиента iSCSI и позволяет ему подключиться к серверу. Для просмотра описания параметров программы введите команду `iscsi /?`.

waitfor.exe

Позволяет отправить сигнал всем компьютерам сети или только одному из компьютеров. Перед отправкой сигнала на удаленных компьютерах нужно запустить программу `waitfor.exe` в режиме ожидания.

Синтаксис данной программы следующий:

- `waitfor /S <удаленный компьютер> /U <пользователь> /P <пароль> /SI <сигнал>` — немедленно отправляет сигнал, указанный в команде, удаленному компьютеру;
- `waitfor <сигнал> /T <количество секунд ожидания>` — запускает программу `waitfor.exe` в режиме ожидания получения сигнала (как только программа получит сигнал, переданный с помощью описанной выше команды, она завершит свою работу, отобразив сообщение о том, что сигнал получен).

whoami.exe

Выводит сведения об определенном пользователе компьютера. Если вы выполните программу без параметров, то отобразится имя компьютера и ваше имя. Можно также ввести команду `whoami /?`, чтобы просмотреть описание параметров данной программы.

Рассмотрим некоторые возможности программы.

- `Whoami /user` — выводит список работающих в данный момент пользователей. В списке отображается имя компьютера, имя пользователя и его SID.
- `Whoami /groups` — отображает список групп, имеющихся на данном компьютере, а также их SID, тип группы, указания, разрешена ли по умолчанию и разрешена ли в данный момент.
- `Whoami /priv` — выводит список возможных привилегий, их описание и указание, установлены ли они для текущего пользователя.
- `Whoami /all` — отображает список пользователей, групп и возможных привилегий.
- `Whoami /logonid` — выводит SID текущего пользователя.
- `Whoami /fqdn` — отображает имя пользователя в формате FQDN.
- `Whoami /upn` — выводит имя пользователя в формате UPN.

WSManHTTPConfig.exe

Данная программа имеет три параметра:

- `Install` — создает параметр `REG_BINARY`-типа `http://+:80/wsman/` в ветви `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HTTP\Parameters\UrlAclInfo`;
- `Uninstall` — удаляет параметр `REG_BINARY`-типа `http://+:80/wsman/` из ветви `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HTTP\Parameters\UrlAclInfo`;
- `Quickconfig` — выполняет быструю настройку.

Работа со сценариями

choice.exe

Эта программа может применяться в сценариях для отображения сообщения выбора определенного действия. Рассмотрим ее возможности на примерах.

- `Choice /M "Select Y for start script. Select N for load script. Select C for exit" /C YNC` — в командной строке отображает строку, определенную в параметре `/M`. После нее идет список клавиш, которые можно нажать, определенный параметром `/C`. Пользователь должен нажать одну из возможных клавиш, чтобы программа `choice.exe` завершила свою работу. При завершении работы программа возвращает нажатую пользователем клавишу в переменную `ERRORLEVEL`. При этом если пользователь нажал первую клавишу набора, то значение этой переменной будет равно `1`, если нажал вторую клавишу набора, то будет равно `2`, и т. д.

  Если пользователь нажмет клавишу, которая не определена в параметре `/C`, то прозвучит звуковой сигнал. В этом случае работа программы `choice.exe` завершена не будет.

- `Choice /M "Select Y for start script. Select C for exit" /C YC /T 3 /D Y` — в командной строке выводит строку, определенную в параметре `/M`. После нее идет список клавиш, которые можно нажать, определенный параметром `/C`. Если пользователь не сделает выбор в течение количества секунд, определенного параметром `/T`, то программа `choice.exe` завершит свою работу, вернув символ, определенный в параметре `/D`, в переменную `ERRORLEVEL` (точнее, вернув не символ, а его расположение в наборе, определенном параметром `/C`).

  Если пользователь нажмет клавишу, которая не определена в параметре `/C`, то прозвучит звуковой сигнал. В этом случае работа программы `choice.exe` завершена не будет.

- `Choice /M "Select button "S" for start script. Select button "E" for exit" /C SE /N` —в командной строке отображает строку, определенную в параметре `/M`. После этой строки не будет идти список клавиш, которые можно нажать. В остальном работа данной команды аналогична предыдущим рассмотренным нами командам.

timeout.exe

Данная программа предназначена для работы в сценариях и позволяет указать время ожидания определенного события. Синтаксис данной команды следующий: `timeout /T <количество секунд>`. После вызова команды на экране командного процессора отобразится строка обратного отсчета. После окончания количества указанных в команде секунд или после нажатия пользователем любой клавиши работа программы `timeout.exe` будет завершена.

Можно также запретить завершение работы программы после нажатия пользователем любой клавиши. Для этого при запуске программы нужно указать параметр `/NOBREAK`.

Другие программы

clip.exe

С помощью данной команды можно поместить содержимое файла или вывод определенной команды в буфер обмена операционной системы Windows Vista. Например, с помощью команды `diskraid /? | clip` можно поместить описание новой программы операционной системы `diskraid.exe` в буфер обмена Windows, а с помощью команды `clip < "путь к файлу и его имя"` можно поместить в буфер обмена содержимое указанного файла.

cmdkey.exe

Программа позволяет управлять хранилищем паролей пользователя. Примером ее использования являются следующие команды.

- `Cmdkey /list` — выводит список всех хранимых пользователем паролей. Данные пароли ему больше не нужно будет вводить при аутентификации — операционная система сама будет их предоставлять требующим аутентификации программам.
- `Cmdkey /add:<адрес компьютера> /user:<логин> /pass:<пароль>` — добавляет к хранилищу пользовательских паролей новый пароль для указанного удаленного компьютера.
- `Cmdkey /delete:<адрес компьютера>` — удаляет пароль для подключения к данному компьютеру.
- `Cmdkey /delete /ras` — удаляет пароли для удаленного подключения через модем.

Данным хранилищем можно управлять и с помощью окна Сохранение имен пользователей и паролей. Чтобы вызвать его, достаточно запустить программу `netplwiz.exe`, перейти на вкладку Дополнительно и нажать кнопку Управление паролями.

ПРИМЕЧАНИЕ

Окно Сохранение имен пользователей и паролей можно вызвать и с помощью команды rundll32.exe KEYMGR.dll, KRShowKeyMgr или команды rundll32.exe shell32.dll, Control_RunDLL Keymgr.dll.

diskraid.exe

Если на вашем компьютере установлен RAID-массив, то для управления им вы можете воспользоваться новой программой `diskraid.exe`. Для ее запуска необходимо, чтобы в операционной системе был зарегистрирован провайдер VDS.

dispdiag.exe

Эта программа имеет несколько возможностей, которые могут быть полезны пользователям. Если запустить программу `dispdiag.exe` без параметров, то будет создан файл дампа в каталоге `%userprofile%\AppData\Local\Temp`. Можно также запустить программу с параметром `-testacpi`. После этого будет запущен режим интерпретации клавиш: когда вы будет нажимать клавиши, на экране будет отображаться нажатая клавиша, а также ее код и скан-код. Чтобы выйти из этого режима, достаточно нажать клавишу Esc.

gpscript.exe

Регистрирует сценарии для автоматического запуска при входе или выходе пользователя (или всех пользователей) из системы в GPO. Для этого применяются следующие параметры программы: `/RefreshSystemParam`, `/Shutdown`, `/Startup`, `/Logoff`, `/Logon`.

setx.exe

Позволяет изменять состояние переменных окружения локального или удаленного компьютера. Фактически данная программа изменяет или создает параметры ветви реестра `HKEY_CURRENT_USER\Environment` (для пользовательских переменных окружения) или для системных переменных окружения параметры в ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment`.

ПРИМЕЧАНИЕ

Список переменных окружения компьютера можно просмотреть с помощью свойств стандартного класса Win32_Environment, принадлежащего пространству имен \\root\cimv2. Он поддерживает следующие свойства: Name (ключевое свойство, определяющее название переменной окружения), SystemVariable (указывает, является ли данная переменная окружения системной), UserName (ключевое свойство, определяющее компьютер и пользователя, создавшего переменную окружения), VariableValue (указывает значение переменной окружения).

Для просмотра описания всех возможностей данной программы введите команду `setx.exe`. Мы же рассмотрим только основные способы ее использования.

- `Setx MACHINE vista` — создает на локальном компьютере пользовательскую переменную `MACHINE`, имеющую значение `vista`.
- `Setx MACHINE vista /M` — создает на локальном компьютере системную переменную `MACHINE`, имеющую значение `vista`.

- `Setx /S vista /U administrator /P 1 MACHINE vista /M` — от имени пользователя Администратор, имеющего пароль 1, создает на удаленном компьютере vista системную переменную `MACHINE`, имеющую значение `vista`.
- `Setx MACHINE /K "HKEY_CURRENT_USER\Control Panel\Desktop\Wallpaper" /M` — создает на локальном компьютере системную переменную `MACHINE`, значение которой равно значению параметра `Wallpaper` ветви реестра `HKEY_CURRENT_USER\Control Panel\Desktop`.
- `Setx MACHINE /F system.ini /A 3,12 /M` — создает на локальном компьютере системную переменную `MACHINE`, значение которой нужно взять из файла `system.ini`. В нем нужное значение расположено на третьей строке, начиная с 12 столбца.

SLsvc.exe

Представляет собой исполняемый файл службы Лицензирование программного обеспечения. Этот файл поддерживает два параметра: `-Install` и `-Delete`. С их помощью можно соответственно установить и удалить данную службу.

sxstrace.exe

Программа предназначена для настройки трассировки компонента операционной системы WinSxS, содержащего сведения обо всех установленных в системе программах.

Синтаксис данной программы, используемый для запуска трассировки, следующий: `sxstrace trace -logfile:<имя файла с расширением ETL> <параметры>`. Можно использовать следующие параметры программы.

- `-nostop` — не завершать процесс трассировки работы WinSxS.
- `-verbose` — этот параметр недокументирован. Он позволяет указать запись в файл трассировки подробных сведений о работе WinSxS.

После запуска процесса трассировки необходимо нажать клавишу Enter, чтобы процесс трассировки был завершен.

Данной программой можно воспользоваться и для фильтрации файла трассировки и его преобразования в удобочитаемый формат. Для этого применяется следующий синтаксис: `sxstrace Parse -logfile:<имя файла с расширением ETL> <параметры>`:

- `-outfile:<дополнительный файл>` — указывает путь к текстовому файлу, в который будут помещаться сведения о трассировке компонента WinSxS, представленные в удобочитаемом формате;
- `-filter:<имя приложения>` — позволяет указать программу, сведения о которой будут заноситься в файл, определенный в параметре `-outfile: <дополнительный файл>`.

Чтобы остановить трассировку, нужно воспользоваться командой `sxstrace stoptrace`.

tssetup.exe

При использовании параметров `/Install:IIS` и `/Remove:IIS` программа позволяет установить или удалить сервер IIS.

wecutil.exe

Позволяет управлять подписками на события, создаваемыми с помощью диспетчера Baseboard Management Controller или службы Журнал событий Windows. Для работы данной программы необходимо, чтобы служба Сборщик событий Windows была запущена. Описание всех параметров программы можно просмотреть, введя команду `wecutil.exe /?`. Вот некоторые возможности данной программы.

- `wecutil.exe es` — отображает список всех существующих в данный момент подписок на события.
- `wecutil.exe gs` — выводит информацию о подписке.
- `wecutil.exe ss <имя подписки> <параметры>` — изменяет параметры подписки. Список параметров можно просмотреть, введя команду `wecutil.exe ss -?`.
- `wecutil.exe cs <файл конфигурации подписки> /cun:<имя пользователя> /cup:<пароль>` — создает новую подписку на основе конфигурационного файла, указанного в команде. Пример конфигурационного файла можно просмотреть, введя команду `wecutil.exe cs -?`.
- `wecutil.exe ds <идентификатор подписки>` — удаляет указанную подписку.
- `wecutil.exe qc` — выполняет следующие шаги настройки работы с подписками: включает канал ForwardedEvents, устанавливает запуск службы Сборщик событий Windows в автоматический режим и запускает данную службу.

wisptis.exe

Устанавливает значения параметров ветви `HKEY_CURRENT_USER\Software\Microsoft\Wisp`, предназначенных для настройки пера при использовании планшетного ПК.

Приложение 4. Использование ActiveX-объектов

История развития ActiveX-объектов начинается еще в 1991 году. Именно тогда появилась такая технология как OLE. Она представляет собой специальные объекты, предназначенные для выполнения операций связывания и внедрения. Уже в 1993 году появилась вторая версия объектов OLE, которая вобрала в себя понятия нескольких технологий, основанных на модели COM (модель компонентного объекта, предназначенная для создания и редактирования компонентных объектов). Особенностью модели COM является независимость COM-объектов от используемого в их создании языка программирования. Например, если раньше какой-то класс был создан с помощью языка C++, то для него приходилось писать дополнительные классы на этом же языке. COM-объект же преобразуется в промежуточный бай-код, не зависящий от языка программирования, на котором был изначально написан COM-объект. Второй же особенностью COM-объектов является то, что они будут одинаково работать, независимо от того, находятся они на локальном компьютере или на удаленном. Все эти особенности COM-объектов переняли и OLE-объекты второй версии.

Через три года, в 1996 году, на свет появилась технология ActiveX. ActiveX-объекты представляют собой полностью скомпилированные программы, которые не могут быть запущены непосредственно пользователем, но могут запускаться браузером Internet Explorer, самой операционной системой или любой другой программой. Несмотря на то что корпорация Microsoft позиционирует ActiveX-объекты как совершенно новую технологию, они являются развитием OLE-объектов и переняли от них основные функции и возможности. Каждый ActiveX-объект должен содержать подпись своего создателя, которая производится одним из центров сертификации и гарантирует, что данный ActiveX-объект не выполняет никаких вредоносных или подозрительных действий.

Каждый ActiveX-объект имеет уникальный идентификатор, называемый CLSID-номером, который позволяет идентифицировать этот ActiveX-объект среди других. CLSID-номера ActiveX-объектов строятся на основе даты создания объекта, случайного числа и конфигурации компьютера. Эти имена состоят из 32 чисел в шестнадцатеричной системе счисления. Первые восемь чисел генерируются случайным образом. Следующие четыре числа создаются на основе текущей даты и времени. Остальные числа генерируются на основе конфигурации компьютера.

Все ActiveX-объекты, чтобы ими можно было пользоваться, должны быть описаны в дочернем подразделе ветви реестра `HKEY_CLASSES_ROOT\CLSID`. Данный подраздел реестра включает в себя набор подразделов, названных в честь CLSID-номеров ActiveX-объектов. В этих подразделах как раз и описываются настройки конкретных ActiveX-объектов.

Но для чего же используются ActiveX-объекты? В операционной системе Windows Vista с помощью ActiveX-объектов можно создать следующее: специальную вкладку

окна Свойства файлов определенного расширения, специальную команду контекстного меню файлов определенного расширения или различных элементов операционной системы Windows, специальный значок с расширенными возможностями настройки, надстройки для операционной системы или сторонних программ и т. д. В контексте данной книги мы сконцентрируемся на описании стандартных ActiveX-объектов операционной системы и на их использовании и только поверхностно рассмотрим создание простых ActiveX-объектов, не требующих знания языков программирования.

Структура подразделов реестра, определяющих ActiveX-объекты

Но перед тем как начать описание существующих ActiveX-объектов, необходимо хотя бы поверхностно знать структуру подразделов реестра, определяющих ActiveX-объекты и параметры, хранящиеся в них.

Параметры подраздела ActiveX-объекта

Сведения обо всех ActiveX-объектах, зарегистрированных в операционной системе, содержатся в ветви реестра `HKEY_CLASSES_ROOT\CLSID`. Каждый подраздел данной ветви определяет настройки одного ActiveX-объекта. Подраздел назван в честь CLSID-номера ActiveX-объекта. Подраздел реестра `HKEY_CLASSES_ROOT\CLSID\{CLSID-номер ActiveX-объекта}` может включать в себя следующие параметры.

- `(По умолчанию)` — определяет название ActiveX-объекта. Значение данного параметра может использоваться и в качестве названия значка, если, конечно, ActiveX-объект создает значок.
- `AppID` — этот параметр строкового типа определяет CLSID-номер COM-приложения, которое использует данный ActiveX-объект.
- `InfoTip` — параметр имеет строковый тип и определяет подсказку, отображаемую при удержании указателя мыши над значком ActiveX-объекта.
- `LocalizedString` — этот параметр типа `REG_EXPAND_SZ` определяет название значка, создаваемого ActiveX-объектом. Значение этого параметра переопределяет значение параметра `(По умолчанию)` ветви ActiveX-объекта.

Некоторые подразделы, которые могут находиться в подразделе ActiveX-объекта

В подразделе ActiveX-объекта могут также находиться дочерние подразделы.

Подраздел DefaultIcon

Параметр `(По умолчанию)` данного подраздела позволяет указать путь к файлу изображения, которое будет использоваться в качестве значка ActiveX-объекта (если ActiveX-объект создает значок).

Подраздел shell

Данный подраздел определяет команды контекстного меню соответствующего ActiveX-объекта. Параметр `(По умолчанию)` данного подраздела может содер-

жать либо название команды, которая будет выполняться при двойном щелчке кнопкой мыши на значке ActiveX-объекта, либо перечисление последовательности всех команд через запятую. В этом случае определяется расположение команд контекстного меню.

Подраздел `shell` включает в себя дочерние подразделы, каждый из которых определяет название одного элемента контекстного меню. Параметр `(По умолчанию)` этих подразделов определяет название команды, отображаемое в контекстном меню значка ActiveX-объекта. Если же параметр `(По умолчанию)` подраздела будет пуст, то именно название подраздела и будет отображаться в контекстном меню значка ActiveX-объекта.

И, наконец-то, в подразделе названия элемента контекстного меню должен содержаться подраздел `command`, параметр `(По умолчанию)` которого как раз и содержит команду, выполняющуюся при выборе соответствующего элемента контекстного меню.

Подраздел shellEx

Кроме `shell`, в подразделе ActiveX-объекта может находиться еще один подраздел, содержимое которого влияет на контекстное меню значка ActiveX-объекта — подраздел `shellex`. Он включате в себя дополнительные команды контекстного меню, которые при своей работе вызывают другие ActiveX-объеты.

Подраздел `shellex` должен содержать другие подразделы, которые, в свою очередь, должны включать в себя подразделы с названием CLSID-номера ActiveX-объекта, вызываемого с помощью соответствующей команды контекстного меню. В зависимости от названия подраздела, являющегося дочерним по отношению к подразделу `shellex`, изменяется и результат выполнения ActiveX-объекта. Далее описаны основные подразделы, дочерние к подразделу `shellex`.

- `IconHandler` — определяет собственный обработчик значка для ActiveX-объекта. Например, так можно использовать рисунок, содержащийся в файле, как значок для этого файла.
- `PropertySheetHandlers` — указывает новую вкладку окна **Свойства** данного ActiveX-объекта или файла.
- `ContextMenuHandlers` — определяет новую команду контекстного меню значка ActiveX-объекта или файла.

Добавление вкладок к окну Свойства

Как вы уже знаете, сведения об этих ActiveX-объектах, добавляющих вкладки к окну **Свойства**, должны содержаться в ветви реестра `HKEY_CLASSES_ROOT\CLSID\{CLSID-номер ActiveX-объекта}\shellex\PropertySheetHandlers` (или, если нужно добавить вкладку к окну **Свойства** для файла стандартного расширения, в ветви реестра `HKEY_CLASSES_ROOT\<идентификатор файла>\shellex\PropertySheetHandlers`).

Стандартные ActiveX-объекты

Теперь рассмотрим стандартные ActiveX-объекты операционной системы Windows Vista, которые добавляют новые вкладки к окну Свойства файлов или значков ActiveX-объектов.

- {00020D75-0000-0000-C000-000000000046} — при открытии окна Свойства отображается дополнительное окно настройки почты, с помощью которого можно добавить новую конфигурацию почты либо выбрать из списка уже созданных ранее. По умолчанию данная вкладка добавлена к ActiveX-объекту {00020D75-0000-0000-C000-000000000046}.
- {2206CDB2-19C1-11D1-89E0-00C04FD7A829} — добавляет вкладки Подключение, Поставщик данных, Дополнительно и Все окна Свойства. По умолчанию данная вкладка добавлена к файлам с расширением UDL.
- {3FC0B520-68A9-11D0-8D77-00C04FD70822} — добавляет вкладку Рабочий стол окна Свойства.
- {42071712-76d4-11d1-8b24-00a0c9068ff3} — добавляет вкладку Адаптер окна Свойства.
- {42071713-76d4-11d1-8b24-00a0c9068ff3} — добавляет вкладку Монитор окна Свойства.
- {596AB062-B4D2-4215-9F74-E9109B0A8153} — добавляет вкладку Предыдущие версии окна Свойства. По умолчанию вкладка Previous Version добавляется к файлам всех типов расширений с помощью ветви реестра HKEY_CLASSES_ROOT\AllFilesystemObjects\shellex\PropertySheetHandlers.
- {5F5295E0-429F-1069-A2E2-08002B30309D} — добавляет вкладки Общие (отображает сведения о файловой системе), Сервис (содержит кнопки для выполнения архивации данных либо проверки и дефрагментации диска), Оборудование (содержит список всех установленных в данный момент на компьютер жестких дисков и устройств записи данных) окна Свойства. По умолчанию данные вкладки добавляются ко всем значкам разделов диска.

  Например, если добавить данные вкладки к каталогам операционной системы, то всегда можно просмотреть сведения о занятом и свободном пространстве на диске, на котором расположена соответствующая папка.
- {60254CA5-953B-11CF-8C96-00AA00B8708C} — добавляет вкладку Сценарий окна Свойства. С помощью данной вкладки можно настроить параметры выполнения сценариев WSH. По умолчанию данная вкладка добавлена к файлам с расширением JSE, JS, VBE, VBS, WSF, WSH.
- {645FF040-5081-101B-9F08-00AA002F954E} — добавляет вкладку Общие окна Свойства. С помощью данной вкладки можно изменить параметры настройки работы Корзины на разных разделах диска операционной системы. По умолчанию данная вкладка добавлена к ActiveX-объекту {645FF040-5081-101B-9F08-00AA002F954E}.
- {6D5313C0-8C62-11D1-B2CD-006097DF8C11} — добавляет вкладки Общие, Вид, Поиск окна Свойства. Фактически это те же вкладки с теми же возможнос-

тями, что и отображаемые в окне Свойства папки, которое можно открыть с помощью команды Свойства папок и файлов из меню Упорядочить любого каталога.

- {86422020-42A0-1069-A2E5-08002B30309D} — добавляет вкладки Общие, Сервис, Оборудование окна Свойства. По умолчанию данные вкладки добавляются ко всем значкам разделов диска.
- {F04CC277-03A2-4277-96A9-77967471BDFF} — добавляет вкладку Общие окна Свойства, с помощью которой можно просмотреть информацию о синхронизации файла или папки. По умолчанию данная вкладка добавляется с помощью ветви реестра HKEY_CLASSES_ROOT\ConflictFolder\shellex\PropertySheetHandlers.
- {f92e8c40-3d33-11d2-b1aa-080036a75b03} — добавляет вкладку Диагностика окна Свойства.
- {FA3E1D55-16DF-446d-872E-BD04D4F39C93} — добавляет вкладку COM+ окна Свойства.

Пример добавления вкладок

В качестве примера создадим свое собственное расширение файла, добавим к его окну Свойства набор основных вкладок, после чего попробуем взглянуть на результат нашей работы.

Шаг 1. Создание нового расширения файла

Первый шаг реализации нашего примера является наиболее творческой задачей — нужно придумать новое расширение, создание файлов которого мы зарегистрируем в операционной системе.

Стало традицией создавать расширения файлов, состоящие из трех символов (реже — из четырех или двух), мы же создадим расширение из четырех символов (чтобы вероятность совпадения нашего расширения с уже существующим была минимальной). Например, создадим файлы с расширением PARA.

Итак, результат действий, которые нужно выполнить для создания своего расширения, представлен в листинге П4.1 в виде REG-файла.

Листинг П4.1. REG-файл двух ветвей реестра, регистрирующих новое расширение

```
REGEDIT4

[HKEY_CLASSES_ROOT\.para]
@="parafile"

[HKEY_CLASSES_ROOT\parafile]
"NeverShowExt"=""
@="Test-File"

[HKEY_CLASSES_ROOT\parafile\shellex]

[HKEY_CLASSES_ROOT\parafile\shellex\PropertySheetHandlers]
```

Шаг 2. Добавление вкладок к окну Свойства

Для примера добавим следующие стандартные вкладки к окну Свойства нашего расширения файлов:

- {645FF040-5081-101B-9F08-00AA002F954E} — позволяет изменить параметры настройки работы Корзины;
- {6D5313C0-8C62-11D1-B2CD-006097DF8C11} — отображает вкладки окна Свойства папки.

Для выполнения этого шага вам достаточно создать в ветви системного реестра HKEY_CLASSES_ROOT\parafile\shellex\PropertySheetHandlers дочерние подразделы {645FF040-5081-101B-9F08-00AA002F954E} и {6D5313C0-8C62-11D1-B2CD-006097DF8C11}.

Шаг 3. Проверка результатов

Чтобы проверить результат нашего творчества, достаточно создать обычный текстовый файл (либо любой другой), после чего изменить расширение TXT этого файла на расширение PARA. После того как вы это сделаете и зайдете в окно Свойства для созданного файла, перед вами отобразится окно, представленное на рис. П4.1.

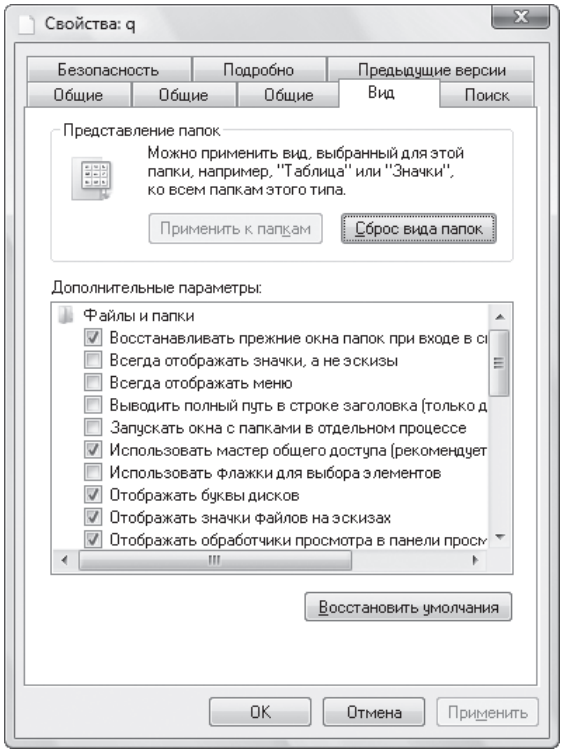

Рис. П4.1. Добавление дополнительных вкладок к окну Свойства

Добавление команд к контекстному меню

Как вы уже знаете, чтобы добавить команду к контекстному меню файлов или ActiveX-объектов, нужно добавить соответствующий команде CLSID-номер ActiveX-объекта к ветви реестра `HKEY_CLASSES_ROOT\CLSID\{CLSID-номер ActiveX-объекта}\shellex\ContextMenuHandlers` либо к ветви системного реестра Windows `HKEY_CLASSES_ROOT\<идентификатор файла>\shellex\ContextMenuHandlers`.

Стандартные ActiveX-объекты

Рассмотрим стандартные ActiveX-объекты операционной системы Windows Vista, которые добавляют новые элементы контекстного меню значка ActiveX-объекта или файла.

- `{0006F019-0000-0000-C000-000000000046}` — добавляет к контекстному меню команду С помощью Microsoft Outlook. С помощью данной команды можно отобразить окно Настройка Outlook.
- `{09799AFB-AD67-11d1-ABCD-00C04FC30936}` — добавляет к контекстному меню команду Открыть с помощью. По умолчанию данная команда добавляется ко всем зарегистрированным в операционной системе расширениям файлов с помощью ветви реестра `HKEY_CLASSES_ROOT\*\shellex\ContextMenuHandlers`.
- `{1a184871-359e-4f67-aad9-5b9905d62232}` — добавляет к контекстному меню команду Установить. С помощью данной команды можно установить шрифт, поэтому она добавляется к контекстному меню файлов различных шрифтов.
- `{2559a1f0-21d7-11d4-bdaf-00c04f60b9f0}` — добавляет к контекстному меню команду Поиск. Данная команда позволяет отобразить окно Результаты поиска.
- `{2559a1f1-21d7-11d4-bdaf-00c04f60b9f0}` — добавляет к контекстному меню команду Справка и поддержка.
- `{C2FBB630-2971-11D1-A18C-00C04FD75D13}` — добавляет к контекстному меню команду Копировать в папку. С помощью данной команды можно отобразить окно, а в нем указать папку, в которую будет скопирован соответствующий файл.
- `{C2FBB631-2971-11d1-A18C-00C04FD75D13}` — добавляет к контекстному меню команду Переместить в папку. С помощью данной команды можно отобразить окно, а в нем указать папку, в которую будет перемещен соответствующий файл.
- `{b8cdcb65-b1bf-4b42-9428-1dfdb7ee92af}` — добавляет к контекстному меню команду Извлечь все. По умолчанию она добавляется с помощью ветви реестра `HKEY_CLASSES_ROOT\CompressedFolder\ShellEx\ContextMenuHandlers`.
- `{f81e9010-6ea4-11ce-a7ff-00aa003ca9f6}` — добавляет к контекстному меню команду Общий доступ. По умолчанию она добавляется ко всем

зарегистрированным в операционной системе расширениям файлов с помощью ветви реестра HKEY_CLASSES_ROOT*\shellex\ContextMenuHandlers.

- {2559a1f3-21d7-11d4-bdaf-00c04f60b9f0} — добавляет к контекстному меню команду Выполнить.
- {2559a1f4-21d7-11d4-bdaf-00c04f60b9f0} — добавляет к контекстному меню команду Обзор Интернета, а также команду Свойства Интернета.
- {2559a1f5-21d7-11d4-bdaf-00c04f60b9f0} — добавляет к контекстному меню команду Чтение почты. Она запускает почтовый клиент Outlook Express.
- {2559a1f7-21d7-11d4-bdaf-00c04f60b9f0} — добавляет к контекстному меню команду Настройка доступа программ и умолчаний. Данная команда запускает одноименное окно.
- {3080F90D-D7AD-11D9-BD98-0000947B0257} — добавляет к контекстному меню команду Показывать поверхность рабочего стола. После выбора данной команды все окна программ будут минимизированы и отобразится Рабочий стол операционной системы.
- {32714800-2E5F-11d0-8B85-00AA0044F941} — добавляет к контекстному меню команду Найти людей. Данная команда отображает окно поиска в адресной книге.
- {596AB062-B4D2-4215-9F74-E9109B0A8153} — добавляет к контекстному меню команду Восстановить прежнюю версию. По умолчанию она добавляется к файлам всех типов расширений с помощью ветви реестра HKEY_CLASSES_ROOT\AllFilesystemObjects\shellex\PropertySheetHandlers.
- {645FF040-5081-101B-9F08-00AA002F954E} — добавляет к контекстному меню команду Очистить корзину. Данная команда позволяет очистить содержимое Корзины.
- {7444C717-39BF-11D1-8CD9-00C04FC29D45} — добавляет к контекстному меню команду Открыть, с помощью которой открываются файлы публичных ключей, имеющие расширение PKO.
- {7968860a-1ac6-482e-8f90-0874a1b6a79f} — добавляет к контекстному меню команду Изменить.
- {7BA4C740-9E81-11CF-99D3-00AA004AE837} — добавляет к контекстному меню команду Отправить. С ее помощью можно переместить файлы или папки в каталоги или объекты, ссылки на которые указаны в каталоге %userprofile%\AppData\Roaming\Microsoft\Windows\SendTo. По умолчанию данная команда добавляется ко всем объектам файловой системы Windows Vista с помощью ветви реестра HKEY_CLASSES_ROOT\AllFilesystemObjects\shellex\ContextMenuHandlers.
- {7D4734E6-047E-41e2-AEAA-E763B4739DC4} — добавляет к контекстному меню команду Воспроизвести с помощью проигрывателя Windows Media. Данная команда запускает Проигрыватель Windows Media и, если обнаруживает музыкальный файл среди содержимого каталога (если команда добавлена к контекстному меню каталога), пытается его воспроизвести. По умолчанию она добавляется с по-

мощью ветви реестра HKEY_CLASSES_ROOT\SystemFileAssociations\Directory.Audio\shellex\ContextMenuHandlers.

- {8DD448E6-C188-4aed-AF92-44956194EB1F} — добавляет к контекстному меню команду Добавить в список записи. С ее помощью можно добавить файл к списку файлов, которые будут записываться на диск. По умолчанию данная команда добавляется с помощью ветви системного реестра Windows HKEY_CLASSES_ROOT\SystemFileAssociations\Directory.Audio\shellex\ContextMenuHandlers.
- {A8E64375-B645-4314-9EFC-C085981786FA} — добавляет к контекстному меню команду Очистить список последних элементов.
- {CE3FB1D1-02AE-4a5f-A6E9-D9F1B4073E6C} — добавляет к контекстному меню команду Воспроизвести с помощью проигрывателя Windows Media. Данная команда запускает Проигрыватель Windows Media и воспроизводит соответствующий музыкальный файл. По умолчанию данная команда добавляется к файлам с расширением AIF, ASF, ASX, AU, AVI, M3U, MID и т. д.
- {F1B9284F-E9DC-4e68-9D7E-42362A59F0FD} — добавляет к контекстному меню команду Добавить в список проигрывателя Windows Media. По умолчанию она добавляется к файлам с расширением AIF, ASF, ASX, AU, AVI, M3U, MID и т. д.
- {f3d06e7c-1e45-4a26-847e-f9fcdee59be0} — этот ActiveX-объект добавляет к контекстному меню файлов команду Копировать как путь. Данная команда отобразится после того, как вы нажмете клавишу Shift и, удерживая ее, вызовете контекстное меню файлов. По умолчанию команда добавляется к файлам всех типов расширений с помощью ветви реестра HKEY_CLASSES_ROOT\AllFilesystemObjects\shellex\PropertySheetHandlers.
- {FBF23B40-E3F0-101B-8488-00AA003E56F8} — добавляет к контекстному меню команду Открыть, предназначенную для открытия файлов ярлыков страниц Интернета. По умолчанию данная команда добавляется к файлам с расширением URL.

Пример добавления команды к контекстному меню

В качестве примера попробуем зарегистрировать свой собственный ActiveX-объект, после чего отобразим его в какой-нибудь папке файловой системы компьютера.

Шаг 1. Регистрируем свой ActiveX-объект

Первым этапом будет регистрация своего ActiveX-объекта в операционной системе Windows Vista. Как и в предыдущем примере, для этого воспользуемся листингом П4.2, отображающим REG-файл тех действий, которые нужно произвести.

ПРИМЕЧАНИЕ

В контексте данной книги не объясняется процесс создания уникального ActiveX-объекта. В примере используется не уникальный CLSID-номер ActiveX-объекта, а введенный наугад.

Листинг П4.2. Файл, регистрирующий новый ActiveX-объект

```
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\CLSID\{FFFFFFFF-FFFF-FFFF-FFFF-F53F46C2B1A7}]
@="TEST_ActiveX"

[HKEY_CLASSES_ROOT\CLSID\{FFFFFFFF-FFFF-FFFF-FFFF-F53F46C2B1A7}\DefaultIcon]
@="%SystemRoot%\\System32\\imageres.dll,-33"

[HKEY_CLASSES_ROOT\CLSID\{FFFFFFFF-FFFF-FFFF-FFFF-F53F46C2B1A7}\shellex]

[HKEY_CLASSES_ROOT\CLSID\{FFFFFFFF-FFFF-FFFF-FFFF-F53F46C2B1A7}\shellex\
ContextMenuHandlers]
```

Шаг 3. Формируем команды его контекстного меню

Для примера добавим следующие стандартные команды к контекстному меню нашего ActiveX-объекта:

- `{32714800-2E5F-11d0-8B85-00AA0044F941}` — позволяет отобразить окно поиска среди контактов адресной книги;
- `{645FF040-5081-101B-9F08-00AA002F954E}` — дает возможность очистить содержимое Корзины;
- `{7D4734E6-047E-41e2-AEAA-E763B4739DC4}` — позволяет запустить Проигрыватель Windows Media.

Для этого достаточно добавить соответствующие дочерние подразделы к ветви системного реестра `HKEY_CLASSES_ROOT\CLSID\{FFFFFFFF-FFFF-FFFF-FFFF-F53F46C2B1A7}\shellex\ContextMenuHandlers`.

Шаг 4. Отображаем зарегистрированный ActiveX-объект

Последний этап — отображение созданного нами ActiveX-объекта.

В следующем разделе будут описаны способы добавления ActiveX-объекта к одной из специальных папок. Сейчас же мы рассмотрим пример добавления ActiveX-объекта к панели быстрого запуска. Для этого достаточно создать в каталоге `%userprofile%\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch` папку, после чего добавить к ее названию строку `.{FFFFFFFF-FFFF-FFFF-FFFF-F53F46C2B1A7}`. Результат этого действия отображается на рис. П4.2.

ActiveX-объекты, отображающие значки

Еще одним примером использования ActiveX-объектов является отображение значков или мастеров и окон операционной системы Windows Vista. Например, вы можете добавить описанные ниже значки ActiveX-объектов на Рабочий стол, в папку Компьютер или в Панель управления. Для этого нужно в специальной ветви реест-

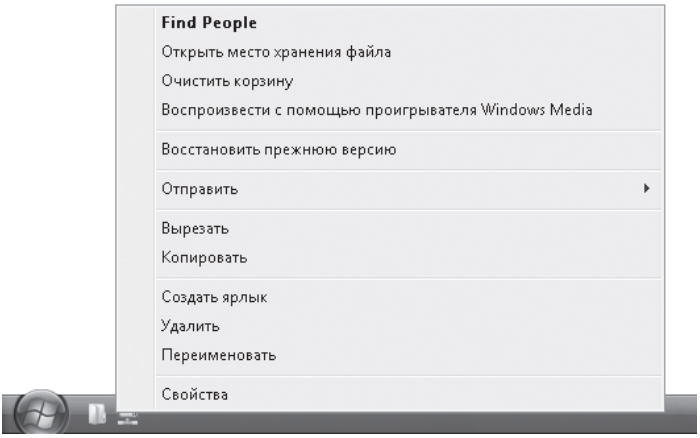

Рис. П4.2. Отображение свойств ActiveX-объекта для папки панели быстрого доступа

ра создать подраздел, названный в честь CLSID-номера ActiveX-объекта. Вы можете воспользоваться следующими ветвями реестра:

- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Desktop\namespace` (или в ветви корневого раздела реестра `HKEY_LOCAL_MACHINE`) — добавляет ActiveX-объект на Рабочий стол;
- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\mycomputer\namespace` (или в ветви корневого раздела реестра `HKEY_LOCAL_MACHINE`) — добавляет ActiveX-объект в папку Компьютер;
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ControlPanel\NameSpace` — добавляет ActiveX-объект в папку Панель управления.

Еще одним способом создания значка ActiveX-объекта является использование папки. Для этого достаточно создать папку и к ее названию добавить `.{CLSID-номер соответствующего ActiveX-объекта}`.

- `{00f2886f-cd64-4fc9-8ec5-30ef6cdbe8c3}` — отображает значок Сканеры и камеры. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду `::{21EC2020-3AEA-1069-A2DD-08002B30309D}\::{00f2886f-cd64-4fc9-8ec5-30ef6cdbe8c3}`.
- `{025A5937-A6BE-4686-A844-36FE4BEC8B6D}` — выводит значок Электропитание. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду `::{21EC2020-3AEA-1069-A2DD-08002B30309D}\::{025A5937-A6BE-4686-A844-36FE4BEC8B6D}`.
- `{0DF44EAA-FF21-4412-828E-260A8728E7F1}` — отображает значок Панель задач и меню "Пуск". Его же можно вызвать с помощью окна Запуск программы, введя в нем команду `::{21EC2020-3AEA-1069-A2DD-08002B30309D}\::{0DF44EAA-FF21-4412-828E-260A8728E7F1}`.

- {1443904b-34e4-40f6-b30f-6beb81267b80} — запускает модуль Speech Recognition при запуске папки.
- {15eae92e-f17a-4431-9f28-805e482dafd4} — отображает значок, вызывающий мастер Получение программ. Он позволяет установить программы, которые были опубликованы по сети администратором домена Active Directory. Также данный ActiveX-объект можно использовать в виде команды ::{21EC2020-3AEA-1069-A2DD-08002B30309D}\::{15eae92e-f17a-4431-9f28-805e482dafd4}.

  Можно также создать папку со свойствами данного объекта (она должна называться "название".{15eae92e-f17a-4431-9f28-805e482dafd4}).
- {17cd9488-1228-4b2f-88ce-4298e93e0966} — выводит значок Программы по умолчанию. Этот ActiveX-объект можно использовать и в виде команды ::{21EC2020-3AEA-1069-A2DD-08002B30309D}\::{17cd9488-1228-4b2f-88ce-4298e93e0966} окна Запуск программы.

  Свойства данного окна можно также присвоить папке.
- {1FA9085F-25A2-489B-85D4-86326EEDCD87} — отображает значок Управление беспроводными сетями. Его же можно вызвать, присвоив свойства ActiveX-объекта папке.
- {208D2C60-3AEA-1069-A2D7-08002B30309D} — выводит значок Сеть (WORKGROUP). Его же можно вызвать с помощью окна Запуск программы, введя в нем команду ::{208D2C60-3AEA-1069-A2D7-08002B30309D}.

  Это окно также можно вызвать, присвоив его свойства папке.
- {20D04FE0-3AEA-1069-A2D8-08002B30309D} — отображает значок Компьютер. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду ::{20D04FE0-3AEA-1069-A2D8-08002B30309D}.

  Это окно также можно вызвать, присвоив его свойства папке.
- {21EC2020-3AEA-1069-A2DD-08002B30309D} — показывает значок Панель управления. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду ::{21EC2020-3AEA-1069-A2DD-08002B30309D}.
- {2227A280-3AEA-1069-A2DE-08002B30309D} — отображает значок Принтеры. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду ::{2227A280-3AEA-1069-A2DE-08002B30309D}.

  Это окно также можно вызвать с помощью окна Запуск программы, введя в нем команду ::{21EC2020-3AEA-1069-A2DD-08002B30309D}\::{2227A280-3AEA-1069-A2DE-08002B30309D}.

  Те же самые действия выполняются, если присвоить свойства папки Принтеры обычной папке.
- {2559a1f0-21d7-11d4-bdaf-00c04f60b9f0} — отображает значок Поиск.
- {2559a1f1-21d7-11d4-bdaf-00c04f60b9f0} — выводит значок Справка и поддержка.

- {2559a1f3-21d7-11d4-bdaf-00c04f60b9f0} — отображает значок Выполнить.
- {2559a1f7-21d7-11d4-bdaf-00c04f60b9f0} — выводит значок Настройка доступа программ и умолчаний.
- {26EE0668-A00A-44D7-9371-BEB064C98683} — отображает значок Панель управления, открываемый в виде по категориям. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду ::{26EE0668-A00A-44D7-9371-BEB064C98683}.
- {289978AC-A101-4341-A817-21EBA7FD046D} — выводит значок Просмотр конфликтов синхронизации. Его же можно отобразить, присвоив его свойства папке.
- {2E9E59C0-B437-4981-A647-9C34B9B90891} — отображает значок Настройка новой связи синхронизации. Его же можно отобразить, присвоив его свойства папке.
- {3080F90D-D7AD-11D9-BD98-0000947B0257} — выводит значок Свернуть все окна.
- {335a31dd-f04b-4d76-a925-d6b47cf360df} — отображает значок Центр архивации и восстановления. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду ::{21EC2020-3AEA-1069-A2DD-08002B30309D}\ ::{335a31dd-f04b-4d76-a925-d6b47cf360df}.

  Это окно также можно отобразить, присвоив его свойства папке.
- {36eef7db-88ad-4e81-ad49-0e313f0c35f8} — выводит значок Центр обновления Windows. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду ::{21EC2020-3AEA-1069-A2DD-08002B30309D}\ ::{36eef7db-88ad-4e81-ad49-0e313f0c35f8}.

  Это окно также можно вызвать, присвоив его свойства папке.
- {37efd44d-ef8d-41b1-940d-96973a50e9e0} — отображает значок Свойства боковой панели Windows. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду ::{21EC2020-3AEA-1069-A2DD-08002B30309D}\ ::{37efd44d-ef8d-41b1-940d-96973a50e9e0}.
- {3e7efb4c-faf1-453d-89eb-56026875ef90} — отображает значок Приобретение программ через Интернет. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду ::{21EC2020-3AEA-1069-A2DD-08002B30309D}\::{3e7efb4c-faf1-453d-89eb-56026875ef90}.
- {3f6bc534-dfa1-4ab4-ae54-ef25a74e0107} — выводит значок Восстановление системы.
- {4026492F-2F69-46B8-B9BF-5654FC07E423} — отображает значок Брандмауэр Windows. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду ::{21EC2020-3AEA-1069-A2DD-08002B30309D}\::{4026492F-2F69-46B8-B9BF-5654FC07E423}.

  Это окно также можно вызвать, присвоив его свойства папке.

- {437ff9c0-a07f-4fa0-af80-84b6c6440a16} — отображает значок Command Folder.
- {450D8FBA-AD25-11D0-98A8-0800361B1103} — выводит значок Документы. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду ::{450D8FBA-AD25-11D0-98A8-0800361B1103}.
- {48e7caab-b918-4e58-a94d-505519c795dc} — отображает значок Главное меню. Его же можно отобразить, присвоив его свойства папке.
- {4D1209BD-36E2-4e2f-840D-6C7FB879DD9E} — выводит значок Windows Ultimate. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду ::{21EC2020-3AEA-1069-A2DD-08002B30309D}\::{4D1209BD-36E2-4e2f-840D-6C7FB879DD9E}.

  Это окно также можно вызвать, присвоив его свойства папке.
- {5399E694-6CE5-4D6C-8FCE-1D8870FDCBA0} — отображает значок Панель управления.
- {58E3C745-D971-4081-9034-86E34B30836A} — выводит значок Speech Recognition. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду ::{21EC2020-3AEA-1069-A2DD-08002B30309D}\::{58E3C745-D971-4081-9034-86E34B30836A}.

  Его также можно отобразить, присвоив свойства данного ActiveX-объекта папке.
- {59031a47-3f72-44a7-89c5-5595fe6b30ee} — отображает значок доступа к каталогу %userprofile%. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду ::{59031a47-3f72-44a7-89c5-5595fe6b30ee}.

  Его также можно отобразить, присвоив свойства данного ActiveX-объекта папке.
- {5ea4f148-308c-46d7-98a9-49041b1dd468} — выводит значок Центр устройств Windows Mobile. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду ::{21EC2020-3AEA-1069-A2DD-08002B30309D}\::{5ea4f148-308c-46d7-98a9-49041b1dd468}.

  Это окно также можно отобразить, присвоив свойства ActiveX-объекта папке.
- {60632754-c523-4b62-b45c-4172da012619} — отображает значок Учетные записи пользователей. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду ::{21EC2020-3AEA-1069-A2DD-08002B30309D}\::{60632754-c523-4b62-b45c-4172da012619}.

  Это окно также можно вызвать, присвоив его свойства папке.
- {645FF040-5081-101B-9F08-00AA002F954E} — отображает значок Корзина. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду ::{645FF040-5081-101B-9F08-00AA002F954E}.

  Это окно также можно вызвать, присвоив свойства ActiveX-объекта папке.
- {67718415-c450-4f3c-bf8a-b487642dc39b} — выводит значок Компоненты Windows. Его же можно вызвать, присвоив свойства ActiveX-объекта папке.

- {692F0339-CBAA-47e6-B5B5-3B84DB604E87} — присвоение свойств данного ActiveX-объекта папке приводит к тому, что эта папка будет ссылаться на другую папку, содержащую набор XML-файлов. Данная папка содержит все установленные надстройки браузера Internet Explorer.
- {6DFD7C5C-2451-11d3-A299-00C04F8EF6AF} — отображает значок Свойства папки. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду ::{21EC2020-3AEA-1069-A2DD-08002B30309D}\::{6DFD7C5C-2451-11d3-A299-00C04F8EF6AF}.

  Это окно также можно вызвать, присвоив его свойства папке.
- {7007ACC7-3202-11D1-AAD2-00805FC1270E} — отображает значок Сетевые подключения. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду ::{7007ACC7-3202-11D1-AAD2-00805FC1270E}.

  Это окно также можно вызвать с помощью окна Запуск программы, введя в нем команду ::{21EC2020-3AEA-1069-A2DD-08002B30309D}\::{7007ACC7-3202-11D1-AAD2-00805FC1270E}.
- {71D99464-3B6B-475C-B241-E15883207529} — выводит значок Результаты выполнения синхронизации. Его же можно вызвать, присвоив его свойства папке.
- {74246bfc-4c96-11d0-abef-0020af6b0b7a} — отображает значок Диспетчер устройств. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду ::{21EC2020-3AEA-1069-A2DD-08002B30309D}\::{74246bfc-4c96-11d0-abef-0020af6b0b7a}.
- {78F3955E-3B90-4184-BD14-5397C15F1EFC} — выводит значок Счетчики и средства производительности. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду ::{21EC2020-3AEA-1069-A2DD-08002B30309D}\::{78F3955E-3B90-4184-BD14-5397C15F1EFC}.

  Это окно также можно отобразить, присвоив его свойства папке.
- {7A979262-40CE-46ff-AEEE-7884AC3B6136} — отображает значок Установка оборудования. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду ::{21EC2020-3AEA-1069-A2DD-08002B30309D}\::{7A979262-40CE-46ff-AEEE-7884AC3B6136}.

  Это окно также можно отобразить, присвоив его свойства папке.
- {7A9D77BD-5403-11d2-8785-2E0420524153} — выводит значок Учетные записи пользователей.
- {7b81be6a-ce2b-4676-a29e-eb907a5126c5} — отображает значок Программы и компоненты. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду ::{21EC2020-3AEA-1069-A2DD-08002B30309D}\::{7b81be6a-ce2b-4676-a29e-eb907a5126c5}.

  Это окно также можно отобразить, присвоив его свойства папке.
- {7be9d83c-a729-4d97-b5a7-1b7313c39e0a} — выводит значок, который комбинирует в себе содержимое сразу двух папок — папки, хранящейся в каталоге %userprofile%\Главное меню, и папки, находящейся в каталоге

`%systemdrive%\Users\All Users\Главное меню`. Данный значок можно отобразить, только присвоив его свойства папке.

- `{85BBD920-42A0-1069-A2E4-08002B30309D}` — отображает значок Портфель. Его можно отобразить, только присвоив его свойства папке.
- `{865e5e76-ad83-4dca-a109-50dc2113ce9a}` — если присвоить свойства данного ActiveX-объекта папке, то она будет отображать каталог, содержащий все программы из меню Пуск.
- `{8E908FC9-BECC-40f6-915B-F4CA0E70D03D}` — выводит значок Центр управления сетями и общим доступом. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду `::{21EC2020-3AEA-1069-A2DD-08002B30309D}\::{8E908FC9-BECC-40f6-915B-F4CA0E70D03D}`.

  Это окно также можно отобразить, присвоив его свойства папке.
- `{9343812e-1c37-4a49-a12e-4b2d810d956b}` — отображает значок Результаты поиска. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду `::{9343812e-1c37-4a49-a12e-4b2d810d956b}`.

  Данный значок можно отобразить, только присвоив его свойства папке.
- `{96AE8D84-A250-4520-95A5-A47A7E3C548B}` — выводит значок Родительский контроль. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду `::{21EC2020-3AEA-1069-A2DD-08002B30309D}\::{96AE8D84-A250-4520-95A5-A47A7E3C548B}`.

  Это окно также можно отобразить, присвоив его свойства папке.
- `{992CFFA0-F557-101A-88EC-00DD010CCC48}` — выводит значок Сетевые подключения.
- `{9C60DE1E-E5FC-40f4-A487-460851A8D915}` — отображает значок Автозапуск. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду `::{21EC2020-3AEA-1069-A2DD-08002B30309D}\::{9C60DE1E-E5FC-40f4-A487-460851A8D915}`.

  Это окно также можно отобразить, присвоив его свойства папке.
- `{9C73F5E5-7AE7-4E32-A8E8-8D23B85255BF}` — выводит значок Центр синхронизации. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду `::{21EC2020-3AEA-1069-A2DD-08002B30309D}\::{9C73F5E5-7AE7-4E32-A8E8-8D23B85255BF}`.

  Это окно также можно отобразить, присвоив его свойства папке.
- `{9f433b7c-5f96-4ce1-ac28-aeaa1cc04d7c}` — отображает значок Центр обеспечения безопасности. Его же можно отобразить, присвоив его свойства папке.
- `{A304259D-52B8-4526-8B1A-A1D6CECC8243}` — выводит значок Инициатор iSCSI. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду `::{21EC2020-3AEA-1069-A2DD-08002B30309D}\::{A304259D-52B8-4526-8B1A-A1D6CECC8243}`.
- `{AFDB1F70-2A4C-11d2-9039-00C04F8EEB3E}` — отображает значок Автономные файлы.

- {b155bdf8-02f0-451e-9a26-ae317cfd7779} — выводит значок delegate folder that appears in Computer.
- {B2C761C6-29BC-4f19-9251-E6195265BAF1} — отображает значок Управление цветом, вызывающий одноименный мастер. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду ::{21EC2020-3AEA-1069-A2DD-08002B30309D}\::{B2C761C6-29BC-4f19-9251-E6195265BAF1}.
- {BB06C0E4-D293-4f75-8A90-CB05B6477EEE} — выводит значок Система. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду ::{21EC2020-3AEA-1069-A2DD-08002B30309D}\::{BB06C0E4-D293-4f75-8A90-CB05B6477EEE}.
- {CB1B7F8C-C50A-4176-B604-9E24DEE8D4D1} — отображает значок Центр начальной настройки. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду ::{21EC2020-3AEA-1069-A2DD-08002B30309D}\::{CB1B7F8C-C50A-4176-B604-9E24DEE8D4D1}.
- {D20EA4E1-3957-11d2-A40B-0C5020524152} — выводит значок Шрифты. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду ::{21EC2020-3AEA-1069-A2DD-08002B30309D}\::{D20EA4E1-3957-11d2-A40B-0C5020524152}.
- {D20EA4E1-3957-11d2-A40B-0C5020524153} — отображает значок Администрирование. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду ::{21EC2020-3AEA-1069-A2DD-08002B30309D}\::{D20EA4E1-3957-11d2-A40B-0C5020524153}.
- {d34a6ca6-62c2-4c34-8a7c-14709c1ad938} — выводит значок Common Places FS Folder. Его же можно отобразить, присвоив его свойства папке.
- {d450a8a1-9568-45c7-9c0e-b4f9fb4537bd} — отображает значок Установленные обновления. Его же можно отобразить, присвоив его свойства папке.
- {D555645E-D4F8-4c29-A827-D93C859C4F2A} — выводит значок Центр специальных возможностей. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду ::{21EC2020-3AEA-1069-A2DD-08002B30309D}\::{D555645E-D4F8-4c29-A827-D93C859C4F2A}.

  Это окно также можно отобразить, присвоив его свойства папке.
- {D8559EB9-20C0-410E-BEDA-7ED416AECC2A} — выводит значок Защитник Windows. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду ::{21EC2020-3AEA-1069-A2DD-08002B30309D}\::{D8559EB9-20C0-410E-BEDA-7ED416AECC2A}.

  Его также можно отобразить, присвоив свойства папке.
- {D9EF8727-CAC2-4e60-809E-86F80A666C91} — выводит значок Шифрование диска BitLocker, вызывающий одноименный мастер. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду ::{21EC2020-3AEA-1069-A2DD-08002B30309D}\::{D9EF8727-CAC2-4e60-809E-86F80A666C91}.

  Его также можно отобразить, присвоив свойства папке.

- {E7E4BC40-E76A-11CE-A9BB-00AA004AE837} — перезагружает оболочку.
- {E95A4861-D57A-4be1-AD0F-35267E261739} — отображает значок Windows SideShow. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду ::{21EC2020-3AEA-1069-A2DD-08002B30309D}\::{E95A4861-D57A-4be1-AD0F-35267E261739}.

  Это окно также можно отобразить, присвоив его свойства папке.
- {ED228FDF-9EA8-4870-83b1-96b02CFE0D52} — выводит значок Игры. Его также можно вызвать с помощью окна Запуск программы, введя в нем команду ::{ED228FDF-9EA8-4870-83b1-96b02CFE0D52}.

  Это окно также можно отобразить, присвоив его свойства папке.
- {ED834ED6-4B5A-4bfe-8F11-A626DCB6A921} — отображает значок Персонализация. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду ::{21EC2020-3AEA-1069-A2DD-08002B30309D}\::{ED834ED6-4B5A-4bfe-8F11-A626DCB6A921}.

  Его также можно отобразить, присвоив его свойства папке.
- {F02C1A0D-BE21-4350-88B0-7367FC96EF3C} — выводит значок Сеть. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду ::{F02C1A0D-BE21-4350-88B0-7367FC96EF3C}.
- {FCFEECAE-EE1B-4849-AE50-685DCF7717EC} — отображает значок Отчеты о проблемах и их решениях. Его же можно вызвать с помощью окна Запуск программы, введя в нем команду ::{21EC2020-3AEA-1069-A2DD-08002B30309D}\::{FCFEECAE-EE1B-4849-AE50-685DCF7717EC}.

  Это окно также можно вызвать, присвоив его свойства папке.

На этом мы заканчиваем рассмотрение ActiveX-объектов операционной системы Windows Vista.