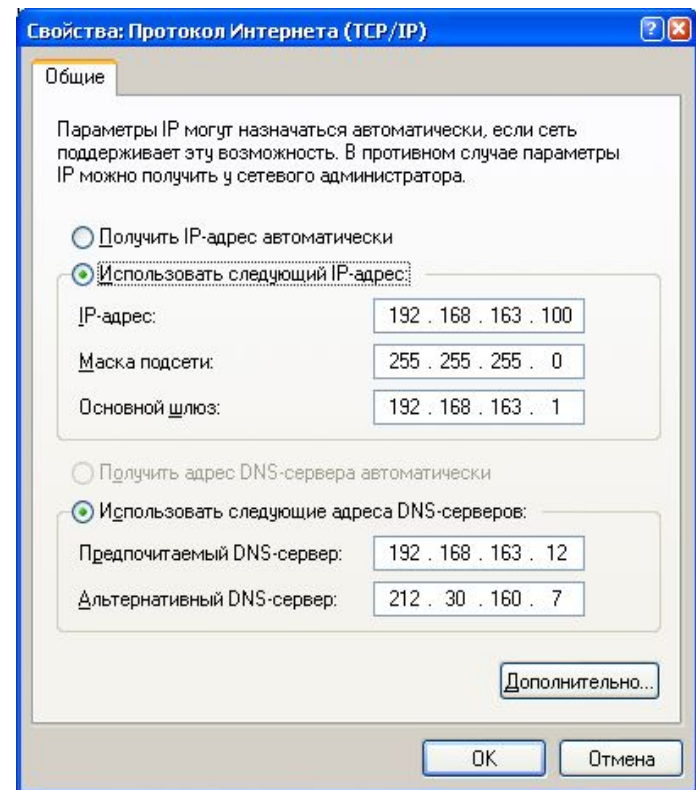
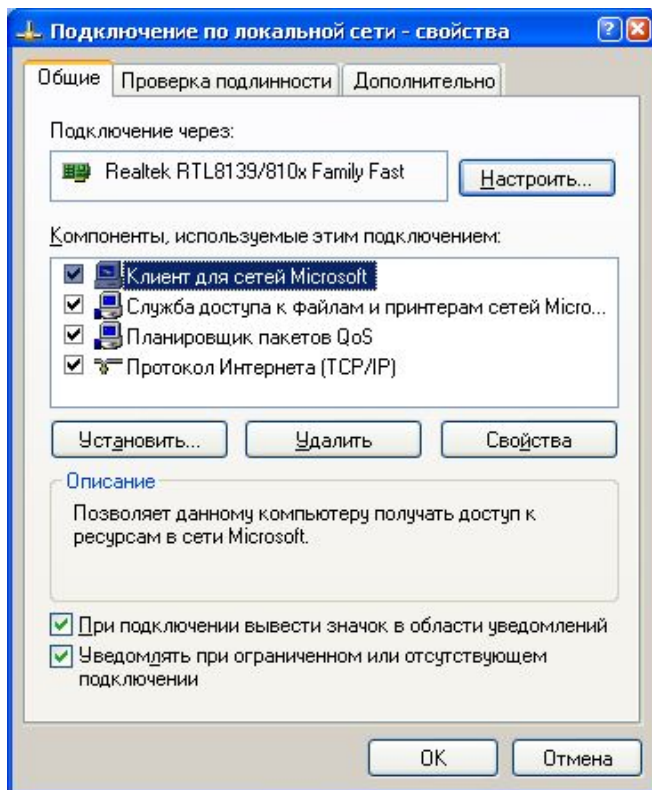


Администрирование информационных систем

Администрирование сетей
Microsoft

Первоначальная настройка сети

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



Управление службами

- Для управления службами можно использовать GUI интерфейс.

The screenshot shows the 'Управление компьютером' (Computer Management) console window with the 'Службы' (Services) snap-in selected. The main pane displays a list of services with columns for Name, Description, Status, Start Type, and Log On As. The 'Расширенный' (Advanced) view is selected at the bottom.

Имя	Описание	Состояние	Тип запуска	Вход от имени
SQLAgent\$MICROSOFTBCM			Вручную	Локальная си
Telnet	Позволяет удаленному пользователю входить...		Отключено	Локальная си
Windows Audio	Управление звуковыми устройствами для Win...	Работает	Авто	Локальная си
Windows Installer	Позволяет добавлять, изменять и удалять пр...		Вручную	Локальная си
Windows Media Connect (WMC)	Передача общего содержимого мультимедиа ...		Вручную	Сетевая служ
Windows User Mode Driver Framework	Включение драйверов пользовательского реж...	Работает	Авто	Локальная сл
Автоматическое обновление	Загрузка и установка обновлений Windows. Ес...	Работает	Авто	Локальная си
Адаптер производительности WMI	Предоставляет информацию о библиотеках пр...		Вручную	Локальная си
Беспроводная настройка	Предоставляет автоматическую настройку 8...	Работает	Авто	Локальная си
Брандмауэр Windows/Общий досту...	Обеспечивает поддержку служб трансляции а...	Работает	Авто	Локальная си
Веб-клиент	Позволяет Windows-программам создавать, по...	Работает	Авто	Локальная сл
Вторичный вход в систему	Позволяет запускать процессы от имени друг...	Работает	Авто	Локальная си
Диспетчер авто-подключений уда...	Создает подключение к удаленной сети, когд...		Вручную	Локальная си
Диспетчер логических дисков	Обнаружение и наблюдение за новыми жестк...	Работает	Авто	Локальная си
Диспетчер очереди печати	Загружает в память файлы для последующей ...	Работает	Авто	Локальная си
Диспетчер подключений удаленно...	Создает сетевое подключение.	Работает	Вручную	Локальная си
Диспетчер сеанса справки для уда...	Управляет возможностями Удаленного помощ...		Вручную	Локальная си
Диспетчер сетевого DDE	Управляет сетевыми общими ресурсами динам...		Отключено	Локальная си
Диспетчер учетных записей безоп...	Хранит информацию о безопасности для учетн...	Работает	Авто	Локальная си
Доступ к HID-устройствам	Обеспечивает универсальный доступ к HID-ус...	Работает	Авто	Локальная си
Журнал событий	Обеспечивает поддержку сообщений журнало...	Работает	Авто	Локальная си
Журналы и оповещения производи...	Управляет сбором данных о производительн...		Вручную	Сетевая служ
Запуск серверных процессов DCOM	Обеспечивает запуск для служб DCOM.	Работает	Авто	Локальная сл
Защищенное хранилище	Обеспечивает защищенное хранение секретн...	Работает	Авто	Локальная си
Инструментарий управления Windo...	Предоставляет общий интерфейс и объекту...	Работает	Авто	Локальная си
Источник бесперебойного питания	Управляет работой источников бесперебойно...		Вручную	Локальная сл



Команды обслуживания сети

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



Диагностика сети

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



Диагностика сети

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



Устранение неполадок

- Для выявления участков в сети TCP/IP, на которых присутствуют неполадки имеется несколько команд
 - ping
 - **Синтаксис** ping [-t] [-a] [-n число] [-l размер] [-f] [-i TTL] [-v TOS] [-r число] [-s число] [[-j списокУзлов] | [-k списокУзлов] [-w таймаут] конечноеИмя
 - **Параметры:**
 - -t Отправка пакетов на указанный узел до команды прерывания. Для вывода статистики и продолжения нажмите <Ctrl>+<Break>, для прекращения - <Ctrl>+<C>.
 - -a Определение адресов по именам узлов.
 - -n число Число отправляемых запросов.
 - -l размер Размер буфера отправки.
 - -f Установка флага, запрещающего фрагментацию пакета.
 - -i TTL Задание срока жизни пакета (поле "Time To Live").
 - -v TOS Задание типа службы (поле "Type Of Service").
 - -r число Запись маршрута для указанного числа переходов.
 - -s число Штамп времени для указанного числа переходов.
 - -j списокУзлов Свободный выбор маршрута по списку узлов.
 - -k списокУзлов Жесткий выбор маршрута по списку узлов.
 - -w таймаут Таймаут каждого ответа в миллисекундах.
 - /? Вызов справки



Устранение неполадок

- Другими командами устанавливающими наличие соединения с удаленным ip-узлом являются команды:
 - **tracert** – выводит имена и ip-адреса всех маршрутизаторов, через которые проходит пакет
 - **Параметры:**
 - -d Без разрешения в имена узлов.
 - -h максЧисло Максимальное число прыжков при поиске узла.
 - -j списокУзлов Свободный выбор маршрута по списку узлов.
 - -w интервал Интервал ожидания каждого ответа в миллисекундах.
 - **pathping** – выводит сетевую статистику при каждом переходе пакета через маршрутизатор
 - **Параметры:**
 - -g Список При прохождении по элементам списка узлов игнорировать предыдущий маршрут.
 - -h Число_прыжков Максимальное число прыжков при поиске узла.
 - -i Адрес Использовать указанный адрес источника.
 - -n Не разрешать адреса в имена узлов.
 - -r Пауза Пауза между отправками (мсек).
 - -q Число_запросов Число запросов при каждом прыжке.
 - -w Таймаут Время ожидания каждого ответа (мсек).
 - -P Тестировать на связность пути полученного с помощью RSVP.
 - -R Тестировать, если каждый прыжок резервируется с помощью RSVP.
 - -T Тестировать возможность взаимодействия для каждого
 - -4 Принудительно использовать IPv4.
 - -6 Принудительно использовать IPv6.



Конфигурирование сети

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



Конфигурирование сети

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



Сетевые службы

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



Запуск и остановка служб

- Для запуск и остановки служб в Windows используются команды:
 - `sc <server> [command] [service name] <option1> <option2>...`
 - `net start <служба>`
 - `net stop <служба>`
 - `net pause <служба>`
 - `net continue <служба>`



Сетевые службы

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



Сетевые службы

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



Мониторинг служб

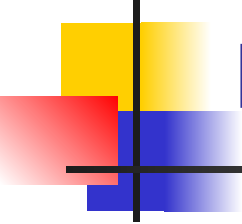
- Для мониторинга служб Workstation и Server ИСПОЛЬЗУЮТСЯ КОМАНДЫ:
 - Net statistics workstation – выводит статистику соединений, работы в сети и сеансов для службы со времени ее последнего запуска
 - Net statistics server – выводит статистику сеансов, нарушения безопасности и информацию о доступе к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



Общие сетевые ресурсы

- Набор команд net share позволяет просматривать и управлять общими ресурсами на сервере:
 - Net share – отображает все активные папки на сервере
 - Net share <имя общего ресурса>=<имя диска>:\<каталог> - создание общей папки
 - Net share <имя общего ресурса> /delete – удаление общего ресурса
 - Net share <имя общего ресурса> /users:<#> задание максимального числа подключений
 - Net share <имя общего ресурса> /remark:“описание” – добавление описания общего ресурса

Просмотр сетевых КОМПОНЕНТОВ



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

Использование сетевых ресурсов

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

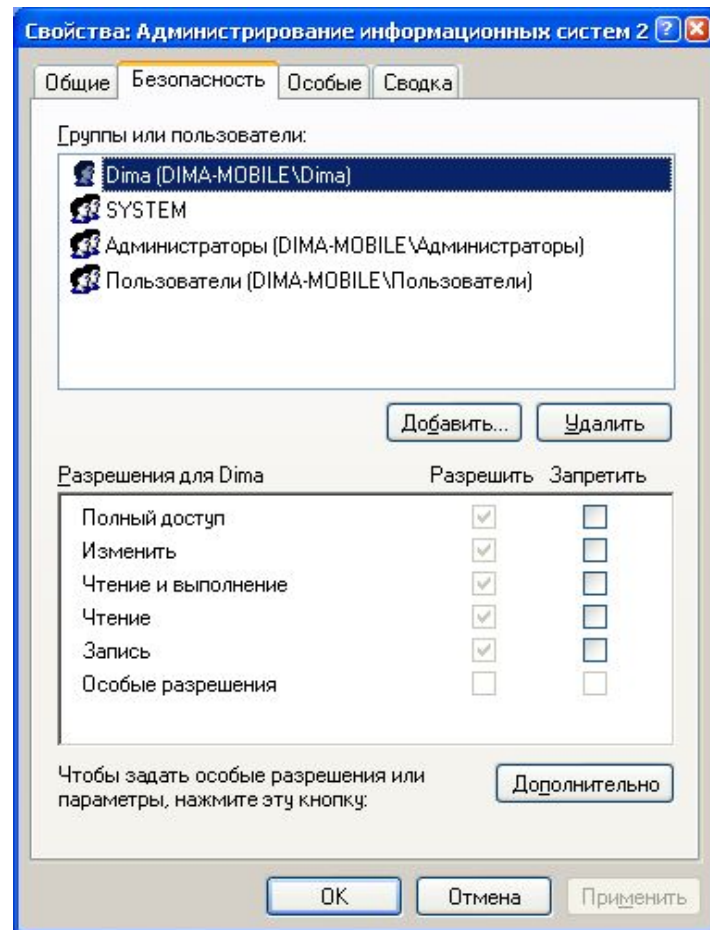
Синхронизация часов с сервером времени



- Для управления работой компьютерных систем в вычислительной сети необходима их синхронизация (выставление одинакового времени). Для синхронизации используется команда `net time`:
 - `Net time \\имя сервера` – выводит текущее время
 - `Net time \\сервер /set` – синхронизирует время на текущем компьютере со временем на сервере
 - `Net time /setsntp:<ip-адрес сервера>` - синхронизирует время со временем внешнего сервера времени в сети, например 194.149.67.130

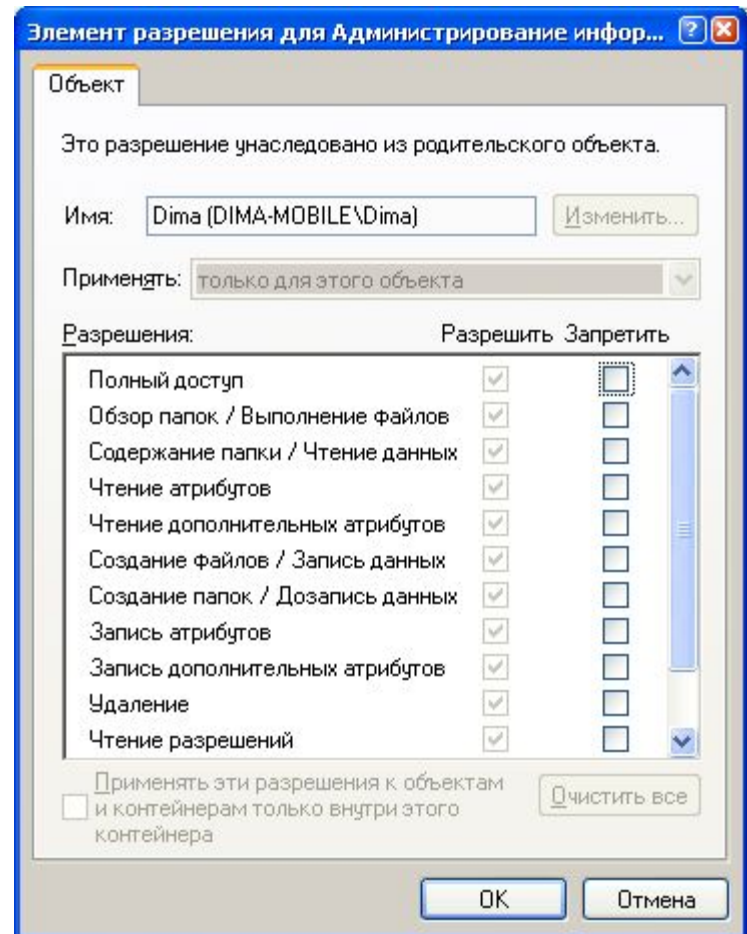
Безопасность

- При организации общего доступа к ресурсам компьютера вопросы безопасности имеют важное значение.
- Одним из средств обеспечения требуемой информационной безопасности являются NTFS разрешения и разрешения для общих папок.
- Для установки разрешений к объектам используются списки прав доступа (ACL – access control list).



Безопасность

- Используя кнопку **Дополнительно** можно установить разрешения и запреты на доступ более детально.
- Возможности ограничения доступа к объектам Windows в полной мере возможны при использовании файловой системы NTFS.





Безопасность

- Управление доступом на разделах NTFS доступно и из командной строки.
- Команда **CACLS** может быть использована для просмотра и изменения списков контроля доступа.
 - **Синтаксис**
 - **CACLS** имяФайла [/T] [/E] [/C] [/G имя:доступ] [/R имя [...]] [/P имя:доступ [...]] [/D имя [...]]
 - имяФайла Вывод таблиц управления доступом.
 - /T Замена таблиц управления доступом для указанных файлов в текущем каталоге и всех подкаталогах.
 - /E Изменение таблицы управления доступом вместо ее замены.
 - /C Продолжение при ошибках отказа в доступе.
 - /G имя:доступ Определение разрешений для указанных пользователей.
 - "доступ": R Чтение
 - W Запись
 - C Изменение (запись)
 - F Полный доступ
 - /R имя Отзыв разрешений для пользователя (только вместе с /E).
 - /P имя:доступ Замена разрешений для указанного пользователя.
 - "доступ": N Отсутствует
 - R Чтение
 - W Запись
 - C Изменение (запись)
 - F Полный доступ
 - /D имя Запрет на доступ для указанного пользователя.

Разрешения для сетевых ресурсов

- Для установки разрешений сетевых ресурсов используется соответствующий пункт контекстного меню. Окно для управления имеет вид:
- Вариантами общего доступа являются:
 - Полный доступ
 - Изменение
 - Чтение

