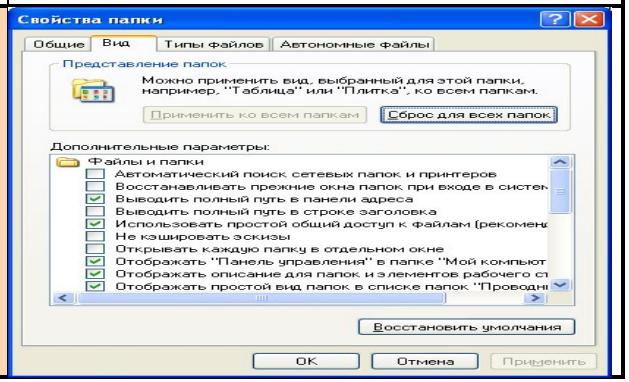
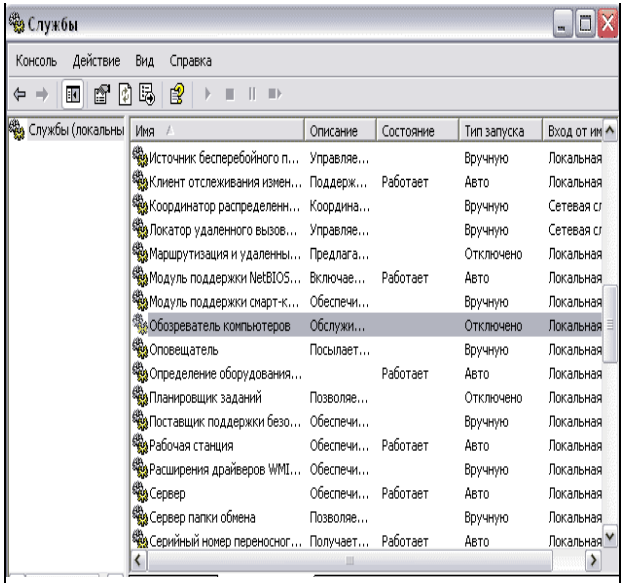
| ВОПРОС | ОТВЕТ | ИЛЛЮСТРАЦИЯ |
|---|---|---|
| ***Как сделать доступ к общим ресурсам (для ГОСТЯ)*** | 0. Убедись, что включена учетная запись Guest Правой кнопкой мышки на папке - меню Properties 1. Выбери вкладку Sharing, убедись что выбрана опция Share this folder, Share name: *** 2. Кнопка Permissions на вкладке Sharing, убедись, что для Everyone как минимум стоит разрешение на чтение (Read) 3. Вкладка Security, убедись что в верхнем списке (Group or user names) есть имя учетной записи Guest, если нет, то кнопка Add.. -> Advanced.. -> Find Now из списка выбери Guest, нажми Ok, и еще раз Ok 4. Выбери запись Guest на вкладке Security (см. в п. 3 как добавить) и убедись, что у этого пользователя есть как минимум право на чтение (Read) После этого нажми должно работать. Примечание: если у диалога Properties нет вкладки Security, то открой Explorer, меню Tools->Folder Options... Вкладка View. Убедись, что галочка "Use simple file sharing (Recommended)" не установлена. | |
| ***Нет доступа на комп вообще, через: сетевое окружение - рабочая группа - виден мой комп, но зайти на него нельзя (для ГОСТЯ)*** | На компе на который требуется зайти, включил пользователя "Гость" и в групповой политике ("Пуск" >> "Выполнить" >> "**gpedit.msc**" (ОТКРЫТИЕ ГРУППОВОЙ ПОЛИТИКИ) >> "Конфигурация компьютера" >> "Конфигурация Windows" >> "Параметры безопасности" >> "Локальные политики" >> "Назначение прав пользователя") из политики "Отказ в доступе к компьютеру из сети" удалить **"Гость"**. После этого доступ к компьютеру восстановился. | |
| ***Гостевой доступ*** | Это доступ для пользователя «Гость». Запомните, что пользователем «Гость» считается любой пользователь который не найден в базе пользователей данного компьютера и что он входит в группу «Все» Чтобы обеспечить подобный доступ необходимо: - разблокировать пользователя «Гость» (по-умолчанию в 2000 и XP он заблокирован) - задать этому пользователю пустой пароль<br>Конфигурация компьютера – Конфигурация Windows – параметры безопасности – локальные политики - назначение прав пользователя – Отказ в доступе к компьютеру по сети - проверить что группа «Все» присутствует в локальной политике XP (2000) в разделе. Плюсом данного метода можно считать только простоту реализации. К недостаткам относится снижение уровня безопасности сети | |
| ***Доступ пользователей по сети*** | Сначала необходимо ввести на компьютере учетную запись для соответствующего пользователя. Имя и пароль этого пользователя должны совпадать с именем и паролем под которыми он залогинился на своем компьютере. Включить этого пользователя в одну из локальных групп своего компьютера (это не обязательное, но желательное условие – выдавать права доступа не лично пользователю, а группе, в которую он входит). Далее, как и в случае с «Гость», надо проверить параметры политики Отказ в доступе к компьютеру по сети и Доступ к компьютеру по сети. Для предоставления доступа к ресурсам XP необходимо дополнительно отключить Simple Files Sharing. Так же обратите внимание что в политике Windows XP есть параметр "Сетевой доступ: модель совместного доступа и безопасности..." с двумя режимами Обычная и Гостевая | |
| ***Все сделал (см.выше) на XP, а по сети не пускает (этот же пользователь может зайти локально)*** | Проверить параметры политики Отказ в доступе к компьютеру по сети и Доступ к компьютеру по сети. Если пароль у пользователя пустой – изменить параметр политики: Конфигурация компьютера – Конфигурация Windows – параметры безопасности - локальные политики - параметры безопасности - Ограничить использование пустого пароля только для консольного входа | |

| | | |
|---|---|---|
| ***Пользователь на XP (2000) есть, но все равно требует ввести пароль (пишет «Отказ в доступе»)*** | Имя пользователя совпадает, а пароль нет. Синхронизируйте пароли (сделайте их одинаковыми) и проверьте не стоит ли «галочка» в «запомнить пароль» на компьютере с которого подключается ресурс. Вполне возможно, что там хранится старый пароль | |
| ***Как разграничить доступ к ресурсам по паролю (Windows XP)? Одному и тому же пользователю надо предоставить чтение к одной папке на сервере и полный доступ на другую (т.е. сделать как было в Windows 9x)*** | По паролям это не сделать. Подобные права регулируются либо правами на общий ресурс («на шару») либо правами на NTFS на сервере. | |
| ***Как сделать доступ с компьютера Windows 9x к ресурсам XP и 2000?*** | на компьютере с Windows 9x : - выбрать «вход в сеть Microsoft», ввести имя и пароль пользователя, существующего на XP/2000 (либо на компьютере XP/2000 разрешить гостевой доступ) | |
| ***Ещё раз о доступе к расшаренным рессурсам*** | Доступ к расшаренным ресурсам в WinNT-based системах осуществляется по имени пользователя и паролю. Для того, чтобы пользователь с удаленного компа мог посмотреть содержимое расшаренной папки, он должен ввести в ответ на запрос о пользователе имя и пароль пользователя, ЗАРЕГИСТРИРОВАННОГО на машине, к которой он коннектится. Именно этому пользователю можно назначать конкретные права на доступ к шаре. Если имя пользователя и пароль юзверя на удаленной машине совпадает с именем пользователя и паролем юзверя, зарегистрированного на локальной машине, то доступ дается сразу без запроса пароля (это верно для рабочих групп, для домена немного другая ситуация). В Windows XP введено новшество в Local Security Policy - теперь она может иметь 2 режима аутенификации - 1- любой пользователь может рассматриваться ей как Guest, и 2- классическая схема аутенификации, когда система сравнивает данные о пользователе удаленного компа с информацией своей базы данных и уже на основании сделанных выводов предоставляет доступ или нет. Меняется режим аутенификации таким образом: Control Panel-Administrative Tools - Local Security Policy - Local Policies - Security Options - параметр Network Access: Sharing and Security Model for local accounts. После изменения этого параметра либо перезагрузка, либо в командной строке пишешь: gpupdate /force | |
| ***Как задействовать процессор на сетевой карте (для ускорения работы по сети)*** | На многих современных сетевых картах имеется процессор, призванный разгрузить центральный процессор системы при работе с сетью. Но по умолчанию он не задействован. Чтобы включить его в Windows 2000/XP, надо в разделе реестра: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters, создать dword-параметр "DisableTaskOffload" и присвоить ему значение 0. | |

| | | |
|---|---|---|
| ***Простой способ настройки Windows 2000/XP для работы ноутбука в другой сети*** | Если ноутбук используется в различных сетях (например, дома и на работе), вам, вероятно, приходится всякий раз перенастраивать сетевые установки. Утилита Netsh позволяет сохранить настройки в файл, который впоследствии может быть использован для восстановления изменённых настроек. Чтобы сохранить текущие настройки, наберите команду: netsh -c interface dump > networksetting.txt. Чтобы восстановить настройки, выполните команду: netsh -f networksetting.txt. Используя Netsh, можно с лёгкостью переключаться между различными сетевыми настройками для нормальной работы в меняющихся условиях. | |
| ***Проблемы с сетью у компьютеров с Windows 98 при подключении к сети компьютера с Windows XP*** | После подключения компьютера с Windows XP локальная сеть может "подвешиваться" — на рабочих станциях с Windows 98 может перестать работать сетевое окружение. Наиболее вероятная причина — операционная система Windows XP пытается управлять всей сетью. Для начала попробуйте поставить на эту машину протокол NetBEUI (если он не был установлен). Для этого найдите на компакт-диске с дистрибутивом Windows XP папку Valueadd\Msft\Net\Netbeui и скопируйте из неё два файла: nbf.sys в папку %SystemRoot%\System32\Drivers и netnbf.inf в папку %SystemRoot%\Inf. После этого откройте Свойства сети и установите протокол NetBEUI. Если этот протокол не поможет — измените в системном реестре параметры, отвечающие за сетевые "амбиции" Windows XP. В разделе реестра: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Browser\Parameters строковому параметру "IsDomainMaster" присвойте значение "FALSE", а строковому параметру "MaintainServerList" — значение "No". | |
| ***Ускорение просмотра сетевых ресурсов локальной сети в Windows 2000/XP*** | Просмотр сетевых ресурсов в сетевом окружении может происходить очень медленно, так как Windows 2000/XP предварительно проверяет назначенные задания и принтеры на компьютере, к которому происходит подключение. Откройте раздел реестра: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RemoteComputer\NameSpace Для запрета проверки назначенных заданий удалите подраздел: {D6277990-4C6A-11CF-8D87-00AA0060F5BF} Для запрета проверки принтеров и факсов удалите подраздел: {2227A280-3AEA-1069-A2DE-08002B30309D} | |
| ***Как отменить автоматический поиск сетевых папок и принтеров? (для ускорения работы сети)*** | Панель управления - Свойства папки - Убарать "Автоматический поиск сетевых папок и принтеров" |  |

| | | |
|---|---|---|
| ***Периодическая недоступность сетевого окружения для всех пользователей сети, а если это большая сеть, то приводит к увеличению трафика*** | Щелкните по службе Обозреватель компьютеров два раза. Откроется окно управления службой. В нем сначала нажмите кнопку Стоп, а затем, из списка Тип запуска выберите Отключено. Теперь служба Обозреватель компьютеров стартовать не будет, а эта машина не будет претендовать на роль мастер-браузера в сети. Если Вы включили общий доступ и доустановили компоненту, то нужно определиться с одной немаловажной настройкой, о которой многие забывают и неверная настройка которой ведет к периодической недоступностью сетевого окружения для всех пользователей сети, а если это большая сеть, то приводит к увеличению трафика. Эта настройка - мастер-браузер (master browser) в сети. В каждой ОС есть настройка, которая запрещает, разрешает или предоставляет решение вопроса о возможности стать мастер-броузером в сети операционной системе. Если эта настройка включена, то после загрузки ОС попытается стать мастер-браузером, что может вызвать проблемы с отображением содержимого сетевого окружения на других машинах в сети. Мастер-браузером должна быть только одна машина в сети. Желательно, чтобы эта машина включалась раньше всех других, а выключалась последней (или вообще не выключалась). Так же, желательно, чтобы на этой машине была установлена самая старшая ОС семейства Windows.<br>Если машина, входящая в сеть, является потенциальным мастер-браузером, то она попытается отобрать у текущего мастер-браузера его функции. Это у нее может получится, а может и нет. Это зависит от многих причин. В любом случае, такие ситуации крайне нежелательны и поэтому в сети должна присутствовать только одна машина, которая может становится мастер браузером. |  |
| ***Подключение к Windows XP по сети без пароля*** | Windows XP разрешает локальным пользователям не иметь пароля и без проблем пускает таких пользователей в систему. Но при попытке подключиться по сети, как правило, выдаётся "Unknown error 31", если пароль отсутствует. Если вы точно уверены, что хотите подключаться по сети без пароля, то - запустите gpedit.msc (групповая политика); - перейдите в раздел Конфигурация компьютера (Computer Configuration) - Конфигурация Windows (Windows Settings) - Параметры безопасности (Security Settings) - Локальные политики (Local Policies) - Параметры безопасности (Security Options); - сделайте двойной щелчок мышью на параметре "Учётные записи: ограничить<br>использование пустых паролей только для консольного входа" (Accounts: Limit local account use of blank passwords to console login only) и отключите эту опцию. | |
| | | Для решения проблемы следует увеличить значение параметра реестра **IRPStackSize**.<br>1. Нажмите кнопку **Пуск** и выберите команду **Выполнить**.<br>2. Введите команду regedit и нажмите кнопку **ОК**.<br>3. Найдите следующий раздел:<br>**HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters** |

| | | |
|---|---|---|
| ***<u>Компьютеры видны, но попасть на диск невозможно - недоступны общие рессурсы.</u> " Неудалось выполнить сопоставление сетевого диска из-за следующей ошибки: Недостаточно памяти сервера для обработки команды. "*** | В просмотре событий - система --> возникает ошибка В конфигурации сервера параметр "irpstacksize" имеет слишком малое значение для использования локального устройства сервером. Увеличьте значение данного параметра. ПРИЧИНА в **Acronis**-е, который был установлен перед этим. Метод решения - удалить Acronis True Image, либо поэкспериментировать с параметром "irpstacksize" в реестре. | 4. В правой области окна редактора реестра дважды щелкните параметр **IRPStackSize**.<br><br>**Примечание.** Если параметр **IRPStackSize** отсутствует, создайте его, выполнив следующие действия:<br><br>a. В папке реестра Parameters дважды щелкните в правой области окна редактора реестра.<br>b. Подведите курсор к пункту **Создать** и щелкните пункт **Параметр DWord**.<br>c. Введите IRPStackSize.<br><br>**Внимание!** Имя параметра «IRPStackSize» вводится с учетом регистра.<br>Для параметра «Система исчисления» выберите значение «Десятичная».<br>В поле «Значение» введите значение, превышающее текущее.<br><br>Если параметр **IRPStackSize** был создан в результате действий, описанных в пункте 4, значением по умолчанию будет 15. Рекомендуется увеличить значение на 3. Таким образом, если предыдущим значением было 11, введите **14** и нажмите кнопку «ОК».<br>Закройте редактор реестра.<br>Перезагрузите компьютер. |
| ***Как определить свой внешний IP адрес в интернете?*** | Запускаете браузер, набираете в адресной строке адрес сайта и вы в сети. Чтобы удалённо с интернета просматривать свою интернет-камеру вы должны знать свой внешний IP-адрес (т.е. IP-адрес вашего модема), узнать его можно двумя способами. Первый-в браузере набираете **http://www.leader.ru**. Когда сайт загрузится щёлкаете на картинке Шерлок Холмс. Найденный адрес-это и есть ваш внешний IP-адрес. ИЛИ через **http://internet.yandex.ru/** (позволяет также изменрить скорость работы в интернете) ИЛИ **http://2ip.ru/** | |
| ***Тормозит компьютер из-за забивки кеша очереди печати (файл spoolsv.exe - диспетчер очереди печати) - загружает систему ~98%.*** | Нужно очистить очередь печати принтеров, в том числе принтера, который автоматически создаётся при установки MS Office - Microsoft Office Document Image Writer | |

| | | |
|---|---|---|
| ***IP адреса, используемые в локальной сети*** | При подключении пользовательского компьютера к Интернету, IP-адреса выбираются из диапазона, предоставленного провайдером. Компьютеры, не имеющие IP-адреса, выданного провайдером, могут (при правильной настройке маршрутизации[1]) работать с другими локальными компьютерами, имея IP-адреса из диапазонов, зарезервированных для локальных сетей: 10.0.0.0 — 10.255.255.255 (одна сеть класса A или 16777216 хостов) 172.16.0.0 — 172.31.255.255 (шестнадцать сетей класса B или 1048576 хостов ) 192.168.0.0 — 192.168.255.255 (256 сетей класса C или 65536 хостов) Компьютеры с такими адресами могут получать доступ к Интернету посредством **прокси-серверов** или **NAT**. Иногда в компьютерном сленге адреса из указанных диапазонов для локальных сетей называются серыми или плю́шевыми IP. | |
| ***Маска сети*** | Маской подсети или маской сети называется битовая маска, определяющая, какая часть IP-адреса узла сети относится к адресу сети, а какая — к адресу самого узла в этой сети. Например, узел с IP-адресом 12.34.56.78 и маской подсети 255.255.0.0 находится в сети 12.34.0.0. Чтобы получить адрес сети, зная IP-адрес и маску подсети, необходимо применить к ним операцию поразрядной конъюнкции (логическое И). Маска сети - фактически размер сети, задает число адресов в се- ти. в десятично-побайтной записи, например:<br>255.255.255.192 - маска на 64 адреса<br>255.255.255.0 - маска на 256 адресов<br>255.255.0.0 - маска на 64Kb адресов<br>Кол-во адресов хостов в подсети:<br>Это набор IP-адресов, которые могут быть выданы хостам. Чтобы подсчитать количество адресов, нужно от общего количества адресов подсети отнять два адреса, т.к. при обмене пакетами между хостами в одной подсети маршрутизатор и шлюз не нужны. В двоичном виде маска подсети всегда(!) как правило представляет собой единицы идущие подряд слева направо. Т.е. масок вида 11111111.11111111.11111111.11001100 не бывает. При таком разбиении существует всего 8 возможных окончаний для масок в сетях класса “C”. http://www.ispreview.ru/ipcalc.html (калькулятор сетей) | |
| ***Основные сетевые команды, выполняемые через командную строку*** | **ping** IP адрес --- выполняет "проверку связи" с компьютером с указанным IP-адресом **ipconfig** --- выводит информацию о сетевых соединениях. Если через пробел дописать параметр **/all**, будет более подробная информация. **tracert адрес** --- выполняет "проверку связи" с компьютером с указанным IP-адресом и выводит маршрут, по которому идёт запрос, то есть список узлов, через которые идёт сетевой пакет. **route print** --- выводит таблицу сетевых маршрутов. | |
| ***Почему в сети часто невозможно установить соединение с ICQ (если не принимать во внимание firewall)*** | При работе через gprs/edge/cdma часто невозможно установить соединение с ICQ **из-за превышения числа одновременных соединений с сервером ICQ с одного IP адреса, так как все пользователи работающие через сотовых операторов, используют небольшое число IP адресов через NAT сотового оператора** и число одновременных соединений с одного IP адреса слишком велико. | |
| ***После подключения компьютера с XP сеть "подвешивается" - на рабочих станциях с Windows 98 не работает сетевое окружение...*** | Наиболее вероятная причина - операционная система пытается управлять всей сетью. Для начала попробуйте поставить на эту машину протокол **NetBEUI** (если он не был установлен), а затем - если не поможет - измените в системном реестре параметры, отвечающие за "амбиции" операционной системы:<br>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Browser\Parameters<br>IsDomainMaster = FALSE<br>MaintainServerList = No | |

| | | |
|---|---|---|
| ***Как в Windows XP установить протокол NetBEUI?*** | Найдите на компакт-диске с дистрибутивом Windows XP папку Valueadd\Msft\Net\Netbeui и скопируйте из нее два файла: **nbf.sys** в папку %SystemRoot%\System32\Drivers и **netnbf.inf** в папку % SystemRoot %\Inf. После этого откройте Свойства сети и установите протокол NetBEUI. | |
| ***Можно ли полностью отключить скрытые общие ресурсы (ADMIN$, C$ и т.д.)?*** | Эти ресурсы в Windows XP (как и в W2K) существуют по умолчанию (доступ к ним возможен только из под эккаунта администратора), причем, если удалить эти ресурсы через "Управление компьютером" (Computer Management) -> "Общие папки", то после перезагрузки они появятся снова, и полностью отключить их можно только с помощью внесения изменений в реестр.<br>Открываем :<br>HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters<br>и измененим (или добавляем) следующий параметр:<br>AutoShareWks (его тип - REG_DWORD) значение 0 | |
| ***В чём разница между доступом в Интернет посредством NAT сервера и Proxy сервера*** | Обычно для подключения локальной сети к Интернету через Интернет шлюз используется один или несколько внешних IP-адресов, а компьютерам локальной сети присваиваются внутренние IP-адреса.<br><br>Существует несколько причин такого способа подключения:<br><br>Ограниченное количество реальных IP-адресов. За каждый IP-адрес необходимо оплачивать аренду у провайдера;<br>Нет проблем при расширении локальной сети. С появлением необходимости присвоить новым компьютерам IP-адреса, нет надобности обращаться за выделением дополнительных внешних IP-адресов;<br><br>Надежная защита компьютеров в локальной сети от внешних атак. Компьютеры с внутренними IP-адресами недоступны напрямую из внешней сети.<br><br>**Для подключения локальной сети к Интернет существует несколько способов. Самые популярные из которых - использование в качестве Интернет шлюза proxy сервера и NAT сервера. Proxy сервер работает на уровне приложений, а драйвер NAT - на уровне стека протоколов TCP/IP.**<br><br>Главные минусы использования proxy сервера - необходимость настройки каждого клиентского приложения, несовместимость некоторых приложений с работой через proxy сервер (например, банковские программы, игры), очень низкая производительность и высокое потребление системных ресурсов Интернет сервера.<br><br>Использование NAT обеспечивает прозрачность для приложений - их не нужно настраивать, с NAT работают практически все протоколы и приложения. Поскольку NAT представляет собой низкоуровневый сетевой драйвер, то его производительность по сравнению с proxy серверами выше в несколько раз. Соотвтетственно выше скорость работы Интернет сервера.<br><br>Для построения локальных сетей необходимо использовать специально определенные в **RFC 1918** группы приватных IP-адресов:<br><br>Для сетей класса A: 10.0.0.0-10.255.255.255 | |

Для сетей класса B: 172.16.0.0-172.31.255.255
Для сетей класса C: 192.168.0.0-192.168.255.255

Иногда диапазоны этих IP-адресов также называют частные или *серые IP-адреса* . Внешние реальные адреса имеют название *белые IP-адреса* . Таким образом, компьютерам локальной сети могут назначаться IP-адреса из указанных диапазонов. Однако, непосредственный доступ в Интернет из таких сетей невозможен.

Для подключения всей локальной сети достаточно иметь единственный узел с доступом в Интернет, имеющий уникальный *белый IP-адрес* . Такой узел называется **Интернет шлюзом** или **Интернет сервером**. Интернет шлюз должен иметь, как минимум, два сетевых адаптера. Один из которых обеспечивает доступ в Интернет. Этому внешнему адаптеру присвоен *белый IP-адрес* . Внутренним адаптерам могут быть присвоены как *белые* , так и *серые IP-адреса* .

При прохождении сетевых пакетов через Интернет сервер, с внутреннего адаптера на внешний и обратно, происходит трансляция сетевых адресов (NAT). Такой механизм обеспечивает прозрачный доступ в Интернет для узлов с *серыми IP-адресами* . Кроме того, все соединения после шлюза выглядят так, как если бы они были установлены с единственного *белого IP-адреса* . Тем самым обеспечивается сокрытие конфиденциальной информации о локальной сети.

## Принцип работы NAT

Трансляция сетевых адресов выполняется в процессе контроля транзитных соединений на Интернет сервере. Когда пакет IP-соединения с *серым IP-адресом* источника передается драйвером внутреннего сетевого адаптера к драйверу стека TCP/IP, сетевой драйвер Lan2net NAT Firewall перехватывает пакет, изменяя в нем IP-адрес источника и номер порта источника для протоколов UDP и TCP. Для пакетов протокола ICMP модифицируется идентификатор запроса. После модификации пакета он передается драйверу внешнего сетевого адаптера Интернет шлюза и далее отсылается необходимому узлу в Интернет.

При передаче в сеть Интернет пакет выглядит так, как будто, он отправлен с белого внешнего IP-адреса. Тем самым обеспечивается уникальность IP-адреса источника соединения в рамках всей сети Интернет.

Получив ответные пакеты, драйвер внешнего сетевого адаптера передает их драйверу стека TCP/IP. В этот момент пакеты перехватываются драйвером Lan2net NAT Firewall. Сетевой драйвер Lan2net NAT Firewall определяет принадлежность пакетов исходному IP-соединению. Так как при модификации номеров TCP-, UDP-портов или идентификатора ICMP-запроса в исходящих пакетах им были присвоены уникальные значения, то теперь на основе этих значений драйвер может восстановить оригинальный, *серый IP-адрес* источника запроса.

| | | |
|---|---|---|
| | Таким образом, в ответных пакетах IP-адрес назначения заменяется на IP-адрес источника запроса, а номера TCP-, UDP-портов или идентификатора ICMP-запроса также восстанавливают свои оригинальные значения. После этого ответные пакеты передаются драйверу TCP/IP и далее, через внутренний адаптер, к узлу, сделавшему запрос. | |
| ***Команда NETSTAT*** | **Netstat** – отображает активные подключения TCP, портов, прослушиваемых компьютером, статистики Ethernet, таблицы маршрутизации IP, статистики IPv4 (для протоколов IP, ICMP, TCP и UDP) и IPv6 (для протоколов IPv6, ICMPv6, TCP через IPv6 и UDP через IPv6). Запущенная без параметров, команда **nbtstat** отображает подключения TCP.<br>**netstat** [**-a**] [**-e**] [**-n**] [**-o**] [**-p** *протокол* ] [**-r**] [**-s**] [*интервал* ]<br><br>**Параметры команды Netstat**<br>**Netstat -a**<br>Вывод всех активных подключений TCP и прослушиваемых компьютером портов TCP и UDP.<br>**Netstat -e**<br>Вывод статистики Ethernet, например количества отправленных и принятых байтов и пакетов. Этот параметр может комбинироваться с ключом **-s**.<br>**Netstat -n**<br>Вывод активных подключений TCP с отображением адресов и номеров портов в числовом формате без попыток определения имен.<br>**Netstat -o**<br>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**.<br>**Netstat -p** *протокол*<br>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**.<br>**Netstat -s**<br><br>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.<br><br>**Netstat -r**<br>Вывод содержимого таблицы маршрутизации IP. Эта команда эквивалентна команде **route print**.<br>*интервал*<br><br>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. | |

**Netstat /?**
Отображение справки в командной строке.

## Примечания

Параметрам, используемым с данной командой, должен предшествовать дефис (**-**), а не косая черта (**/**).

Команда **Netstat** выводит статистику для следующих объектов.

Протокол
Имя протокола (TCP или UDP).

Локальные адреса

IP-адрес локального компьютера и номер используемого порта. Имя локального компьютера, соответствующее IP-адресу и имени порта, выводится только в том случае, если не указан параметр **-n**. Если порт не назначен, вместо номера порта будет выведена звездочка (*).

Внешние адреса

IP-адрес и номер порта удаленного компьютера, подключенного к данному сокету. Имена, соответствующие IP-адресу и порту, выводятся только в том случае, если не указан параметр **-n**. Если порт не назначен, вместо номера порта будет выведена звездочка (*).

(Состояние)

Указание состояния подключения TCP. Возможные значения:
CLOSE_WAIT
CLOSED
ESTABLISHED
FIN_WAIT_1
FIN_WAIT_2
LAST_ACK
LISTEN
SYN_RECEIVED
SYN_SEND
TIMED_WAIT

Эта команда доступна, только если в свойствах сетевого адаптера в объекте Сетевые подключения в качестве компонента установлен **протокол Интернета (TCP/IP)**.

## Примеры Netstat

Для вывода статистики Ethernet и статистики по всем протоколам введите следующую команду:
**netstat -e -s**

Для вывода статистики только по протоколам TCP и UDP введите следующую команду:

| | | |
|---|---|---|
| | **netstat -s -p tcp udp**<br>Для вывода активных подключений TCP и кодов процессов каждые 5 секунд введите следующую команду:<br>**nbtstat -o 5**<br>Для вывода активных подключений TCP и кодов процессов каждые с использованием числового формата введите следующую команду:<br>**nbtstat -n -o** | |