

ПРАКТИЧЕСКАЯ РАБОТА

Настройка сетевого доступа

Содержание: название, формулировка темы и цели, время выполнения, необходимое обеспечение, теоретическая часть, практическая часть, технология выполнения, описание заданий, рефлексия самоконтроля, контрольные вопросы

Время выполнения: 2 ч.

Материально-техническое обеспечение: персональный компьютер (системный блок, монитор, клавиатура, мышь)

Программное обеспечение: ОС Windows, интегрированная среда разработки, офисные программы Microsoft Office.

Учебно-методическое обеспечение: конспект лекций, описание работы, встроенная справочная система ОС Windows и сред разработки.

Порядок выполнения практической работы: изучить теоретический материал, выполнить задания, составить отчёт с выводами о проделанной работе, ответить на контрольные вопросы, сдать выполненную работу и отчёт.

Требования к отчёту: отчёт должен быть оформлен в соответствии с «ГОСТ 19.XXX ЕСПД».

Цель: приобретение навыков настройки сетевого доступа.

Теоретическая часть

Предназначение сети - организация доступа к ресурсам Интернет и/или другого компьютерам (жёсткие диски, принтеры, файлы, папки и т. д.).

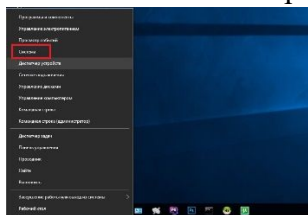
Практическая часть

Настройка сетевого доступа Windows 10

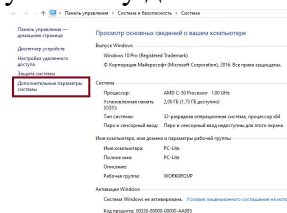
Сетевая карта, которой оснащен каждый компьютер, способна предоставлять пользователю доступ в глобальную и локальную сеть. Настройки следует провести на всех компьютерах, которые вы хотите подключить по локальной сети, а не на одном. Настройка сетевого доступа для Ethernet-кабеля и маршрутизатора отличаются.

- Настройка сетевого доступа через Ethernet-кабель

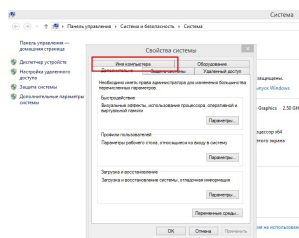
Нажмите на сочетание кнопок «Win+X» и выберите меню «Система». Также данное контекстное меню вы можете открыть с помощью нажатия правой клавиши мыши на меню «Пуск».



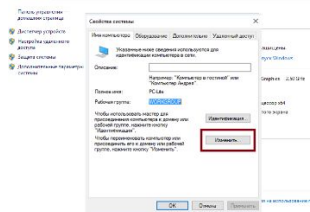
Нажимаем на сочетание кнопок «Win+X» и выбираем меню «Система». Перейдите в меню, отвечающее за установку дополнительных параметров. Оно находится слева.



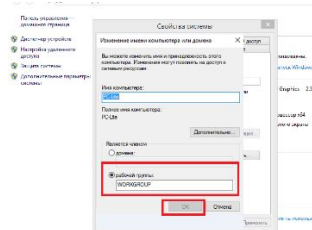
Зайдите во вкладку «Имя компьютера».



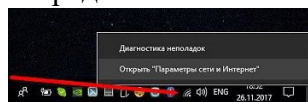
Кликните на кнопку «Изменить...».



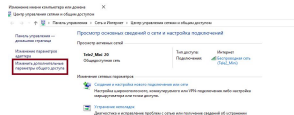
Теперь будьте внимательны. Имя рабочей группы должны совпадать на всех устройствах, а имя компьютера - отличаться. Не перепутайте. После переименования нажмите «ОК».



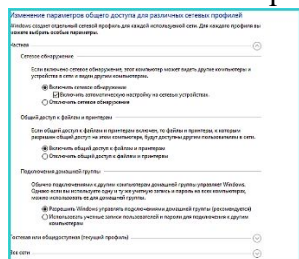
Следующий этап - это настройки сетевого обнаружения. Наведите курсор мыши на иконку сети (она находится на панели задач), щелкните правым кликом мыши, затем левым по опции «Открыть параметры сети и Интернет». Раньше это меню называлось «Центр управления сетями и общим доступом», но после очередного обновления Windows 10 название изменилось.



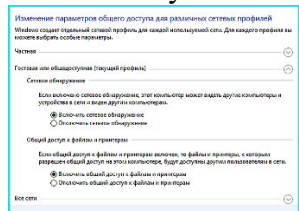
Выберите меню, отвечающее за установку дополнительных сетевых параметров.



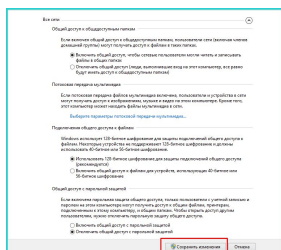
Откроется окно с глобальными настройками для разных видов сети. Произведите настройки таким образом, чтобы они соответствовали скриншотам ниже. Их много, поэтому проявите внимательность, чтобы ничего не перепутать.



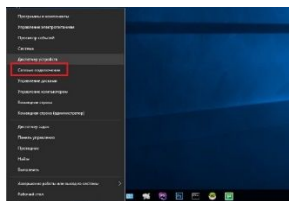
Отмечаем пункты:



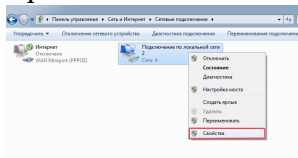
После проделанных настроек нажмите на «Сохранить изменения» и закройте данное окно.



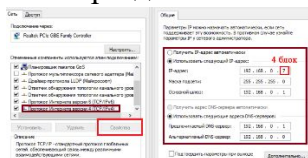
Вновь нажмите клавиши «Win+X», только на этот раз выберите «Сетевые подключения».



Правым кликом мыши выберите ваше подключение и запустите меню «Свойства».



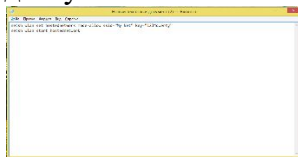
Выберите четвёртую версию интернет-протокола, кликните на «Свойства» и задайте настройки, как на скриншоте. Обратите внимание, что цифра в последнем блоке IP-адреса должна отличаться у каждого компьютера. Каждый IP-адрес делится на 4 блока, а в каждом блоке указывается значение от 0 до 255. Эти блоки разделены точкой.



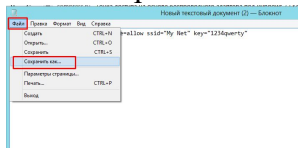
После проведения всех установок вы успешно создадите локальную сеть между несколькими компьютерами и сможете пользоваться всеми её возможностями.

• Настройка сетевого доступа через маршрутизатор

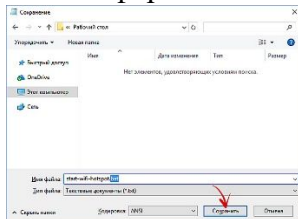
Многие пользователи предпочитают использовать роутер (он же маршрутизатор), так как он удобнее и безопаснее, особенно для ноутбука (если часто переносить ноутбук, то можно повредить вставленный в него кабель, а маршрутизатор никуда переносить не нужно). Откройте блокнот или любой другой текстовый редактор, затем впишите туда текст, который показан на скриншоте ниже (скопировать его можно [здесь](#)). В качестве параметра «ssid» введите имя вашей сети, а в качестве «пароль» - пароль для доступа к ней. Оба этих параметра нужно указывать без кавычек.



Затем сохраните текстовый файл, нажав на «Файл» и «Сохранить как».



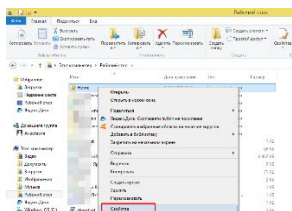
Вместо формата «.txt» укажите «.bat» и нажмите «Сохранить».



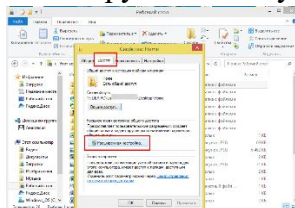
Для этого вам нужно всего лишь открыть созданный вами файл двойным кликом мыши. Делать это нужно каждый раз после включения компьютера или ноутбука. Это гораздо удобнее, чем каждый раз вручную вводить эти команды в консоль.



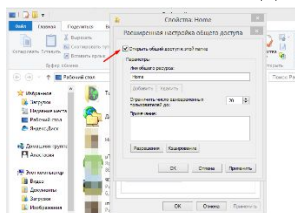
Следующий этап - настройка доступа. Вы можете предоставить доступ как ко всему диску, так и к отдельным директориям. Правым кликом мыши щелкните на отдельной папке (или диске) и нажмите на «Свойства».



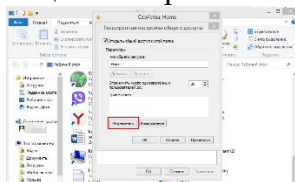
Активируйте вкладку «Доступ» и перейдите в меню «Расширенная настройка».



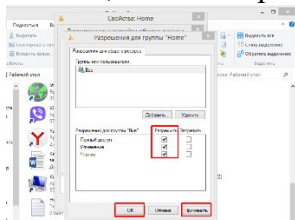
Затем поставьте галочку напротив параметра, отвечающего за предоставление доступа. Т. о., выбранная вами папка станет доступна для всех компьютеров, соединённых сетью.



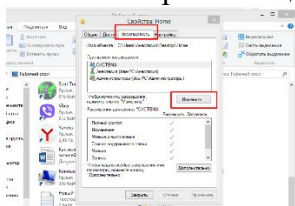
Теперь вы можете настроить доступ к отдельным операциям с папкой. Чтобы сделать это, нажмите на опцию «Разрешения».



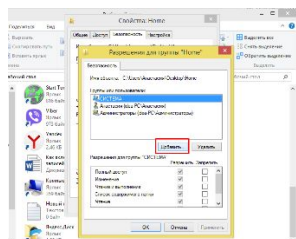
Расставьте галочки, чтобы разрешить или запретить какую-то операцию, нажмите на опции «Применить» и «ОК», чтобы сохранить настройки.



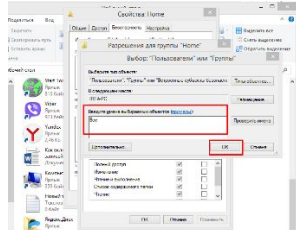
Следующий шаг, который вам нужно предпринять - это настройки безопасности. Для этого в окне свойств папки выберите вкладку «Безопасность» и нажмите на кнопку «Изменить».



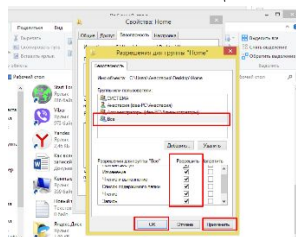
Теперь кликните на «Добавить...».



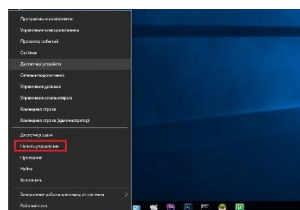
Введите в поле ввода имени «Все» и нажмите «ОК». После этого появится новая группа.



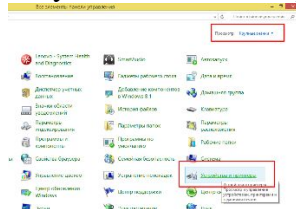
Выберите только что созданную группу и установите галочки возле нужных вам параметров, затем нажмите по опциям «Применить» и «ОК». После всех проделанных изменений перезагрузите компьютер.



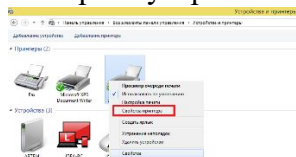
Если вы провели настройки, которые описаны выше, вы можете легко добавить в локальную сеть новое устройство для общего доступа. Откройте «Панель управления». Сделать это можно с помощью того же контекстного меню, которое вызывается посредством нажатия на «Win+X».



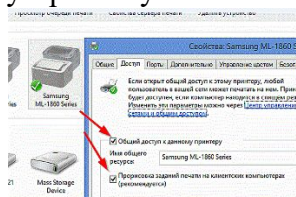
Запустите меню «Устройства и принтеры», выбрав в режиме «Просмотр» значение «Крупные значки».



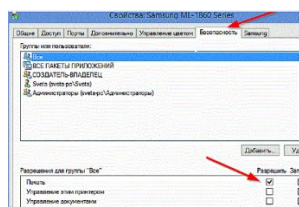
Выберите устройство из списка правым кликом мыши, затем щелкните по строке «Свойства принтера».



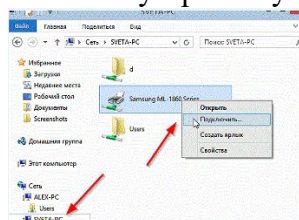
Перейдите во вкладку «Доступ» и активируйте параметр, отвечающий за предоставление общего доступа к устройству.



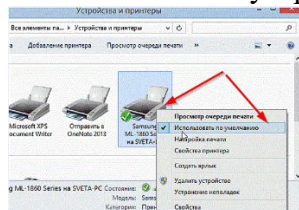
Теперь откройте вкладку «Безопасность» и в нижнем блоке расставьте галочки напротив тех операций, к которым хотите дать доступ другим компьютерам.



Чтобы подключить устройство, выберите его в проводнике, в перечне «Сеть», кликните правой кнопкой мыши по устройству и нажмите «Подключить».



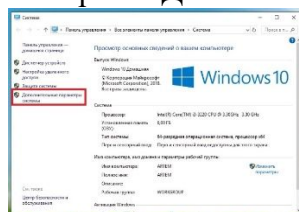
После подключения устройство будет отображаться в меню «Устройства и принтеры». Вам осталось лишь назначить его как устройство по умолчанию с помощью правой кнопки мыши.



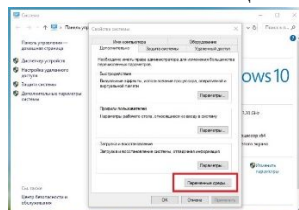
Для удаления локальной сети откройте окно свойств операционной системы. Сделать это можно либо с помощью нажатия правой кнопки мыши по ярлыку «Этот компьютер» и выбора, соответствующего меню, либо с помощью комбинации клавиш «Win+Pause», на ноутбуке необходимо добавить к сочетанию клавишу «Fn».



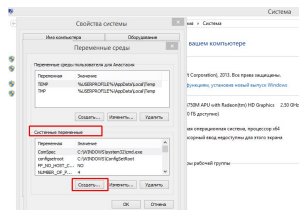
Выберите «Дополнительные параметры системы», а после - «Переменные среды...».



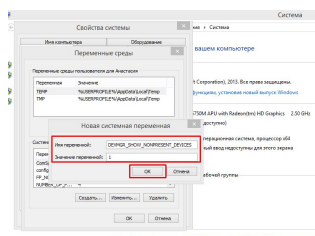
Нажимаем по опции «Переменные среды»



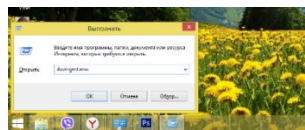
В нижней части второго блока, отвечающего за системные переменные, будет кнопка «Создать» - нажимайте её.



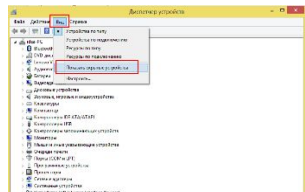
Задайте имя переменной «DEVMGR_SHOW_NONPRESENT_DEVICES» и укажите её значение «1», после чего подтвердите изменения нажатием по кнопке «ОК». После создания переменной в диспетчере устройств будут отображаться скрытые устройства.



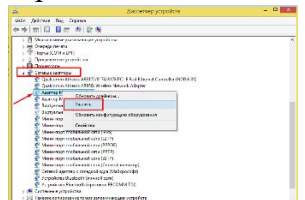
Перейдите в «Диспетчер устройств». Для этого нажмите «Win+R», введите «devmgmt.msc» и кликните «ОК».



Нажмите на «Вид» и активируйте параметр показа скрытых устройств.



После этого в сетевых адаптерах будут отображены локальные сети. Вы можете отключать их или удалять через контекстное меню - оно вызывается нажатием правой кнопки мыши.



В разделе «Сетевые адаптеры» нажимаем по локальной сети правой кнопкой мыши, затем левой по опции «Удалить»

Настройка сетевого доступа через командную строку и bat-файл

Способ 1. Команда на смену IP адреса, маски подсети, шлюза по умолчанию и метрики интерфейса. "Подключение по локальной сети" меняем на название своего сетевого подключения. 192.168.0.100 - IP адрес, 255.255.255.0 - маска подсети, 192.168.0.1 - шлюз, единица (1) следующая за шлюзом (192.168.0.1) это метрика интерфейса.

```
netsh interface ip set address "Подключение по локальной сети" static 192.168.0.100 255.255.255.0 192.168.0.1 1
```

Команда на смену DNS серверов. Первая строчка кода меняет/прописывает предпочитаемый DNS сервер, а вторая строчка кода меняет/прописывает альтернативный DNS сервер.

```
netsh interface ip set dns "Подключение по локальной сети" static 192.168.0.2 primary
netsh interface ip add dns "Подключение по локальной сети" 192.168.0.3 index=2
```

Способ 2. Смена сетевых настроек через BAT файл. Создаем текстовый документ, открываем его, жмем кнопку "Файл", выбираем пункт "Сохранить как". Откроется окно сохранения файла. В меню "Тип файла" выбираем пункт "Все файлы" (по умолчанию будет стоять "Текстовый документ"), выбираем кодировку ANSI (если изменено на другое). Далее к названию файла дописываем ".bat", таким образом у вас должно получиться примерно такое название файла: "Текстовый документ.bat". Жмем кнопку "Сохранить". Далее можно изменить название файла на свое. Теперь жмем правой кнопкой мыши на bat файле и в меню выбираем пункт "Изменить". Вводим в окно следующие команды:

```
chcp 1251
netsh interface ip set address "Подключение по локальной сети" static 192.168.0.100 255.255.255.0 192.168.0.1 1
netsh interface ip set dns "Подключение по локальной сети" static 192.168.0.2 primary
netsh interface ip add dns "Подключение по локальной сети" 192.168.0.3 index=2
```

Команда "chcp 1251" устанавливает кодировку. Если этого не сделать, то через BAT файл нельзя будет сменить настройки на сетевом интерфейсе с названием, состоящим из русских символов. По умолчанию в командной строке используется точечный шрифт. В связи с этим вместо кириллицы будут отображаться "кракозябры". Для того, чтобы русский текст отображался правильно, нужно сделать следующее: в открытом окне командной строки нажмите правой кнопкой мыши на заголовке окна. Откроется меню - в

нем выберите пункт "Свойства". В открывшемся окне перейдите на вкладку "Шрифты" и выберите шрифт Lucida Console. Нажмите кнопку "ОК". Всё, теперь шрифты в командной строке будут отображаться нормально. При запуске данного пакетного файла вам будет предложено выбрать один из двух вариантов настройки - дом или работа. В примере кода меняем название сетевого подключения на своё, если оно отличное от по умолчанию, т.е. "Подключение по локальной сети". Так же меняем сетевые настройки - IP, маску, шлюз и DNS сервера. После смены сетевых настроек будет предложено посмотреть текущие сетевые настройки (команда ipconfig /all). Отвечаем да или нет в зависимости от того нужно вам это или нет.

```
@echo off
chcp 1251
set /p settings="Выберите настройки (1 - дом, 2 - работа):"
echo Выбраны настройки - %settings%

if %settings% equ 2 goto work

:home
set IFACE="Подключение по локальной сети"
set IP=172.30.0.100
set MASK=255.255.255.0
set GATEWAY=172.30.0.1
set GWMETRIC=1
set DNS1=172.30.0.2
set DNS2=172.30.0.3
goto dalee

:work
set IFACE="Подключение по локальной сети"
set IP=192.168.254.100
set MASK=255.255.255.0
set GATEWAY=192.168.254.1
set GWMETRIC=1
set DNS1=192.168.254.1
set DNS2=192.168.254.2

:dalee
echo Установлены настройки сети:
echo IP-адрес: %IP%
echo Маска подсети: %MASK%
echo Основной шлюз: %GATEWAY%

netsh interface ip set address %IFACE% static %IP% %MASK% %GATEWAY% %GWMETRIC%
echo Предпочитаемый DNS сервер: %DNS1%
netsh interface ip set dns %IFACE% static %DNS1% primary
echo Альтернативный DNS сервер: %DNS2%
netsh interface ip add dns %IFACE% %DNS2% index=2

set /p ipinfo="Показать настройки сети? (y - да, n - нет):"
echo Текущие настройки сети: %ipinfo%

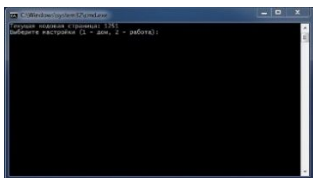
if %ipinfo% equ n goto ipdontshow

:ipshow
ipconfig /all
goto dalee2

:ipdontshow
echo Отмена показа настроек сети.

:dalee2
pause
```

Консольный вывод:



Работа с сетью в командной строке Windows (CMD)

Сетевые утилиты командной строки Windows: arp, ipconfig, getmac, nbtstat, netsh, netstat, netnslookup, pathping, ping, route, telnet, tracert.

ARP.EXE позволяет просматривать и изменять записи в кэш ARP (Address Resolution Protocol - протокол разрешения адресов), который представляет собой таблицу соответствия IP-адресов аппаратным адресам сетевых устройств.

arp -a - отобразить все записи таблицы ARP.
arp -a 192.168.0.9 - отобразить запись, соответствующую IP-адресу 192.168.0.9
arp -a 192.168.1.158 -N 192.168.1.1 - отобразить таблицу ARP для адреса 192.168.1.158 на сетевом интерфейсе 192.168.1.1
arp -a -N 10.164.250.148 - отобразить все записи таблицы ARP на сетевом интерфейсе 10.164.250.148 .
arp -s 192.168.0.1 00-22-15-15-88-15 - добавить в таблицу ARP статическую запись, задающую соответствие IP - адреса 192.168.0.1 и MAC-адреса 00-22-15-15-88-15
arp -s 192.168.0.1 00-22-15-15-88-15 192.168.0.56 - то же самое, что и в предыдущем случае, но с указанием сетевого интерфейса, для которого выполняется добавление статической записи.
arp -d 192.168.1.1 192.168.1.56 удаление записи из таблицы ARP для IP-адреса 192.168.1.1 на сетевом интерфейсе 192.168.1.56
arp -d * - полная очистка таблицы ARP. Аналогично - arp -d без параметров. Если имеется несколько сетевых интерфейсов, то очистка может быть выполнена только для одного из них - arp -d * 192.168.0.56.

IPCONFIG.EXE присутствует во всех версиях Windows. Некоторые параметры командной строки не поддерживаются в версиях, предшествующих Windows Vista/Windows 7. Команда IPCONFIG используется для отображения текущих настроек протокола TCP/IP и для обновления некоторых параметров, задаваемых при автоматическом конфигурировании сетевых интерфейсов при использовании протокола Dynamic Host Configuration Protocol (DHCP).

ipconfig - отобразить базовые сетевые настройки для всех сетевых адаптеров.
ipconfig /all - отобразить все сетевые настройки для всех сетевых адаптеров.
ipconfig /renew "Подключение по локальной сети 2" - обновить сетевые настройки, полученные от DHCP - сервера только для адаптера с именем " Подключение по локальной сети 2"
ipconfig /displaydns - вывести на экран содержимое кэш службы разрешения имен DNS
ipconfig /showclassid "Подключение по локальной сети" - отобразить все допустимые для этого адаптера идентификаторы классов DHCP.
ipconfig /setclassid "Local Area Connection" TEST - установить для адаптера с именем "Local Area Connection" идентификатор класса DHCP "TEST". Если идентификатор класса DHCP не указан, то он будет удален.

GETMAC.EXE присутствует в версиях Windows XP и старше. Используется для получения аппаратных адресов сетевых адаптеров (MAC-адресов) как на локальном, так и на удаленном компьютере.

GETMAC /? - отобразить краткую справку об использовании GETMAC
GETMAC /FO csv - выдать информации о MAC-адресах всех существующих на локальном компьютере сетевых адаптеров в формате CSV (полей с разделителями в виде запятой)
GETMAC /S COMPUTER /NH /V - получить MAC адреса сетевых адаптеров для удаленного компьютера COMPUTER, не отображать заголовки столбцов в таблице и использовать отображение подробной информации. Для подключения к удаленному компьютеру используется текущая учетная запись пользователя
GETMAC /S 192.168.1.1 /NH /V - то же самое, но вместо имени компьютера задан его IP-адрес
GETMAC /S COMPUTER /U user /P password - получить MAC - адрес адаптеров удаленного компьютера COMPUTER. Для подключения к нему используется имя пользователя "user" и пароль "password"
GETMAC /S COMPUTER /U mydomain\user - для подключения к удаленному компьютеру используется учетная запись пользователя "user" в домене "mydomain". Пароль пользователя вводится по запросу

```
GETMAC /S COMPUTER /U mydomain\user /P password - то же самое, что и в предыдущем случае, но пароль задан в командной строке
```

NBTSTAT.EXE позволяет получить статистику протокола NetBIOS over TCP/IP (NetBT), таблицу имен локальных и удаленных компьютеров и содержимое кэш NetBIOS имен. Применение NBTSTAT позволяет принудительно обновить кэш NetBIOS-имен компьютеров и имена, зарегистрированные с помощью серверов Windows Internet Name Service (WINS).

```
nbtstat -a SERVER - вывести список зарегистрированных NetBIOS-имен на компьютере SERVER.
```

```
nbtstat -A 192.168.1.1 - вывести список зарегистрированных NetBIOS-имен на удаленном компьютере с IP-адресом 192.168.1.1 .
```

```
nbtstat -RR - выполнить очистку и перерегистрацию NetBIOS-имен на локальном компьютере.
```

NETSH.EXE (NETwork SHell) - наиболее полное и функциональное стандартное средство управления сетью с использованием командной строки в среде Windows XP и старше. Набор внутренних команд сетевой оболочки пополняется с появлением новых версий операционной системы, что необходимо учитывать при работе в локальной сети с различными ОС.

Сохранить сетевую конфигурацию в файл:

```
netsh
set file open C:\mynet.sav
dump
quit
```

Восстановление сетевой конфигурации из файла:

```
netsh exec C:\mynet.sav
```

Иногда требуется выполнить некоторые команды на одном уровне, перейти на другой, и снова вернуться на предыдущий:

```
netsh> - приглашение первого уровня команды nesh
pushd - введена команда запоминания контекста в стек
netsh> - приглашении netsh не меняется, контекст прежний.
interface ipv4 - переход на уровень interface и уровень ipv4
netsh interface ipv4> - изменилась строка приглашения, отображая текущий контекст netsh
set address local static 192.168.1.9 255.255.255.0 192.168.1.1 1 - смена настроек IP протокола.
netsh interface ip> - выполнение команды, отображаемый в приглашении не изменяется.
popd - команда извлечения из стека запомненного контекста.
netsh > - строка приглашения изменилась, отображая текущий контекст выполнения netsh.
```

Настройка сетевых интерфейсов:

```
#=====
# Конфигурация интерфейса
#=====
pushd interface
reset all
popd
# Конец конфигурации интерфейса
# -----
# Настройка IP-интерфейсов
# -----
pushd interface ip
# Интерфейс настройки IP для "Подключение по локальной сети"
set address name=" Подключение по локальной сети " source=static addr=192.168.0.1 mask=255.255.255.0
set dns name="Подключение по локальной сети" source=static addr=192.168.0.2 mask=255.255.255.0
set wins name=" Подключение по локальной сети " source=static addr=192.168.0.9
```

Смена IP-адреса:

```
netsh interface ip set address name="Подключение по локальной сети" source=static addr=192.168.0.58 mask=255.255.255.0
```

Смена адреса DNS-сервера в настройках сетевого подключения "Подключение по локальной сети 2" на адрес публичного DNS-сервера Google в среде Windows:

```
netsh interface ipv4 set dnsservers name="Подключение по локальной сети 2" static 8.8.8.8 primary
```

Изменение адреса шлюза по умолчанию:

```
netsh interface ip set address name="Подключение по локальной сети" source=static addr=192.168.0.58 mask=255.255.255.0 gateway=192.168.0.1 gwmetric=1
```

NETSTAT.EXE присутствует во всех версиях Windows, однако, существуют некоторые отличия используемых параметров командной строки и результатов ее выполнения, в зависимости от операционной системы. Используется для отображения TCP и UDP -соединений, слушаемых портов, таблицы маршрутизации, статистических данных для различных протоколов.

```
netstat -a | more - отобразить все соединения в постраничном режиме вывода на экран
netstat -a > C:\netstatall.txt - отобразить все соединения с записью результатов в файл C:\netstatall.txt.
netstat -a | find /I "LISTENING" - отобразить все соединения со статусом LISTENING. Ключ /I в команде find указывает, что при поиске текста не нужно учитывать регистр символов.
netstat -a | find /I "listening" > C:\listening.txt - отобразить все соединения со статусом LISTENING с записью результатов в файл C:\listening.txt.
netstat -ab - параметры командной строки можно объединять. Параметр -ab эквивалентен -a -b
netstat -a -n -b - отобразить список всех соединений с числовыми номерами портов
netstat -anb - аналогично предыдущей команде.
netstat -anbv - при использовании параметра -v отображается последовательность компонентов, участвующих в создании соединения или слушаемого порта.
netstat -e - получить статистические данные для Ethernet. Отображаются суммарные значения принятых и полученных байт для всех сетевых адаптеров.
netstat -e -v - кроме суммарных статистических данных для Ethernet, отображается статистика для каждого сетевого интерфейса.
netstat -e -s - дополнительно к статистике Ethernet, отображается статистика для протоколов IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP и UDPv6
netstat -s - получить статистику по протоколам IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP и UDPv6
netstat -s -p udp - получить статистику только по протоколу UDP
netstat -s -p icmp - получить статистику только по протоколу ICMP
```

NET.EXE существует во всех версиях Windows и является одной из самых используемых в практической работе с сетевыми ресурсами. Позволяет подключать и отключать сетевые диски, запускать и останавливать системные службы, добавлять и удалять пользователей, управлять совместно используемыми ресурсами, устанавливать системное время, отображать статистические и справочные данные об использовании ресурсов и многое другое.

Работа с системными службами:

```
net help services - список служб, которыми можно управлять
net stop dnscache - остановить службу dnscache
net start dnscache - запустить службу dnscache
net stop "DNS-клиент" - остановить службу DNS-клиент
net pause "Планировщик заданий" - приостановить службу "Планировщик заданий"
net continue schedule - продолжить работу службы "Планировщик заданий". Полное имя службы можно скопировать из "Панель управления" - "Администрирование" - "Службы" - Имя службы - "Свойства" - "Выводимое имя".
```

Работа с сетевыми дисками:

```
net use - отобразить список сетевых дисков, подключенных на данном компьютере
NET config server /hidden:yes - скрыть в сетевом окружении отдельный компьютер
NET config server /hidden:no - вернуть отображение компьютера в сетевом окружении
net use X: /delete - отключить сетевой диск X:
net use X: \\server\shares - подключить сетевой диск X: которому соответствует разделяемый сетевой каталог с именем shares на компьютере с именем server
net use Y: C$ /USER:Администратор адmpass - подключить сетевой диск Y: которому соответствует скрытый ресурс C$ (корневой каталог диска C:).
net use Y: C$ /SAVECRED - выполнить подключение с запоминанием полномочий
net use /PERSISTENT:NO - не запоминать сетевые подключения
net use /PERSISTENT:YES - запоминать сетевые подключения
```

Работа с файлами и каталогами:

```
net share INSTALL - получить информацию о разделяемом ресурсе с именем INSTALL
```

```
net share TEMP="C:\Documents And Settings\LocalSettings\games" - добавить новый разделяемый каталог под именем TEMP
net share TEMP="C:\Documents And Settings\LocalSettings\games" /users:5 - добавить новый разделяемый каталог под именем TEMP с максимальным числом одновременно подключающихся пользователей равным 5.
net share TEMP /DELETE - удалить разделяемый ресурс под именем TEMP
net file - получить список открытых по сети файлов
net file 4050 /close - принудительно закрыть файл, идентификатор которого равен 4050
```

Работа с сетевым окружением:

```
net view - отобразить список компьютеров в сетевом окружении.
net view | more - отобразить список компьютеров в постраничном режиме вывода на экран.
net view > C:\computers.txt - отобразить список компьютеров с записью результатов в текстовый файл.
net view \server - отобразить список сетевых ресурсов компьютера server
net view /DOMAIN:mydomain - отобразить список компьютеров с разделяемыми ресурсами в домене mydomain
Если имя домена не указано, то выводится список всех доступных компьютеров локальной сети.
net view /NETWORK:NW - отобразить список серверов Novell Netware, доступных в данной локальной сети.
net view /NETWORK:NW \NWServer - отобразить список сетевых ресурсов сервера Netware с именем NWServer
```

Работа с пользователями и компьютерами:

```
net config server - настройки сетевых служб для роли сервера.
net config workstation - настройки сетевых служб для роли рабочей станции.
```

Настройки служб сервера:

```
net config server /SRVCOMMENT:"Игровой сервер" /AUTODISCONNECT:5 - автоотключение при неактивности пользователя = 5 минут
net config server /HIDDEN:YES>/AUTODISCONNECT:-1 - автоотключение при неактивности пользователя не выполняется, сервер не отображается в сетевом окружении.
```

Работа с контроллером домена:

```
net computer \notebook /add - добавить в домен компьютер notebook
net computer \notebook /del - удалить из домена компьютер notebook
net group - отобразить список групп пользователей в текущем домене.
net localgroup - отобразить список групп пользователей данного компьютера.
```

Работа с локальными группами:

```
net localgroup Администраторы - отобразить список пользователей локальной группы Администраторы данного компьютера.
net localgroup Администраторы testuser /add - добавление в группу Администраторы нового пользователя с именем testuser
net localgroup Администраторы testuser /delete - удалить пользователя testuser из группы Администраторы
```

Работа с учётными записями пользователей:

```
net user - отобразить список пользователей
net user /DOMAIN - отобразить список пользователей текущего домена
net user VASYA /USERCOMMENT:"Тестовый пользователь " /add - добавить пользователя с именем VASYA
net user VASYA /delete - удалить созданного пользователя.
net user VASYA password /USERCOMMENT:"Тестовый пользователь " /add - создать учетную запись нового пользователя VASYA с паролем password .
net user VASYA * /USERCOMMENT:"Тестовый пользователь " /add - то же, что и в предыдущей команде, но пароль будет запрошен при создании новой учетной записи.
net user VASYA * - изменить пароль существующего пользователя VASYA. Новый пароль будет запрошен при выполнении команды.
net user VASYA Boss - изменить пароль пользователя VASYA на новое значение Boss
net user VASYA Boss /ADD - создание учетной записи.
net localgroup Администраторы VASYA /ADD - добавление пользователя в группу "Администраторы"
```

Отправка сообщений по локальной сети:

```
msg */server:TSServer "Тестовое сообщение " - отправить тестовое сообщение всем пользователям компьютера TSServet
msg RDP-Tcp#0 /server:TSServer "Тестовое сообщение" - отправить тестовое сообщение пользователю терминальной сессии с именем RDP-Tcp#0 на компьютере TSServer
msg console /server:Windows7 "Тестовое сообщение" - отправить тестовое сообщение текущему локальному пользователю компьютера Windows7
msg console "Тестовое сообщение" - отправка тестового сообщения от пользователя сеанса RDP локальному пользователю
```

Статистика и синхронизация часов:

```
net statistics server - отобразить статистические данные для службы сервера
net statistics workstation - отобразить статистические данные для службы рабочей станции
net time \\COMPUTER - отобразить время на компьютере COMPUTER. Вместо имени компьютера можно использовать его IP-адрес.
net time \\COMPUTER /SET - установить часы текущего компьютера по значению часов компьютера COMPUTER
net time \\COMPUTER /SET /YES - установить часы текущего компьютера по значению часов компьютера COMPUTER без запроса подтверждения. Обычно ключ /YES используется в командных файлах, выполняющихся без участия пользователя.
net time /QUERYSNTP - отобразить сервер времени, определенный для данного компьютера.
net time \\COMPUTER /QUERYSNTP - отобразить сервер времени, определенный для указанного компьютера.
net time /SETSNTP:"1.ru.pool.ntp.org time.windows.com" - задать в качестве NTP-серверов узлы 1.ru.pool.ntp.org и time.windows.com
```

NSLOOKUP.EXE присутствует во всех версиях операционных систем Windows и является классическим средством диагностики сетевых проблем, связанных с разрешением доменных имен в IP-адреса. NSLOOKUP предоставляет пользователю возможность просмотра базы данных DNS-сервера и построения определенных запросов, для поиска нужных ресурсов DNS. Практически, утилита выполняет функции службы DNS-клиент в командной строке Windows.

```
nslookup - запуск утилиты
yandex.ru. - отобразить IP-адрес (а) узла с именем yandex.ru . Точка в конце имени желательна для минимизации числа запросов на разрешение имени к серверу DNS. Если завершающей точки нет, то NSLOOKUP сначала попытается разрешить указанное имя как часть доменного имени компьютера, на котором она запущена.
server 8.8.4.4 - установить в качестве сервера имен DNS-сервер Google с IP-адресом 8.8.4.4
yandex.ru. - повторить запрос с использованием разрешения имени DNS-сервером Google.
set type=MX - установить тип записи MX
yandex.ru. - отобразить MX-запись для домена yandex.ru - В примере узел обмена почтой для домена - mx.yandex.ru
mx.yandex.ru. - отобразить информацию по mx.yandex.ru
set type=A - установить тип записи в A
mx.yandex.ru - получить IP-адреса для mx.yandex.ru .
exit - завершить работу с nslookup
```

Использование утилиты NSLOOKUP не в интерактивном режиме:

```
nslookup odnoklassniki.ru - определить IP-адрес узла odnokassniki.ru с использованием сервера DNS, заданного настройками сетевого подключения.
nslookup odnoklassniki.ru 8.8.8.8 - определить IP-адрес узла odnokassniki.ru с использованием DNS-сервера 8.8.8.8 (публичный DNS-сервер Google)
nslookup 8.8.8.8 - определить имя узла, IP-адрес которого равен 8.8.8.8 с использованием DNS-сервера, заданного настройками сетевого подключения.
```

PATHPING.EXE выполняет трассировку маршрута к конечному узлу аналогично команде TRACERT, но дополнительно, выполняет отправку ICMP-эхо запросов на промежуточные узлы маршрута для сбора информации о задержках и потерях пакетов на каждом из них. При интерпретации результатов выполнения PATHPING.EXE нужно учитывать тот факт, что некоторые маршрутизаторы могут быть настроены на блокировку ICMP-трафика, что не позволяет правильно отработать трассировку, и получить по ним статистические данные.

PING.EXE - это, наверно, наиболее часто используемая сетевая утилита командной строки. Существует во всех версиях всех операционных систем с поддержкой сети и является простым и удобным средством опроса узла по имени или его IP-адресу. Для обмена служебной и диагностической информацией в сети используется специальный протокол управляющих сообщений ICMP (Internet Control Message Protocol). Команда ping позволяет выполнить отправку управляющего сообщения типа Echo Request (тип равен 8 и указывается в заголовке сообщения) адресуемому узлу и интерпретировать полученный от него ответ в удобном для анализа виде. В поле данных отправляемого ICMP-пакета обычно содержатся символы английского алфавита. В ответ на такой запрос, опрашиваемый узел должен отправить ICMP-пакет с теми же данными, которые были приняты, и типом сообщения Echo Reply (код типа в заголовке равен 0). Если при обмене ICMP-сообщениями возникает какая-либо проблема, то утилита ping выведет информацию для ее диагностики.

```
ping 8.8.8.8 - выполнить опрос узла с IP-адресом 8.8.8.8 с параметрами по умолчанию.
```

```
ping -t yandex.ru - выполнять ping до нажатия комбинации CTRL+C, При нажатии CTRL+Break - выдается статистика и опрос узла продолжается  
ping -n 1000 -l 500 192.168.1.1 - выполнить ping 1000 раз с использованием сообщений, длиной 500 байт.  
ping -a -n 1 -r 9 -w 1000 yandex.ru - выполнить ping 1 раз (ключ -n 1), определять адрес по имени (ключ -a), выдавать маршрут для первых 9 переходов (-r 9), ожидать ответ 1 секунду (1000мсек)
```

ROUTE.EXE используется для просмотра и модификации таблицы маршрутов на локальном компьютере.

```
route print - отобразить текущую таблицу маршрутов  
route print 192.* - отобразить таблицу маршрутов только для адресов, начинающихся с 192.  
route add 0.0.0.0 mask 0.0.0.0 192.168.1.1 - установить в качестве шлюза по умолчанию (основного шлюза) адрес 192.168.1.1  
route -p add 10.0.0.0 mask 255.0.0.0 10.0.0.1 - добавить маршрут для подсети 10.0.0.0/255.0.0.0 и запомнить его в реестре  
route delete 10.0.0.0 mask 255.0.0.0 - удалить маршрут для подсети 10.0.0.0/255.0.0.0  
route add 10.10.10.10 192.168.1.158 - добавить маршрут для узла с IP-адресом 10.10.10.10  
route delete 10.10.10.10 - удалить маршрут, созданный предыдущей командой  
route change 10.0.0.0 mask 255.0.0.0 10.10.10.1 - изменить адрес перехода для существующего маршрута к сети 10.0.0.0/255.0.0.0 на значение 10.10.10.1  
route -f - очистить таблицу маршрутов
```

TELNET.EXE используется как средство удаленного администрирования специализированных сетевых устройств. Сервис TELNET входит в состав практически всех сетевых операционных систем и реализован в виде программного обеспечения сервера Telnet и клиентской оболочки с текстовым или графическим интерфейсом. Подключившись к серверу, удаленный пользователь получает доступ к командной строке, поддерживаемой сервером, таким же образом, как если-бы он работал с локальным терминалом. Утилита TELNET работает поверх протокола TCP и позволяет пользователю подключиться к удаленному узлу не только на стандартный порт 23, но и на любой другой TCP-порт, тем самым, позволяя взаимодействовать с любым приложением, управляемым командной строкой. Так, например, с использованием утилиты telnet можно подключиться к серверам, поддерживающим текстовый (telnet-like) ввод команд и данных - SMTP, POP3, IMAP и т.п. Кроме этого, утилиту можно использовать в качестве средства грубой проверки возможности подключения на любой TCP-порт (проверки слушается ли определенный порт TCP).

```
open 192.168.1.1 - подключиться к серверу TELNET узла 192.168.1.1  
open 192.168.1.1 25 - подключиться к серверу, слушающему порт 25/TCP узла 192.168.1.1  
telnet 192.168.1.1 - подключиться к серверу telnet узла 192.168.1.1  
telnet yandex.ru 80 - подключиться к серверу HTTP (TCP порт 80) узла yandex.ru
```

TRACERT.EXE позволяет получить цепочку узлов, через которые проходит IP-пакет, адресованный конечному узлу. В основе трассировки заложен метод анализа ответов при последовательной отправке ICMP-пакетов на указанный адрес с увеличивающимся на 1 полем TTL. ("Время жизни" - Time To Live). На самом деле это поле не имеет отношения к времени, а является счетчиком числа возможных переходов при передаче маршрутизируемого пакета. Каждый маршрутизатор, получив пакет, вычитает из этого поля 1 и проверяет значение счетчика TTL. Если значение стало равным нулю, такой пакет отбрасывается и отправителю посылается ICMP-сообщение о превышении времени жизни ("Time Exceeded" - значение 11 в заголовке ICMP). Если бы не было предусмотрено включение поля TTL в IP пакетах, то при ошибках в маршрутах, могла бы возникнуть ситуация, когда пакет будет вечно циркулировать в сети, пересылаемый маршрутизаторами по кругу. При выполнении команды tracert.exe сначала выполняется отправка ICMP пакета с полем TTL равным 1 и первый в цепочке маршрутизатор (обычно это основной шлюз из настроек сетевого подключения) вычитая единицу из TTL получает его нулевое значение и сообщает о превышении времени жизни. Эта последовательность повторяется трижды, поэтому в строке результата, формируемой tracert.exe, после номера перехода отображаются три значения времени отклика.

```
tracert google.com - трассировка маршрута к узлу google.com
```

Примеры практического использования сетевых утилит командной строки

Определение подмены адреса узла в файле hosts

Одним из последствий вирусного заражения довольно часто является блокировка доступа к сайтам антивирусных компаний, поисковым системам, популярным социальным сетям (Vkontakte, Odnoklassniki, Facebook, Twitter и т. п.). Подобный же прием используется для кражи учетных данных пользователей путем перенаправления на вредоносный сайт, адрес которого берется из зараженного файла hosts. Файл hosts при настройках по умолчанию, находится в каталоге `\Windows\system32\drivers\etc\` и обычно содержит строки, начинающиеся с символа #, являющиеся комментариями, и одну запись для определения имени узла петлевого интерфейса:

```
31.214.145.172 odnoklassniki.ru
31.214.145.172 www.facebook.com
31.214.145.172 www.vk.com
31.214.145.172 www.vkontakte.ru
```

Задача легко решается с использованием 2-х команд (ping и nslookup):

```
ping odnoklassniki.ru - в ответе на пинг будет отображаться адрес, соответствующий имени odnoklassniki.ru при
определении IP-адреса на данном компьютере
nslookup odnoklassniki.ru - получить IP-адрес, соответствующий имени odnoklassniki.ru от сервера DNS
```

Открыть порт в брандмауэре Windows 7-10:

```
netsh firewall set portopening TCP 27015 - открыть TCP порт 27015 с учётом значений по умолчанию и
необязательных параметров
netsh advfirewall firewall add rule name="Open Port 27015" dir=in action=allow protocol=TCP localport=27015 -
открыть порт 27015 в Windows с учётом нового синтаксиса
```

Правила брандмауэра Windows 7-10:

```
netsh advfirewall firewall add rule name="allow QIP" dir=in program="c:\programfiles\qip\qip.exe" action=allow -
добавление правила для входящего трафика для программы qip.exe

netsh advfirewall firewall add rule name="allow80" protocol=TCP dir=out localport=80 action=block - добавление
правила, запрещающего исходящий трафик для TCP порта 80

netsh advfirewall firewall add rule name="Require Encryption for Inbound TCP/80" protocol=TCP dir=in localport=80
security=authdynenc action=allow - добавление правила входящего трафика с требованием безопасности и
шифрования для трафика через TCP-порт 80

netsh advfirewall firewall add rule name="allow messenger" dir=in program="c:\program files\messenger\msmsgs.exe"
security=authenticate action=allow - добавление правила входящего трафика для messenger.exe с требованием
безопасности

netsh advfirewall firewall add rule name="allow scanners" dir=in rmtcomputergrp=<строка SDDL> action=bypass
security=authenticate - добавление правила обхода брандмауэра с проверкой подлинности для группы
acmedomain\scanners, определяемой строкой SDDL

netsh advfirewall firewall add rule name="Allow port range" dir=out protocol=udp localport=5000-5010 action=allow -
добавление правила разрешения исходящего трафика для локальных портов 5000-5010 для udp

netsh advfirewall firewall show rule name=all - просмотр всех правил брандмауэра

netsh advfirewall firewall show rule name=all | more - просмотр всех правил брандмауэра с выдачей результатов на
экран в страничном режиме

netsh advfirewall firewall show rule name=all > C:\firewallrules.txt - просмотр всех правил брандмауэра с выдачей
результатов в файл

netsh advfirewall firewall show rule name=TEST просмотр правила с именем TEST
netsh advfirewall firewall delete rule name=test - удаление правила с именем TEST

netsh advfirewall firewall set rule name="Allow port range" new localport=5000-6000 - изменить диапазон портов для
правила "Allow port range"
```

Wi-Fi точка доступа стандартными средствами Windows 7-10

```
set hostednetwork mode=allow
set hostednetwork ssid=ssid1
set hostednetwork key=passphrase keyUsage=persistent
set hostednetwork mode=allow ssid=MyWiFi key=MyPassWord
```

или - одной командной строкой

```
netsh wlan set hostednetwork mode=allow ssid=MyWiFi key=MyPassWord - создать виртуальную точку доступа Wi-Fi с именем MyWiFi и паролем MyPassWord
```

Созданная программная точка доступа не будет запущена автоматически:

```
netsh wlan start hostednetwork- запуск программной точки доступа
netsh wlan stop hostednetwork – останов программной точки доступа
```

Получить список беспроводных сетей стандартными средствами Windows 7-10

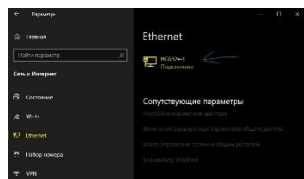
Информация записывается в файл temp\wlans.txt и открывается для просмотра в wordpad:

```
chcp 1251
netsh wlan show networks mode=bssid > %TEMP%\wlans.txt
start "LIST" "%ProgramFiles%\Windows NT\Accessories\wordpad.exe" %TEMP%\wlans.txt
```

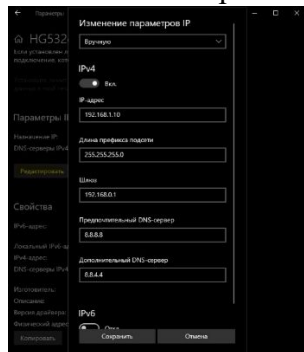
Изменить IP адрес компьютера в Windows 10/7/8.1

Обычно, IP-адрес на компьютере устанавливается по умолчанию и присваивается автоматически адрес, так называемый динамический IP. Если ваш компьютер находится в локальной сети, то нужно изменить IP-адрес компьютера на статический, чтобы он правильно функционировал в этой сети. Изменение IP-адреса может быть по разным причинам, но главная и распространенная - это взаимосвязь между устройствами или какой-либо сетью.

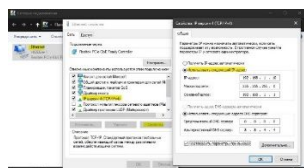
- Изменить IP адрес на компьютере через параметры. Это оптимальный способ для Windows 10. Откройте "Параметры" → "Сеть и Интернет" → "Ethernet" (по проводу) или "WiFi" (беспроводная) в зависимости как вы подключены. Далее с правой стороны, нажмите на сетевой адаптер:



В новом окне нажмите "Редактировать" в графе параметры IP. Далее вы можете изменить IP адрес. Также, вы можете настроить DNS адрес вместе с IPv6, если необходимо.



- Изменить IP адрес компьютера через сетевые адаптеры. Это универсальное решение, которое подойдет для Windows 7/8.1/10. Нажмите Win+R и введите psr.scr, чтобы быстро открыть сетевые адаптеры. Нажмите правой кнопкой мыши по адаптеру, через который осуществляете подключение и выберите "Свойства". Найдите и выделите одним нажатием мыши графу "IP версии 4 (TCP/IPv4)" и ниже нажмите на "Свойства". В новом окне у вас появится возможность изменить IP адрес вручную:



- Изменить IP компьютера через командную строку. Запустите командную строку от имени администратора и выполните: ipconfig /all. Найдите адаптер, в котором хотите изменить IP. В моем случае

это Ethernet. Запомните данные трех значений: IPv4-адрес, Маска подсети, Основной шлюз и DNS-серверы, если будете их менять.



Введите команду, чтобы назначить статический IP-адрес:

```
netsh interface ip set address name="Ethernet" static 192.168.1.10 255.255.255.0 192.168.1.1
```

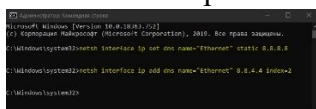
Замените свои данные IP адресов, и не забудьте заменить имя адаптера name="Ethernet", если у вас другое:



Введите команду, чтобы задать DNS адрес:

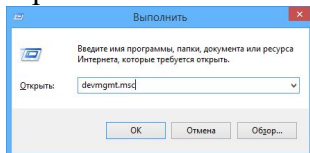
```
netsh interface ip set dns name="Ethernet" static 8.8.8.8 - Предпочитаемый DNS  
netsh interface ip add dns name="Ethernet" 8.8.4.4 index=2 - Альтернативный DNS
```

Не забываем про имя сетевого адаптера Ethernet, если у Вас другое, то замените:

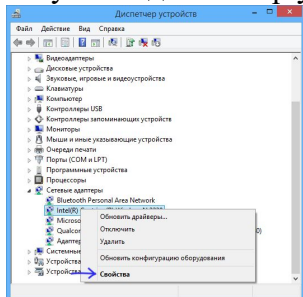


Изменить MAC-адрес сетевой карты компьютера в Windows 10/7/8.1

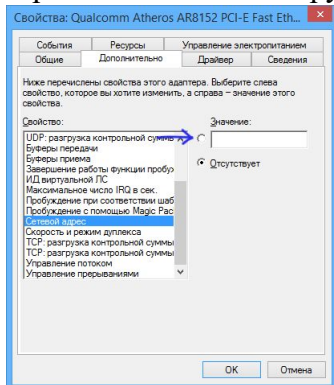
- Изменить MAC-адрес с помощью диспетчера устройств. Первые две цифры задаваемого MAC-адреса не нужно начинать с 0, а заканчивать следует 2, 6, A или E. В противном случае, на некоторых сетевых картах смена может не сработать.



Запустите диспетчер устройств:



В диспетчере устройств откройте раздел «Сетевые адаптеры», кликните правой кнопкой мыши по сетевой карте или Wi-Fi адаптеру, MAC-адрес которого нужно изменить и нажмите «Свойства»:

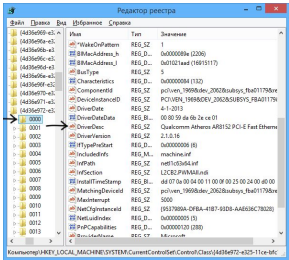


В окне свойств адаптера выберите вкладку «Дополнительно» и найдите пункт «Сетевой адрес», и установите его значение. Чтобы изменения вступили в силу, нужно либо перезагрузить компьютер, либо отключить и включить сетевой адаптер. MAC-адрес состоит из 12 цифр 16-ричной системы и задавать его нужно, не используя двоеточия и другие знаки препинания. Не для всех устройств можно проделать вышеописанное, для некоторых из них пункта «Сетевой адрес» не будет на вкладке «Дополнительно». В

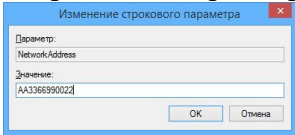
этом случае, следует воспользоваться другими способами. Для проверки, вступили ли изменения в силу, можно использовать команду `ipconfig/all`.

- Изменить MAC-адрес с помощью в редакторе реестра. Для запуска редактора реестра нажмите клавиши Win+R и введите `regedit`. В редакторе реестра откройте раздел:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}
```



В этом разделе будет содержаться несколько «папок», каждая из которых соответствует отдельному сетевому устройству. Найдите то из них, MAC-адрес которого нужно изменить. Для этого обращайтесь внимание на параметр `DriverDesc` в правой части редактора реестра. После того, как Вы нашли нужный раздел, кликните правой кнопкой мыши по нему (в моем случае - по 0000) и выберите → «Создать» → «Строковый параметр». Назовите его `NetworkAddress`:



Дважды кликните по новому параметру реестра и задайте новый MAC-адрес из 12 цифр шестнадцатеричной системы счисления, не используя двоеточий. Закройте редактор реестра и перезагрузите компьютер для того, чтобы изменения вступили в силу.

Самые уязвимые порты Windows 7 - 10

По умолчанию в Windows включены службы не являющиеся необходимыми, и использующие порты:

135	Возможна внешняя ddos-атака по IP
137	Определение netbios-имени ПК; для доступа снаружи лучше закрыть, если не хотите, чтобы вас видели по имени компьютера
138, 139, 445	Samba (общий доступ к файлам и папкам) - порты, которые отвечают за общие ресурсы, открывают удалённому пользователю доступ к жёсткому диску
5000	Порт принадлежит системной службе, называемой "Служба обнаружения SSDP"; если данная служба не применяется, то рекомендуется её отключить (служба имеет ряд уязвимостей)

Команды для закрытия портов 135-139, 445, 5000:

```
netsh advfirewall firewall add rule dir=in action=block protocol=tcp localport=135 name="Block1_TCP-135"
netsh advfirewall firewall add rule dir=in action=block protocol=tcp localport=137 name="Block1_TCP-137"
netsh advfirewall firewall add rule dir=in action=block protocol=tcp localport=138 name="Block1_TCP-138"
netsh advfirewall firewall add rule dir=in action=block protocol=tcp localport=139 name="Block_TCP-139" (команда
помогает закрыть порт 139)
netsh advfirewall firewall add rule dir=in action=block protocol=tcp localport=445 name="Block_TCP-445" (команда
помогает закрыть порт 445)
netsh advfirewall firewall add rule dir=in action=block protocol=tcp localport=5000 name="Block_TCP-5000"
```

Порты, доступ к которым должен предоставляться по принципу «белого» списка, т. е. только определённому кругу лиц:

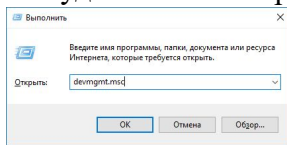
53	DNS
3389	RDP (Remote Desktop Protocol)
5000 ÷ 5050	FTP в пассивном режиме
1433 ÷ 1434	порты SQL
3306	стандартный порт MySQL

Устранение проблем с сетевым подключением в Windows 10

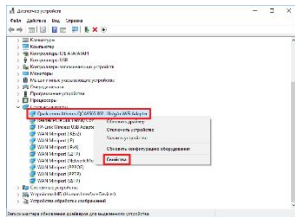
Любое современное устройство на Windows, не подключенное к интернету, теряет большую часть своей функциональности. Именно поэтому проблемы с подключением к сети в Windows - одни из самых неприятных. В этой инструкции мы собрали возможные способы исправить возникшие с сетью неполадки: не работает интернет или не открываются сайты; невозможно подключиться к Wi-Fi; Wi-Fi отключается сам по себе; сеть обозначена как неопознанная или ограниченная. Прежде устранять проблемы, рекомендуется сделать следующее: перезагрузите роутер и компьютер; проверьте, не отошёл ли LAN-кабель; отключите антивирусную программу; позвоните в техническую поддержку Интернет-провайдера.

- Обновить или откатить драйвер сетевого адаптера

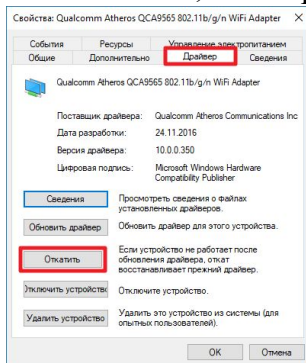
Довольно часто причиной неполадок с сетью становятся ошибки или некорректные настройки драйвера сетевого адаптера. Кроме того, иногда Центр обновления Windows или сторонние программы устанавливают в систему неподходящий для вашей сетевой карты драйвер. Разумеется, в таком случае она не будет стабильно работать. Нажмите Win + R. Введите команду `devmgmt.msc` и нажмите Enter.



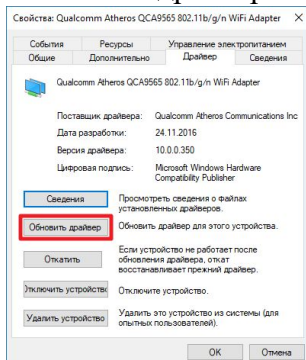
Раскройте категорию Сетевые адаптеры и найдите устройство, с которым возникает проблема (это может быть Wi-Fi адаптер или сетевая карта). Кликните по нему правой клавишей мыши и выберите пункт Свойства.



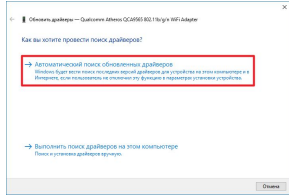
Перейдите во вкладку Драйвер. Если кнопка «Откатить» будет активна, нажмите на неё. Система установит предыдущую версию драйвера. После этого следует перезагрузить компьютер. Если неполадки возникли из-за новой версии, этот шаг вам поможет. Чтобы избежать автоматической установки обновлённого, но неправильного драйвера, вы можете отключить его обновление.



Если откат драйвера не решил проблему (или эта опция неактивна), нажмите на кнопку Обновить драйвер.



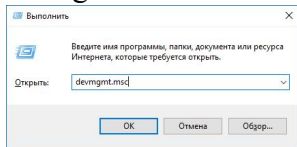
Выберите пункт Автоматический поиск обновленных драйверов. Windows попытается установить новую версию драйвера, если найдёт такую. После этого стоит перезагрузить компьютер.



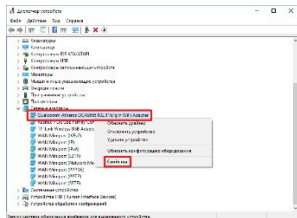
Если предыдущий шаг не исправил неполадку, посетите сайт производителя компьютера или материнской платы, загрузите с него драйвер сетевого адаптера и установите именно его.

- Запретить отключение сетевого адаптера для экономии энергии

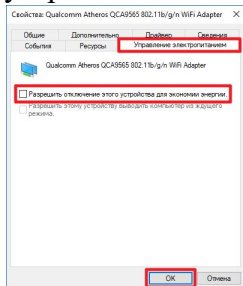
В случае, если какой-либо некритический компонент компьютера не используется, Windows может выключать его для экономии энергии. Сетевой адаптер также входит в разряд "некритических", так что стоит позаботиться об отключении опции энергосбережения. Нажмите Win + R. Введите команду devmgmt.msc и нажмите Enter.



Раскройте категорию Сетевые адаптеры и найдите необходимое устройство. Если их несколько, повторите описанные операции для каждого. Кликните по драйверу правой клавишей мыши и выберите пункт Свойства.



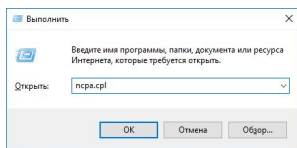
Перейдите во вкладку Управление электропитанием. Снимите галочку «Разрешить отключение этого устройства для экономии энергии» и нажмите ОК.



- Настроить параметры TCP/IP

Если проблема не в драйвере, нужно изучить основные программные настройки, которые влияют на интернет-подключение. Необходимо проверить, активированы ли нужные протоколы, и как работает получение IP-адреса и DNS.

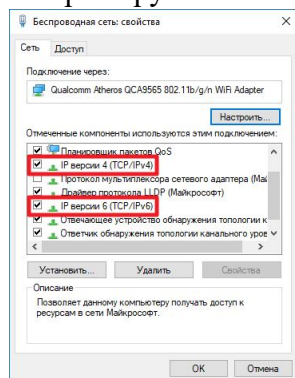
Проверка активированных сетевых протоколов. Для нормальной работы интернета необходимо, чтобы основной протокол IPv4 был активирован. Кроме того, стоит попробовать включить и выключить протокол IPv6 - в некоторых ситуациях сетевое подключение может вести себя непредсказуемо именно из-за него. Нажмите Win + R. Введите команду `ncpa.cpl` и нажмите Enter.



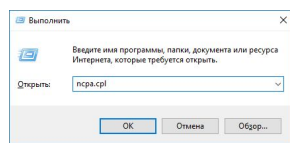
Найдите нужный сетевой адаптер, кликните по нему правой клавишей мыши и выберите пункт Свойства.



Проверьте, стоит ли галочка напротив IP версии 4 (TCP/IPv4). Если нет, то поставьте её и перезагрузите компьютер. Проверьте, стоит ли галочка напротив IP версии 6 (TCP/IPv6). Попробуйте поставить/снять её и перезагрузить компьютер.



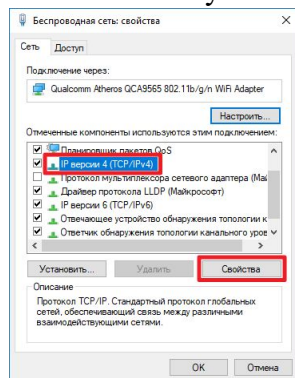
Проверка настроек получения IP-адреса и DNS. Если активация или деактивация протоколов не помогли, стоит проверить настройки IP и DNS. Нажмите Win + R. Введите команду `ncpa.cpl` и нажмите Enter.



Найдите нужный сетевой адаптер, кликните по нему правой клавишей мыши и выберите Свойства.

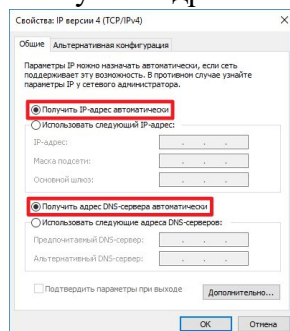


Кликните на пункт IP версии 4 (TCP/IPv4) и нажмите на кнопку Свойства.



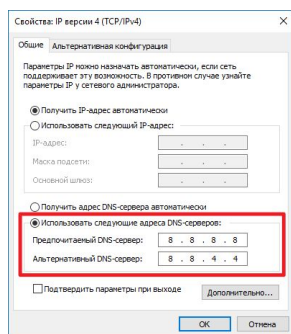
В случае, если в поле категории «Использовать следующий IP-адрес» уже внесены какие-то данные, и вы не вставляли их намеренно, поставьте галочку «Получить IP-адрес автоматически».

Аналогично сделайте с DNS. Если параметры уже настроены, но вы их не изменяли, поставьте галочку «Получить адрес DNS-сервера автоматически».



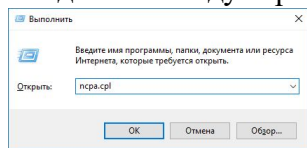
Повторите эти же операции с IP версии 6 (TCP/IPv6). Если это не решило проблему, следует попробовать изменить адреса DNS на предоставляемые Google.

Изменить адреса DNS на предоставляемые Google. Довольно часто это помогает. Поставьте галочку «Использовать следующие адреса DNS-серверов». Введите в поле Предпочитаемый DNS-сервер цифры 8.8.8.8. Введите в поле Альтернативный DNS-сервер цифры 8.8.4.4.



Нажмите ОК. После всех этих операций стоит перезагрузить компьютер, чтобы проверить, помогли они или нет.

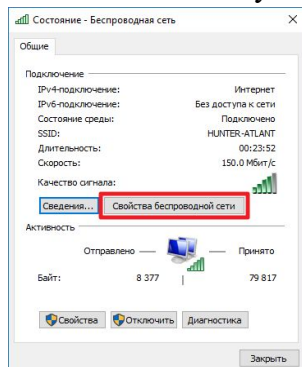
Настройка стандарта FIPS. Иногда может помочь включение или отключение стандарта FIPS (Federal Information Processing Standards или Федеральные Стандарты Обработки Информации). Он создан для государственных учреждений США, но доступен компьютеров в любом регионе. Нажмите Win + R. Введите команду `ncpa.cpl` и нажмите Enter.



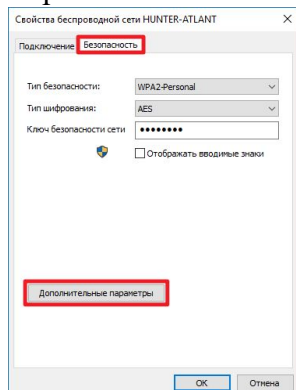
Найдите нужный сетевой адаптер, кликните по нему правой клавишей мыши и выберите пункт Состояние.



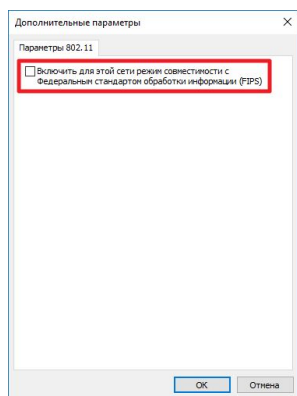
Нажмите на кнопку Свойства беспроводной сети.



Переключитесь на вкладку Безопасность и кликните на Дополнительные параметры.



В зависимости от текущего состояния галочки «Включить для этой сети режим совместимости с федеральным стандартом обработки информации (FIPS)», включите или отключите указанный стандарт.



Перезагрузите компьютер.

- Сбросить параметры сетевого подключения через командную строку

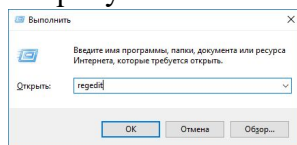
Если изменение параметров сети не помогло, проблема, возможно, находится в системных файлах и настройках. Один из способов сбросить их - выполнить некоторые команды в консоли.

Запустите командную строку от имени администратора. Введите по очереди, следующие шесть команд и перезагрузите компьютер.

```
netsh winsock reset
netsh int ip reset
netsh int tcp reset
ipconfig /release
ipconfig /renew
ipconfig /flushdns
```

- Сбросить параметры сетевого подключения через реестр

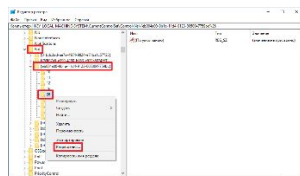
Если при выполнении второй команды Вы получите ошибку «Сбой. Отказано в доступе», попробуйте выполнить следующие шаги: Win + R. → regedit → Enter.



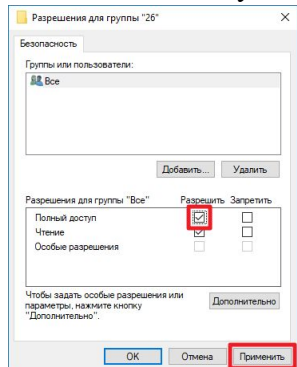
Перейдите в

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Nsi\{eb004a00-9b1a-11d4-9123-0050047759bc}\26

Кликните по папке 26 правой клавишей мыши и выберите пункт Разрешения.



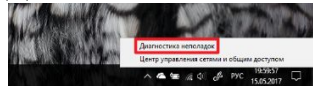
Поставьте галочку «Разрешить» напротив пункта «Полный доступ» и нажмите «Применить».



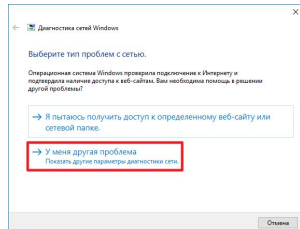
Попробуйте выполнить первую команду снова. После того, как вы проделаете все необходимые операции и перезагрузите компьютер, нужно вернуть всё обратно. Поставьте галочку «Запретить» напротив пункта Полный доступ и нажмите «Применить», затем ОК.

- Диагностика сетевого подключения средствами Windows 10

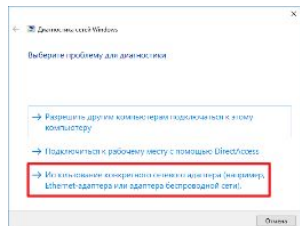
Встроенная утилита диагностики сетевого подключения иногда способна помочь отыскать и решить проблему, поэтому не стоит про неё забывать. Проверить параметры сетевого адаптера можно следующим образом: Кликните по значку подключения в трее правой клавишей мыши и выберите пункт **Диагностика неполадок**.



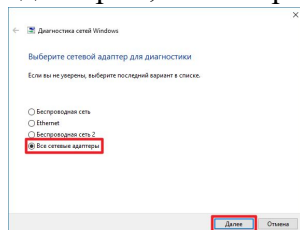
Нажмите на надпись: «У меня другая проблема».



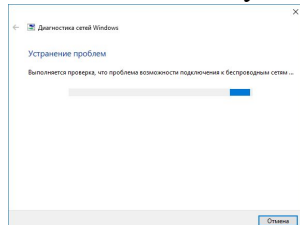
Кликните на Использование конкретного сетевого адаптера.



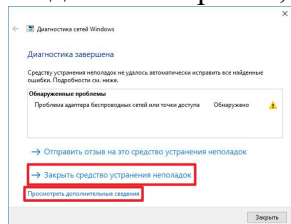
Выберите проблемное устройство и нажмите Далее. В принципе, можно просто указать «Все сетевые адаптеры», чтобы провести диагностику любых проблем.



Подождите, пока утилита выполнит поиск и устранение неполадок.



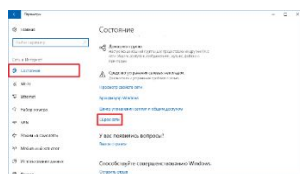
Чтобы увидеть список конкретных проблем, кликните на надпись: «Просмотреть дополнительные сведения». Впрочем, можно сразу «Закрыть средство устранения неполадок».



Можно также попробовать проверить возможность подключения к конкретным сайтам. Впрочем, диагностика всех сетевых адаптеров включает в себя проверку наличия проблем доступа к сети.

- Сбросить параметры сети в Windows 10

Последним возможным решением проблемы с сетевым подключением является полный сброс всех параметров сети. Учтите, что будут удалены абсолютно все настройки, так что, если провайдер требует изменить их, после сброса придётся сделать это заново. Откройте Параметры, перейдите в категорию Сеть и интернет. В самом низу раздела Состояние нажмите на надпись Сброс сети.



Кликните на кнопку «Сбросить сейчас».



Если даже полный сброс не помог, вам следует загрузиться в безопасном режиме с поддержкой сети и проверить, останется ли проблема. Если да, тогда одним из решений неполадки может быть переустановка Windows.

Задания для самостоятельной работы

1. Установить параметры сетевого доступа с помощью интерфейса.
2. Установить параметры сетевого доступа с помощью утилит командной строки.
3. Реализовать примеры практического использования сетевых утилит командной строки
4. Определить, открыты ли самые уязвимые порты (использовать сетевые утилиты командной строки)?
5. Установить параметры сетевого доступа.
6. Выполнить настройку сетевого доступа.
7. При наличии неисправностей сети - определить, зафиксировать и устранить их.

Контрольные вопросы

1. Техник настраивает оборудование. Каким устройствам понадобятся IP-адреса?
2. Что происходит, если часть сообщения с использованием TCP не доставляется на конечный хост?
3. Почему технология беспроводной связи IEEE 802.11 позволяет осуществлять передачу данных на большие расстояния, чем технология Bluetooth?
4. Каковы преимущества технологии беспроводной связи перед технологией проводных ЛВС?
5. Какой стандарт технологии беспроводной связи 802.11 обеспечивает максимальную совместимость с предыдущими стандартами беспроводной связи, но при этом демонстрирует более высокую производительность?
6. В каком случае «подлинность» клиента считается установленной, если в точке доступа включена только фильтрация MAC-адресов?
7. Что должно быть задокументировано после диагностики внутреннего сбоя на Web-сервере?
8. Пользователь звонит в службу поддержки, чтобы сообщить о проблеме, связанной сетевым доступом. Какие три вопроса позволят получить самую полезную информацию для диагностики?
9. Пользователь хочет протестировать соединение между хостом 3 и хостом 8 в сети. Какую команду можно использовать для проверки соединения?
10. Каким образом светодиодный индикатор указывает на то, что через порт передается трафик?
11. Какова одна из наиболее частых причин невозможности подключения хостов?
12. Администратор сети может успешно отправить эхо-запрос на сервер, но не может направить эхо-запрос на веб-сервер компании, расположенный на участке поставщика услуг Интернет в другом городе. С помощью какого инструмента или команды можно определить конкретный маршрутизатор, в котором произошла потеря или задержка пакета?
13. Что делает возможным отправку и получение электронной почты на широком диапазоне устройств, включая смартфоны, ноутбуки и стационарные ПК?
14. Какой вид связи является оптимальным выбором для большого университета с тремя кампусами, расположенными в одном и том же большом городе?
15. Разновидности технологий беспроводных сетей
16. Оборудование для подключения компьютера к беспроводной сети.

17. Риски подключения к публичным беспроводным сетям.

Альтернативные DNS-серверы

Причины использования: нестабильность работы DNS-сервера провайдера (длительное обновление кеша, сбой и т. д.), заражение компьютера вредоносным кодом (который подменил настройки DNS на вредоносные), стремление повысить быстродействие сети и защиту своего компьютера от угроз интернета. DNS (англ. Domain Name System - система доменных имён) - компьютерная распределённая система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста (компьютера или устройства), получения информации о маршрутизации почты, обслуживающих узлах для протоколов в домене (SRV-запись).

Сервис	IPv4	IPv6
Google Public DNS	8.8.8.8 8.8.4.4	2001:4860:4860::8888 2001:4860:4860::8844
OpenDNS	208.67.222.222 208.67.220.220	
Comodo Secure DNS	8.26.56.8 8.20.247.20	
Norton ConnectSafe	199.85.126.10 199.85.127.10	
SkyDNS	193.58.251.251	
Rejector	95.154.128.32 78.46.36.8	
Яндекс.DNS	Базовый (быстрый и надежный DNS): 77.88.8.8 77.88.8.1 Безопасный (без мошеннических сайтов): 77.88.8.88 77.88.8.2 Семейный (без сайтов для взрослых): 77.88.8.7 77.88.8.3	
Cloudflare DNS	1.1.1.1 1.0.0.1	2606:4700:4700::1111 2606:4700:4700::1001
DNS.WATCH	84.200.69.80 84.200.70.40	2001:1608:10:25::1c04:b12f 2001:1608:10:25::9249:d69b