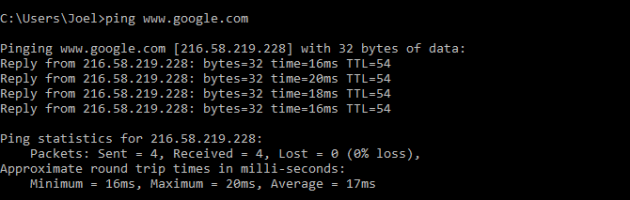
1. PING

PING — одна из базовых и самых полезных CMD-команд. Она отображает качество связи, показывает, может ли ваш компьютер высылать данные по целевому IP-адресу, и если может, то с какой скоростью.

Вот пример использования команды:

[[](https://cdn.lifehacker.ru/wp-content/uploads/2016/12/windows-command-ping_1482583579.png)](https://cdn.lifehacker.ru/wp-content/uploads/2016/12/windows-command-ping_1482583579.png" \o ")

Команда действует по следующему принципу: она высылает определённое количество пакетов данных и определяет, сколько из них вернулось обратно. Если некоторые из них не вернулись, она сообщает о потере. Потеря пакетов ведёт к низкой производительности в играх и интернет-трансляциях. Это отличный способ протестировать ваше интернет-соединение.

По умолчанию команда высылает четыре пакета с тайм-аутом для каждого в четыре секунды. Вы можете увеличить количество пакетов следующим образом: ping www.google.com -n 10

Вы можете также увеличить длительность тайм-аута (значение отображается в миллисекундах): ping www.google.com -w 6000

Команда работает по протоколу ICMP, по этому если на сайте заблокирован данный протокол, то пропинговать сайт не получится

2. **TRACERT** / **TRACEROUTE** (*LINUX*)

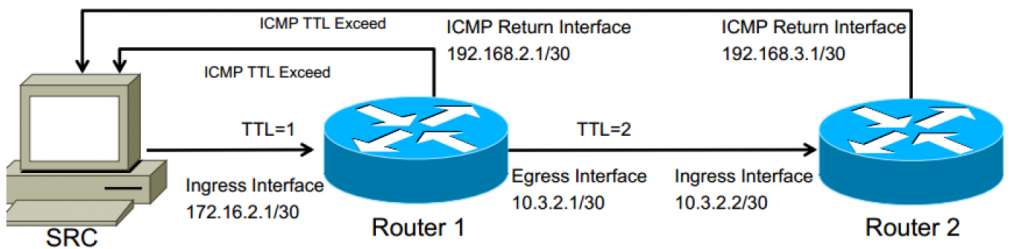
TRACERT означает Trace Route. Как и PING, команда высылает пакет данных для решения сетевых проблем. Однако она определяет не скорость отправки и возврата пакета, а его маршрут.

Пример использования:

[](https://cdn.lifehacker.ru/wp-content/uploads/2016/12/windows-command-tracert_1482584152.png)

Команда отображает список всех маршрутизаторов, через которые проходят данные на пути к конечному узлу. Почему мы видим три показателя длительности для каждого маршрутизатора? Потому что TRACERT высылает три пакета данных на случай, если один из маршрутизаторов потеряется или по какой-то причине потребует слишком много времени.

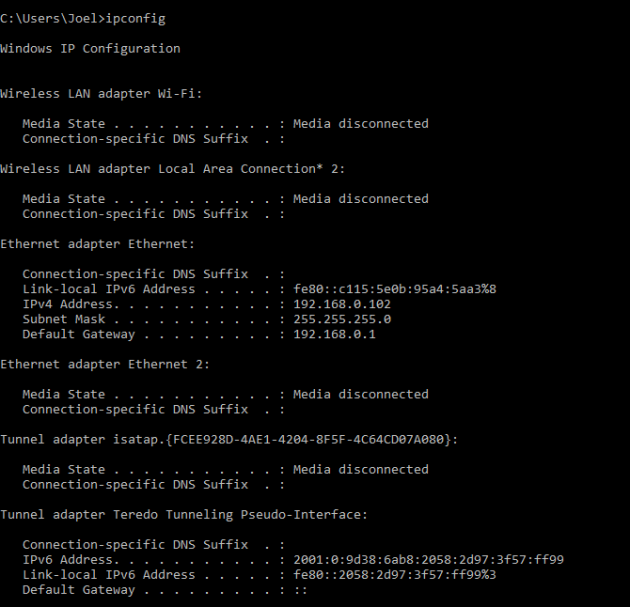
**Отправляется TTL пакет, после прохождения маршрутизатора время жизни пакет обнуляется и маршрутизатор отправляет ответ что пакет умер на нем. После хост отправляет новый запрос, который доходит до следующего маршрутизатора и тд**

****

## 3. IPCONFIG

Эта команда наиболее часто используется для отладки сетей в Windows. И дело не только в объёме информации, которую она предоставляет, но и в том, что она комбинируется с несколькими ключами для выполнения определённых команд.

Пример использования:

[](https://cdn.lifehacker.ru/wp-content/uploads/2016/12/windows-command-ipconfig_1482584251.png)

При вводе без ключей IPCONFIG отражает все сетевые адаптеры на вашем компьютере, а также то, как они работают. IPv4 Addres и Default Gateway содержат наиболее важную информацию.

Что бы отобразить инфу по всем адаптерам: ipconfig/all

Обновление IP адреса для определенного/всех(если не задан) адаптера: ipconfig/renew

Отобразить содержимое кеша DNS: ipconfig/displaydns

Чтобы очистить DNS-кеш, используйте следующий ключ: ipconfig/flushdns

Эта операция может помочь, если интернет работает, однако вы не можете попасть на некоторые сайты или сервера.

1. **ROUTE** **PRINT** / **ROUTE -n** (*LINUX*) – посмотреть таблицу маршрутизации

Первичная функция маршрутизатора - передать пакет к его целевой сети, которая является целевым IP-адресом пакета. Чтобы сделать это, маршрутизатор должен найти маршрутную информацию, сохраненную в его таблице маршрутизации.

**1**. В Interface List отображаются все доступные интерфейсы

**2**. 0.0.0.0 – это адрес сети в интернет (когда мы отправляем запрос в другую сеть)

**3**. Loopback адрес. Сети, Хоста, Широковещательный

**4**. Внутренний IP адрес Сети, Хоста, Широковещательный. Здесь IP адреса хоста (192.168.1.0/24), а так же виртуалки (192.168.56.0/24)

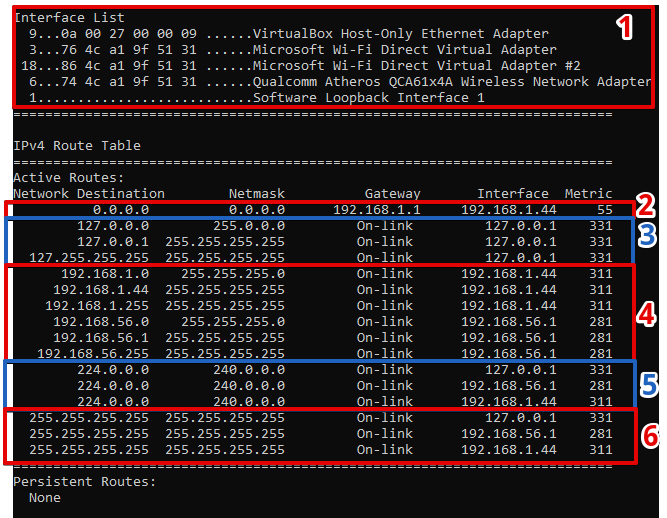
**5**.

**6**. Network Destination 255.255.255.255 and Netmask 255.255.255.255 – interface of those columns is the IP address assigned to WiFi adapter (Local Machine, Virtual Machine)

192.168.1.44 – Local Machine

192.168.56.1 – Virtual Machine

127.0.0.1 – Обратная петля, служит что бы обмениваться трафиком внутри ПК (нужно при разработке, что бы разворачивать сайт на локальной машине)



Назначение сети: целевой сегмент сети

Netmask: маска подсети. Маршруты к отдельным узлам (хостам) имеют маску 32 бит (255.255.255.255).

Шлюз: ***Адрес куда нужно отправить данные***. Также известный как маршрутизатор следующего перехода. При отправке пакетов данных IP шлюз определяет сервер следующего перехода, на который отправляются пакеты данных для определенного сетевого адреса назначения. Если локальный компьютер напрямую подключен к сети (**On-link**), шлюзом обычно является сетевой интерфейс, соответствующий локальному компьютеру, но в настоящее время интерфейс должен быть таким же, как и шлюз; если это удаленная сеть или маршрут по умолчанию, шлюзом обычно является определенная часть сети, к которой подключен локальный компьютер. Серверы или роутеры.

Интерфейс: ***через какой интерфейс будет происходить отправка***. Определяет конкретный сетевой адрес назначения, сетевой интерфейс, используемый локальным компьютером для отправки пакетов данных. Шлюз должен быть расположен в той же подсети, что и интерфейс (за исключением шлюза по умолчанию), в противном случае при использовании этого элемента маршрутизации необходимо вызывать другие элементы маршрутизации, что может вызвать взаимоблокировку маршрутизации.

Метрика: количество переходов, счетчик переходов используется для обозначения стоимости маршрутизации, обычно представляет собой количество переходов, которые необходимо пройти, чтобы достичь адреса назначения, а счетчик переходов представляет маршрутизатор. Чем меньше количество переходов, тем ниже стоимость маршрутизации и выше приоритет. Если есть 2 одинаковых ip адреса с одинаковой маской подсети, то будет выбираться тот, у кого ниже метрика. Так же в метрику входит пропускная способность канала и его загруженность

Если мы подключены к VPN, то маршрутов станет гораздо больше

Маршруты записываются только до ближайших маршрутизаторов. Если нужно попасть в сеть, которая находится через несколько маршрутизаторов, то мы принимаем тот факт, что следующий маршрутизатор будет знать куда отправить дальше

Статические маршруты отображаются в таблице Persistent Routes. Динамические отображаются в верхней таблице

Что бы добавить маршрут **route add [network] mask [networkMask] [gateway] metric [number] IF [interface\_id]**

route add 1.2.3.4 mask 255.255.255.255 0.0.0.0 metric 1 IF 12

Статический маршрут добавляется через ключ –p

route add -p 1.2.3.4 mask 255.255.255.255 0.0.0.0 metric 1 IF 12

Что бы удалить маршрут **route delete [network]**

route delete 1.2.3.4