13 способов, как устранить руками неполадки подключений,
по протоколу TCP/IP в Windows XP .
Only for "direct" hands

Кто хочет, может сразу перейти к оригиналу
http://support.microsoft.com/kb/314067/?sd=RMVP#6

Способ 1. Проверка конфигурации с помощью средства IPConfig

Чтобы проверить конфигурацию TCP/IP на компьютере, где обнаружена проблема, с помощью средства **IPConfig**, нажмите кнопку Пуск, выберите пункт Выполнить и введите команду **cmd**. Для получения сведений о конфигурации компьютера, включая его IP-адрес, маску подсети и шлюз по умолчанию, можно использовать программу ipconfig.

Если указать для **IPConfig** параметр **/all**, будет создан подробный отчет о конфигурации всех интерфейсов, включая адаптеры удаленного доступа. Отчет **IPConfig** можно записать в файл, что позволит вставлять его в другие документы. Для этого введите команду **ipconfig > имя_папкиимя_файла** В результате отчет будет сохранен в файле с указанным именем и помещен в указанную папку.

Отчет команды **IPConfig** позволяет выявить ошибки в конфигурации сети компьютера. Например, если компьютер имеет IP-адрес, который уже присвоен другому компьютеру, то маска подсети будет иметь значение 0.0.0.0.

Если компьютер имеет IP-адрес 169.254.y.z и маску подсети 255.255.0.0, то IP-адрес был назначен средством автоматического назначения IP-адресов APIPA операционной системы **Windows XP Professiona**l. Это означает, что TCP/IP настроен для автоматической конфигурации, сервер DHCP не был найден и не была указана альтернативная конфигурация. В этой конфигурации для интерфейса не задан шлюз по умолчанию.

Если компьютер имеет IP-адрес 0.0.0.0, значит, он был переопределен средством опроса носителя DHCP. Это может быть вызвано тем, что сетевой адаптер не обнаружил подключения к сети, или тем, что протокол TCP/IP обнаружил IP-адрес, который дублирует присвоенный вручную адрес компьютера.

Если не удалось определить проблемы в конфигурации TCP/IP, перейдите к способу 2

Способ 2. Проверка подключения с помощью средства Ping

Если в конфигурации TCP/IP не было обнаружено ошибок, проверьте возможность подключения компьютера к другим компьютерам в сети TCP/IP. Для этого используется средство Ping.

С помощью средства Ping можно проверить подключение на уровне IP. Команда ping отправляет на другой компьютер сообщение с эхо-запросом по протоколу ICMP. С помощью средства Ping можно узнать, может ли главный компьютер отправлять IP-пакеты на компьютер-получатель. Команду Ping можно также использовать для выявления того, чем вызвана проблема – неполадкой сетевых устройств или несовместимостью конфигураций.

Примечание Если была выполнена команда ipconfig /all и отобразилась конфигурация IP, то адрес замыкания на себя и IP-адрес компьютера не нужно проверять с помощью команды Ping. Эти задачи уже были выполнены командой IPConfig при выводе конфигурации. При устранении неполадок следует убедиться, что существует маршрутизация между локальным компьютером и узлом сети. Для этого используется команда ping IP-адрес

Примечание IP-адрес является IP-адресом узла сети, к которому требуется подключиться.

Чтобы использовать команду **ping**, выполните следующие действия:

1. Задайте адрес замыкания на себя, чтобы проверить правильность настройки и установки TCP/IP на локальном компьютере. Для этого служит следующая команда: **ping 127.0.0.1** Если контроль по обратной связи завершится ошибкой, это означает, что стек IP не отвечает.
Подобное поведение наблюдается в следующих случаях:
• Повреждены драйвера TCP.
• Не работает сетевой адаптер.
• Другая служба мешает работе протокола IP.

2. Обратитесь по IP-адресу локального компьютера, чтобы убедиться в том, что он был правильно добавлен в сеть. Если таблица маршрутизации не содержит ошибок, эта процедура просто приведет к направлению пакета по адресу замыкания на себя 127.0.0.1.
Для этого служит следующая команда: ping IP-адрес локального узла Если контроль по обратной связи выполнен успешно, но локальный IP-адрес не отвечает, возможно, проблема заключается в таблице маршрутизации драйвера сетевого адаптера.

3. Обратитесь по IP-адресу шлюза по умолчанию, чтобы проверить его работоспособность и возможность связи с локальным узлом локальной сети. Для этого служит следующая команда: ping IP-адрес шлюза по умолчанию Если обращение завершилось неудачно, это может означать, что проблема заключается в сетевом адаптере, маршрутизаторе/шлюзе, кабеле или другом сетевом устройстве.

4. Обратитесь по IP-адресу удаленного узла, чтобы проверить возможность связи через маршрутизатор. Для этого служит следующая команда: ping IP-адрес удаленного узла. Если обращение завершилось неудачно, это может означать, что удаленный узел не отвечает или проблема заключается в сетевых устройствах между компьютерами. Чтобы исключить возможность отсутствия ответа удаленного узла, проверьте связь с другим удаленным узлом с помощью команды Ping.

5. Обратитесь по IP-адресу удаленного узла, чтобы проверить, может ли быть разрешено имя удаленного узла. Для этого служит следующая команда: ping имя удаленного узла Команда Ping использует разрешение имен для разрешения имени компьютера в IP-адрес. Поэтому, если обращение по IP-адресу производится успешно, а обращение по имени – неудачно, проблема заключается в разрешении имени узла, а не в сетевом подключении. Проверьте, настроены ли для компьютера адреса сервера DNS (вручную в свойствах TCP/IP или автоматически). Если адреса сервера DNS выводятся командой ipconfig /all, обратитесь по адресам сервера, чтобы проверить, доступны ли они.

Если на одном из этапов использования средства Ping возникают ошибки, выполните следующие действия:
• Убедитесь, что IP-адрес локального компьютера действителен и правильно задан на вкладке Общие диалогового окна Свойства протокола Интернета (TCP/IP) или с помощью средства Ipconfig.
• Убедитесь, что настроен шлюз по умолчанию и имеется связь между узлом и шлюзом по умолчанию. Для разрешения проблем должен быть настроен только один шлюз по умолчанию. Хотя шлюзов по умолчанию может быть несколько, все шлюзы кроме первого используются только тогда, когда стек IP определяет, что первый шлюз не работает. При устранении неполадок определяется состояние первого из настроенных шлюзов. Для облегчения задачи все остальные шлюзы можно удалить.
• Убедитесь, что отключен протокол безопасности IPSec. При некоторых политиках IPSec пакеты Ping могут блокироваться или требовать защищенного подключения. Дополнительные сведения о протоколе IPSec см. в способе

7. Проверка протокола IPSec **Внимание!** Если соединение с удаленной системой, к которой происходит обращение, имеет большое время задержки (это относится, например, к спутниковой линии связи), возможно, ответа придется ждать дольше. С помощью параметра -w можно задать более продолжительный период ожидания, чем период по умолчанию, равный 4 секундам.

Способ 3. Проверка маршрутизации с помощью средства PathPing

PathPing – это средство, выявляющее потери пакета на маршрутах, включающих несколько прыжков. Обратившись с помощью PathPing к удаленному узлу, можно убедиться, что маршрутизаторы, через которые проходит пакет, работают нормально. Для этого служит следующая команда: pathping IP-адрес удаленного узла

Способ 4. Очистка кэша ARP с помощью средства Arp

Если обращение по адресу замыкания на себя (127.0.0.1) и собственному IP-адресу выполняется успешно, но ко всем остальным IP-адресам обратиться не удается, попытайтесь очистить кэш протокола ARP (***Address Resolution Protocol***, протокол разрешения адресов).
С помощью командной строки выполните одну из следующих команд.
arp -a (тоже самое **arp -g)**
Чтобы удалить записи, введите команду
arp -d IP-адрес
Для очистки кэша ARP используется следующая команда:
netsh interface ip delete arpcache

Способ 5. Проверка шлюза по умолчанию

Адрес шлюза должен находится в той же сети, что и локальный узел. Иначе сообщения компьютера не будут передаваться вне локальной сети. Если адрес шлюза принадлежит той же сети, что и узел, убедитесь, что адрес шлюза по умолчанию корректен. Шлюз по умолчанию должен являться маршрутизатором, а не только узлом. Маршрутизатор должен иметь возможность передавать IP-датаграммы.

Способ 6. Проверка связи с помощью средств Tracert или Route

Если шлюз по умолчанию отвечает правильно, обратитесь к удаленному узлу, чтобы убедится в правильной работе межсетевых соединений. Если эти соединения работают некорректно, проследите путь сообщения к получателю с помощью служебной программы **Tracert**. Для IP-маршрутизаторов, которые являются компьютерами с операционной системой Microsoft Windows 2000 или Microsoft Windows NT 4.0, просмотрите таблицу IP-маршрутизации с помощью средства маршрутизации или оснастки «Маршрутизация и удаленный доступ» этих компьютеров. На других IP-маршрутизаторах для просмотра таблицы IP-маршрутизации используйте средство, указанное поставщиком используемой операционной системы.

В большинстве случаев при использовании команды **Ping** отображаются четыре следующих сообщения об ошибках: **TTL**
Expired in Transit Это сообщение об ошибке означает, что количество требуемых проходов через маршрутизатор превышает время жизни (TTL). Время жизни можно увеличить с помощью команды ping-i. Возможно, причина этой ошибки в том, что в маршрут является циклическим.

Чтобы узнать, действительно ли возник циклический маршрут (из-за неправильной конфигурации маршрутизаторов), используйте команду **Tracert**
Destination Host Unreachable Это сообщение об ошибке означает, что к узлу-получателю нет локального или удаленного маршрута (на узле-отправителе или маршрутизаторе). Проверьте таблицу маршрутизации на локальном узле или маршрутизаторе.
Request Timed Out Это сообщение об ошибке означает, что сообщения с эхо-запросами не были получены в течение заданного периода ожидания. По умолчанию он равен 4 секундам. Период ожидания можно увеличить с помощью команды **ping -w.**
Ping request could not find host Это сообщение об ошибке означает, что не удается разрешить имя узла-получателя. Проверьте имя и доступность серверов **DNS** или **WINS**.

Способ 7. Проверка протокола IPSec

IPSec может усилить безопасность в сети, но усложнить изменение конфигурации сети и устранение неполадок. В некоторых случаях политика IPSec требует защищенного подключения для компьютера под управлением Windows XP Professional. Это требование затрудняет установку подключения к удаленному узлу. Если службы IPSec развернуты на локальном узле, можно отключить их в оснастке «Службы».

Если после отключения IPSec проблемы больше не возникают, это означает, что политика IPSec блокировала трафик или требовала его защиты. В этом случае нужно попросить у администратора безопасности изменить политику IPSec.

Способ 8. Проверка фильтрации пакетов

Ошибки при фильтрации пакетов могут нарушить работу системы разрешения адресов или подключения. Чтобы узнать, является ли фильтрация пакетов источником проблемы, отключите фильтрацию пакетов TCP/IP.

Для этого выполните следующие действия.

1. Нажмите кнопку Пуск и последовательно выберите пункты Панель управления, Сеть и подключения к Интернету и Сетевые подключения.
2. Щелкните правой кнопкой мыши значок подключения по локальной сети, которое требуется изменить, и выберите пункт Свойства.
3. На вкладке Общие в списке Отмеченные компоненты используются этим подключением выберите вариант Протокол Интернета (TCP/IP) и нажмите кнопку Свойства.
4. Нажмите кнопку Дополнительно и перейдите на вкладку Параметры.
5. В диалоговом окне Необязательные параметры выберите элемент Фильтрация TCP/IP и нажмите кнопку Свойства.
6. Снимите флажок Задействовать фильтрацию TCP/IP (все адаптеры) и нажмите кнопку OK.
Попробуйте обратиться к адресу по его имени DNS, имени NetBIOS компьютера или IP-адресу. Если

обращение выполнено успешно, возможно, параметры фильтрации были неправильно установлены или накладывают слишком жесткие ограничения. Например, фильтрация может разрешить компьютеру выступать в роли веб-сервера, но отключить ряд средств, таких как удаленное администрирование. Чтобы расширить диапазон допустимых параметров фильтрации, измените допустимые значения для порта TCP, порта UDP и протокола IP.

Способ 9. Проверка подключения к определенному серверу

Чтобы определить причину проблемы при подключении к серверу через NetBIOS, выполните команду **nbtstat -n** на этом сервере. Это позволит узнать, под каким именем сервер зарегистрирован в сети. Команда **nbtstat -n** выводит несколько имен, под которыми зарегистрирован компьютер. Среди этих имен должно быть имя, похожее на то, которое указано на вкладке Имя компьютера окна Система, доступного с панели управления. Если такого имени нет, попытайтесь использовать любое другое уникальное имя, выведенное командой nbtstat.
Средство Nbtstat также может отображать кэшированные записи удаленных компьютеров, которые отмечены #PRE в файле Lmhosts или относятся к недавно разрешенным именам.
Если удаленные компьютеры используют для сервера одно и то же имя, а другие компьютеры находятся в удаленной подсети, убедитесь, что для них задано соответствие «имя-адрес» в файлах Lmhosts или в серверах WINS.

Способ 10. Проверка удаленных подключений

Чтобы определить, почему не устанавливается подключение по протоколу TCP/IP с удаленным компьютером, выполните команду **netstat -a**, показывающую состояние всех портов TCP и UDP локального компьютера.
Если подключение TCP работает нормально, в очередях Sent (Отправлено) и Received (Получено) отображается 0 байт.
Если в одной из этих очередей данные блокируются или они имеют состояние «irregular», подключение может быть неисправно.
Если данные не блокируются, а очереди находятся в состоянии «typical», то проблема, вероятно, вызвана задержкой в работе сети или программе.

Способ 11. Проверка таблицы маршрутизации с помощью средства Route

Для того чтобы два узла могли обмениваться IP-датаграммами, они должны иметь маршруты друг к другу или использовать шлюзы по умолчанию, где имеются эти маршруты. Чтобы просмотреть таблицу маршрутизации на компьютере под управлением Windows XP, введите команду **route print**

Способ 12. Проверка путей с помощью средства Tracert

Средство **Tracert** отправляет сообщения с эхо-запросами, увеличивая на каждом шаге значения в IP-заголовке поля TTL, чтобы определить сетевой путь между двумя узлами. Затем средство Tracert анализирует возвращенные сообщения ICMP.
Tracert позволяет прослеживать путь, не превышающий 30 прыжков.
Tracert определяет причину проблемы, когда при проходе через какой-либо маршрутизатор происходит ошибка или маршрут образует замкнутый цикл.

После того, как маршрутизатор, являющийся причиной проблемы, обнаружен, обратитесь к администратору маршрутизатора, если маршрутизатор находится в другой сети, или сами восстановите работоспособность маршрутизатора, если он находится под вашим управлением.

Способ 13. Устранение неполадок в шлюзах

Если при настройке было получено приведенное ниже сообщение, выясните, находится ли шлюз по умолчанию в той же логической сети, что и сетевой адаптер компьютера:
Your default gateway does not belong to one of the configured interfaces
Сравните часть IP-адреса шлюза по умолчанию, соответствующую идентификатору сети, с идентификаторами сети сетевых адаптеров компьютера. В частности, проверьте, равен ли результат логического поразрядного И IP-адреса и маски подсети результату логического поразрядного И основного шлюза и маски подсети.

Например, если компьютер имеет один сетевой адаптер с IP-адресом 172.16.27.139 и маской подсети 255.255.0.0, шлюз по умолчанию должен иметь адрес 172.16.y.z.y.z. Идентификатор сети для этого интерфейса IP — 172.16.0.0.