

Windows troubleshooting сетевого соединения

Тестирование сетевого соединения с помощью Ping и PathPing

Ping – это инструмент, который помогает проверять связь на уровне IP; PathPing – это инструмент, который обнаруживает потерю пакетов при нескольких перехватах. При устранении неполадок команда `ping` используется для отправки ICMP Echo Request на имя целевого узла или IP-адрес. Используйте Ping, когда вы хотите проверить, что хост-компьютер может отправлять IP-пакеты на целевой хост. Вы также можете использовать инструмент Ping для изоляции сетевых аппаратных проблем и несовместимых конфигураций.

Если вы вызываете `ipconfig /all` и получаете ответ, нет необходимости пинговать обратный адрес и собственный IP-адрес. `Ipconfig` уже сделал это для создания отчета.

Лучше всего проверить, существует ли маршрут между локальным компьютером и сетевым хостом, сначала используя пинг и IP-адрес сетевого хоста, к которому вы хотите подключиться. Синтаксис команды:

```
** ping <** IP-адрес>
```

Выполните следующие шаги при использовании Ping:

1. Ping адрес `loopback`, чтобы убедиться, что TCP/IP установлен и правильно настроен на локальном компьютере.

```
ping 127.0.0.1
```

Если шаг петлевого замыкания завершается неудачно, стек IP не отвечает. Возможно, это связано с тем, что драйверы TCP повреждены, сетевой адаптер может не работать или другой сервис мешает IP.

2. Ping IP-адрес локального компьютера, чтобы убедиться, что он был добавлен в сеть правильно. Обратите внимание, что если таблица маршрутизации верна, это просто пересылает пакет в адрес loopback 127.0.0.1.

ping <IP-адрес локального хоста>

3. Ping IP-адрес шлюза по умолчанию, чтобы убедиться, что шлюз по умолчанию работает и что вы можете связываться с локальным хостом в локальной сети.

ping <IP-адрес шлюза по умолчанию>

4. Ping IP-адрес удаленного хоста, чтобы проверить, что вы можете общаться через маршрутизатор.

ping <IP-адрес удаленного хоста>

5. Ping имя хоста удаленного хоста, чтобы убедиться, что вы можете разрешить имя удаленного хоста.

ping <Имя хоста удаленного хоста>

6. Запустите анализ PathPing на удаленный хост, чтобы убедиться, что маршрутизаторы на пути к месту назначения работают правильно.

pathping <IP-адрес удаленного хоста>

Примечание

Если ваш локальный адрес возвращается как 169.254.yz, вам присвоен IP-адрес функцией автоматической приватной IP-адресации (APIPA) Windows 2000. Это означает, что локальный DHCP-сервер не настроен должным образом или не может быть достигнут с вашего компьютера, и IP-адрес был назначен автоматически с маской подсети 255.255.0.0. Включите или исправьте DHCP-сервер, перезапустите локальный компьютер и проверьте, не устранена ли проблема с сетью.

Если ваш локальный адрес возвращается как 0.0.0.0, переопределение программного обеспечения Microsoft MediaSense

запускается, потому что сетевой адаптер обнаруживает, что он не подключен к сети. Чтобы устранить эту проблему, отключите MediaSense, убедившись, что сетевой адаптер и сетевой кабель подключены к концентратору. Если соединение прочное, переустановите драйвер сетевого адаптера или новый сетевой адаптер.

Ping использует разрешение имени хоста для разрешения имени компьютера на IP-адрес, поэтому, если проверка ping по адресу завершается успешно, но сбой по имени, тогда проблема заключается в разрешении имени узла, а не в подключении к сети. Дополнительные сведения об устранении неполадок разрешения имен узлов см. В разделе «Не удалось получить хост или имя NetBIOS» ранее в этой главе.

Если вы не можете успешно использовать Ping в любой момент, проверьте следующее:

- IP-адрес локального компьютера действителен и отображается правильно на вкладке IP-адрес диалогового окна свойств протокола Интернета (TCP / IP) или при использовании инструмента Ipconfig.
- Шлюз по умолчанию настроен, и связь между хостом и шлюзом по умолчанию работает. Для устранения неполадок убедитесь, что настроен только один шлюз по умолчанию. Хотя можно настроить более одного шлюза по умолчанию, шлюзы за пределами первого используются только в том случае, если стек IP определяет, что исходный шлюз не работает. Поскольку проблема устранения неполадок заключается в определении статуса первого настроенного шлюза, удалите все остальные, чтобы упростить устранение неполадок.

Important

Если удаленная система, находящаяся под пингом, находится через высокоскоростную связь, такую ​​□□как спутниковая связь, ответы могут потребовать больше времени для возврата.

Переключатель -w (wait) может использоваться для указания более длительного тайм-аута. В следующем примере показан набор из двух пинов, каждый размером 1450 байт, которые ждут две секунды (2000 миллисекунд) для ответа до истечения времени ожидания.

```
C: \> ping -w 2000 -n 2 -l 1450 172.16.48.10
```

Pinging 172.16.48.10 с 1450 байтами данных:

Ответить от 172.16.48.10: bytes = 1450 раз = 1542мс TTL = 32

Ответ от 172.16.48.10: байты = 1450 раз = 1787 мс TTL = 32

Статистика Ping для 172.16.48.10:

Пакеты: Отправлено = 2, Получено = 2, Потеряно = 0 (потеря 0%),

Приблизительное время прохода в миллисекундах:

Minimum = 0ms, Maximum = 10ms, Average = 1664ms

Clear ARP Cache/Очистить кеш ARP

Если вы можете выполнить ping как loopback-адрес, так и собственный IP-адрес, следующим шагом будет очистить кеш ARP и перезагрузить его. Это можно сделать с помощью утилиты Arp, сначала для отображения записей кэша с arp -a или arp -g. Удалите записи с помощью arp -d <IP-адрес>.

Verify Default Gateway/Проверка шлюза по умолчанию

Затем посмотрите на шлюз по умолчанию. Адрес шлюза должен находиться в той же сети, что и локальный хост; если нет, сообщения с главного компьютера не могут быть отправлены в любое место за пределами локальной сети. Затем проверьте, правильно ли указан адрес шлюза по умолчанию, как указано. Наконец, убедитесь, что шлюз по умолчанию – это маршрутизатор, а не только хост, и что он включен для пересылки IP-дейтаграмм.

Ping Remote Host/Удаленный хост Ping

Если шлюз по умолчанию отвечает правильно, выполните ping на удаленном хосте, чтобы обеспечить связь между сетью и сетью.

Если это не удастся, используйте Tracert для проверки пути к месту назначения. Для IP-маршрутизаторов, которые являются компьютерами под управлением Windows NT или Windows 2000, используйте утилиту маршрутизации или средство администрирования маршрутизации и удаленного доступа на этих компьютерах для проверки таблицы IP-маршрутизации. Для IP-маршрутизаторов, которые не являются компьютерами под управлением Windows NT или Windows 2000, используйте соответствующую утилиту или средство для проверки таблицы IP-маршрутизации.

Четыре сообщения об ошибках обычно возвращаются Ping во время устранения неполадок. Они есть:

TTL Expired in Transit/TTL истек в транзите

Количество перелетов, необходимых для достижения пункта назначения, превышает установленный передающим хостом TTL для пересылки пакетов. Значение TTL по умолчанию для запросов ICMP Echo, отправленных Ping, равно 32. В некоторых случаях этого недостаточно для перемещения необходимого количества ссылок на пункт назначения. Вы можете увеличить TTL, используя ключ -i, до 255 ссылок.

Если увеличение значения TTL не позволяет решить проблему, пакеты пересылаются в цикле маршрутизации, круговой путь между маршрутизаторами. Используйте Tracert для отслеживания источника цикла маршрутизации, который отображается в виде повторной серии тех же IP-адресов в отчете Tracert. Затем внесите соответствующие изменения в таблицы маршрутизации или сообщите администратору удаленного маршрутизатора о проблеме.

Destination Host Unreachable/Хост назначения недоступен

Это сообщение указывает на одну из двух проблем: либо локальная система не имеет маршрута к желаемому адресату, либо удаленный маршрутизатор сообщает, что у него нет маршрута к месту назначения. Две проблемы можно различить по форме

сообщения. Если сообщение просто «Destination Host Unreachable», тогда нет маршрута из локальной системы, и отправляемые пакеты никогда не помещаются в провод. Используйте утилиту Route для проверки локальной таблицы маршрутизации.

Если сообщение «Reply From <IP address>: Destination Host Unreachable», тогда проблема маршрутизации возникла на удаленном маршрутизаторе, адрес которого указан поле «<IP-адрес>». Используйте соответствующую утилиту или средство для проверки таблицы IP-маршрутизации маршрутизатора, назначенного IP-адресу <IP-адреса>.

Если вы используете ping с использованием IP-адреса, повторите попытку с именем хоста, чтобы убедиться, что IP-адрес, который вы попытались, правильный.

Request Timed Out/Истекло время запроса

Это сообщение указывает, что не было получено сообщений об эхо-сигнале в течение 1 секунды по умолчанию. Это может быть вызвано многими различными причинами; наиболее распространенными являются перегрузка сети, сбой запроса ARP, фильтрация пакетов, ошибка маршрутизации или молчащий сброс. Чаще всего это означает, что маршрут назад к отправляющему хосту не удался. Возможно, это связано с тем, что целевой хост не знает маршрут назад к отправляющему узлу, или один из промежуточных маршрутизаторов не знает пути назад, или даже, что шлюз по умолчанию хоста-получателя не знает пути назад. Проверьте таблицу маршрутизации хоста назначения, чтобы узнать, имеет ли он маршрут к отправляющему узлу перед проверкой таблиц на маршрутизаторах.

Если таблицы удаленной маршрутизации верны и содержат действительный маршрут обратно на отправляющий узел, чтобы убедиться, что в кеше ARP отсутствует правильный адрес, используйте команду arp -a для печати содержимого кеша ARP. Кроме того, проверьте маску подсети, чтобы убедиться, что

удаленный адрес не был интерпретирован как локальный.

Затем используйте Tracert, чтобы следовать по маршруту до пункта назначения. В то время как Tracert не записывает адрес последнего прыжка или путь, по которому пакет должен следовать по пути возврата, он может показать, что пакет добрался до адресата. Если это так, проблема, вероятно, связана с проблемой маршрутизации на пути возврата. Если трассировка не достигает цели, возможно, это связано с тем, что целевой хост защищен брандмауэром. Когда брандмауэр защищает получателя, фильтрация пакетов ICMP предотвращает пересылку пакетов ping или любых других сообщений ICMP через брандмауэр и их назначение.

Чтобы проверить перегрузку сети, просто увеличьте допустимую задержку, установив более высокое время ожидания с помощью ключа -w, например, 5000 миллисекунд. Повторите попытку. Если запрос все еще не работает, перегрузка не является проблемой; проблема с разрешением адреса или ошибка маршрутизации является более вероятной проблемой.

Unknown Host/Неизвестный хост

Это сообщение об ошибке указывает, что запрошенное имя хоста не может быть разрешено к его IP-адресу; убедитесь, что имя введено правильно и что DNS-серверы могут его решить.

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc940095\(v=technet.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc940095(v=technet.10))