

## How to troubleshoot TCP/IP connectivity with Windows XP

This article was previously published under Q314067

For a Microsoft Windows 2000 version of this article, see [102908](http://support.microsoft.com/kb/102908/) (<http://support.microsoft.com/kb/102908/>).

Article ID	: 314067
Last Review	: July 16, 2004
Revision	: 1.0

### INTRODUCTION

There are tools that can provide useful information when you are trying to determine the cause of TCP/IP networking problems under Microsoft Windows XP. This article lists recommendations for using these tools to diagnose network problems. Although this list is not complete, the list does provide examples that show how you can use these tools to track down problems on the network.

### MORE INFORMATION

#### TCP/IP troubleshooting tools

The following list shows some of the TCP/IP diagnostic tools that are included with Windows XP:

##### Basic tools

- **Network Diagnostics in Help and Support**  
Contains detailed information about the network configuration and the results of automated tests.
- **Network Connections folder**  
Contains information and configuration for all network connections on the computer. To locate the Network Connections folder, click **Start**, click **Control Panel**, and then click **Network and Internet Connections**.
- **IPConfig command**  
Displays current TCP/IP network configuration values, updates, or releases, Dynamic Host Configuration Protocol (DHCP) allocated leases, and display, register, or flush Domain Name System (DNS) names.
- **Ping command**  
Sends ICMP Echo Request messages to verify that TCP/IP is configured correctly and that a TCP/IP host is available.

##### Advanced tools

- **Hostname command**  
Displays the name of the host computer.
- **Nbtstat command**  
Displays the status of current NetBIOS over TCP/IP connections, updates the NetBIOS name cache, and displays the registered names and scope ID.
- **PathPing command**  
Displays a path of a TCP/IP host and packet losses at each router along the way.
- **Route command**  
Displays the IP routing table and adds or deletes IP routes.
- **Tracert command**  
Displays the path of a TCP/IP host.

To view the correct command syntax to use with each of these tools, type `-?` at a command prompt after the name of the tool.

#### Windows XP Professional tools

Windows XP Professional contains the following additional tools:

- **Event viewer**  
Records system errors and events.
- **Computer Management**  
Changes network interface drivers and other components.

### Troubleshooting

The procedure that you use to troubleshoot TCP/IP issues depends on the type of network connection that you are using and the connectivity problem that you are experiencing.

#### Automated troubleshooting

For most issues that involve Internet connectivity, start by using the Network Diagnostics tool to identify the source of the issue. To use Network Diagnostics, follow these steps:

1. Click **Start**, and then click **Help and Support**.
2. Click the link to **Use Tools to view your computer information and diagnose problems**, and then click **Network Diagnostics** in the list on the left.
3. When you click **Scan your system**, Network Diagnostics gathers configuration information and performs automated troubleshooting of the network connection.
4. When the process is completed, look for any items that are marked "FAILED" in red, expand those categories, and then view the additional details about what the testing showed.

You can either use that information to resolve the issue or you can provide the information to a network support professional for help. If you compare the tests that failed with the documentation in the Manual Troubleshooting section later in this article, you may be able to determine the source of the issue. To interpret the results for TCP/IP, expand the Network Adapters section of the results, and then expand the network adapter that failed the testing.

You can also start the Network Diagnostics interface directly by using the following command:

```
netsh diag gui
```

### Manual troubleshooting

To manually troubleshoot your TCP/IP connectivity, use the following methods in the order that they appear:

#### Method 1: Use the IPConfig tool to verify the configuration

To use the IPConfig tool to verify the TCP/IP configuration on the computer that is experiencing the problem, click **Start**, click **Run**, and then type **cmd**. You can now use the **ipconfig** command to determine the host computer configuration information, including the IP address, the subnet mask, and the default gateway.

The **/all** parameter for IPConfig generates a detailed configuration report for all interfaces, including any remote access adapters. You can redirect IPConfig output to a file to paste the output into other documents. To do this, type:

```
ipconfig > \folder_name\file_name
```

The output receives the specified file name and is stored in the specified folder.

You can review the IPConfig output to identify issues that exist in the computer network configuration. For example, if a computer is manually configured with an IP address that duplicates an existing IP address that is already detected, the subnet mask appears as 0.0.0.0.

If your local IP address is returned as 169.254.y.z with a subnet mask of 255.255.0.0, the IP address was assigned by the Automatic Private IP Addressing (APIPA) feature of Windows XP Professional. This assignment means that TCP/IP is configured for automatic configuration, that no DHCP server was found, and that no alternative configuration is specified. This configuration has no default gateway for the interface.

If your local IP address is returned as 0.0.0.0, the DHCP Media Sensing feature override turned on because the network adapter detected its lack of connection to a network, or TCP/IP detected an IP address that duplicates a manually configured IP address.

If you do not identify any issues in the TCP/IP configuration, go to Method 2.

#### Method 2: Use the Ping tool to test your connectivity

If you do not identify any issues in the TCP/IP configuration, determine whether the computer can connect to other host computers on the TCP/IP network. To do this, use the Ping tool.

The Ping tool helps you verify IP-level connectivity. The **ping** command sends an ICMP Echo Request message to a destination host. Use Ping whenever you want to verify that a host computer can send IP packets to a destination host. You can also use Ping to isolate network hardware problems and incompatible configurations.

**Note** If you ran the **ipconfig /all** command, and the IP configuration appeared, you do not have to ping the loopback address and your own IP address. IPConfig has already performed these tasks to display the configuration. When you troubleshoot, verify that a route exists between the local computer and a network host. To do this, use the following command:

```
ping IP address
```

**Note** *IP address* is the IP address of the network host that you want to connect to.

To use the **ping** command, follow these steps:

1. Ping the loopback address to verify that TCP/IP is installed and correctly configured on the local computer. To do this, type the following command:

```
ping 127.0.0.1
```

If the loopback test fails, the IP stack is not responding. This problem may occur if any one or more of the following conditions is true:

- The TCP drivers are corrupted.
- The network adapter is not working.
- Another service is interfering with IP.

2. Ping the IP address of the local computer to verify that the computer was correctly added to the network. If the routing table is correct, this procedure just forwards the packet to the loopback address of 127.0.0.1. To do this, type the following command:

```
ping IP address of local host
```

If the loopback test succeeds but you cannot ping the local IP address, there may be an issue with the routing table or with the network adapter driver.

3. Ping the IP address of the default gateway to verify that the default gateway is working and that you can communicate with a local host on the local network. To do this, type the following command:

```
ping IP address of default gateway
```

If the ping fails, you may have an issue with the network adapter, the router or gateway device, the cabling, or other connectivity hardware.

4. Ping the IP address of a remote host to verify that you can communicate through a router. To do this, type the following command:

```
ping IP address of remote host
```

If the ping fails, the remote host may not be responding, or there may be a problem with the network hardware between computers. To rule out an unresponsive remote host, use Ping again to a different remote host.

5. Ping the host name of a remote host to verify that you can resolve a remote host name. To do this, type the following command:

```
ping Host name of remote host
```

Ping uses name resolution to resolve a computer name into an IP address. Therefore, if you successfully ping an IP address but you cannot ping a computer name, there is a problem with host name resolution, not with network connectivity. Verify that DNS server addresses are configured for the computer, either manually in the properties of TCP/IP, or by automatic assignment. If DNS server addresses are listed when you type the `ipconfig /all` command, try to ping the server addresses to make sure that they are accessible.

If you cannot use Ping successfully at any point, verify the following configurations:

- Make sure that the local computer's IP address is valid and that it is correct on the **General** tab of the **Internet Protocol (TCP/IP) Properties** dialog box or when it is used with the `Ipconfig` tool.
- Make sure that a default gateway is configured and that the link between the host and the default gateway is working. For troubleshooting purposes, make sure that only one default gateway is configured. Although you can configure more than one default gateway, gateways after the first gateway are used only if the IP stack determines that the original gateway is not working. The purpose of troubleshooting is to determine the status of the first configured gateway. Therefore, you can delete all the other gateways to simplify your task.
- Make sure that Internet Protocol security (IPSec) is not turned on. Depending on the IPSec policy, Ping packets may be blocked or may require security. For more information about IPSec, go to [Method 7: Verify Internet Protocol security \(IPSec\)](#).

**Important** If the remote computer that you are pinging is across a high-delay link such as a satellite link, response may take longer. You can use the `-w (wait)` parameter to specify a longer timeout period than the default timeout of four seconds.

#### Method 3: Use the PathPing tool to verify a route

The PathPing tool detects packet loss over multiple-hop paths. Run a PathPing analysis to a remote host to verify that the routers on the way to the destination are operating correctly. To do this, type the following command:

```
pathping IP address of remote host
```

#### Method 4: Use the Arp tool to clear the ARP cache

If you can ping both the loopback address (127.0.0.1) and your IP address but you cannot ping any other IP addresses, use the Arp tool to clear out the Address Resolution Protocol (ARP) cache. To view the cache entries, type any one of the following commands:

```
arp -a
```

```
arp -g
```

To delete the entries, type the following command:

```
arp -d IP address
```

To flush the ARP cache, type the following command:

```
netsh interface ip delete arpccache
```

#### Method 5: Verify the default gateway

The gateway address must be on the same network as the local host. Otherwise, messages from the host computer cannot be forwarded outside the local network. If the gateway address is on the same network as the local host, make sure that the default gateway address is correct. Make sure that the default gateway is a router, not just a host. And make sure that the router is enabled to forward IP datagrams.

#### Method 6: Use the Tracert tool or the Route tool to verify communications

If the default gateway responds correctly, ping a remote host to make sure that network-to-network communications are working correctly. If communications are not working correctly, use the Tracert tool to trace the path of the destination. For IP routers that are Microsoft Windows 2000-based or Microsoft Windows NT 4.0-based computers, use the Route tool or the Routing and Remote Access snap-in to view the IP routing table. For other IP routers, use the vendor-designated appropriate tool or facility to examine the IP routing table.

Most frequently, you receive the following four error messages when you use Ping during troubleshooting:

#### **TTL Expired in Transit**

This error message means that the number of required hops exceeds the Time to Live (TTL). To increase TTL, by use the `ping -i` command. A routing loop may exist. Use the Tracert command to determine whether misconfigured routers have caused a routing loop.

#### **Destination Host Unreachable**

This error message means that no local or remote route exists for a destination host at the sending host or at a router. Troubleshoot the local host or the router's routing table.

### Request Timed Out

This error message means that the Echo Reply messages were not received in the designated timeout period. By default, the designated timeout period is four seconds. Use the `ping -w` command to increase the timeout.

### Ping request could not find host

This error message means that the destination host name cannot be resolved. Verify the name and the availability of DNS or WINS servers.

#### Method 7: Verify Internet Protocol security (Ipsec)

IPSec can improve security on a network, but changing network configurations or troubleshooting problems more difficult. Sometimes, IPSec policies require secured communication on a Windows XP Professional-based computer. These requirements can make it difficult to connect to a remote host. If IPSec is implemented locally, you can turn off the IPSEC Services service in the Services snap-in.

If the difficulties end when you stop the IPSec services, IPSec policies are either blocking the traffic or requiring security for the traffic. Ask the security administrator to modify the IPSec policy.

#### Method 8: Verify packet filtering

Because of mistakes in packet filtering, address resolution or connectivity may not work. To determine whether packet filtering is the source of a network problem, turn off TCP/IP packet filtering. To do this, follow these steps:

1. Click **Start**, click **Control Panel**, click **Network and Internet Connections**, and then click **Network Connections**.
2. Right-click the local area connection that you want to modify, and then click **Properties**.
3. On the **General** tab, in the **This connection uses the following items** list, click **Internet Protocol (TCP/IP)**, and then click **Properties**.
4. Click **Advanced**, and then click the **Options** tab.
5. In the **Optional Settings** dialog box, click **TCP/IP Filtering**, and then click the **Properties** tab.
6. Click to clear the **Enable TCP/IP Filtering (All adapters)** check box, and then click **OK**.

To ping an address, use its DNS name, its NetBIOS computer name, or its IP address. If the ping succeeds, the packet filtering options may be misconfigured or too restrictive. For example, the filtering can allow the computer to act as a Web server, but, to do this, the filtering may turn off tools such as remote administration. To restore a wider range of permissible filtering options, change the permitted values for the TCP port, the UDP port, and the IP protocol.

#### Method 9: Verify the connection to a specific server

To determine the cause of connectivity problems when you are trying to connect to a specific server through NetBIOS-based connections, use the `nbtstat -n` command on the server to determine what name the server registered on the network.

The `nbtstat -n` output command lists several names that the computer has registered. The list will include a name that looks similar to the computer's name that is configured on the **Computer Name** tab under **System** in Control Panel. If not, try one of the other unique names that the `nbtstat` command displays.

The `Nbtstat` tool can also display the cached entries for remote computers from `#PRE` entries in the `Lmhosts` file or from recently resolved names. If the name that the remote computers are using for the server is the same, and the other computers are on a remote subnet, make sure that the other computers have the computer's name-to-address mapping in their `Lmhosts` files or WINS servers.

#### Method 10: Verify remote connections

To determine why a TCP/IP connection to a remote computer stops responding, use the `netstat -a` command to show the status of all activity for TCP and UDP ports on the local computer.

Typically, a good TCP connection shows 0 bytes in the **Sent** and **Received** queues. If data is blocked in either queue or the state of the queues is irregular, the connection may be faulty. If data is not blocked, and the state of the queues is typical, you may be experiencing network or program delay.

#### Method 11: Use the Route tool to examine the routing table

For two hosts to exchange IP datagrams, both hosts must have a route to each other, or they must use default gateways that have a route. To view the routing table on a Windows XP-based host, type the following command:

```
route print
```

#### Method 12: Use the Tracert tool to examine paths

Tracert sends ICMP Echo Request messages that have incrementally higher values in the IP header TTL field to determine the path from one host to another through a network. Then Tracert analyzes the ICMP messages that are returned. With Tracert, you can track the path from router to router

for up to 30 hops. If a router has failed, or the packet is routed into a loop, Tracert reveals the problem. After you locate the problem router, you can contact the router administrator if the router is offsite, or you can restore the router to fully functional status if the router is under your control.

#### Method 13: Troubleshoot gateways

If you receive the following error message during configuration, determine whether the default gateway is located on the same logical network as the computer's network adapter:

**Your default gateway does not belong to one of the configured interfaces**

Compare the network ID part of the default gateway IP address with the network IDs of the computer's network adapters. Specifically, verify that the bitwise logical AND of the IP address and the subnet mask equals the bitwise logical AND of the default gateway and the subnet mask.

For example, a computer that has a single network adapter that is configured with an IP address of 172.16.27.139 and a subnet mask of 255.255.0.0 must use a default gateway of the form 172.16.y.z. The network ID for this IP interface is 172.16.0.0.

#### Additional resources

The following resources contain additional information about how to troubleshoot Microsoft TCP/IP:

See the "Configuring TCP/IP" topic in the documentation for the Microsoft Windows XP Professional Resource Kit.

See "Introduction to TCP/IP" in the *TCP/IP Core Networking Guide* of the Microsoft Windows 2000 Server Resource Kit for general information about the TCP/IP protocol suite.

See "Unicast Routing Overview" in the *Internetworking Guide* of the Microsoft Windows 2000 Server Resource Kit for more information about routing principles.

See "TCP/IP Troubleshooting" in the *TCP/IP Core Networking Guide* of the Microsoft Windows 2000 Server Resource Kit for more information about IP packet filtering.

#### REFERENCES

For additional information, click the following article numbers to view the articles in the Microsoft Knowledge Base:

[308007](http://support.microsoft.com/kb/308007/) (<http://support.microsoft.com/kb/308007/>) How to troubleshoot home networking in Windows XP

[325487](http://support.microsoft.com/kb/325487/) (<http://support.microsoft.com/kb/325487/>) How to troubleshoot network connectivity problems

[299357](http://support.microsoft.com/kb/299357/) (<http://support.microsoft.com/kb/299357/>) How to reset Internet Protocol (TCP/IP) in Windows XP

[307874](http://support.microsoft.com/kb/307874/) (<http://support.microsoft.com/kb/307874/>) How to disable simplified sharing and set permissions on a shared folder in Windows XP

[810881](http://support.microsoft.com/kb/810881/) (<http://support.microsoft.com/kb/810881/>) "Access is denied" error message when you try to open a folder

[308418](http://support.microsoft.com/kb/308418/) (<http://support.microsoft.com/kb/308418/>) How to set, view, change, or remove file and folder permissions in Windows XP

[214759](http://support.microsoft.com/kb/214759/) (<http://support.microsoft.com/kb/214759/>) Access denied error when attempting to connect to a network share

---

#### APPLIES TO

- Microsoft Windows XP Home Edition
- Microsoft Windows XP Professional Edition

**Keywords:** kbhowto kbinfo kbtshoot kbenv kbnetwork KB314067