

Troubleshooting TCP/IP

One of the primary reasons to study networking is so that you can troubleshoot a network when problems occur. At this point, you're probably aware that many puzzle pieces must be in place when a user accesses network resources or just surfs the Internet. If any single piece is not exactly where it should be, the user will be asking for help. With a little bit of knowledge on troubleshooting, you can be the person who identifies the problem and fixes it. In this chapter, you'll learn about key troubleshooting tools.

- ▶ **Using the command prompt**
- ▶ **Checking TCP/IP configuration with `ipconfig`**
- ▶ **Troubleshooting connectivity with `ping`**
- ▶ **Identifying routers with `tracert`**
- ▶ **Verifying the routed path with `pathping`**
- ▶ **Viewing TCP/IP statistics with `netstat`**
- ▶ **Installing Telnet**

All the troubleshooting commands in this chapter use the command prompt.

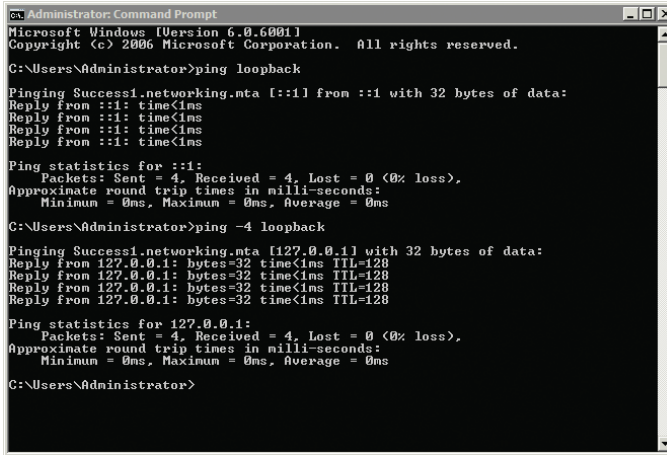
Using the Command Prompt

Although the Windows graphical user interface (GUI) is easy to use for most end user tasks, it does have some limitations when troubleshooting network connectivity issues. In contrast, the *command prompt* can be very useful in troubleshooting basic problems. That is, of course, if you know how to use it.

You can launch the command prompt in just about any Windows system by clicking Start, selecting Run, typing **cmd** in the text box, and pressing Enter. You have a wealth of help available if you know how to ask. For example, you can just enter the `Help` command to identify the available commands.

Figure 14.1 shows the Command Prompt window with the results of the `ping -loopback` command. The first command is using IPv6, and the second command is using IPv4.

There are many other ways to launch the command prompt, but this method will work with most Windows systems.



```

C:\Users\Administrator>ping loopback

Pinging Success1.networking.mta [::1] from ::1 with 32 bytes of data:
Reply from ::1: time<1ms
Reply from ::1: time<1ms
Reply from ::1: time<1ms
Reply from ::1: time<1ms

Ping statistics for ::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>ping -4 loopback

Pinging Success1.networking.mta [127.0.0.1] with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>

```

FIGURE 14.1 Viewing the Command Prompt window

Getting Help at the Command Prompt

Most commands have help available by typing in the command and adding a space, a slash (/), and then a question mark (?). For example, all the following commands will give you help:

- ▶ Ipconfig /?
- ▶ Ping /?
- ▶ Pathping /?
- ▶ Tracert /?
- ▶ Netstat /?
- ▶ Telnet /?

The telnet /? command will fail if Telnet is not installed on the system. Steps to install Telnet are included later in this chapter.

Sometimes the output can scroll past the screen before you have time to read it. You can use the More command with the command to show a single page at a time like this:

```
ipconfig /? | more
```

You can also redirect the output to a text file that you can read later. The following example sends the output to a text file named config.txt:

```
ipconfig /? > config.txt
```

Using Switches

Most commands support additional options. These options are added with switches. A switch is a forward slash (/) which would then be followed by the additional option. For example, if you enter `ipconfig` by itself, it gives minimal information. If you enter it as `ipconfig /all` (using the `/all` switch), it gives much more information. Entering the command with the `/?` switch will show you the switches supported by the command.

Although most commands use the forward slash (/) as a switch, some commands use a hyphen (-). Most Windows commands will accept either a forward slash or a hyphen. For example, the following two commands will both work the same way:

- ▶ `ipconfig /all`
- ▶ `ipconfig -all`

Understanding Case Sensitivity

With very little exception, command prompt commands are not case sensitive. In other words, you can enter them all uppercase, all lowercase, or any combination. For example, each of the following commands will provide the same results:

- ▶ `ping loopback`
- ▶ `PING LOOPBACK`
- ▶ `PiNg LoOpBaCk`

You'll often see commands shown with the first letter capitalized for readability. This doesn't mean it has to be entered that way. If a command is case sensitive, the documentation will usually stress it.

LAUNCHING THE COMMAND PROMPT WITH ADMINISTRATIVE PERMISSIONS

Some commands require administrative permissions to run. For example, if you try to release a DHCP lease using the `ipconfig /release` command in Windows 7, you'll see the following error if you haven't logged on as the administrator or started the command prompt with administrative permissions:

The requested operation requires elevation.

(Continues)

The dash is more common in UNIX systems. The forward slash is more common in Microsoft systems. However, you'll see both in Microsoft systems.

None of the commands presented in this chapter is case sensitive.

LAUNCHING THE COMMAND PROMPT WITH ADMINISTRATIVE PERMISSIONS *(Continued)*

If you're logged on with the system "administrator" account, the command prompt is automatically started with administrative permissions. However, if you're logged on with an account that is a member of the Administrators group, the command prompt does not start with administrative permissions.

The solution is to launch the command prompt with administrative permissions before executing the command. You can use the following steps in Windows 7 or Windows Server 2008 with administrative permissions:

1. Click Start.
2. Type **cmd** in the Start Search box.
3. The cmd shortcut will appear in the Programs list. Right-click cmd. Your display will look similar to the following graphic.



4. Select Run As Administrator. If prompted by User Account Control, click Yes to continue or enter appropriate administrator permissions depending on the prompt.

Checking the TCP/IP Configuration with ipconfig

ipconfig is one of the most valuable tools you have available to check and troubleshoot basic TCP/IP settings. You've already seen it in many of the chapters in this book, as shown in Table 14.1.

As a reminder, Listings 14.1 and 14.2 show the output of the ipconfig /all command with several key items highlighted.

TABLE 14.1 Use of ipconfig covered in previous chapters

Command	Chapter	Comments
ipconfig /all	3	Showed how to check the MAC address
ipconfig /all	5	Showed how to identify the IP address and DHCP status
ipconfig /all	6	Showed how to see whether your system is using Teredo for IPv6 compatibility
ipconfig	7 and 9	Showed how to identify the IP address of the default gateway
ipconfig /displaydns	10	Showed how to display the contents of the host cache
ipconfig /flushdns	10	Showed to remove the contents of the host cache
ipconfig /all	10	Showed how to determine the node type used for NetBIOS name resolution

Listing 14.1 identifies several pieces of key information shown by the ipconfig /all command. The Host Name value is the name of the computer. The Primary DNS Suffix value indicates that the computer joined the network.mta domain. The Node Type of Hybrid value indicates that NetBIOS names are resolved using WINS first and then broadcast.

Listing 14.1 ipconfig /all Windows IP configuration

```
C:\>ipconfig /all
```

```
Windows IP Configuration
```

◀

The NetBIOS name is created from the first 15 characters of the host name. If the first 15 characters of the host name are not unique, duplicate NetBIOS names will result.

```

Host Name . . . . . : Success1
Primary Dns Suffix . . . . . : networking.mta
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : Yes
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : networking.mta

```

Listing 14.2 shows the configuration of a network interface card (NIC) on the system. Some systems may have more than one NIC, and all of the NICs will be displayed.

Listing 14.2 ipconfig /all NIC data

Ethernet adapter Local Area Connection:

```

Connection-specific DNS Suffix . :
Description . . . . . :
    Intel 21140-Based PCI Fast Ethernet Adapter (Emulated)
Physical Address. . . . . : 00-03-FF-31-C4-CA
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . :
    fe80::1089:d255:6fa6:c8b%10(Preferred)
IPv4 Address. . . . . : 192.168.3.10(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.3.1
DNS Servers . . . . . : ::1
    192.168.3.10
Primary WINS Server . . . . . : 192.168.1.55
NetBIOS over Tcpi. . . . . : Enabled

```

Tunnel adapter Local Area Connection* 8:

```

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . :
    isatap.{EE889A77-7A07-4D8B-A288-595E1FA01
800}
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

```

The Physical Address value shows you the media access control (MAC) address of the NIC.

If it's a DHCP client, DHCP Enabled will be listed as Yes, and you'll also see the IP address of the DHCP server as long as the client was able to get an IP address from the DHCP server. In Listing 14.2, DHCP Enabled is set to No, so an IP address of a DHCP server is not available.

Autoconfiguration Enabled refers to Automatic Private IP Address (APIPA), and it is Yes by default. If the system couldn't get an IP address from the DHCP server and Autoconfiguration Enabled is set to Yes, you'll see an IPv4 address that starts with 169.254. If Autoconfiguration Enabled is set to No, then APIPA addresses are not assigned when a DHCP server can't be reached.

A link-local IPv6 address always starts with fe80 and indicates that an IPv6 address isn't assigned, but IPv6 is enabled.

You can use the subnet mask with the IPv4 address to determine the network ID. In Listing 14.2, the IP address of 192.168.3.10 and a subnet mask of 255.255.255.0 indicates a network ID of 192.168.3.0. The network ID must be the same as other hosts on the subnetwork, including the default gateway. The default gateway and the IPv4 address share the same subnet mask.

The address of the Domain Name System (DNS) server is needed for most host name resolution. In Listing 14.2, the same computer is the DNS server. You can tell this from the IPv6 loopback address (::1) and the same IPv4 address (192.168.3.10) that is assigned to the computer. If the DNS server address information is misconfigured, you'll probably experience problems with name resolution.

A Windows Internet Naming Server (WINS) server resolves NetBIOS names. If the network includes a WINS server, the computer configuration should include the IP address in the Primary WINS server section.

If you have a NIC but it isn't connected, it will be listed as follows:

```
Media State . . . . . : Media disconnected
```

This is an obvious sign that the cable isn't connected. If it does have a cable connected, check the link and activity lights on the NIC. If there are lights lit but the Media State indicates disconnected, check the cabling to ensure the following:

- ▶ The cable is seated completely in the NIC.
- ▶ The cable is seated completely in the wall jack.
- ▶ The cable is seated completely in the switch port (the switch will usually be in a separate room).
- ▶ Each of the cables is wired correctly.
- ▶ The cables are not bent excessively (beyond tolerance) when installing.

◀ An IP address starting with 169.254 in a network with DHCP should send alarm bells ringing in your head. The client is unable to get a DHCP address.

◀ The "Troubleshooting Connectivity with ping" section shows how to use ping to verify name resolution is working.

◀ Ethernet NICs have LED lights to indicate they are connected and have activity. Some have a single LED, and others have two LEDs.

▶
Before replacing hardware, you should always reboot the system first. It's a simple step and cures many ills.

One of the simplest ways to check the wiring is to identify a known good path to the switch and use it. For example, if another computer is working, unplug the cable from that computer, and plug it into the computer you're troubleshooting. If the problem computer now works, you know it's the wiring. If it doesn't work, you know the problem is internal to the computer, and you may need to replace the NIC.

Although the `ipconfig /all` command is very valuable, the `ipconfig` command has other switches you can use. Table 14.2 shows these other commands with some comments.

TABLE 14.2 Important `ipconfig` commands

Command and switch	Comments
<code>ipconfig /release</code> <code>ipconfig /release6</code>	Releases an IPv4 lease (or an IPv6 lease with <code>release6</code>) obtained from a DHCP server. This doesn't have any effect if a system has a statically assigned IP address instead of a DHCP-assigned IP address.
<code>ipconfig /renew</code> <code>ipconfig /renew6</code>	Renews the IPv4 lease process (or IPv6 lease process with <code>renew6</code>) from a DHCP server.
<code>ipconfig /displaydns</code>	Displays host cache (includes names from hosts file and names resolved from a DNS server). This is useful to determine whether a name is in cache with a specific IP address.
<code>ipconfig /flushdns</code>	Remove items from host cache (removes items resolved from a DNS server but not items placed in cache from the hosts file).
<code>ipconfig /registerdns</code>	Registers the computer's name and IP address with a DNS server. This creates a host (A) record on the DNS server so that the DNS server can resolve the IP address for other computers.

Here's one way you can use the `/displaydns` and `/flushdns` switches. Suppose you are troubleshooting a problem where you can't connect to another computer. You know that the remote computer's IP address is 192.168.1.5. However, when

▶
The `ipconfig /registerdns` command will work in a Microsoft domain using a DNS server. It will not create a record on an Internet DNS server from a home computer.

you use `ipconfig /displaydns`, it shows the remote computer with a different IP address of 10.5.4.3.

Use `ipconfig /flushdns` This should remove it from cache. If you enter `ipconfig /displaydns` but the faulty address is still in cache, it indicates it's in cache from the hosts file (not from DNS).

Try to Connect Again If the `ipconfig/flushdns` command removed the entry from cache, try to connect to the remote computer again. If it's successful, the problem is resolved. If not, use `ipconfig /displaydns` to see what address is displayed. If it's still not the correct address (10.5.4.3 instead of 192.168.1.5), then DNS is giving the wrong address for the computer. In other words, the problem is with DNS.

Use `ipconfig /registerdns` Go to the remote computer that you can't connect to, and enter `ipconfig /registerdns`. This should correct the record in DNS.

Flush DNS and Try Again Go back to the original computer, and enter `ipconfig /flushdns` to remove the cache entries. Try to connect again, and it should be successful. If not, check the cache with `ipconfig /displaydns`. If it shows the wrong address (10.5.4.3 instead of 192.168.1.5), you need to let the DNS administrator know.

Troubleshooting Connectivity with ping

`ping` is a valuable command to check connectivity with other computers. It uses Internet Control Message Protocol (ICMP), which is the messenger service of the networking world.

THE HISTORY OF PING

Mike Muus wrote the original Ping program used with UNIX systems while studying radar and sonar in 1983. Sonar sends echo signals out, and the reply sounds like “ping,” so he called his program Ping. He explained this at <http://ftp.arl.army.mil/~mike/ping.html>.

Somewhere along the line, someone decided that Ping was actually an acronym (PING) that stood for Packet INternet Groper. However, the source of this name is a little harder to find and verify.

You can ping an IP address or a host name. However, if you do use a host name, the first step in the process is that the ping will resolve the host name to an IP address. Listing 14.3 shows a basic ping command used to check connectivity with a server named DC1 in a network.

Listing 14.3 Successfully ping a computer

```
C:\>ping dc1

Pinging dc1 [192.168.1.112] with 32 bytes of data:
Reply from 192.168.1.112: bytes=32 time=1ms TTL=128
Reply from 192.168.1.112: bytes=32 time=1ms TTL=128
Reply from 192.168.1.112: bytes=32 time=1ms TTL=128
Reply from 192.168.1.112: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.112:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Two very important point things occurred here, and both provide you with valuable information.

First, the computer named dc1 was resolved to the IP address of 192.168.1.112. You can see that in the first line after the ping dc1 command. If name resolution did not work, you would instead see this error:

```
Ping request could not find host dc1. Please check the name and
try again.
```

Second, the ping command sent four packets to the server named dc1 and received four packets back. This reply verifies that the computer named dc1 is operational and able to respond to the ping request. If the server was not operational or not able to respond to the ping request, you would instead see a response similar to Listing 14.4.

Listing 14.4 Unsuccessfully ping a computer

```
C:\>ping dc1

Pinging dc1 [192.168.1.112] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.112:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Notice that even though the requests timed out, name resolution still worked. The ping command provides a reliable method to test name resolution. ping assumes the name (dc1 in the example) is a host name so attempts host name resolution methods first (such as DNS).

It's also important to realize that just because you receive a "Request timed out" response doesn't necessarily mean that the other computer is not operational. Secure networks and secure computers often have firewall rules blocking ICMP. If ICMP is blocked, the ping will fail even when the computer is operational.

The following are some other error messages you may see from the ping command:

Destination Host Unreachable This usually indicates a problem with routing. The local computer may not be configured with the correct default gateway, the remote computer may not be configured with the correct default gateway, or a router between the two may be misconfigured or faulty.

TTL Expired in Transit The time to live (TTL) value starts at 128 on Windows Server 2008 and 64 on Windows 7. It is decremented each time the ping passes through a router (also called a *hop*). If the TTL value is lower than the number of routers the ping must pass through to reach its destination, the ping packet is discarded. However, it's very rare that a ping will need to go through 64 or 128 routers, unless there is a problem with routing.

Consider Figure 14.2 for an example of how to use the ping command to troubleshoot a system. It shows several systems on two subnetworks separated by a router. Imagine that Sarah is unable to connect with the server named FS1 and she asks you for help. You can use the ping command to check for several different situations.

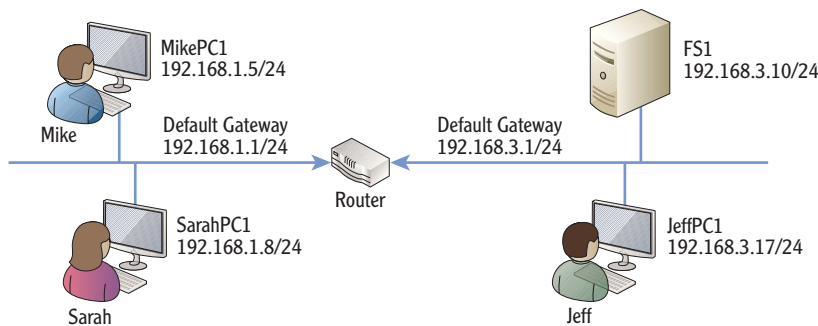


FIGURE 14.2 Using ping to test connectivity

◀ It's common for Windows 7 and Windows Server 2008 firewalls to block incoming ICMP traffic.

Copyright © 2011, John Wiley & Sons, Incorporated. All rights reserved.

You don't have to use the same order shown in these steps. You can use any order desired as long as you are able to identify the problem.

You may choose to do step 3 first to reduce troubleshooting steps. If it fails, the problem is on Sarah's side of the router (or the router itself).

Chapter 10 covered name resolution in depth, including DNS, the hosts cache, and the hosts file.

The following steps show how you can troubleshoot the problem with ping:

1. Enter **ping localhost** or **ping 127.0.0.1**.
By pinging the localhost or the loopback address (127.0.0.1), you can verify that TCP/IP is functioning correctly on Sarah's local system. You should get four successful replies. You can also use **ping -4 localhost** or **ping -6 localhost** to check IPv4 or IPv6, respectively.
2. Enter **ping 192.168.1.5**.
This checks connectivity through a switch (or a hub) but not the router. You can also ping any other computer with the same network ID. If these pings fail, the problem is on this side of the router.
3. Enter **ping 192.168.1.1**.
This pings the default gateway. Remember, you can use `ipconfig` to determine the IP address of the default gateway.
4. Enter **ping 192.168.3.1**.
This is the far side of the router. If successful, it indicates the router is successfully routing traffic. If it fails but you can ping 192.168.1.1 (the default gateway for 192.168.1.1), it indicates the router is causing the connectivity problem and may be misconfigured or faulty.
5. Enter **ping 192.168.3.10**.
This pings the IP address of the server named FS1. If this succeeds, it indicates that the server is up and operational. Remember, though, if it fails, it could be because the server is blocking ICMP traffic.
6. Enter **ping fs1**.
The first step of the ping should be to resolve the name `fs1` to the IP address of 192.168.3.10. If it can't resolve the name, the problem is with name resolution. The primary name resolution methods to check are DNS, the host cache, and the hosts file.

You can use other switches with ping as outlined in Table 14.3.

TABLE 14.3 Some ping switches

Switch	Comments
-4 Ping fs1 -4	Forces the use of an IPv4 address instead of IPv6.
-6 Ping fs1 -6	Forces the use of an IPv6 address instead of IPv4.

(Continues)

TABLE 14.3 (Continued)

Switch	Comments
-t Ping fs1 -t	Continuing pinging until stopped. You can press Ctrl+C to stop the pings.
-a Ping -a 192.168.1.5	Resolves IP addresses to host names. This requires that DNS has reverse lookup zones and associated pointer records, which are both optional. In other words, it may not work but doesn't indicate a problem.
-w Ping 192.168.1.5 -w 5000	This changes the timeout from the default of one second to five seconds (5,000 milliseconds). In cases when a computer is heavily loaded or under an attack, ping may fail with a timeout even when it is operational and ICMP is not blocked.

Identifying Routers with tracert

If your network includes multiple routers, you can use the `tracert` (pronounced as “trace route”) command to trace the path a packet takes through these routers. The `tracert` command can verify the path throughout an entire network.

`tracert` is similar to `ping` in that it checks connectivity. However, it also includes information on all routers between your computer and the destination computer.

The `tracert` command also uses ICMP. Although this normally works well, the results may be incomplete if ICMP is blocked.

Listing 14.5 shows the results of the `tracert` command from a home computer to the computer hosting the Microsoft.com website. Notice in a few of the lines that the result indicates that the request timed out. This isn't because the path is faulty but instead because ICMP is being blocked.

Listing 14.5 Output of tracert command

```
C:\>tracert microsoft.com
```

```
Tracing route to microsoft.com [207.46.232.182]
over a maximum of 30 hops:
```

```
  0  3 ms  <1 ms  <1 ms  [192.168.1.1]
  1  10 ms  8 ms  9 ms  10.10.184.1
  2  11 ms  11 ms  10 ms  68.10.14.77
  3  14 ms  10 ms  13 ms  172.22.48.33
```

Although the primary troubleshooting value of `tracert` is on internal networks, you can also use it to view the routing path to computers on the Internet.

Attackers often use ICMP to launch attacks. It's common for Internet systems to block ICMP traffic to protect against these attacks.

```

5    12 ms    9 ms    9 ms  nrfkdsrj02-ge600.0.rd.hr.cox.net
      [68.10.14.17]
6    16 ms    16 ms   54 ms  ashbbprj02-ae4.0.rd.as.cox.net
      [68.1.1.232]
7    15 ms    15 ms   17 ms  209.240.199.130
8    17 ms    22 ms   18 ms  ge-3-1-0-0.blu-64c-1a.ntwk.msn.net
      [207.46.47.29]
9    16 ms    17 ms   19 ms  ge-7-0-0-0.blu-64c-1b.ntwk.msn.net
      [207.46.43.113]
10   41 ms    78 ms   40 ms  xe-0-1-3-0.ch1-16c-1b.ntwk.msn.net
      [207.46.46.151]
11   44 ms    40 ms   51 ms  xe-7-0-0-0.ch1-16c-1a.ntwk.msn.net
      [207.46.43.146]
12   93 ms    90 ms   92 ms  ge-3-1-0-0.co1-64c-1a.ntwk.msn.net
      [207.46.46.118]
13   95 ms    93 ms   93 ms  ge-2-3-0-0.co1-64c-1b.ntwk.msn.net
      [207.46.35.151]
14   95 ms    95 ms   94 ms  ge-0-1-0-0.wst-64cb-1b.ntwk.msn.net
      [207.46.43.185]
15   93 ms    94 ms   94 ms  ge-4-3-0-0.tuk-64cb-1b.ntwk.msn.net
      [207.46.46.162]
16  142 ms    96 ms   97 ms  ten2-4.tuk-76c-1b.ntwk.msn.net
      [207.46.46.23]
17  107 ms   181 ms  101 ms  po16.tuk-65ns-mcs-1b.ntwk.msn.net
      [207.46.35.142]
18   *       *       *      Request timed out.
...
Trace complete.

```

▶ The round-trip times are recalculated for each hop. Additional packets are sent for each router to calculate the round-trip time for that router.

The `tracert` command identifies round-trip times for each hop listed in milliseconds (ms). Three different times are listed as `tracert` sends three separate probe requests by default for each hop. Shorter times indicate the trip is faster than longer times. You can see that the round-trips take progressively longer for each additional hop. Those routers are farther away.

It also lists the name of the routers when it can identify them. If `tracert` can't identify the name of the router, it just lists the IP address.

If the path between two systems is not working and `tracert` fails to complete, you can use the output to determine the location of the problem. For example, Listing 14.5 showed that the path was successful up to the 17th step. This indicates the 17th router from the source computer. The problem could be one of three things:

- ▶ The routing information on the 17th router is incorrect. This will prevent the data from reaching the 18th router.

- ▶ The 18th router is faulty.
- ▶ ICMP is blocked on the 18th router.

Table 14.4 lists some additional switches you can use with the `tracert` command.

TABLE 14.4 Some `tracert` switches

Switch	Comments
-4 <code>tracert -4 microsoft.com</code>	Forces the use of an IPv4 address instead of IPv6.
-6 <code>tracert -6 microsoft.com</code>	Forces the use of an IPv6 address instead of IPv4.
-d <code>tracert -d microsoft.com</code>	Suppresses IP address to name resolution. Only the IP addresses are listed.

Verifying the Routed Path with pathping

`pathping` is a combination of both `ping` and `tracert`. It starts by checking the route between the two computers similar to how `tracert` does so. It then uses `ping` to check for connectivity at each router.

It will send each router 100 echo request commands, and it expects to receive 100 echo replies back. It then calculates the percentage of data loss based on what it receives. For example, if it receives 100 replies, there is 0 percent packet loss. However, if it receives only 95 replies, there is 5 percent packet loss.

Listing 14.6 shows the output of a `pathping` command. Notice that in the first part of the `pathping` process, it checks the path similar to `tracert`. Lines 1 through 13 represent routers identified as hops. After it calculates the path, it then starts calculating the statistics by measuring loss. By default, the calculation process takes five minutes.

Listing 14.6: Output of `pathping` command

```
C:\Users\Dar>pathping microsoft.com

Tracing route to microsoft.com [207.46.197.32]
over a maximum of 30 hops:
  0  Laptop.hr.cox.net [192.168.1.114]
  1  [192.168.1.1]
  2  10.10.184.1
```

```

3 68.10.14.77
4 172.22.48.33
5 nrfkdsrj02-ge600.0.rd.hr.cox.net [68.10.14.17]
6 ashbbprj02-ae4.0.rd.as.cox.net [68.1.1.232]
7 209.240.199.130
8 ge-3-1-0-0.blu-64c-1a.ntwk.msn.net [207.46.47.29]
9 xe-0-1-3-0.ch1-16c-1a.ntwk.msn.net [207.46.46.169]
10 ge-3-1-0-0.co1-64c-1a.ntwk.msn.net [207.46.46.118]
11 ge-1-0-0-0.wst-64cb-1a.ntwk.msn.net [207.46.43.163]
12 ge-7-1-0-0.cpk-64c-1b.ntwk.msn.net [207.46.43.228]
13 ten3-4.cpk-76c-1a.ntwk.msn.net [207.46.47.197]
14 * * *
Computing statistics for 325 seconds...
Hop  RTT      Source to Here   This Node/Link
      Lost/Sent = Pct Lost/Sent = Pct  Address
0
      0/ 100 = 0%   0/ 100 = 0%     [192.168.1.114]
1   3ms      0/ 100 = 0%     0/ 100 = 0%     [192.168.1.1]
      0/ 100 = 0%   |
2   ---     100/ 100 =100%  100/ 100 =100%  10.10.184.1
      0/ 100 = 0%   |
3   11ms    0/ 100 = 0%     0/ 100 = 0%     68.10.14.77
      0/ 100 = 0%   |
4   ---     100/ 100 =100%  100/ 100 =100%  172.22.48.33
      0/ 100 = 0%   |
5   14ms    0/ 100 = 0%     0/ 100 = 0%
      nrfkdsrj02-ge600.0.rd.hr.cox.net
      [68.10.14.17]
      0/ 100 = 0%   |
6   25ms    0/ 100 = 0%     0/ 100 = 0%
      ashbbprj02-ae4.0.rd.as.cox.net
      [68.1.1.232]
      0/ 100 = 0%   |
7   21ms    0/ 100 = 0%     0/ 100 = 0%     209.240.199.130
      100/ 100 =100% |
8   ---     100/ 100 =100%  0/ 100 = 0%
      ge-3-1-0-0.blu-64c-1a.ntwk.msn.net
      [207.46.47.29]
. . .
Trace complete.

```

The last few hops are similar to hop 8 and aren't listed. They are showing 100 percent loss since 100 packets were sent and 100 packets were lost. Again, this is likely because the routers are blocking ICMP, not because there is actual data loss.

If you have a large network with many routers, the `pathping` command can be useful to help you identify whether you are experiencing any data loss at specific routers. It could be that the routers simply have too much traffic for their

capacity. You can either offload some of the traffic to another subnet or increase the capacity of the router.

Table 14.5 lists some additional switches you can use with the pathping command.

TABLE 14.5 Some pathping switches

Switch	Comments
-4 pathping -4 microsoft.com	Forces the use of an IPv4 address instead of IPv6.
-6 pathping -6 microsoft.com	Forces the use of an IPv6 address instead of IPv4.
-n pathping -n microsoft.com	Suppresses IP address to name resolution. Only the IP addresses are listed.
-q pathping -q 50 microsoft.com	Changes the number of queries per hop. By default, 100 queries per hop are used.

Viewing TCP/IP Statistics with netstat

You can use the netstat (short for network statistics) command to display information on any TCP/IP connections on your computer. You can use it show all the connections, ports, and applications involved with network connections. You can also use it to check TCP/IP statistics.

Table 14.6 shows the common netstat commands.

TABLE 14.6 Common netstat commands

Command	Comments
Netstat -a	Shows all connections and listening ports.
Netstat -b	Shows connections that all applications are using to connect on the network (including the Internet if the client is connected to the Internet).
Netstat -e	Shows Ethernet statistics.
Netstat -f	Shows fully qualified domain names (FQDNs).
Netstat -n	Shows both addresses and port numbers in numerical form.

Switches can be combined. For example, the netstat -ano command combines the output of the -a, -n, and -o switches.

(Continues)

TABLE 14.6 (Continued)

Command	Comments
Netstat -o	Includes the process that owns the connection.
Netstat -p protocol Netstat -p TCP	Shows connections for specific protocols. You can use any of the following protocols: IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6. For example, netstat -p TCP would show connections for TCP only.
Netstat -r	Shows the routing table. This is the same routing table you can see with the route print command.
Netstat -s	Shows statistics for the protocols running on the system. This includes packets received, packets sent, errors, and more.
Netstat interval Netstat 15	Redisplays the statistics after waiting the interval period. The interval is specified in seconds as netstat 15 to wait 15 seconds before executing the netstat command again.

Listing 14.7 shows a basic listing of open ports for a computer running on a network without any Internet Explorer sessions opened. With a few web pages open in Internet Explorer, the number of open ports can easily fill a page.

Listing 14.7: Output of netstat command

```
C:\Users\Dar>netstat
```

```
Active Connections
```

Proto	Local Address	Foreign Address	State
TCP	192.168.1.114:135	WIN7-PC:49766	ESTABLISHED
TCP	192.168.1.114:1030	WIN7-PC:49767	ESTABLISHED
TCP	192.168.1.114:1060	MYBOOKWORLD:microsoft-ds	ESTABLISHED
TCP	192.168.1.114:2078	beta:http	ESTABLISHED
TCP	192.168.1.114:3389	Server08R2:56080	ESTABLISHED
TCP	[fe80::41f0:f763:5451:198a%10]:135	Darri1-PC:50506	ESTABLISHED

The local address indicates the local computer (with an IP address of 192.168.1.114) and is in the format of *IP address: port*. The foreign address indicates the name

Chapter 4 explained ports in depth. It includes a listing of many of the well-known ports in the range of 0 to 1023.



or IP address of the remote computer. The State column indicates the state of the connection.

Some of the common states of a connection are as follows:

ESTABLISHED Indicates that a TCP session is established

LISTENING Indicates the system is ready to accept a connection

CLOSE_WAIT Indicates that the system is waiting for a final packet from the remote system to close the connection

For a full listing of all possible session connections, check out RFC 793 (www.faqs.org/rfcs/rfc793.html). Some connection states are described in RFC 793 with a hyphen, but netstat displays them with an underscore. For example, RFC 793 uses CLOSE-WAIT, but netstat displays CLOSE_WAIT.

You may run the netstat command and see something that looks suspicious. For example, the Foreign Address of beta:http looks a little odd, and you may want to get more information about it. You can use the netstat -b command to identify the application or process using the port, as shown in Listing 14.8. The netstat -b command is one of the commands that must be run from an administrator prompt.

Listing 14.8 Using netstat -b to identify applications and processes

```
C:\>netstat -b

Active Connections

    Proto Local Address           Foreign Address         State
    TCP    192.168.1.114:135     WIN7-PC:49766          ESTABLISHED
    RpcSs
    [svchost.exe]
    TCP    192.168.1.114:1030    WIN7-PC:49767          ESTABLISHED
    [spoolsv.exe]
    TCP    192.168.1.114:1060    MYBOOKWORLD:microsoft-ds ESTABLISHED
    Can not obtain ownership information
    TCP    192.168.1.114:2078    beta:http               ESTABLISHED
    [OUTLOOK.EXE]
    TCP    192.168.1.114:3389    Server08R2:56080        ESTABLISHED
    CryptSvc
    [svchost.exe]
```

If you have a little information about ports, you can use the output of the netstat command, the names of the applications, and the port numbers to determine what each of the ports is doing.

If you want to search RFC 793, you need to search with the hyphen. For example, you can search CLOSE-WAIT, but you won't find anything if you search on CLOSE_WAIT.



netstat can be useful in detecting spyware and malware. If the applications are unknown, they may be malicious.

Port 135 Port 135 is used for NetBIOS and Remote Procedure Calls (RPCs) in Windows systems. This shows an IPv4 connection (the first line) with another computer named Win7-PC in the network.

Port 1030 This is being used by the print spooler service (`spoolsv.exe`).

Port 1060 This port is being used to connect to a network drive (named MYBOOKWORLD) that is mapped to the system as an additional drive.

Port 2078 This is being used by Microsoft Outlook for a connection to the Internet.

Port 3389 CryptSvc is short for the Cryptographic Services service. Port 3389 is the port used by Microsoft for Remote Desktop Services (RDS). Combined, they indicate an RDS session is established with a remote computer named Server08R2.

That still may not be enough information if the application looks suspicious. You can use the following steps to get more information about any of these connections:

1. Enter **netstat** at the command prompt.
2. Review the listing, and determine whether there are ports you want to investigate more.

Note the port number in the Local Address column. For example, you may want to investigate the `beta:http` line, which shows port 2078.

3. Enter **netstat -ano** at the command prompt.

This provides a more detailed listing including the process ID (PID). Look for the line with your port number. The following code snippet shows the line for this port:

```
Proto Local Address      Foreign Address  State           PID
TCP    192.168.1.114:2078  65.55.11.163:80  ESTABLISHED    5356
```

The PID column shows a PID of 5356 for port 2078.

4. Launch Task Manager by pressing the Ctrl+Shift+Esc keys at the same time.
5. Select the Processes tab.
6. Click View, and click Select Columns.
7. Select the PID (Process Identifier) box. Click OK.

8. Look for the entry with the PID you're interested in. Your display will look similar to Figure 14.3.

Notice that it shows that the Image Name value (the process) is Outlook.

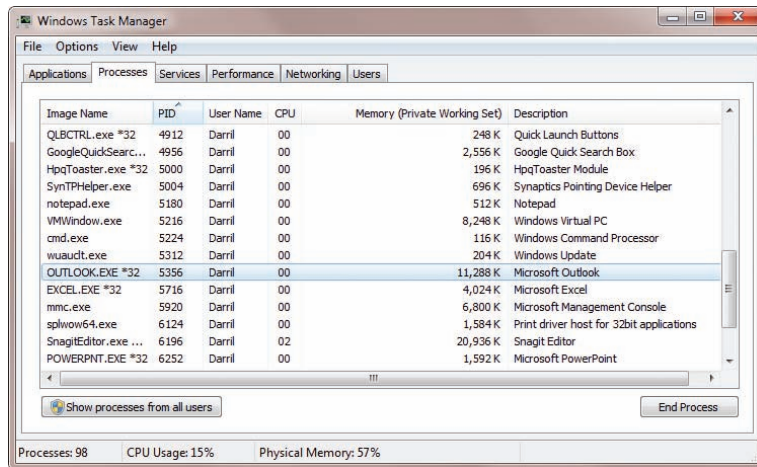


FIGURE 14.3 Locating the PID in Task Manager

9. Launch the Performance Monitor by clicking Start, typing in **perfmon**, and pressing Enter.
- In Windows Server 2008, the default display shows the resource overview. This provides the information you need.
 - In Windows Server 2008 R2 and Windows 7, you need to launch the Resource Monitor by right-clicking Monitoring Tools and selecting Resource Monitor.
10. Look for the PID in the CPU, Disk, Network, and Memory sections.

This allows you to get additional information on the process such as how much resources the process is consuming. Figure 14.4 shows the Resource Monitor on a Windows 7 system.

You can get more advanced in your searches to narrow down the source of connections. The goal of these steps isn't to make you a master at identifying all the resources that an open port may be using but instead to show you some of the possibilities. It gives you a chance to dig into your system and learn a little more about it.

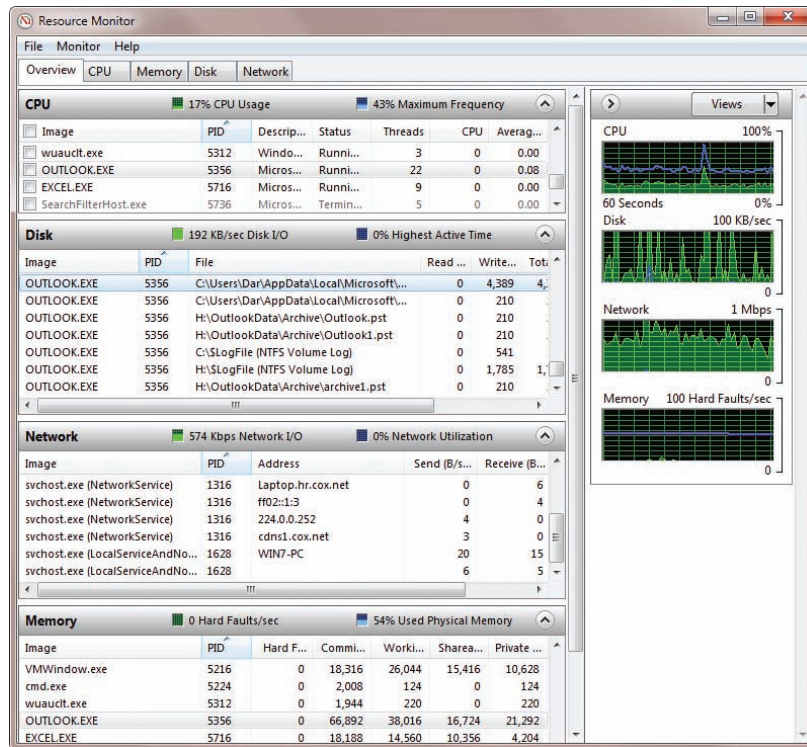


FIGURE 14.4 Viewing resource usage in the Resource Monitor on a Windows 7 system

Installing Telnet

Telnet is a lesser used tool for troubleshooting. It is not installed in Windows systems by default because of security risks, but it can be added. Attackers often use Telnet to check for open ports on a system that has Telnet enabled, so it is more secure to keep Telnet disabled unless it's needed.

When Telnet is installed on client and server computers, you can connect a Telnet client to a Telnet server. It provides a command-line interface that allows you to run Telnet commands from the Telnet client that are executed on the Telnet server. Commands include command-line programs, shell commands, and scripts.

Many programs that use Telnet can be configured to encrypt the traffic with Secure Shell (SSH). This ensures that attackers are not able to read the traffic.

▶
One of the risks with Telnet is that commands go across the network in clear text. An attacker with a sniffer can capture the traffic and easily read it.

You can use the following steps to install both the Telnet client and the Telnet server on a Windows Server 2008 server:

1. Click Start > Administrative Tools > Server Manager.
2. Select Features. Click Add Features.
3. Scroll down, and select Telnet Client and Telnet Server, as shown in Figure 14.5. Click Next.
4. Click Install. When the installation is complete, click Close.

At this point, Telnet is installed. If you enter `telnet /?` at the command prompt, it will show the output of a help file. You can start a Telnet session from a Telnet client with the following command:

```
Telnet TelnetServerName
```

If you have more interest in Telnet, you can check out Microsoft's Telnet Operations Guide at <http://technet.microsoft.com/library/cc753164.aspx>.

Telnet presents significant risks to computers in a network. You should not install Telnet on a computer in a production environment unless it's actually needed.

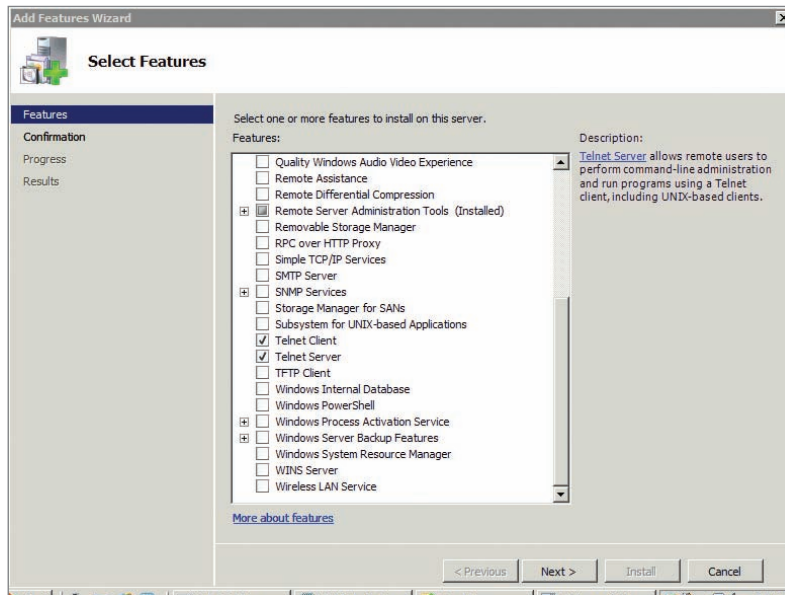


FIGURE 14.5 Adding the Telnet Client and Telnet Server features

THE ESSENTIALS AND BEYOND

In this chapter, you learned about many different methods for troubleshooting network and connectivity problems. You use these tools from the command prompt. Useful commands include `ipconfig`, `ping`, `tracert`, `pathping`, and `netstat`. You learned how to use these tools to check the configuration of a system and check its interoperability on a network. You also learned how Telnet can be added to a system if needed.

ADDITIONAL EXERCISES

- ▶ Remove all of the entries in your hosts cache that have been resolved by DNS.
- ▶ Identify your default gateway, and check connectivity with it.
- ▶ Identify the DNS server you are using, and identify how many routers are between your computer and the DNS server.
- ▶ Identify whether there is any packet loss on routers between your computer and your DNS server.

To compare your answers to the author's, please visit www.sybex.com/go/networkingessentials.

REVIEW QUESTIONS

1. What switch can you use to view help for a command?
A. `/?` **C.** `/hlp`
B. `?` **D.** `/?Help`
2. What command can you use to determine a computer's default gateway? (Choose all that apply.)
A. `ipconfig` **C.** `netstat`
B. `ipconfig /all` **D.** `telnet`
3. You want to verify a computer can connect with the default gateway. It has an IP address of 192.168.1.1. What command should you use?
A. `netstat 192.168.1.1` **C.** `ping 192.168.1.1`
B. `192.168.1.1 Netstat` **D.** `192.168.1.1 Ping`
4. You want to ensure that the `ping` command only uses IPv4. What switch should you use?

(Continues)

THE ESSENTIALS AND BEYOND *(Continued)*

5. You use the `ping` command to check connectivity with a server named DC1 and receive the following error: "Ping request could not find host dc1. Please check the name and try again."
What does this error mean?
- A.** DHCP is down. **C.** A router is not configured properly.
B. Name resolution didn't work. **D.** The default gateway isn't configured.
6. You use the `ping` command to check connectivity with a server named FS1 and receive the following error: "Destination Host Unreachable."
What is the most likely reason for this error?
- A.** DHCP is down. **C.** A router is not configured properly.
B. Name resolution didn't work. **D.** DNS isn't configured.
7. True or false. You can measure packet loss using the `tracert` command.
8. What tool can you use to view TCP/IP statistics including the number of packets that have been sent and received?
9. What is the command to view all open ports including known applications on a Windows Server 2008 system?
- A.** `ipconfig /all` **C.** `netstat`
B. `pathping` **D.** `netstat -b`
10. True or false. The Telnet client is installed by default in Windows Server 2008.

