CHAPTER 4

Troubleshooting Cisco TCP/IP

This chapter offers suggestions for troubleshooting problems that may arise when installing and using Cisco TCP/IP Suite. This chapter includes:

- Understanding General Application Error Messages
- Testing Your Network Connection
- Troubleshooting the TCP/IP Stack
- Advanced Network Troubleshooting
- Troubleshooting Dialer Serial Connections
- Troubleshooting FTP Client and Server
- Troubleshooting Netscape Mail
- Troubleshooting NFS
- Troubleshooting Netscape Navigator
- Troubleshooting Telnet
- Troubleshooting Kerberos

Understanding General Application Error Messages

This section identifies general error messages you might see for various Cisco TCP/IP Suite applications. Each message includes an explanation and recommended actions for resolving the problem.

Error Message `Address already in use`

Explanation Another application is running and using the same port number as the application displaying this message. This usually occurs with a server application listening on a well known port.

Recommended Action Using the Monitor application, show the Connection Table to verify that another application has the port number.

Error Message `Broken pipe`

Explanation An operation was requested on a socket that is no longer connected or considered a socket.

Recommended Action If the remote host has a logging facility, use it to determine why the connection was disconnected. Use any available network analysis tools to determine why the connection was disconnected.

Error Message `Connection refused`

Explanation The remote host refused this connection request.

Recommended Action Make sure a server application that can accept the connection is running on the target host. Use available tools on the target host to display the connection table. Typical commands are **netstat** on UNIX hosts, and **MULTINET SHOW/CONNECTIONS** on VMS hosts using Cisco MultiNet for OpenVMS. Ask the network administrator if there are any access restrictions on the server application.

Error Message `Connection reset by peer`

Explanation An operation was requested on a socket that is no longer connected or considered a socket.

Recommended Action If the remote host has a logging facility, use it to determine why the connection was disconnected. Use any available network analysis tools to determine why the connection was disconnected. Also look for duplicate *WINSOCK.DLL* files.

Error Message `Connection timed out`

Explanation The application could not establish a connection with the remote host.

Recommended Action Use the Ping application to verify that you have a route to the target host and that the target host is running. However, firewalls often allow Ping to work but not other services such as Telnet or FTP. You may have to contact the network administrator for the remote host for assistance.

Error Message `Could not contact DNS Server`

Explanation The Ping application cannot communicate with the DNS server.

Recommended Action Verify that the IP address of the DNS server is correct, the DNS server is operational, and the network is operational.

Error Message `DNS Server failure`

Explanation The DNS server failed to respond to the request for name service.

Recommended Action Verify that the DNS server is operational.

Error Message `Host not found`

Explanation Either the name entered for the target host is not a valid name or it cannot be resolved by DNS.

Recommended Action Verify that you entered the name correctly. Verify that the host name and IP address are accurate in DNS.

Error Message `Network is down`

Explanation The Cisco TCP/IP Suite kernel is not loaded properly or cannot communicate with the network card driver.

Recommended Action Check the ODI, NDIS 2.0, or NDIS 3.0 configuration.

Error Message `Network is unreachable`

Explanation The network portion of the destination IP address is different from the local network. There is no route to the remote network.

Recommended Action Using the Configuration Utility, verify that the default route is correct in the Routing tab. Using network analysis tools on another machine, check the route that the packet takes to the remote network and verify that packets are being forwarded to the default gateway.

Testing Your Network Connection

If your workstation does not communicate on the network as expected, you can use the Ping application to test Cisco TCP/IP Suite and network communications. Your network administrator may be able to provide additional assistance.

Ping tests network connections by sending ICMP (Internet Control Message Protocol) echo requests to a target host and waiting for replies. When testing a connection, Ping tracks the number of packets sent, the number of replies received, the percentage of packets lost, and the amount of time required for the packets to reach the destination and for replies to be received. This information lets you verify whether your workstation can communicate with other hosts and whether information was lost.

To start Ping, choose Ping from the Cisco Suite 100 group on the **Start** menu, or double-click the Ping icon in the Cisco Suite 100 program group. As an alternative, you can start Net Tools and click the Ping tab.

If all of the following Ping attempts are successful, Cisco TCP/IP Suite is configured correctly and working as it should. However, firewalls often allow Ping to work but not other services such as Telnet or FTP. If you encounter problems, check your configuration to make sure that you entered all information correctly. You can do this by using the

Configuration Utility. If you are not using the Cisco TCP/IP stack, use the configuration utility for your stack. If TCP/IP is configured correctly, and you are having trouble connecting to a remote host, contact the administrator for that host for assistance.

If the Cisco TCP/IP Suite installed correctly and the configuration information is correct but you are still experiencing difficulties, contact your network administrator.

See the online help for more information about how to use Ping.

This section includes the following topics. Check your installation by carrying out the Ping attempts in the order given.

1. Ping Your Workstation by Loopback Address
2. Ping Your Workstation by IP Address
3. Ping Another Workstation on Your Network by IP Address
4. Ping Your Default Router's IP Address
5. Ping a Remote System by IP Address
6. Ping Your Workstation by Name
7. Ping Another Workstation on Your Network by Name
8. Ping a Remote System by Name

Ping Your Workstation by Loopback Address

To verify that your workstation can receive and send responses, and that TCP/IP is operating correctly, Ping the special loopback address 127.0.0.1.

If the Ping is not successful:

1. Make sure Cisco TCP/IP Suite was installed correctly.
2. Call Technical Support.

Ping Your Workstation by IP Address

To verify that your workstation's network interface card and driver are working correctly, Ping your workstation by IP address.

If the Ping is not successful:

1. Verify that the network adapter is configured correctly for your workstation.
2. Use the Configuration Utility to verify that your workstation's IP address and subnet mask are correct.

Ping Another Workstation on Your Network by IP Address

To verify that your workstation can communicate with other systems on the local network, Ping another local system by IP address.

If the Ping is not successful:

1. Verify the other system is securely attached to the network and is running.
2. Verify you are using the correct IP address for the other system.

Ping Your Default Router's IP Address

To verify that your workstation is successfully communicating with the router used to connect your network to other networks, Ping your network router's IP address.

If the Ping is not successful:

1. Verify that your workstation is plugged into the network.
2. Use the Configuration Utility to verify that your workstation's IP address and subnet mask are correct.
3. Verify that you are using the correct router address, and that the default route is correctly defined in the Configuration Utility.
4. Verify that an Ethernet, Token-Ring, or FDDI interface is enabled.
5. Contact your network administrator and ask if the router is working properly.

Ping a Remote System by IP Address

To verify that your workstation can communicate with hosts on other networks, Ping a host on a close, but different, network by IP address (for example, on another network connected to your router). If the Ping is successful, you might also try Pinging hosts on increasingly remote networks if you are trying to isolate a specific connectivity problem.

If the Ping is not successful:

1. Use the Configuration Utility to verify that the IP address of the default route is correct.
2. Verify that the remote host is running and securely attached to the network.
3. Use Net Tools TraceRoute to determine where the failure occurs.

Ping Your Workstation by Name

To verify that host names are being resolved to IP addresses correctly, Ping your workstation by host name.

If the Ping is not successful:

1. Verify your workstation is securely attached to the network.
2. Use the Configuration Utility to verify that your workstation's host name and domain name are correct.
3. If your workstation uses DNS to resolve names, use the Configuration Utility to verify that the IP address of the DNS server is correct. Ping the DNS server by IP address to verify the DNS server is running and available.
4. If your workstation uses a host table to resolve names, use the Configuration Utility to verify that your workstation's host name and IP address are correct.

Ping Another Workstation on Your Network by Name

To verify that your workstation can communicate with other systems on the local network by name, Ping another system on your local network by host name.

If the Ping is not successful:

1. Verify you entered the host name correctly.

2 Verify the other machine is running and securely attached to the network.

3 If your workstation uses DNS to resolve names, use the Configuration Utility to confirm that the IP address of the DNS server is correct. Ping the DNS server by IP address to verify it is running and available.

4 If your workstation uses a host table to resolve names, use the Configuration Utility to verify that the host name and IP address of the other system are correct in the host table.

Ping a Remote System by Name

To verify that your workstation can communicate with hosts on other networks, Ping a host on a close, but different, network by name (for example, on another network connected to your router). If the Ping is successful, you might also try Pinging hosts on increasingly remote networks if you are trying to isolate a specific connectivity problem.

If the Ping is not successful:

1 Verify you entered the host name correctly.

2 Verify that the remote host is running and securely attached to the network.

3 If your workstation uses DNS to resolve names, use the Configuration Utility to confirm that the IP address of the DNS server is correct. Ping the DNS server by IP address to verify it is running and available.

4 If your workstation uses a host table to resolve names, use the Configuration Utility to verify that the host name and IP address of the other system are correct in the host table.

5 Use the Configuration Utility to verify that the IP address of the default route is correct.

6 Use Net Tools TraceRoute to determine where the failure occurs.

Troubleshooting the TCP/IP Stack

The following sections provide troubleshooting advice for the TCP/IP stack. The information in this section only applies to the Cisco TCP/IP stack: if you are using Microsoft's stack, consult the Microsoft documentation for help on troubleshooting the TCP/IP stack.

Monitoring the TCP/IP Stack

Use Monitor to troubleshoot TCP/IP stack problems. Monitor displays the contents of various caches maintained by the Cisco TCP/IP stack.

To start Monitor on Windows 95 systems, choose it from the Cisco Suite 100 program group on the **Start** menu. On Windows 3.x, double-click the Monitor icon in the program group. Monitor is not available on Windows NT.

With Monitor, you can view:

- The ARP cache, which contains IP-to-hardware-address mappings for local systems with which your workstation communicates
- Buffer statistics, which indicate the amount of available space for temporary storage of IP data being sent or received
- The connection table, which shows your workstation's current connections
- The interface table, which displays information about your workstation's interfaces and their configuration
- The protocol statistics, which show detailed networking statistics for all current connections
- The routing table, which identifies the hosts or networks with which your workstation is communicating and the routes being used

See the online help for Monitor for information about how to use these statistics, on how to print and save statistics, and on other things you can do with Monitor.

Understanding Stack Error Messages

The TCP/IP stack displays an error message if it cannot perform as expected or if it encounters other errors as part of its normal operation. These messages either appear in a pop-up window or are reported through another utility, such as Ping.

If you encounter these error messages:

1. Follow any instructions that appear in the message. For example, some messages may ask you to close all applications, exit Windows, and reboot your workstation.

2. Refer to the following error message descriptions for more suggestions on how to resolve the problem.
3. Ask your network administrator for help.
4. Contact Technical Support.

Error Message `ARP: Changed hardware address for IP address` *`n.n.n.n`*

Explanation The TCP/IP stack has detected that the IP address specified in the error message has a new hardware address.

Recommended Action Verify that the ARP cache reflects the correct hardware address for the specified IP address, or ignore the message.

Error Message `ARP: Host hardware address is broadcast`

Explanation The TCP/IP stack has detected that the hardware address of the host it is trying to reach is a broadcast address.

Recommended Action Verify that the hardware address for the target host is the correct hardware address.

Error Message `Default Gateway ioctl failed`

Explanation The default route is either missing from *MULTINET.INI* or is incorrect.

Recommended Action Verify that the default route, host IP address, and subnet mask are correct in the Configuration utility.

Error Message `Duplicate IP address detected`

Explanation The TCP/IP stack has detected one IP address with two hardware addresses.

Recommended Action Identify the host with the incorrect IP address and correct it.

Error Message `Error: n`
`Please close all applications, exit Windows, and reboot your system`

Explanation The TCP/IP stack has detected an error in the kernel.

Recommended Action Close any open applications, exit Windows, and reboot your workstation. Contact Technical Support.

Error Message `Initialization of Cisco TCP/IP Suite Kernel failed`

Explanation The TCP/IP stack detected a problem with system files or with the stack configuration.

Recommended Action Using the Configuration Utility, delete the enabled interface and add it to the configuration again. Contact Technical Support if the problem persists.

Error Message `Initialization of system timer failed`

Explanation Windows is out of resources.

Recommended Action Reboot your workstation. Contact Technical Support if the problem persists.

Error Message `Initialization of VMULTINT.386 failed.`

Explanation The TCP/IP stack detected a problem with system files or with the stack configuration.

Recommended Action Using the Configuration Utility, delete the enabled interface and add it to the configuration again. Contact Technical Support if the problem persists.

Error Message `Interface n: Broadcast address ioctl failed`

Explanation The broadcast address is either missing from *MULTINET.INI* or is incorrect.

Recommended Action Verify that the broadcast address, host IP address, and subnet mask are correct in the Configuration Utility.

Error Message `Interface n: IP Address ioctl failed`

Explanation Your workstation's IP address is either missing from *MULTINET.INI* or is incorrect.

Recommended Action Verify that your workstation's IP address and subnet mask are correct in the Configuration Utility.

Error Message `Interface n: Net Mask ioctl failed.`

Explanation The subnet mask is either missing from *MULTINET.INI* or is incorrect.

Recommended Action Verify that the subnet mask and the IP address are correct in the Configuration Utility.

Error Message `Interface n: wrong Broadcast Address`

Explanation The broadcast address is either missing from *MULTINET.INI* or is incorrect.

Recommended Action Verify that the broadcast address and subnet mask are correct in the Configuration Utility.

Error Message `Interface n: wrong IP Address`

Explanation The IP address is either missing from *MULTINET.INI* or is incorrect.

Recommended Action Verify that the IP address is correct in the Configuration Utility.

Error Message `Interface n: wrong Net Mask`

Explanation The subnet mask is either missing from *MULTINET.INI* or is incorrect.

Recommended Action Verify that the subnet mask and IP address are correct in the Configuration Utility.

Error Message `Loading TGVMOD.MOD failed`

Explanation TGVMOD.MOD is either missing or corrupt, or does not have sufficient DOS memory to load properly.

Recommended Action For Windows 3.x, make sure TGVMOD.MOD is in the DOS path. If you cannot locate TGVMOD.MOD, reinstall the Cisco TCP/IP stack. For both Windows 95 and Windows 3.x, make sure your system has sufficient DOS memory. Close any unused applications to free memory.

Error Message `mbuf map full`

Explanation The TCP/IP stack does not have enough memory to complete the requested action.

Recommended Action Make sure your system has sufficient memory. Close any unused applications to free memory. Contact Technical Support if the problem persists.

Error Message `Memory allocation failed.`

Explanation The TCP/IP stack does not have sufficient DOS memory to operate properly.

Recommended Action Make sure that your system has sufficient DOS memory. Reboot your workstation. Contact Technical Support if the problem persists.

Error Message `No available Callout structures`

Explanation The TCP/IP stack does not have enough memory to complete the requested action.

Recommended Action Make sure your system has sufficient memory. Close any unused applications to free memory. Contact Technical Support if the problem persists.

Error Message `No interface defined`

Explanation Your workstation does not have an interface defined for use on the network.

Recommended Action Use the Configuration Utility to add an interface to your workstation's configuration.

Error Message `Registering a notification callback failed`

Explanation Windows is out of resources.

Recommended Action Reboot your workstation. Contact Technical support if the problem persists.

Error Message `Route` *`n`*`: route ioctl failed`

Explanation The route is either missing from *MULTINET.INI* or is incorrect.

Recommended Action Verify that the route, subnet mask, and host IP address are correct in the Configuration Utility.

Error Message `Route` *`n`*`: wrong Address Qualifier`

Explanation The destination address of the specified route was incorrectly identified as a host or network.

Recommended Action Specify the correct address qualifier (that is, either host or network) for the specified route in the Configuration Utility.

Error Message `Route` *`n`*`: wrong Destination Address`

Explanation The destination address of the specified route is incorrect.

Recommended Action Correct the destination address for the specified route in the Configuration Utility.

Error Message `Route` *`n`*`: wrong Gateway Address`

Explanation The IP address of the gateway is incorrect for the specified route.

Recommended Action Correct the gateway IP address in the Configuration Utility.

Error Message `Socket allocation failed`

Explanation Windows is out of resources.

Recommended Action Reboot your workstation. Contact Technical Support if the problem persists.

Error Message `VMULTINT.386: driver initialization failed`

Explanation The TCP/IP stack detected a problem with system files or with TCP/IP configuration.

Recommended Action Using the Configuration utility, delete the enabled interface and add it to the configuration again.

Error Message `Wrong default gateway`

Explanation The default gateway is either missing from *MULTINET.INI* or is incorrect.

Recommended Action Verify that the IP address of the default gateway is correct in the Configuration Utility. Contact Technical Support if the problem persists.

Error Message `Wrong host name`

Explanation Your workstation's host name is either missing from *MULTINET.INI* or is incorrect.

Recommended Action Verify that your workstation's host name is correct in the Configuration Utility.

Getting the TCP/IP Kernel to Start

If the TCP/IP kernel does not start, the system files probably contain incomplete or incorrect information. The Cisco TCP/IP Suite installation program makes several changes to various system and configuration files. If the installation program does not complete properly, or if these files are later changed manually, the Cisco TCP/IP Suite-specific information in these files may be incorrect.

To correct the condition, reinstall Cisco TCP/IP Suite, or edit the system files and insert the correct information.

Checking WINSOCK.DLL

If Cisco TCP/IP Suite is not working properly:

- If you are using Windows 3.x, verify that your workstation has only one *WINSOCK.DLL* file on the DOS path. If Cisco TCP/IP Suite encounters another *WINSOCK.DLL*, it will not work correctly. Use the Search command in the File Manager (in the **File** menu) to search for *WINSOCK.DLL*, and compare its location to the path displayed with the DOS PATH command.
- If you are using Windows 95, verify that your workstation has *WINSOCK.DLL* in the Windows installation directory, and *WSOCK32.DLL* in the Windows system directory. Use the Find command on the **Start** menu to search for these files.

Handling Kernel Initialization Errors with Windows for Workgroups

The SMC NDIS3 drivers distributed with Windows for Workgroups are not truly NDIS3-compliant. If you are using Windows for Workgroups and NDIS3 network drivers, and have an SMC-brand network interface card, you may experience errors during TCP/IP kernel initialization. To correct the problem, obtain updated NDIS3 drivers from SMC.

Getting Other WinSock-based Applications to Run

If you cannot run WinSock-based applications, or can run them only after running a Cisco TCP/IP Suite application, Windows may not be able to locate the necessary *.DLL* files for operation. These are the possible causes:

- If you are using Windows 3.x:
  - The Cisco TCP/IP Suite installation directory (for example, *MULTINET*) is not in your system path. The *.DLL* files that are required for operation are in this directory. If this directory is not in your path, Windows cannot locate the files. To correct the condition, add the directory to your system path, and reboot your workstation.

— You have another vendor's *.DLL* files or older versions of the *.DLL* files provided by Cisco either in a directory in the system path before the Cisco TCP/IP Suite installation directory or in the Windows system directory. To correct this condition, locate and remove all instances of *WINSOCK.DLL*, except for the one located in the Cisco TCP/IP Suite installation directory.

- If you are using Windows 95, make sure the only instance of *WINSOCK.DLL* is in the Windows directory, and the only instance of *WSOCK32.DLL* is in the Windows system directory. These files should not be in the Cisco TCP/IP Suite installation directory.

Using Cisco TCP/IP Suite with Digital's Pathworks for DOS

Digital's Pathworks for DOS uses NDIS2 drivers for its network device driver architecture. However, Digital's NDIS2 implementation differs from the NDIS2 standard. Using Cisco TCP/IP Suite with Pathworks for DOS results in `VMULTINT.386 failed to load` error messages. To correct the condition, the N2GLUE.DOS device driver must be loaded in the Pathworks current template file.

To load the N2GLUE.DOS driver:

Step 1 Remove all references to Cisco TCP/IP Suite's NDIS2 drivers from the *CONFIG.SYS* file.

Step 2 Locate the template currently being used by Pathworks. This file can be identified by locating the line in *STARTNET.BAT* that refers to the PWTPL environment variable. For example, this line indicates the current template is *C:\DECNET\CFG00001.TPL*:

```
set PWTPL=c:\decnet\CFG00001.TPL
```

Step 3 Open the template using a text editor, and locate the [Network] section of the file.

Step 4 Insert a load statement for N2GLUE.DOS after the line that loads PROTMAN.DOS, but before the line that loads NETBIND. For example, if you are using an NE2000 network adapter and have installed Cisco TCP/IP Suite into the default directory, your template file might look like the following:

```
{LOADDRV} {+DEST}PROTMAN.DOS {SW_PROTMAN
{LOADDRV} {+DEST}NE2000.DOS
{LOADDRV} c:\multinet\ndis2\n2glue.dos
{+DEST}NETBIND.COM
```

Step 5 Save the template file.

Step 6 Reboot your workstation.

Advanced Network Troubleshooting

Occasionally, you might run into problems that require some ingenuity to diagnose and resolve. Although we cannot anticipate every problem you might run into, this section covers some example problems, and shows you some techniques you might find useful in diagnosing other problems.

Diagnosing a Failing Connection to a Network Resource

You might find that a connection to a network resource such as a printer or workstation is failing even though it had been working fine. For example, you might suddenly find that you can no longer print on your network printer.

This might indicate that another machine on the network has taken over the IP address for the machine that is causing problems.

To check out a bad network connection:

Step 1 If you can, check the machine to ensure that it is turned on and working properly. If the machine is not working properly, fix it and retry your connection.

Step 2 Start Net Tools and use Host Lookup to check the DNS listing for the machine's host name. Make note of the IP address. If there is no entry for the machine, it may no longer be on the network. Contact your network administrator.

Step 3 Ping the machine. If the machine does not respond, then there might be something wrong with the machine. Contact the person responsible for managing the machine.

Step 4 Use Net Tools TraceRoute to determine where the failure occurs.

Step 5 If the machine does respond to Ping, TraceRoute does not help, and you are familiar with the hardware network cards and their hardware addresses (also called media access control (MAC) addresses), start Monitor and look at the ARP table.

Look at the entry for the problem machine. If the hardware address is not within the expected range given the hardware manufacturer for the machine you are expecting at that address, the IP address is probably being used by a different machine.

For example, the expected range of addresses for an HP printer is different than the range for a workstation's ethernet card. Your hardware manufacturer can tell you the hardware addresses that they use.

To restore the connection to the machine, the network administrator must find the machine that has taken over the IP address and change its configuration to use a new, unique IP address.

If you have a network sniffer, or a UNIX or Cisco MultiNet for OpenVMS system that can run a TCP dump in promiscuous mode, you can also check for ARP problems by watching for ARP replies. You should see only one response for an ARP request. If you see two or more responses, they will be from different hardware addresses. Only one system will have the correct hardware address.

Step 6 If you still cannot determine the problem, contact the network administrator, who might be able to examine a TCP dump or call Technical Support for help in isolating the problem.

Determining Why You Cannot Connect to a System

Occasionally you might find that you cannot connect to a particular system. Often this is due to heavy network activity on the target machine (for example, a popular Web site). If you know the system is popular, you might simply try reconnecting later.

If your problems connecting to the system are regular, or if the system is critical to you, you can follow these steps to determine if there is another problem besides the system being too busy to respond:

Step 1 Start Net Tools and use TraceRoute to trace the route between your machine and the target, unresponsive machine. If the trace makes it to the unavailable system, the system may be too busy at this time to respond to your attempted connection, or may be configured improperly. Try your connection again, and if the problem persists, contact your network administrator or the system administrator of the remote system.

Step 2 If the trace stops before making it to the remote system, the network connection is broken at the last location. If the location is within your company, or is provided as a service for which your company is paying, call the owner of the resource. (Whois in Net Tools can help you locate a contact if you do not know who to call, or call your help desk or network administrator).

Step 3 If the trace does not stop, but at some point circles back on itself, look at the trace information to find the point at which the route is circling back. The machine routing the packets back needs to be fixed.

Determining Why You Cannot Connect Outside the Local Network

If you cannot connect outside your local network, you have a routing problem.

Use Monitor to look at the routing table. You should have at least these three destinations:

- 0.0.0.0

  This is the default route, and should be the IP address of a gateway. It is defined in the Cisco TCP/IP Suite configuration under Routing. You can configure your workstation to use a specific route (by supplying a specific IP address), or you can have your workstation find a route by specifically asking the network or by listening for routing information from the network. In any of these cases, you should get an entry for 0.0.0.0 in the routing table.

- 127.0.0.1

  This is your workstation's loop-back address. If there is no entry for this address, your Cisco TCP/IP Suite configuration is incorrect. Contact your network administrator to get the information you need and update the configuration using the Configuration Utility. The information you need is the same information needed during Cisco TCP/IP Suite installation.

- Subnet IP address

  This is the IP address of the subnet that your machine is on. The Gateway address for this destination should be your machine's IP address.

Determining Why Network Connections Are Dropped

If you find that, when using an application like Telnet or FTP, your connections to the remote system drop more often than you deem reasonable, there might be a hardware problem on the network.

Here are some things you can do to determine if there is a hardware problem on the network:

Step 1 Start Monitor and look at the protocol statistics. These statistics are accumulated since the last time TCP/IP was started on the machine (typically during boot). Some of these statistics cover "timeout" errors (for example, "dropped due to keepalive timeouts").

In general, the ratio of timeout errors to TCP connections should be no more than 1 to 2 percent. Anything more than 10 percent indicates a problem, and ratios between 2 and 10 indicate a possible problem. (These ratios are rules-of-thumb; it is up to you to determine the ratios that indicate what is a significant problem.)

An excessive number of connections dropped due to timeouts might indicate a faulty bridge on the network.

Step 2 Ping the host that is timing out. To make the Ping useful, you must make it emulate the type of connections that are being dropped by the host.

For example, if users typically Telnet to the host, set up Ping to resemble Telnet. Start Ping and click the Ping button. For data length, use 1000. For number of packets, pick a large number that will keep the Ping going long enough to resemble a normal Telnet session, or the Telnet sessions that are getting dropped. As an alternative, enter 0 to have the Ping continue until you stop it.

If you are emulating FTP connections, use a larger data length (such as 1500 for Ethernet or 4352 for FDDI). Send enough packets so that the Ping resembles the FTP sessions that are being dropped. The reason for sending large packets is to determine if a router is handling large packets incorrectly.

Start Ping and look at the %Loss figure when Ping finishes. A high packet loss might indicate a hardware problem on the network, either in the line itself or in a bridge, router, or other machine. Use Net Tools TraceRoute to help isolate which machines are used in the connection.

Finding Out Who is Responsible for a Problem Router

If you know which part of a network is failing, you also want to know who is responsible for fixing that part. If the machine's owner has registered with a "white pages" server to which you have access, you can use Net Tools Whois to find out who to notify about the failing machine. You can use Whois to look up contact information on full machine names, domain names, and IP addresses.

White pages contain information about Internet hosts only, not hosts internal to your organization's network.

Troubleshooting Dialer Serial Connections

Serial connections to networks are frequently unreliable. Many factors can break a connection, from poor telephone service to unreliable modems or other hardware. The online help for Dialer contains extensive information on setting up and troubleshooting connections. The following sections cover more general points.

Note You can only use Cisco's Dialer with the Cisco TCP/IP stack: for example, you cannot use the built-in Microsoft dialer. Also, if you are only using serial network connections on the machine, be sure to install the Cisco Dial-Up Adapter using the Windows Network Control Panel.

General Troubleshooting Tips for Dialer

If you are having trouble making a serial connection using a profile:

- Retry the connection and click the **Message Log** button on the Connect status dialog. The message log shows the interaction between Dialer, the modem, and the remote host.
  - If the script times out before the telephone number is dialed, the modem is not getting properly reset. Retry the connection until the modem gets dialed.
  - If the modem gets dialed, but the remote host does not answer, contact the network administrator for the host for help.
  - If the modem gets dialed, the remote host answers, but the host sends unexpected data, retry the connection a few times to see if the data sent remains consistent between retries. If it does, you must rewrite your Dialer script to accommodate the changed login process on the remote host.
- If you continue to have problems, try making a manual connection. If you are successful, print out your interaction with the host and compare it with the Dialer script in the failing profile. You might need to update the script.
- If the modem does not dial after repeated attempts, try a different modem type. Also, check to ensure the modem is turned on and connected to your workstation.
- If a serial connection is made but no data is transmitted, change the serial interface speed. If the speed value in the Modem tab or in the Configure Interface dialog box is set too high for your workstation's serial port, this can cause problems when transmitting data. Change the speed to a lower value to correct the problem.

Troubleshooting the “WINSOCK error 10017” Error Message

If you receive the error message `WINSOCK error 10017`, Dialer cannot open the serial interface. This can indicate any of the following:

1. The last time the serial interface was opened, it was not closed properly. If this is the case, turn the modem off, then on (if the modem is external to your machine) and reboot Windows.
2. An attempt is being made to open more serial interfaces than have been configured. If this is the problem, configure and enable additional serial interfaces using the Configuration Utility.
3. Both serial and LAN interfaces are running at the same time with the same network number. If this is the problem, disable the LAN interface using the Configuration Utility.

Troubleshooting FTP Client and Server

If you encounter any problems when using FTP Client or Server, the easiest way to resolve the problems is to review the contents of the FTP message logs.

The message logs list all commands sent and received during your FTP session. If you are using the Client and Server together, you can see the sequence of commands and replies in both message logs. Otherwise, you can see only your end of the transaction.

By examining these logs, you might spot the reason for the problems you encounter.

General Troubleshooting Tips for FTP Client

If the information in the FTP Client message log does not help you, check the following items:

- If you can send and receive files, but the files are corrupted after transmission, verify you are using the correct file transfer mode. Use ASCII mode for text files, binary mode for executable files, compressed files, graphics files, and other non-text files, and local-8 mode if the remote host is a system that does not use the standard 8-bit byte.
- Ping the machine running the FTP server to make sure the machine is available.
- If you cannot connect to the FTP server, call the server administrator and make sure the FTP server is running.

- Make sure that the host to which you are trying to connect is not running behind an IP packet-filtering firewall. If it is, check Passive Mode in the Advanced options in the Connect dialog. If your network uses another kind of firewall, fill in the firewall proxy attributes in the Advanced options.
- If you chose Auto Detect in the Host System Type drop-down list in the Connect dialog box, view the contents of the message log to discover the correct system information. Then, either choose the correct system type from the Host System Type drop-down list or choose Unknown.
- Make sure you have entered the correct user name and password for the FTP server.
- Make sure you are only attempting to work in authorized directories and that you have adequate privileges for the work you are attempting to do. If you cannot access the directories and files you need, contact the FTP server administrator.

General Troubleshooting Tips for FTP Server

If the information in the FTP Server log does not help you, check the following items:

- Make sure the FTP Server is running by viewing the contents of the FTP Server window. You should see the words "`Server started.`"
- Make sure your workstation is properly connected to the network and the network is running.
- Make sure the system on which the FTP client is running is properly connected to the network and that the network is running.
- Make sure the user is entering the correct user name and password. Give the user a new password to ensure the password is correct.
- Make sure the user is working in the authorized directories and has adequate privileges for the work the user is attempting to do.

Troubleshooting Netscape Mail

In order to send and receive your mail, Netscape Mail must be able to connect to the appropriate servers. If you are having problems sending and receiving mail, first check your Netscape Mail Preferences (under **Options>Mail and News Preferences**) and ensure these settings are correct:

- If you are having problems receiving mail, check the entry for the POP server, including your account name. Netscape Mail must log into the POP server to get your mail. If the server name and your user name are correct, and you are using the correct password, contact your network administrator for help.
- If you are having problems sending mail, check the entry for the SMTP server. Netscape Mail must connect to the SMTP server (which might be the same server as your POP server) in order to send mail. If the server name is correct, contact your network administrator for help.

Troubleshooting Netscape Navigator

If you cannot open a file on the Web using Netscape Navigator:

1. Try again after a few minutes in case the server is overloaded.
2. Try to open a different URL. If you can open other URLs, verify that you entered the URL using the correct case and that it does not begin with a space.
3. If you are using a proxy server, verify it is configured correctly.
4. Try other TCP/IP applications, such as email or FTP. If they do not work properly either, there may be a problem with your network connection.
5. In the URL field, type the IP address of the server rather than its domain name. If this works, your DNS (Domain Name System) server may be unavailable.

Troubleshooting NFS

Problems can occur when connecting to the NFS server, logging into the NFS server, and working on files on the NFS server.

Troubleshooting NFS Connection Problems

If you cannot connect to an NFS server, Ping the server by IP address and by name to ensure that it is available on the network and that host names are being resolved. Contact your network administrator for help.

If you can connect to the NFS server, but not log into it:

1. Make sure you have a valid account on the remote host.
2. Make sure you are entering the correct user name and password.
3. Contact your network administrator to determine if you should specify an authentication server when starting an NFS connection.

In Windows 3.x, if you have configured each profile so that NFS automatically maps each connection when Windows starts but the mappings do not appear in the Current Connections list, make sure you check Enable Permanent Connections on Startup on the Global Options tab.

If you are trying to connect to a non-NFS drive, such as a Netware or Microsoft Networking drive, and the NFS logon dialog appears, press the **Ctrl** key and click the **Cancel** button on the dialog (you might have to repeat this). NFS tries to pass the connection request to the other network clients.

If you get the message "`Windows Networking. The following error occurred while you were trying to connect to: <drive>. Device not connected.`," make sure that the LASTDRIVE setting in *CONFIG.SYS* is set to a drive after the drive you are trying to map.

Troubleshooting Problems Accessing Files on the NFS Server

This section explains how to resolve problems that may arise when accessing, writing, or displaying files on an NFS server. Problems in this areas can usually be resolved by changing the options used for connecting to the drive. In Windows 95, the Wide Area Network, Fast Read, Server Port, and Maximum Packet Size options can only be changed if you first dismount the NFS drive.

Correcting General Access Problems

These are some problems you might encounter in accessing NFS drives:

- In Windows 95, you cannot create a briefcase on an NFS drive.
- If you have problems saving files that use a proprietary format (such as Word or Excel files) to an NFS drive, check the Enable Network Locking option for the drive. If problems persist, contact your network administrator and ask if the NFS server is running the Lock Manager (the Lock Manager must be running to use network locking).

  Although you can set any NFS connection options you want when connecting to an NFS drive, these options are negotiated with the NFS server, and any options not supported by the server are disabled. You can view the actual options that are enabled by right-clicking the connection in Windows 95 Explorer or My Computer and choosing **Properties**. For example, if you enable network locking when you connect to a drive, you can then check to see if the server actually enables it.
- If the / directory is exported on the NFS server, it appears as an entry with a blank name. You cannot browse this mount point.

Improving File Reading Performance

If the NFS server appears to run slower when accessing files, your workstation is using a low-end Ethernet adapter, or a copy request appears to stop completely, disable fast read for the connection.

In Windows 95, to disable fast read:

Step 1 Disconnect the drive by right-clicking its icon in My Computer or Windows Explorer and selecting **Disconnect**.

Step 2 Reconnect the drive by finding its mount point in the NFS Servers and Printers workgroup in the Entire Network entry in Network Neighborhood. Right-click the mount point and select **Map Network Drive**.

Step 3 When the NFS client asks you to log in, click **Options** and uncheck Enable Fast Read. You can further improve performance by setting the maximum packet size to 1024 and checking Wide Area Network (especially if you are using serial connections). Click **OK** and log into the NFS server.

In Windows 3.x, to disable fast read:

Step 1 Double-click the NFS Assistant icon in the Cisco Suite 100 program group.

Step 2 Select the problem connection in the Current Connections list on the Connections tab and click **Modify**.

Step 3 Uncheck Enable Fast Read. You can further improve performance by setting the maximum packet size to 1024 and checking Wide Area Network (especially if you are using serial connections).

Improving File Writing Performance

If writing files to the NFS server seems to take a longer time than usual, it may be that the server is overloaded. If the problem is persistent, disable fast write for the connection.

In Windows 95, to disable fast write:

Step 1 Right-click the drive's icon in My Computer or Windows Explorer and select **Properties**.

Step 2 Choose the NFS Options tab and uncheck Enable Fast Write.

To permanently disable fast write for a drive in Windows 95, you must first disconnect the drive and uncheck Enable Fast Write when you reconnect the drive.

In Windows 3.x, to disable fast read:

Step 1 Double-click the NFS Assistant icon in the Cisco Suite 100 program group.

Step 2 Select the problem connection in the Current Connections list on the Connections tab and click **Modify**.

Step 3 Uncheck Enable Fast Write.

Correcting File Display Problems

Some applications do not properly handle or display Stream-LF text files obtained from an NFS server. To make the files display correctly, disable the Convert Text Files to Stream-LF option.

In Windows 95, to prevent files from being converted to Stream-LF:

Step 1 Right-click the drive's icon in My Computer or Windows Explorer and select **Properties**.

Step 2 Choose the NFS Options tab and uncheck Convert Text Files to Stream-LF.

To permanently prevent conversion for a drive in Windows 95, you must first disconnect the drive and uncheck Convert Text Files to Stream-LF when you reconnect the drive.

In Windows 3.x, to prevent files from being converted to Stream-LF:

Step 1 Double-click the NFS Assistant icon in the Cisco Suite 100 program group.

Step 2 Select the problem connection in the Current Connections list on the Connections tab and click **Modify**.

Step 3 Uncheck Convert Text Files to Stream-LF.

Troubleshooting LPD Printing Problems

If your Windows 3.x NFS print requests are not successful, check the information that appears in the Current Connections list in the Connections tab of the Print Assistant. The Windows 3.x Print Assistant displays error messages in the list next to the affected printer. In Windows 95, use the Print Manager to check printer status.

If your print requests are not successful when using an LPR/LPD queue, make sure you are using the right filter. If you specify an incorrect filter, the print server cannot interpret your print request. Your network administrator can give you the information you need.

If you receive the error message `The server is not configured to accept print jobs from this PC`, this means that LPD is running at the server, but the LPD server has rejected your request to submit a job. In this case, if the remote machine is running Cisco MultiNet for OpenVMS, use the **MULTINET CONFIGURE/SERVER** command to verify that LPD is accepting requests from your machine. Contact your network administrator for more information.

If NFS and Print Assistant reports no errors and it appears that the job was successfully printed, but no output appears at the printer:

1 Make sure your user name specifies a valid user account on the server.

2. If the remote machine is running Cisco MultiNet for OpenVMS, enter **REPLY/ENABLE = NETWORK/TEMP** at the server. Then submit another print job and review the error messages generated by the LPD server.
3. Make sure that the target queue is not stopped at the server. To do this on an OpenVMS server, use **SHOW QUEUE** *queue-name*. On a UNIX server, you can try the **status** command in the **lpc** utility to determine the state of the queue.

Troubleshooting Stream Printing Problems

If your Windows 3.x NFS print requests are not successful, check the information that appears in the Current Connections list in the Connections tab of the Print Assistant. The Windows 3.x Print Assistant displays error messages in the list next to the affected printer. In Windows 95, use the Print Manager to check printer status.

If you are using the Cisco MultiNet for OpenVMS print server and the NFS print application did not report any error messages, but the printed output appears improperly formatted, verify the logical name MULTINET_PCNFSD_USE_FIX_512_FILES is defined as TRUE at the print server. Contact your network administrator for more information.

If the NFS print application displays the message `Connection to printer timed out: make sure the printer is online` a few seconds after submitting a print job:

1. Verify the printer is powered on.
2. On Windows 95, verify that the port number is correct.
3. Use Net Tools Ping and TraceRoute to ensure that the print server is reachable on the network.

If the printer only partially prints the job, but Print Assistant does not report any errors, and the job is no longer in the queue, make sure that you enabled Telnet negotiation for the connection.

If the print job is shown in the “Printing” state from the Print Manager utility and no error messages are reported by Print Assistant, but nothing appears at the printer:

1. Verify the printer is online.

2 Make sure the printer is not busy with other requests, causing the print job to take longer than usual.

If you receive the message `Could not connect to printer` after a minute or longer delay, the remote server is not reachable from your machine. The long delay indicates that the server is not reachable. A software configuration error would cause the error message to display immediately.

If the NFS print application displays the message `Could not create a spool file at the print-server: access denied`, verify that your user account at the server has permission to submit jobs to the target queue.

Troubleshooting Telnet

If you cannot log into the remote host using Telnet, make sure you have a valid account on the remote host, and that you are entering the correct user name and password. If you continue to have problems logging in, contact your network administrator.

If you are successful connecting to the host, but your Telnet session produces unexpected characters in the activity window, choose **Host>Reset Terminal** to reset your session to the default terminal settings.

Incorrect terminal type negotiation can also cause session problems. If Telnet cannot correctly negotiate a correct terminal type, you need to send an identification string to the host. This string is defined in the Identification String field on the VT, TN3270, or TN5250 tabs in the Settings dialog. Ask your network administrator for the exact string required by the host.

Troubleshooting Kerberos

These messages describe the main problems you might encounter when using Kerberos:

Error Message `Password incorrect`

Explanation You entered the wrong password.

Recommended Action Your Kerberos password is not necessarily the same as the one you use to log into systems that prompt for a user name and password, even if you can log directly into the Kerberos server. If you still get this message after retrying your Kerberos password, ask your Kerberos administrator to reset your password for you.

Error Message `Time is out of bounds`

Explanation Your workstation's clock is not within five minutes of the Kerberos server's clock or the clock of the host to which you are connecting.

Recommended Action Call your help desk or network administrator to find out the time on the other systems. Update the Windows settings to reflect this time: be sure to specify AM or PM correctly. On Windows 3.x systems, you might also need to use the Configuration Utility to set the correct time zone, if it is in error.

Error Message `Can't send request`

Explanation There was a problem contacting the Kerberos server.

Recommended Action Verify that you entered the correct name of the server in the Kerberos utility in the Configure Kerberos dialog. Ping the server to verify that it is on the network. Contact your network administrator for more help.