

[Previous](#)[Search](#)[Next](#)[TA Home](#)

30/60

I installed a network interface card (NIC); now I'm having networking problems.

Keywords

openserver v5 unixware internet faststart unix ifs installed network card interface nic ping telnet tcpip troubleshooting trouble shoot performance desktop open dns routing nodes local locks protocol stack lockups hangs telnet dies slow down creep crawl intermittent sporadic 5.0.0 5.0.2 1.0.0 1.1.0 3.0 4.2 2.01 2.02 2.03 2.1.0 2.1.1 2.1.2 odt connections lost 5.0.5 5.0.6

Release

SCO OpenServer Enterprise System Release 5.0.2, 5.0.5, 5.0.6
SCO OpenServer Desktop System Release 5.0.0, 5.0.2
SCO OpenServer Host System Release 5.0.0, 5.0.2
SCO Internet FastStart Release 1.0.0, 1.1.0
SCO UnixWare Application Server Release 2.1.0, 2.1.1, 2.1.2
SCO UnixWare Application Server Release 2.01, 2.02, 2.03
SCO UnixWare Personal Edition Release 2.1.0, 2.1.1, 2.1.2
SCO UnixWare Personal Edition Release 2.01, 2.02, 2.03
SCO Internet Family Layered Products Release 1.0.0, 1.1.0
SCO Open Desktop Release 3.0.0
SCO Open Server Network System Release 3.0.0
SCO Open Server Enterprise System Release 3.0.0
SCO UNIX System V/386 Release 3.2 Operating System Version 4.2

Problem

I have installed a network interface card (NIC) into my machine. I am now having networking problems. There are several common scenarios that you may run across:

- (1) The NIC is configured successfully but doesn't respond or gives errors during reboot;
- (2) Ping or telnet to other machines on the local network fails;
- (3) Node can only communicate with certain machines on the local network;
- (4) Networking locks up or has sporadic slowdowns.

Cause

There are many different things that could be wrong at this point. Diagnosis may involve troubleshooting both the hardware and the software. The problem may also be related to DNS, routing, or another hardware problem outside this machine.

Solution

Since networking software -- the "protocol stack" -- is configured on top of the underlying layer of hardware, it makes sense to begin troubleshooting at the lowest level first. Start with the hardware, and then the software that is configured above that.

Newly Installed NIC Doesn't Function:

The NIC was configured successfully but doesn't respond or gives errors during bootup.

This problem implies that either the hardware is not being detected at all, or it is being detected but there is a gross configuration mismatch in the hardware or software (or both).

(1) Make sure you are using a supported NIC. Lists of supported hardware are available from:

<http://www.sco.com/Third/hch/category/8.htm>

or from your support provider.

(2) Using the NIC hardware setup utility (if there is one) that shipped with your card, boot into DOS to confirm the resource settings for IRQ, I/O address, RAM address, media type, and so on. Some older NICs have jumpers that do the same thing, so you may want to confirm those settings on the card itself.

If the card is a newer model, it may not have a configuration utility or jumpers, so you should enter the machine's EISA or PCI setup and confirm the settings that are autodetected on the bus. See other articles in this database for hints on configuring high-speed PCI NICs.

Some cards are also shipped with card diagnostics and testing utilities, which may be helpful in determining if the card itself is bad.

(3) Check for resource conflicts: in UnixWare, use the DCU; in OpenServer, use "hwconfig -hc". Check for errors during bootup, such as "card not found" or "unable to start" or other errors similar to these. These messages imply that the software configuration doesn't match the hardware configuration.

(4) Next, confirm you are using the correct driver for the card you are configuring. When running netconfig (OpenServer) or niccfg (UnixWare), you saw a list of driver names or NIC names. Be absolutely certain you selected the correct entry for the particular card you are using. If you are unsure, see other articles in this database for the driver name to NIC mappings.

You will have to relink and reboot after making NIC changes.

While reconfiguring the card, you should also determine if the NIC is correctly configured to match the hardware values we confirmed in #2 (above). You can also use [ping\(ADMN\)](#) and [netstat\(TC\)](#) to check for resource conflicts: Check the Ipkts and Opkts output of "netstat -i", ping another machine on the local net, then check the output of "netstat -i" again. If Ipkts is increasing but Opkts stays at 0, the I/O address is incorrect. If Ipkts stays at 0 but Opkts increases, the IRQ is incorrect. See other articles in this database for a more detailed description of this.

(5) If you have any doubts as to the quality of the NIC, media (cabling), hub, or any other hardware, you should swap out various pieces and retest the connection. Check to make sure other machines on the local network are working correctly, move the NIC to a new slot on the motherboard, change out cable, move to another port on the hub, try another card of same type, try a card from another manufacturer, use a new transceiver, and so on.

Cannot connect with other machines on network:

This problem is most often due to an incorrect netmask or broadcast address, bad routing, a specific networking service that has failed, incorrect framing, or corrupted binaries.

(1) First check to see that you can ping your own machine by IP address, name, and loopback/localhost. If these work, then the TCP stack is usually trustworthy; if these fail, you should reconfigure the protocol through netconfig (OpenServer) or /etc/inet/menu (UnixWare) and start again. You may also have garbage or duplicate entries in /etc/hosts. A simple example of /etc/hosts would be like this:

```
127.0.0.1      localhost
192.168.144.252 machinename machinename.domain.dom
```

The format is:

```
IP    nodename    fully-qualified-domain-name
```

You shouldn't see the same IP address or machinename listed more than once in the file, and you shouldn't see entries with control characters or network card names.

(2) Compare the output of "ifconfig -a" with a working UNIX machine on the same local network. The netmask and broadcast address should be the same. An example of ifconfig output would be something like this:

```
cet0: flags=4043<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 132.147.144.216 netmask ffffffff0 broadcast 132.147.144.255
      perf. params: rcv size: 24576; send size: 24576; full-size frames: 1
      ether 00:80:5f:70:b2:f5
lo0:  flags=4049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 8232
      inet 127.0.0.1 netmask ff000000
      perf. params: rcv size: 57344; send size: 57344; full-size frames: 1
```

You can also do "grep ifconfig /etc/tcp" to get the same information in a slightly less crowded

format.

(3) Look at the output of "netstat -i" before and after a ping to another machine to make sure Ipkts and Opkts are increasing. If they are not increasing, you are not sending or receiving packets on the media. Check your connection, replace the cable, and check the output of "arp -a" to see if you are detecting any broadcast traffic.

Arp keeps track of the mapping between IP address (what the software is configured to) and Ethernet address (the hardware address). Since [arp\(ADMN\)](#) is broadcast based -- meaning the information is broadcast to the entire local network -- you should be able to detect other machines at the hardware level. If no arp entries are listed, you are probably either not connected to the media properly or are using an incorrect netmask/broadcast combination. See the [arp\(ADMN\)](#) man page for more information.

(4) Try to ping a remote machine by name, by IP, and with the -n flag to ping to disable DNS lookups. You can also use the -R flag to check the routing used for the ICMP packets. The [traceroute\(ADMN\)](#) command is also useful to see where the packets are stopping. This is especially useful if you suspect a router is blocking traffic. In general, DNS problems will give errors such as "unknown host", so moving DNS out of the picture is useful.

(5) In general, if routing is the problem, you will see errors like "destination unreachable" or "no route to host" when you ping or telnet to another machine. In any case, check the routing table on the problematic machine (using the command "netstat -rn") to make sure you have at least a route to your local network, your own IP, and your localhost. You will also need explicit routes to subnets if you are subnetting.

(6) When you reboot after making any final hardware-level changes, you will see various daemons starting. Note any errors seen during the networking startup, since these daemons are key to many different services. For instance, you may see an error from named, which would indicate possible DNS problems, or routed, which would indicate routing problems.

(7) In netconfig or /etc/inet/menu, verify that the framing used on this interface is the same as the other nodes on your local network. EthernetII, 802.3, and 802.5 are the most common options.

(8) If using token ring, make sure source routing is enabled.

(9) Do a complete system verify (OpenServer), fixperm (SCO UNIX Version 4.2), or pkgchk (UnixWare) to make sure all required files are loaded and are not corrupted. Check to see if [telnet\(TC\)](#) works where [rlogin\(TC\)](#) fails, or vice-versa; see if [ping\(ADMN\)](#) can get through where [traceroute\(ADMN\)](#) fails, and so on.

Can only communicate with certain other local machines:

This is usually the result of incorrect routing or subnetting, incorrect routing on the destination machine, or framing.

(1) Use [traceroute\(ADMN\)](#) to see where the packets stop when connecting to a problem machine.

- (2) Verify that the destination machine has correct routing back to the source machine. Sometimes, the source machine is getting the incoming packets but has no way to route them back to the originator, resulting in a "host is down" message on the sending machine.
- (3) Verify that routing between subnets is correct. If you are unsure about what your routing should look like, see other articles in this database on what the routing should be. The netmask and broadcast addresses used in the subnets should also be consistent.
- (4) Verify that all machines on the local net are using the same framing format.

Networking works intermittently, with slowdowns or lockups:

This problem could be due to a misbehaving application, overall system load, STREAMS **failures**, bad **device** drivers or hardware conflicts, poor kernel tuning, or many other reasons. If connecting to a site on a remote network, there may be general routing problems or other slowdowns on the Internet.

- (1) Check to see if the hangs or lockups are load-dependent. Your users could be pushing the machine beyond its capability with certain applications, at certain times of day. You may need to increase system resources or adjust kernel tuning.
- (2) Check for STREAMS **failures** with "netstat -m" (OpenServer) or the strstat command in [crash\(1M\)](#) in UnixWare. You may need to allocate more memory for the overall STREAMS pool. See other articles in this database on STREAMS tuning.
- (3) Make sure "ifconfig -a" shows the problematic interface and that it is marked UP.
- (4) Gather statistics from the following commands to see if overall networking or general system performance is degrading over time:

```
sar -u 5 5
sar -r 5 5
swap -l
netstat -i
netstat -s
l1stat -l
netstat -m
```

(Note that the last two commands won't work with UnixWare.) If the lockup or hang is sudden, this points more to a bad **device** driver or resource conflict (IRQ, I/O address, RAM address) Make sure you have the latest revision of your NIC **device** driver and that there are no conflicts.

- (5) Finally, if connecting to a site at least one hop away, try the following shell script to test where exactly the bottleneck is:

```
#clip here
:
for i in `traceroute -n www.sco.com | awk ' { print $2 } ' `
do
```

```
ping $i
done
#clip here
```

Simply replace the "www.sco.com" with the site you are trying to reach, and the script will give you the average milliseconds to reach each hop to the destination. This will help you determine if the slowdown is on your network or a general problem on the Internet.

See Also

Other articles in this database, [SCO OpenServer Networking Guide](#), [UnixWare Network Administration Guide](#), [UnixWare System Owner Handbook](#).

TA107687 created on 25 June 1997 , last updated on 04 May 2001

SSL #: 640470 IT #: tcpip470

Please click this box if this article solved your problem

 Previous

 Search

 Next

 TA Home

Suggestions for improving the content of this article.

 Comments

We appreciate your continued interest in improving the quality of SCO's technical library and welcome your input regarding this technical article. Suggestions submitted from this form will be forwarded to the Documentation department. If you are looking for technical help beyond that provided in the current article, please contact [SCO Support Services](#).

Copyright © 1996-
1998 The Santa
Cruz Operation, Inc.

All Rights Reserved.