

## Re: Network bottle neck, ow to investigate CSocket.

**Source:**

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.networking/2005-03/0599.html>

---

**From:** Todd J Heron (*todd\_heron\_no\_spam\_at\_hotmail.com*)

**Date:** 03/17/05

Date: Thu, 17 Mar 2005 07:19:36 -0500

26-step improvement plan for: Windows runs too slowly, hangs or freezes. I know it's a lot but your answer is bound to be in here somewhere!

1. Check system uptime (pagefile.sys modified date or in Task Manager: CPU Time, or remotely with Uptime.exe). A reboot may be needed if the system has been up for several days.
2. Check free disk space; delete Temp files/ Temporary Internet files & Netscape cache
3. Check then clear the Event Viewer
4. Check size of user's profile
5. Turn off unneeded services
6. Check Virtual memory (pagefile size) locally (Control Panel > System > Performance tab > Change) or remotely: (Remotely: Regedt32 to \\computername then navigate to: HKey Local Machine\System\ CurrentControlSet\ Control\ SessionManager\Memory Management. The pagefile size may need to be increased.
7. Open Task Manager, click Processes then CPU column to sort by processes using the highest percentage of CPU time in descending order (highest at the top). A common culprit is NTVDM.exe. DOS-based and 16-bit applications have to run inside NTVDM.exe. As they may try to access the hardware continually, such as non-stop keyboard polling, CPU cycles will be used up quickly. There are very few good solutions to this problem, other than upgrading the application to 32-bit. Also, a scheduled task invoking a CMD or BAT file which is running continuously in the background due to script logic error or a resource the script is calling cannot be found.
8. Lower video resolution via Control Panel > Display > Settings tab > lower Refresh Frequency
9. Turn off any OpenGL screensaver or change to a system default screensaver
10. Check for real-time Anti-virus running (no need to run more than one type of AV engine simultaneously)
11. Turn off FindFast (via Control Panel & "All Users" Startup folder)
12. Remove unnecessary network protocols (NWLink IPX/SPX is often at fault in networks no longer running Novell NetWare)
13. Defragment (and ensure not defragmentation is not running in the background as a process - DiskKeeper is notorious for this. A badly

fragmented hard drive or MFT, a corrupted MFT or FAT, or physical damage to the drive (particularly if the MFT or page file is trying to use a bad sector) are possible causes of slow performance

14. Check Control Panel > System > Performance > and verify that the total amount of paging is equal to at least 12MB greater than physical RAM. Determine how much RAM is installed via Control Panel > System > Performance > *General. Setting the MIN and MAX size of the pagefile to the same number* will prevent pagefile fragmentation.
14. Recreate the user's profile
15. Investigate a possible Network problem (is there a broadcast storm somewhere, is someone copying large files (such as movie files), over the network, or from the Internet? Is a deployment team or a Helpdesk downloading or copying images (such as those built using Norton Ghost) over the network, are backing up large amounts of user data during production hours?)
16. Ensure client NIC speed is equals the same setting as all switches and servers in the network (for example, every client workstation and network device set to 100mbs/full duplex)
16. Look into a Wiring closet problem
17. Add more RAM (open Task Manager, verify that the Total Physical Memory is greater than Total Commit Charge during normal system operation. If it isn't, more RAM is needed)
18. Hard drive is slow or there is a mainboard problem
19. Verify proper SCSI termination
20. Run CHKDSK to verify the physical integrity of the disk. A bad sector in an area used by a critical file – such as pagefile.sys – can slow the system to a crawl
21. Stop and restart the Spooler service
22. Investigate whether this could be a poorly-written, unsigned, or out-dated device driver which is not releasing the CPU. Each device interacts with the computer by interrupting the processor so that the device can send or retrieve data or carry out a function. A device must have a method for telling the computer's processor that it needs attention. A hardware device must have a method for telling the computer's processor that it needs attention. A hardware device tells the CPU it needs attention through an interrupt request (IRQ) line. By using this method of interruption, the CPU can function without the need to ask a device every few seconds whether it needs service. When a device interrupts a CPU, the CPU stops what it is doing and handles the service request. Because each device is assigned an IRQ number when the device is configured, the system knows which device needs attention. After the CPU has attended to the device, it returns to the function it was performing before the interruption. Now, what if a device is constantly requesting the attention of the CPU? Other devices would not get attention and hence the appearance of a "freeze". A technician can investigate wheter an unsigned driver is the source of the problem by running the File Signature Verification utility. To run this, go to Start > Run > enter Sigverif then click OK. After pressing Start on the resulting dialog window, the process will notify you if it finds any unsigned drivers on the system. Note, this can also be outputted to a log. Remove any unsigned drivers and replace with devices which have signed drivers (such hardware is sold with a Microsoft Windows

microsoft.public.windows.server.networking: Re: Network bottle neck, ow to investigate CSocket.

compatible logo on it).

23. The problem may be SMB signing or LAN Manager authentication level. In Windows 2003, default server policy forces all SMB traffic to be digitally signed which seems to cause a problem in some configurations of XP Pro. In Local Security Policy (Start > Run > secpol.msc > OK) navigate to security options (Security settings > Local policies > Security) and try disabling the option for Microsoft network server:digitally sign communications(always). Ensure you do this on all machines involved (such as via a GPO for an OU). Run gpupdate /force on the server after making the change and do the same on the client machine afterwards.

321169 Slow SMB performance when you copy files from Windows XP to a Windows  
<http://support.microsoft.com/?id=321169>

Security settings that can cause a problem with downlevel client access:  
<http://support.microsoft.com/default.aspx?scid=kb:%5BLN%5D:811497>  
<http://support.microsoft.com/default.aspx?scid=kb:en-us:823659>

24. Or this, if XP and/or Windows 2003 computers are involved:  
New registry entry for controlling the TCP Acknowledgment (ACK) behavior in Windows XP and in Windows Server 2003:

<http://support.microsoft.com/default.aspx?kbid=328890>

25. Possible problem with Lsass.exe.

Windows Server 2003–Based Computer Becomes Slow and Unresponsive After Running for Several Days:

<http://support.microsoft.com/?scid=kb:en-us:821008>

Computer Does Not Respond to Client Requests After Lsass.exe Stops Responding:

<http://support.microsoft.com/?scid=kb:en-us:821265>

The Server Stops Responding and an Access Violation Occurs in Lsass.exe When the Server Reloads Certain Policy Parameters:

<http://support.microsoft.com/Default.aspx?scid=kb:en-us:826819>

26. Have you run an adware/spyware scan?

Dealing with Unwanted Malware, Parasites, Toolbars and Search Engines:

<http://mvps.org/winhelp2002/unwanted.htm>

See also:

<http://www.Microsoft.com/spyware>

Free online spyware scanner:

[http://download.zonelabs.com/bin/promotions/spywaredetector/index\\_email.html](http://download.zonelabs.com/bin/promotions/spywaredetector/index_email.html)

28. If none of the above resolves the problem, perform the following:

1. Click Start->Run->Msconfig
2. Goto the Startup tab, and click the Disable All button.
3. Goto the Services tab, click to check "Hide All Microsoft Services" and click the Disable All button.

Re: Network bottle neck, ow to investigate CSocket.

microsoft.public.windows.server.networking: Re: Network bottle neck, ow to investigate CSocket.

4. Click Ok to exit and reboot your machine.

Check to see if this resolves the problem. If so, then the cause is among the disabled startup programs and services. Enable them one by one to find out which one is slowing the machine down.

<http://support.microsoft.com?kbid=822219> "You Experience Slow File Server Performance and Delays Occur When You Work With Files That Are Located on a File Server "

--

Todd J Heron, MCSE  
Windows Server 2003/2000/NT; CCA

-----  
This posting is provided "as is" with no warranties and confers no rights.  
"Simon" <not\_valide\_email\_address@example.com> wrote in message  
news:eoMLq1tKFHA.128@tk2msftngp13.phx.gbl...

Hi,

We have an application that uses CSocket to send and receive messages,  
(written in VC++6).

We have one 'server' application where all the messages are send to, and  
from time to time the server does send messages to the 'clients'.

The system has been working for quite sometime so we know there is no  
memory/handle leaks of any sort, (24hours a day 7 days a week).

All the machines are WinNT(SP6) and Win2000(SP2), (one server and 9  
clients).

The problem we are having is that from time to time, (on a daily basis), the  
server slows to a crawl. It is as if there are so many messages to deal with  
that the server is battling to handles them all.

And to make it worse, the clients are programmed to ensure that the server  
is still running and start sending messages if the server takes too long to  
get back to them.

But after some time the server seems to get back on it's feet and back to  
speed. So the server does get out of the mess once all the messages are  
handled.

I now have to go on client site and investigate, (it's in another country  
where technology is a bit behind to say the least).

But before I go there, I was wondering if some of you could give me some  
pointers.

How can I test the network traffic between the server and the clients.

How could I log that the server is getting itself into a mess?

Is there a way to log if another program is using the network? and if so,  
can I log what it is and what share of the network they are using.

How can I test if there are collisions?

How can I log if the server is working too long on a certain message?

And, the server also uses ODBC, (MS Access), to log important messages.

Could that cause a problem on a daily basis? Maybe the table backs itself  
up?

Many thanks for any help you can give me.

Simon