Net Admin Weekly
59,000 Subscribers Worldwide
Aug 28, 2002
Issue #6

Feature

The Ten Commandments of Troubleshooting

to top

What do you get paid to do? Some people are paid to strip search you at the airport, some people get paid for sitting around and watching TV, and some people get paid to keep the streets and the world safe. If you're anything like me, you probably get paid to keep a business network running smoothly.

Keeping a network running involves a number of skills: planning and design, change management, security, and user psychology. However, most of us spend a relatively small percentage of our time on those activities. If you're a working stiff, you spend the lion's share of your time troubleshooting and fixing problems. If there were never problems, you probably wouldn't have a job.

The good news is there will always be problems. There must be problems. No technology is perfect, and far, far down on the perfection scale are computer hardware and software. I don't expect this situation to change in the foreseeable future, regardless of marketing hype.

How do you approach troubleshooting? If you have a lot of experience, you probably don't even think about how you troubleshoot computer and network problems. You just look at the issue and start clicking. It's like your mouse hand knows more than your brain! After about 5 minutes of clicking, a problem that others spent a week failing to solve quickly dissolves under the deft massage of your right mouse button.

Regardless of the nature of your problem, there are some general troubleshooting guidelines you can use organize your thoughts and speed up the process.

1: Know thy network

When trouble hits, you're already one step ahead of the game if you've taken the time – when things were running smoothly – to get acquainted with your network. You should not wait until a network outage or slowdown occurs to start examining your network's performance. Get out the protocol analyzer, fire up the network monitor, and get to know how your "net" works, while it is working properly.

One of the benefits of planning and designing a network from scratch is having known your network "all its life," watched it grow, seen it through minor and major crises, and learned what was normal and what was not in terms of its operation and performance. Even if you "adopt" a network that's been around for a while, a good way to get to know it is to do a complete diagram and inventory. This will require that you find out what equipment you have, where it is, and how it works.

2: Use the tools of the trade

Having access to and knowing how to use the troubleshooting "tools of the trade" are essential elements in successfully resolving TCP/IP problems. Your training and experience are your first, albeit intangible,

important pieces of "equipment." But it's not always enough.

A doctor, despite long years put in studying and practicing medicine, is often unable to diagnose a patient's illness if he/she doesn't have access to basic "tools" like a stethoscope, X-ray or other imagining machine, sphygmomanometer (blood pressure cuff), and all those other mysterious instruments used to measure or better observe various bodily functions.

In troubleshooting connectivity problems, you too will often require help in the form of hardware devices or software tools, either to confirm (or negate) your initial suspicions or to give you a starting point in your investigation.

At the very least, you should have access to diagnostic utilities, network monitoring and protocol analyzer software, as well as LAN testing devices for tracking down cable and other physical layer problems. Of course, having the tools is only half the battle – you also need to know how to use them properly.

There is a great deal of information that can be gathered using just the utilities built into most vendors' implementations of the TCP/IP suite, but many network administrators have only a vague idea of what they do and how to use them. You need to be familiar with common tools like PING, TRACERT, ARP and other utilities and known how to make them work more effectively for you.

3: Take it one change at a time.

Modern computers are good at multitasking. They can have several entirely separate and distinct processes going on simultaneously, because their "brains" (microprocessors) are able to use "time slicing" to allocate time to one problem after another in rapid succession, switching back and forth so quickly that it appears both tasks are being performed continuously.

People don't perform multiple activities nearly as well. That's why it's important, when troubleshooting network problems, that you make changes one at a time and evaluate the effect before making another.

When you have a problem such as an inability to connect to the server from a workstation, the tendency is to try everything you can think of that might fix the problem. An administrator in a hurry might uninstall, reinstall and reconfigure the protocol, unplug the Ethernet cable and plug it back in, then reboot the computer and try logging on with a different account. If he's able to connect this time, that's great – but which action actually caused the difference?

By trying only one "fix" at a time, you're able to pinpoint what works – and what doesn't.

4: Isolate the problem.

Problem isolation is another important step in troubleshooting. More

often than you might think, problems hang out in groups. Even if the original problem had a single source, attempts (by you or by the user before calling you) may have created new "companion" problems. When we have multiple problems, we will probably need to address each one separately in order to get the network running smoothly again.

Isolating the problem also means defining the specific nature of the problem. You will find it as hard to address a general problem like "I can't get on the Internet" as a doctor would have in treating a patient who only reported "I don't feel well." It's important to pinpoint the specific problem.

Note: "Specific" is a relative term. If a user initially reports the problem as "my computer's not working," he may think he is being specific when he then tells you that he can't get on the Internet. Specificity may have to be accomplished in steps.

Users often have as much trouble describing their connection problems with specificity as sick people have in telling their physicians exactly what their physical symptoms are. Good questioning may help overcome this to an extent (we'll talk about how to get information from your users a little later in this chapter) but you can't always rely on others' descriptions to be accurate and complete. You'll have to use your own observation skills, as well. Which brings us to the next step:

5: Recreate the problem

It's no coincidence that this is listed as the fifth commandment out of ten. When you are able to reliably reproduce the problem, you're halfway home on the road to solving it. If you know that the user is able to send and receive email, but receives a "404: File not found" error every time she tries to access the website of your company's main competitor, you already have a lot of good information that will prevent you from wasting your time checking her modem's configuration or the status of the ISP.

Once you've narrowed down the problem, from "I can't get on the Internet" to "I can't access the website at www.thoseotherguys.com," and you've verified that the problem can be reproduced by trying again to connect to the URL and getting the same message, you can consider the different things that might cause the problem.

In this case, there are several possibilities. One way to narrow it down further is to attempt to reproduce the problem again, from a different computer. If you type www.thoseotherguys.com into the browser on another machine, and you get the same error message, you've gained a valuable clue – the problem probably is not caused by an incorrect configuration on the first system; it's more likely the problem is at the server end, or possibly a problem with the DNS server on your network.

Summary

This week we went over the first five laws of troubleshooting. Next week we'll go over the last five laws, and then examine some applications of these principles.

This week's feature article by
Deb Shinder
Net Admin Weekly Author

Q & A

Building a Fortress and Giving the Bad Guys a Free Pass

to top

Question:

Hey Dr. Tom,
We just spend beaucoup dollars installing a sophisticated and expensive array of ISA Server and Checkpoint machines. This setup is hot! No traffic gets in or out without my say so. But I'm having a problem – I want to let WinMX into and out of my network, but I can't figure out what ports I need to open. Can you help out? Thanks! –Chase Eng Owen Tale

Answer:

Whoa Chase! You need to step back and think about what you doing here. You guys have dropped a wad of dough on this ten-foot concrete wall in front of your network. In fact, it sounds like you got yourself the Colorado Springs of corpnets! You want to allow WinMX in? What's up with that? Do you wear shirts that say "Kick Me"? Do you have a fear of success? Don't allow warez sites into your network! You set yourself up for viruses, worms, and all sorts of unauthorized access when you open up the warez spigots. If you allowed WinMX into your network, you might as well tear down that firewall and open all your ports; they'll be opened for you soon enough. Do yourself a favor, save your warezing for personal use on your home AOL account. An even better idea, bag the warezing – you'll be glad you did.

When Should You Re-service Pack in Windows 2000?

to top

Question:

Hey Uncle Bill,,
I have a Windows 2000 server and have applied a service pack (SP2). If I then install IIS on this machine will I need to reapply the service pack? (as was the case with NT). During the installation of IIS I was prompted for the origional disk and I am concerned that I am running an unsecure version. - Chris Shiltone

Answer:

Listen up Chris, Uncky Bill kicked the bucket. The dude was 107 years old, so his time was about up anyway. You ask a very good question. When should you reinstall the service pack in Windows 2000? I did a broad search of TechNet and various Web sites and I can confidently tell you the consensus is there is no consensus. Some articles state confidently you never need to reinstall the SP, some say you don't need to reinstall the SP *if* the SP is on your local hard disk, some articles say that you only need to reinstall the SP if you have a troublesome

service, like the SMTP service, some articles say you should reinstall the SP when you're asked by the OS, and some articles say you should always reinstall the SP.

I'm pretty conservative. If I can't tell from the executable or from a splash screen for a particular service that its been updated to the latest SP, then I'll reapply the SP. Better safe than sorry.

Security Advisories

Google Toolbar Exploit

to top

If you haven't tried out the free Google toolbar browser add-on, you should. It's great at helping you quickly find info you need to succeed. One small problem: GreyMagic Software discovered a number of exploits that can be run against the toolbar. If you haven't updated the toolbar recently, you should. The first link shows the advisory and the second is a link to the toolbar download site.

Read more...
Read more...

Unsafe Functions in Office Web Components

to top

The Office Web Components (OWC) contain several ActiveX controls that give users limited functionality of Microsoft Office in a web browser without requiring that the user install the full Microsoft Office application. This allows users to utilize Microsoft Office applications in situations where installation of the full application is infeasible or undesirable. The control contains three security vulnerabilities, each of which could be exploited either via a web site or an HTML mail. This flaw affects many Servers and applications, so check out the site for a long list of affected software.

Read more...

Mac OS X 10.2: inetd Replaced by xinetd

to top

Mac OS X 10.2 replaces inetd with xinetd. Xinetd offers an easier way to add, delete, or modify entries in the inetd daemon list. Instead of editing a single file (/etc/inetd.conf), a directory can have xinetd "modules" added or removed to change the configuration, making it easier to modify system behavior. Xinetd also adds features such as access control and logging.

Read more...

News Headlines and Resources

Performance Optimization, Part 3

to top

In the first part of her series on performance optimization, Deb Shinder discussed how you to max out the hard disk. In the second part, she released secrets of RAM optimization. In this third and final part of the Performance Optimization series, she shows you how to max out your processor.

Read more...

The Dangers of Instant Messaging

to top

It takes a very brave soul to be an early adopter of a Your company may have an agent provocateur in its midst. No, it's not a employee acting as a spy for the competition. It's the instant messenger. Your network usage policy probably prohibits using Instant Messengers, but users may still be toking on the chat pipe. Check out this article to learn more of the dangers.

Read more...

Preparing a Mixed Mode Exchange Organization for Native Mode

to top

You had a slew of Exchange 5.5 Servers on your network, but you've finally upgraded that last one to Exchange 2000. Now it's the moment of truth: convert your mixed mode domain to native mode. Will it work? Check out this article and find out what you need to do before it's too late.

Read more...

Office XP Service Pack 2 Hits the Streets

to top

Are you one of the few, the proud, and the wealthy who runs Office XP? If so, you need to know Office XP Service Pack 2 is now available. Heck, you might as well get it while it's still free. BTW – you need to install SP1 before you install SP2.

Read more...

Scheduling Command-Line Win2K Backups

to top

Backing up is hard to do but you must do it. Windows 2000 has a nice GUI scheduling interface, but sometimes you can get more done, more easily, by climbing into the command line pig sty and slopping around a little bit. In this article, Mark Minasi shows you how to schedule complete and differential backups.

Read more...

Hacker Steals NASA Shuttle Design Plans

to top

Hackers are up to their old tricks. This times it's our old friend RaFa from the allegedly defunct World of Hell hackers group. This guy was able to get into NASA boxes and rip off over 43MB of detailed info on the space shuttle's internal workings. How's that for network security?

Read more...

Linux Terminal Service Client for Windows 2000 Terminal Server

to top

It's been a great year for Windows 2000 Terminal Services clients! Matt

Chapman wrote a program called rdesktop that allows you to connect to Windows NT 4.0 and Windows 2000 Terminal Servers. This is great because you no longer have to deal with Citrix ICA junk. Check it out!

Read more...

Download of the Week

Anti-Keylogger

to top

Being a network admin has its advantages. You can lay down the law and enforce network policies. Hey, living in a Police State isn't too bad when you're the Police. But what happens when they start coming after you? Maybe they're after you already! Sure, you installed that keylogger on someone else's machine, but did someone install one on yours? Find out with Anti-Keylogger! It works in all versions of Windows. The eval version detects the intruder and the full version will deactivate it! Check it out.

Read more...