





WHITEPAPER

Network troubleshooting: A how-to guide for modern businesses



GFI Software™

Table of Contents

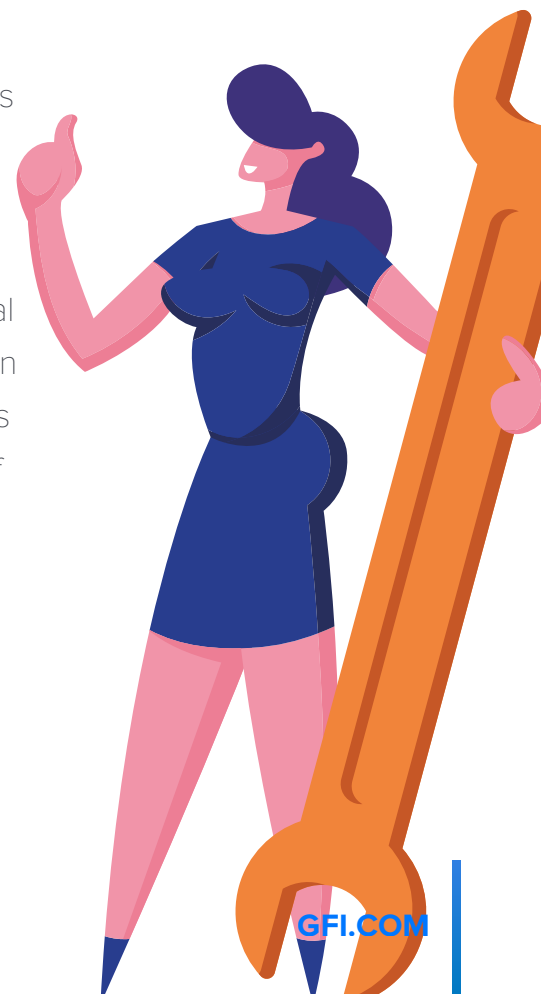
	Introduction	3
	Network troubleshooting strategies	4
	Additional strategies and tools	7
	Request a live demo of exinda NetworkOrchestrator	10

Introduction

Network troubleshooting has come a long way since the early years of computing. It used to be all about pinging hosts and jiggling cables in the server room when your users complained that “the network is down again.” Fast forward to today however and now your business is delivering apps to users directly from the cloud instead of from the server in the closet down the hall. There are cloud services, cloud storage, cloud backup—almost everything nowadays seems to have the word “cloud” in it when it comes to how your organization delivers IT.

This transformation poses new challenges when trying to troubleshoot network problems in hybrid and cloud-first environments. For one thing, it means that an increasingly larger portion of your organization’s network is no longer under your direct control. This is especially happening with small and mid-sized businesses (SMBs) where outsourcing IT services is on the rise and accelerating as businesses try to become more cost-effective and agile in today’s competitive marketplace. And when the edges of your network infrastructure become blurred like this, the question becomes “Who’s in charge?” when something breaks down or goes wrong on a portion of the network.

Troubleshooting network problems when you don’t have total visibility into what’s happening across your entire network can be challenging to say the least. The goal of this whitepaper is to provide some guidance in this area for IT administrators of modern SMB environments. The reader is assumed to have been working in IT for at least several years and already be familiar with using basic network troubleshooting tools such as ipconfig, ping, pathping, traceroute, netstat, nslookup and their various PowerShell equivalents Get-NetIPConfiguration, Test-NetConnection, Get-NetTCPConnection and Resolve-DnsName.





Network troubleshooting strategies

Perhaps the most important thing to understand about troubleshooting issues with your network is that many the-network-is-down kinds of problems are not really network-related at all. From the perspective of end-users, when they can't log on to their devices or send/receive email or access resources on servers or in the cloud, the problem in their minds is that the network—the path connecting them with what they need to perform their job—is broken somehow. But today's networking hardware and infrastructure elements are generally highly reliable, so it's usually more likely that some other kind of failure has occurred like a server going down or misconfiguration being pushed out.

That's why the first thing one should generally ask oneself when troubleshooting a network problem is "What has changed?" Has a new application been provisioned that may be hogging network resources? Is a new lab environment being spun up for some project? Have patches just been applied to a server or cloud instance? Has your company just released a new product that has generated a high amount of interest in your website from customers? Has some sudden event occurred somewhere that has your employees transfixed to watching news sites instead of performing their work? Has an unsanctioned application suddenly become popular with certain users who lean towards the shadow IT approach despite your company proscribing such practices? Has a power failure just happened over in your server room or at the datacenter? Is a contractor currently at work somewhere tearing down walls or moving furniture or equipment during renovations? Is your perimeter firewall currently being reconfigured to block unwanted traffic that's seeking entry into your network? Is your cloud provider experiencing problems that are causing services your company utilizes to lose availability? Asking these types of questions whenever a networking problem arises can often save you a lot of time in reaching a satisfactory resolution. And if you do discover a change that may be connected to your networking problem then asking the concomitant questions "Who did that?" and "Why was that done" can also be helpful in cutting to the chase and narrowing down the root cause of your problem. And if you have a good way to ask several of these questions in parallel, rather than sequentially, it can speed up your troubleshooting effort as well.

If nothing obvious appears to have changed anywhere on your network—and remember this also includes remote sites, WAN links and cloud services—then you may need to approach your problem more methodically. There are two basic ways you can do this. The first approach is to systematically work up the stack beginning with hardware (e.g. hosts, routers, switches, access points, firewalls, load balancers, WAN appliances) and operating systems (be sure to check the event logs on Windows hosts and syslogs on all network devices). Then you go up through the various protocol layers and verify TCP/IP connectivity, IP routing, and finally DNS, HTTP, SMTP and other application-specific protocols. This approach can be effective if there are no obvious clues initially as to what has gone wrong with your network or when the issue you're experiencing is transient or intermittent. Be careful also to resist the temptation to put off investigating transient networking issues as these can quickly spiral into huge catastrophes if you take an "I'll get back to it later" attitude instead of investigating them immediately.



If the issue you are experiencing is relatively well-defined and narrow in scope, then the opposite strategy of working down the stack may be useful. Examples of network problems that are narrowly bounded would be a web site or cloud service going down, performance degradation happening with a suite of apps, or complaints about WiFi access failing by users in a single department or locale. In such situations it can often be best to test application layer protocols first to understand more clearly the nature of the problem. Then if no clues are uncovered you can dig more deeply into the session, transport and network layer protocols for more information about what's happening with your network.

For both of these approaches the additional value gained from having a good network monitoring solution in place can save you lots of time and prevent your business from suffering losses resulting from network downtime. By having a system in place that can monitor your network in real-time and show how applications are performing and where problem areas like bottlenecks may be happening, you will often be able to jump several steps ahead as you methodically investigate the problem happening on your network. Network monitoring solutions can also help you catch incipient problems before they grow and reach the point where users are affected and customers impacted; the proactive benefit from utilizing such solutions can easily pay back their investment and are worth investigating if your company is serious about protecting their business from the risks of network downtime.

Don't forget too that the performance and security of your network can often be related. Infection by worms, viruses and other forms of malware can negatively impact the way both client and servers on your network perform on the network, so it's always a good idea to check your antimalware solution to see whether anything was flagged prior to when your networking problem arose. Certain forms of malware can also infect routers causing LAN or WiFi failures or bottlenecks if they're not dealt with, so part of the task of proactively preventing network problems is to learn to keep abreast of various threats and vulnerabilities that can affect anything that is part of your network infrastructure.

One final tip that is often overlooked when it comes to network troubleshooting is the value of documenting your network infrastructure. Have network documentation that is detailed, comprehensive and up to date can expedite things considerably when you're under pressure trying to get some portion of your network up and running again.

In today's fast-paced world of DevOps and agile approaches to business and technology, it's worthwhile having tools that can automatically document every aspect of your network including the systems you're running, software you're using and cloud services you're consuming. Most network management solutions are able to do this to various degrees but there are also some specialized tools available you may want to look into. Tools for automatically generating accurate point-of-time documentation for your network are often expensive, but they can be worth it when a crisis occurs. There are also Open Source tools available that may meet the needs of certain SMBs.



Additional strategies and tools

We mentioned at the beginning of this whitepaper some of the tools commonly used for troubleshooting networking issues in Microsoft Windows environments, and similar tools exist for the Linux/UNIX platforms. And for problems that resist simple explanation there are always network packet sniffing, capture and analysis tools like Wireshark or Ettercap you can pull out of the closet as long as you're well versed in using them. But what about when a good portion of your network resides on the edge of your network or is somewhere out there in the cloud? The good news is that there is now a wealth of online tools for troubleshooting network problems on the larger scale of the Internet.

A good place to begin is by troubleshooting your company's Internet connectivity since that's how the cloud services you utilize are delivered to you. Basic testing involving the measurement of the availability, bandwidth and latency of your Internet connection should be conducted right away when a cloud outage is experienced. A simple site like Speedtest by Ookla can be used for this purpose; there are also other alternatives such as OpenSpeedTest and TestMy. To test connectivity by pinging a host from multiple locations around the world, the site Ping.PE is invaluable; it can also be used to perform TCP port checks and do digs. The tool My Traceroute (MTR) combines the functions of ping and traceroute and there are websites that let you run this tool from various locales around the world. Global Traceroute can perform pings, traceroutes and DNS queries using either IPv4 or IPv6. And for the truly enterprising there is always Multi-Probe Looking Glass (MTR.sh) which can run ping, traceroute, MTR and BGP lookups from anywhere in the world.

All such network troubleshooting tools, both built-in and online, are useful primarily for the experienced networking professional as the results they provide can often be difficult to interpret properly. For example, the commonly used troubleshooting tool traceroute (called tracert in Windows) is usually described as a simple tool for determining where packets are being dropped or where latency is high as packets travel across a series of router hops between the user and some remote host. Unfortunately on today's Internet it rarely works this way—see Richard Steenbergen's presentation at NANOG 47 titled "A Practical Guide to (Correctly) Troubleshooting with Traceroute" (available online as PDF) if you want to understand how naïve this simple explanation is of traceroute's usefulness.

When it comes to keeping your users productive and customers happy, most of us who work in IT administration and support don't have the time or experience to utilize many of these tools properly or for realization of their full potential. Once again this highlights the importance for businesses to have a good network monitoring solution in place, one that can not only identify problems on the on-premises network and recommend possible steps for resolution but also monitor WAN connections and the availability, bandwidth and latency of websites and cloud services your company uses.

One strategy that can be extremely helpful when troubleshooting network problems in cloud-connected environments is building good relationships. If your business relies for its success on services delivered by a cloud provider, you need to make an effort to ensure clear and responsive lines of communications with your provider. Make sure you have their status and incident report pages bookmarked in your browser favorites and learn how to understand and quickly navigate through their outage reporting maps. Follow any Twitter feeds they regularly use for announcements and subscribe to any email mailing lists they use as support channels.



If your business with them is enough to warrant them having a Technical Account Manager (TAM) assigned to you on their side, try to cultivate a good relationship with that individual so they will respond promptly to your urgent emails and phone calls when something happens with their service that affects your business. It may be that the problem is actually caused by something happening on your side of the network where you are the one who is in control of things. In that case getting a fast response from your TAM which allows you to cross out your provider as the source of your problem enables you to avoid wasting precious time and focus your energy on examining the operation of your own network. Don't forget also to establish good relationships with any other vendors of IT products and services your company utilizes.

Finally, a well of assistance you can draw from during a troubleshooting emergency is leveraging your peer community of colleagues in the IT profession. Managing a corporate network is often a lonely endeavor and can easily become a sink for all your time, and neglecting building connections with other IT pros can leave you feeling even more alone when faced with a crisis. It's important to remember that participation in advance will often make it easier to obtain timely assistance afterwards. In other words, you have to "put the bucks in to get the bucks out" so start by helping others in the larger IT community when they encounter difficulties and they'll be more disposed to return the favor. The Spiceworks community is one of the more established and helpful resources in this regard, but there are others you may want to look at like Experts Exchange and several others specializing in different areas. Whatever way you decide to build out your network of specialists you can draw upon, whether it's by hanging out for beer with them on Fridays or meeting them online in forums or using Teams or Zoom, you'll find that the time and effort you put into building good relationships will help you mitigate your risks, and not just in troubleshooting but also during the planning, purchasing and implementation stages of administering with your network.



exinda **NetworkOrchestrator**

Manage network performance by focusing on the user experience of key applications

[Learn more](#)

[Request a live demo](#)

- ✔ See your network from the user's perspective
- ✔ Control network traffic & applications
- ✔ Improve application performance



All product names and companies mentioned may be trademarks or registered trademarks of their respective owners. All information in this document was valid to the best of our knowledge at the time of its publication. The information contained in this document may be changed without prior notice.