whitepaper

Bad Network Experience? Fix the Right Problem.

solarwinds

If you run a network, you know how complaints start. Lowly users or high-placed executives come to you complaining of lousy bandwidth, applications that freeze mid-transaction, phone calls breaking up, video scrambled — and whatever the cause, it's your fault. Often, even the most non-technical people have their own ideas about what's wrong with the health of your network and how to fix it, which might involve switching telecom companies, buying more bandwidth, or swapping out hardware.

More often than not, these theories are hilariously misguided. Career Tip: You don't have to tell them that. Acknowledge their pain, let them know you're sorry they are having a crummy experience, but not to worry — you're on the case. You don't want to jump to conclusions by making hasty (and expensive) decisions, but you will get it figured out.

Don't waste your time giving long-winded technical explanations of what you think the real cause of their misery is, especially if you don't yet know. Job one is to come up with a correct diagnosis of what's going wrong and why, so you can fix the right problem.

This paper covers the components of good & bad network performance and how to perform that correct diagnosis.

Checking the Vitals

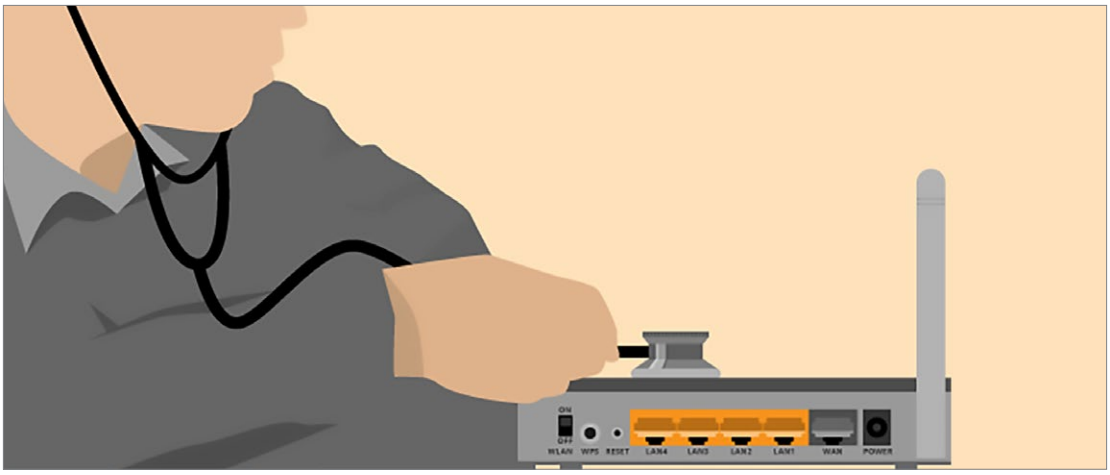
The symptom is not the disease. When an emergency room patient comes in and complains of nausea and fever, it could be influenza or the plague, and it's important to find out which one. If you were running a hospital, you wouldn't want doctors putting everyone who has the flu into quarantine, but neither would you want them to be responsible for starting an epidemic because they failed to ask the right questions or perform the right tests.

It's the same in networking. The symptom (perception of awful network performance) is causing real misery, but it could be the result of more than one disease. Broadly, the malady might result from:

- **Hardware** – equipment is overworked, fried, or faulty
- **Configuration** – incorrect settings and illogical routing
- **Network** – fundamental characteristics such as bandwidth and latency

You could get lucky: the first thing you check could be the real cause, making the solution straightforward. But if you've been doing this for more than 15 minutes, you know that life as a network administrator is seldom that easy. The way to crack tough-to-solve problems is to systematically examine each possible cause, keeping in mind that you might find more than one thing that needs fixing.

whitepaper



Hardware Failure

Hardware issues can be either blazingly obvious (the router catches fire) or devilishly subtle (the intermittent failure that occurs only when you're not around). You wouldn't be in network detective mode if the cause of all your problems was immediately obvious, so the question is, how do you diagnose tricky hardware problems?

Network hardware issues to watch out for include:

- **Environmental** – overheating, faulty wiring, and other sources of sabotage
- **CPU** – inadequate processing power
- **RAM** – inadequate memory
- **NIC** – network interface card(s) need to be replaced

Which of these is your problem, if any of them?

One of your best diagnostic tools is ongoing network monitoring, which lets you back-track and see what went wrong even when you weren't watching. You want to be able to spot patterns.

Here's an example: one big city school system was receiving complaints from a school that the Internet connection was dropping several times a day, and the problem was worse for some reason during summer school. An examination of the network logs showed a clear pattern: the connection would drop almost every afternoon — particularly on hot days. After 20 minutes or so, the connection would come back up and behave for a while, but then often it would fail again.

The explanation was simple: the equipment was overheating, and no wonder: the router was on the top shelf of a closet — not a telecom closet, but an actual janitor's closet — with the fan right up against the wall blasting the expelled heat right back into the machine. On hot days, the temperature of that hard-working router would reach about 220 degrees.

Since plastic melts at 225, the manufacturer had programmed the device to shut down at 220 before permanent damage was done. Once it cooled down, the router would gamely restart — only to overheat again a little while later.

Sometimes timing tells the story. Another example: a municipal agency had its networking cables running through a storm sewer. Overlaying the local weather map on analysis of network failures and slowdowns made it easy to see how things went wrong — even to the order of failures — every time a storm came through and equipment started shorting out.

CPU and RAM issues, on the other hand, are more likely to crop up in cases where fairly old networking equipment is still in use, or the size and complexity of the network has increased dramatically since the equipment was first installed. This makes the challenge of computing optimal network routes a steeper one.

You might be dealing with a CPU or memory overload if you see one or more of these symptoms:

- *"Lost connection"* messages and other intermittent interruptions
- Applications halting for no apparent reason and then resuming equally randomly
- Overall slow response from applications that you connect through from a particular device

Similarly, a bad NIC is probably an outdated NIC. Symptoms to watch for include:

- Slow response times
- Corrupt data
- Timeouts and retry messages

Determining which piece of hardware is slow or drops connections should be simple with proper network monitoring, which lets you see failures associated with a specific network segment associated with that device. Determining the exact cause of the problem is harder: slow or failing connections associated with a particular piece of hardware can be the result of CPU, RAM, NIC issues, or more than one thing going wrong simultaneously. Once you identify the problem device, often the simplest fix is to replace it with another unit, rather than worrying about whether the fault is in the CPU, RAM, or NIC.

Configuration Errors

Bad hardware happens, but bad network device configurations happen more frequently. Various studies indicate that between 60% and 80% of network downtime is the result of faulty configurations, with a few famous Facebook® and Xbox LIVE® network outages among the most glaring examples.

The IT advisory firm Gartner Inc. says 80% of network downtime can be traced to people or process issues (an estimate that it has left unchanged for more than a decade) and

currently puts the cost of downtime to a major corporation at $5,600 per minute or well over $300,000 per hour.

While there may be a few switches to flip on the outside of the box, most device configuration is done in software. The embedded software could have a bug, or the latest bug-fix update to the software could contain a worse bug than the last one. Certainly, checking for software updates from the manufacturer should be part of your debugging routine. And if none of your configuration changes seems to work, you might consider whether you've found a brand new bug.

More often, the problem is with the people using the software. Sorry to say, that's you and your colleagues (although sometimes you can blame a former colleague or contractor, which is more fun). To quote HAL 9000, *"This sort of problem has come up before, Dave, and it has always been due to human error."*

Since humans also write the software, every software error is ultimately a human error.

What sort of errors should we watch out for? Anything where the parameters entered in some configuration screen don't match reality. For example, the specified bandwidth doesn't match the actual circuit speed, leaving things in a confused state. Or there could be a duplex mismatch, a conflict in configuration between two pieces of equipment resulting in degraded performance.

Routing is fundamental to network configuration. A router's job is to keep track of all the other routers on the network and the optimal series of connections it needs to make to transmit any signal. But the routing tables that govern this behavior can become confused, causing a router to send traffic on a roundabout journey. On older equipment, the routes may have been set manually and never been updated. Or the routes may have been calculated automatically by the software on a day when the optimal path between two points was unavailable due to maintenance or a service outage. On that one day, the path made the most sense, but for whatever reason the router never went back and recalculated.

If traffic from Manhattan to Newark is being routed through San Francisco, your network monitoring ought to make that plain. The cure is often as simple as resetting the router so it recalculates all network routes.

Sensible precautions can go amiss. Configuring a network to failover to a backup circuit can make the network more reliable and perform more consistently. However, if the failover parameters are configured incorrectly and the backup circuit kicks in when it shouldn't, that can be another way of sowing chaos.

For example, we know of one business branch office where employees constantly complained about poor WAN bandwidth — they were forever enduring slowdowns in their connections to corporate applications at headquarters or a remote data center. It turned out the backup circuit in this case was the cellular network, that is, a wireless network card in the router that was supposed to kick in if the landline connection dropped for some reason. Instead, the backup circuit switched on randomly throughout the day due to a misconfiguration. As soon as that was corrected, complaints faded fast.

Some of the most critical configuration issues concern Quality of Service (QoS) parameters. The point of QoS is to make the network experience better, but that's only true if it's configured correctly. A botched implementation can make the user experience worse.

QoS technology prioritizes traffic that is important, sensitive to delay, or both. The most prominent examples of traffic that needs to be delivered at a steady reliable pace are voice and video calls. Without proper QoS, Voice over IP and video calls easily can be distorted if multimedia data is forced to compete with a large file download simultaneously happening on the network. QoS gives voice and video data and other synchronous communications higher priority than other transmissions that don't have the same real-time requirements.

On Cisco® networks, you can verify that your QoS configuration is tuned properly for voice and video by monitoring and using Cisco's IP SLA protocol as a way to verify Service Level Agreements for network capacity. WAN routers use IP SLA to send simulated voice calls to each other and verify the call quality.

You might assume that IP SLA would be a good indicator of the overall health of your network — with VoIP as the canary in the coal mine, the sensitive application that lives and dies with the network. That's true up to a point, but you must be able to look at more than one factor to really understand your network.

Suppose the QoS prioritization of voice and video is cranked up to 11, Spinal Tap style. While other applications may not be as sensitive to delay, their transmission of data can't be allowed to slow to a snail's pace every time someone is holding a videoconference.

Network Capacity

If the problem is not in the hardware or the configuration, then it may be in the basic qualities of the network: bandwidth and latency. Bandwidth is the raw capacity of a link to deliver a given number of bits per second, while latency is the time required to get a response from a remote application.

If users complain about performance issues with a particular networked application, the problem could be with that application, not the network. Usually, when the problem re-

ally is the network, performance is degraded for all applications, not just one. That would be true if a branch office was being served with inadequate WAN bandwidth, for example — users would see poor performance from all remote applications. So you definitely want to ask around at that site to verify.

If users complain about a single application, on the other hand, the network is not necessarily off the hook. It's always possible that there could be problem with the network segment in the data center or whatever facility the application server is hosted in.

One diagnostic tool that's invaluable for answering the question, *"Is It the Network or the Application?"* is Deep Packet Inspection (DPI). DPI lets us examine network traffic more closely, going beyond the addressing headers to understand what applications are generating traffic and how quickly those application packets are being delivered.

A simple way to separate networking from application issues is to examine the time difference between a server's initial response to a request from a client — the initial ACK acknowledgement reply — and when the server starts sending back data. The difference between the speed of the acknowledgement and the speed of the application response is the processing time of the application server. If the difference is significant, that's a clue to some deeper problem with the application, which might be inadequate CPU or poorly written database queries. There could still be a network issue in the mix, like a poor connection between the application server and the database server. Otherwise, this is the network administrator's cue to throw that over the wall to the application administrator.

Consumption of bandwidth by various applications is the other application issue network administrators must be alert to recognize. If your bandwidth is being eaten up by hard-working employees doing their jobs, then you need to find some way to give them more of it. On the other hand, if you discover your biggest bandwidth hog is a security guard who has been streaming Netflix in HD, the solution might be to block that application or, perhaps, a staffing change.

As discussed in a separate paper, *"Is It Really the Bandwidth,"* nontechnical employees (including senior executives) often jump to the conclusion that a bandwidth upgrade is required when often more efficient use of existing bandwidth is a more cost-effective solution. To the layperson, bandwidth and latency also seem like two aspects of the same thing—a poor network experience. You can diagnose the issue quickly by looking at the symptoms:

- Inadequate bandwidth symptoms: Files take forever to upload or download and applications like video are impractical.
- Latency symptoms: You submit a web form and several seconds pass before a response appears on your screen. Using the ACK-to-data delay test described above, if both the ACK and the data are slow to be delivered, then the problem is most likely network latency rather than a slow application.

One component of latency is geographic distance. Even signals traveling at close to the speed of light take time to travel between cities on opposite sides of the country, and it's worse between cities on opposite sides of the world. Network routes also are not necessarily the shortest distance between two points; they are dictated by practicalities such as the rights of way telecommunications companies have secured along highways or over open land.

The speed of light is a constant you can't change, but latency isn't all Einsteinian physics. On anything short of an intercontinental WAN link, latency is more likely to be a side effect of network overload. When the network is fed more data than it has capacity to transmit, you get queuing delays because data is being buffered or held until room opens up to squeeze it onto available bandwidth.

So a branch office with inadequate bandwidth is likely to experience problems with both high latency and more bandwidth-centric issues like slow downloads.

Another place queuing delays can occur is at the intersections between high-capacity and low-capacity links. Think of it like taking the off ramp from a four-lane highway to a country road. Taking that exit means you have to slow down, of course, but it could be worse than that. If a few hundred cars take that exit at once, a minor slowdown can turn into a major traffic jam.

Again, the result is latency, and latency can be a major drag on employee productivity. Nobody wants to spend long minutes looking at a *"page loading"* message on web applications or frozen screens on thin clients.

By monitoring your traffic to identify traffic jams, you can spot patterns to use to adjust your capacity plans or network configuration.

Diagnostic Tools

Network monitoring is key to understanding what is going right or wrong on the network and why. Network monitoring tools take advantage of several fundamental technologies and protocols, some of which we have already mentioned:

- **Simple Network Management Protocol (SNMP)** – the Internet standard for devices to report their status, including whether the element is online and operating as well as detailed statistics, such as how much data it is processing, how many users are connected and more. SNMP traps, on the other hand, are triggered when something goes wrong, firing off alerts that the monitoring system can store and analyze.
- **Syslog** – a logging mechanism that reports errors and other events similar to SNMP traps, but the message format is more freeform, and requires less processing overhead in terms of encoding and decoding.

- **IP SLA** – a Cisco router-to-router protocol that mimics the transmission of time-sensitive traffic, such as Voice over IP, to test whether a connection is robust enough to support voice calls and other real-time applications.
- **NetFlow** – a protocol for monitoring network traffic by *"conversations,"* letting you see which network nodes are exchanging the most traffic and over what protocols.
- **DPI** – peers into the application characteristics of traffic and measures how quickly packets are being delivered for specific applications. Helps answer the question, *"Is It the Network or the Application?"*
- **QoS** – prioritizes the delivery of packets for applications that are most sensitive to delay, such as voice or video. In addition to measuring QoS using IP SLA, we can alter QoS parameters to balance the traffic allocated to all applications.

SolarWinds® offers a variety of products, including Network Performance Monitor, NetFlow Traffic Analyzer, and VoIP & Network Quality Manager that build on these standards to help you monitor the health and performance of your network.

With proper diagnosis, you should be able to trace any set of symptoms to the true cause, rather than prescribing a bandwidth upgrade when the real problem is a bad configuration or faulty hardware.

So, Doc, Am I Cured?

If your patient is the network, how do you know when it's cured? If user complaints stop or slow down, that's a good sign. By being systematic about the process of diagnosis, you can be more confident that you have identified the root cause of the problem. Because you want to be thorough, you don't necessarily stop with the first possible explanation, understanding that there could be more than one thing wrong. But you've done it! You've taken action, and now things are better.

Does that mean you're done? No.

Much as our healthcare system needs to move away from just being about *"sick care"* to focusing on ongoing wellness, a really good network administrator wants to monitor for small problems before they become big problems, while always remaining alert for opportunities for further optimization. To keep your network healthy, you want to be able to visualize how well it performs at any time. You want to be able to see where the bottlenecks and slowdowns are, which applications are associated with them, and whether they demand immediate attention.

With the right diagnosis, you can nurse your patient back to health. The ultimate goal is to go beyond that. You want your network to be positively glowing with health: fast and dependable, performing at the top of its game.

That's a job that's never done, but it's one worth doing.

whitepaper

Related Resources

For more on network monitoring and troubleshooting best practices, check out these related resources:

- Monitoring 101 – Community-sourced white paper sharing basic vocabulary and concepts for network monitoring.
- Is It Really the Bandwidth? – White paper discussing 3 techniques to help you address demands for more bandwidth.
- Basics of Routing Protocols – 4 part blog post series sharing the basics of routing protocols.