solarwinds

eBOOK

Network Mapping

The Journey From Data to Information to Visualization and Finally to Action

by Leon Adato and Destiny Bertucci

Table of Contents

Chapter 1: Introduction

The first known map was of the stars. Carved into the walls of the Lascaux cave complex in southwest France over 16,000 years ago, the cluster of dots depicts star formations observed by people at the time, and were used, as all maps are to one extent or another, to communicate important information about their surroundings. Earlier maps exist, of course—some dating back over 27,000 years—but those proto-maps depicted land formations that might be recognizable to folks who were already familiar with the locale, not to outsiders. What's my point? Throughout the history of humanity, we have wanted to tell stories of things we have seen, whether it was to avoid trouble or to help others find their way. And for the vast majority of that history, we've told those stories in pictures.

Archaeological studies tell us this isn't just a pretty picture of "what I poked with my spear on my summer vacation." Viewed in the correct light (literally: in a dark cave with flickering torches, these images appear to move), this picture transmits complex information about hunting techniques and safety, migration patterns, food choices, and more.

The ability to turn data into a visual form, and more than that, into a USEFUL visual form, is a trait that humans have exhibited since the dawn of time. And while some ancient images, such as the one above, were intent on delivering raw information, far more are pictures which we've come to think of as "maps."

But how does this help us in the here-and-now, as IT practitioners coping with a barely-manageable barrage of mixed technologies? First, knowing this basic truth about ourselves—that our very core is visual—serves as a reminder that we understand complex ideas more clearly with diagrams, blueprints, and layouts. It also reveals an uncomfortable truth: that networking is in need of new, improved methods of visualization. Yes, we have the printed diagrams and some software that will allow us to see our network pathways. But to truly understand what a device is doing, it needs to be brought to life with images that, like the torch-lit carvings of the past, move with a life of their own and therefore impart greater understanding.

In this eBook, we intend to dig into the current state of mapping in the IT space, with a focus on network mapping, to find out which techniques are oldies-but-goodies, and which may, like those old Medieval maps that proclaimed, "here there be dragons," be sorely in need of an update.

To put it more plainly: Network engineers and administrators create network maps, graphical representations of devices and their connections, to understand how those devices are connected. Network devices like routers, switches, firewalls, and the devices that access enterprise networks, such as PCs, can be pictorially represented in a network map. By providing an accurate and interactive point of reference, administrators can maintain day-to-day operations and keep track of not only the simple status (up/down) of the network infrastructure, but also the nuances of how that infrastructure operates under typical (and often atypical) load. In a large enterprise, network maps are a key factor in reducing the time taken for troubleshooting network issues because they help administrators quickly identify and locate devices that cause problems.

IS THIS BOOK FOR YOU?

This guide gives you insight into the theories and techniques available to create a variety of maps, and to understand when and where in an IT environment they are best used.

It is geared for IT professionals, people who create, maintain, and support networks and their users, who know what monitoring is capable of. Whether you've had actual hands-on experience with monitoring software matters not.

If you are interested in this topic, but feel a bit behind on monitoring concepts, we can recommend several free guides:

» It's Automation, Not Art

» Monitoring 101

» Monitoring 201

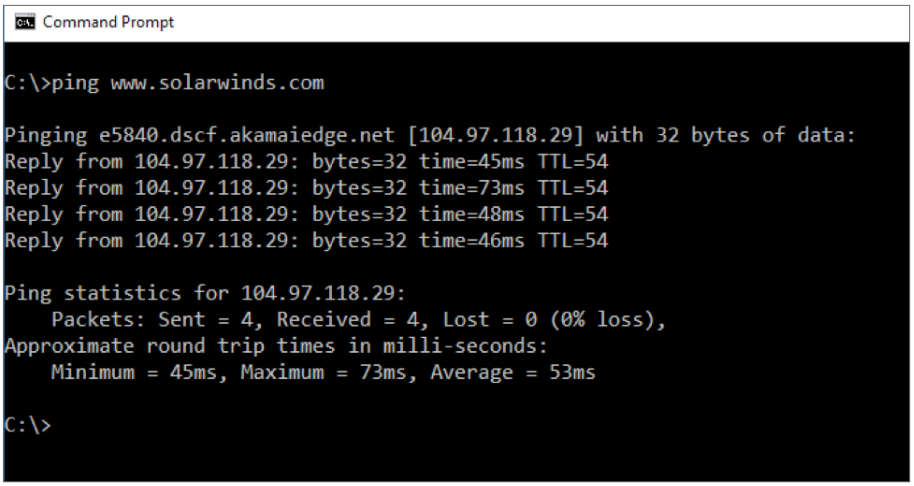
Chapter 2: What *IS* a Map, Anyway?

While the introduction describes a bit about why we, as humans, might create and use a map, it doesn't really get to the heart of what characteristics are essential for a picture to be a map. Simon Wardley, one of the pre-eminent voices in mapping as it relates to IT and business, states (https://blog.gardeviance.org/2015/05/what-is-map-what-isnt.html) that two elements are fundamental for something to be considered a map: position and movement. Some visualizations, such as business process diagrams, show relationships, but not movement.

However, it's easy to fall into the trap of thinking that, according to Mr. Wardley's definition, a map must actually move to be a map. This is, of course, impossible for the vast majority of objects we call maps today. To clarify, we'll use his example of what IS a map, although it may not be thought to be one initially: a chess board. Rather than a static image of a game at a particular point in time, a chess board conveys (for those who can read it) both the current position of pieces and where each piece could potentially move in the future. Moreover, to someone VERY familiar with the game, a snapshot of the current board can also provide insight into where the pieces were. All with a single picture.

THAT is a map: position and movement.

In IT, we run afoul of considering lots of things "maps" that really aren't. One example is the venerable "ping" command. Some would go so far as to say that without the pictures, ping still "describes" a map-like environment.



But looking closer, you will realize that this confuses active behavior (each ping status) with "movement." What I'm really getting is ONE position of ONE thing at ONE moment in time. I just get a sequence of 5 of those snapshots, but I have no idea where the next hop will land.

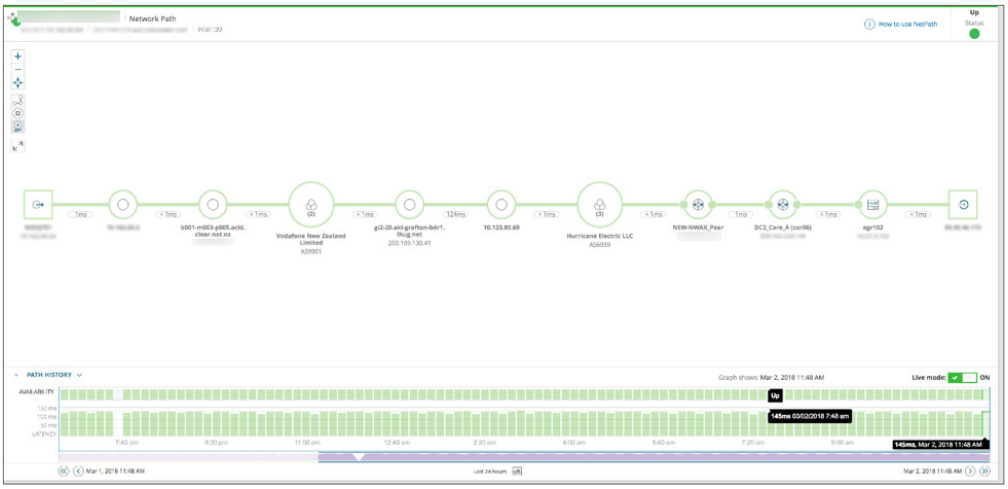
Which means traceroute is equally challenged.

```
Command Prompt

C:\>tracert www.solarwinds.com

Tracing route to e5840.dscf.akamaiedge.net [104.97.118.29]
over a maximum of 30 hops:

  1     3 ms     5 ms     5 ms  SecGwy [192.168.101.1]
  2    14 ms    14 ms    15 ms  142.254.157.105
  3    27 ms    30 ms    31 ms  po63.bcwdohct02h.midwest.rr.com [24.164.114.37]
  4    51 ms    17 ms    17 ms  24.33.100.22
  5    26 ms    21 ms    22 ms  be14.clevohek02r.midwest.rr.com [65.29.1.98]
  6    24 ms    22 ms    19 ms  be25.clevohek01r.midwest.rr.com [65.29.1.32]
  7    53 ms    46 ms    44 ms  so-7-1-0.ar0.dca10.tbone.rr.com [66.109.6.66]
  8    43 ms    46 ms    45 ms  bu-ether12.nwrknjmd67w-bcr00.tbone.rr.com [66.109.6.29]
  9    54 ms    55 ms    47 ms  66.109.5.138
 10    44 ms    43 ms    43 ms  66.109.1.59
 11    57 ms    42 ms    44 ms  a104-97-118-29.deploy.static.akamaitechnologies.com [104.97.118.29]

Trace complete.

C:\>
```

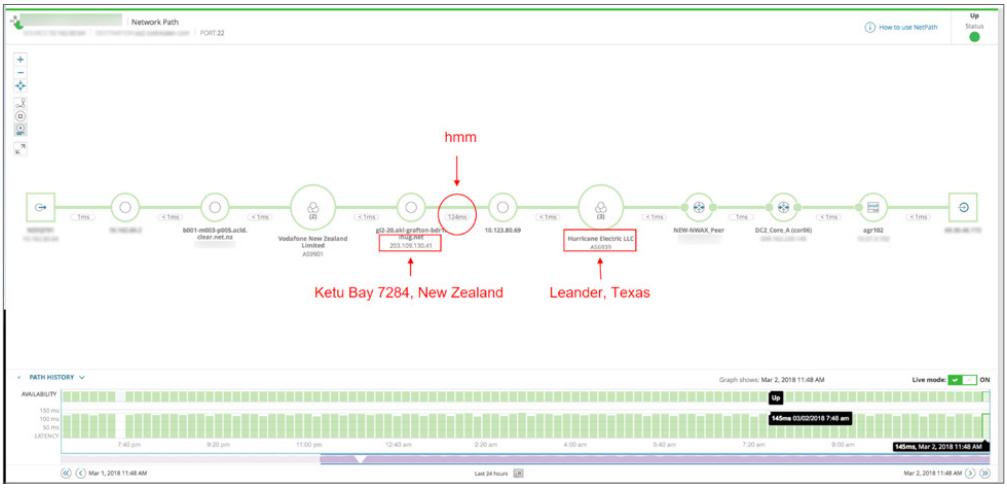
Here I get a better explanation of where I've been, but still no sense of where I might go next. But that's not to say that the action we're describing—the movement of a packet through a set of network devices—is not a good use case for mapping.

To show an example that would satisfy Mr. Wardley's fundamental description, we're going to draw on an example from THWACK MVP Byron Anderson.

Byron had a client who was complaining about slow network speeds between two offices. Folks in the office told him that ping routinely showed a 124-millisecond delay. Using a mapping tool specifically designed to show the path that packets were taking, the delay was immediately obvious.



The cause was less obvious. However, a bit more digging revealed the likely source of the problem.



It turns out the delay was a matter of physics. You see, with nearly 6,000 miles between New Zealand and Texas, the speed of light becomes a limiting factor.

But it was only with a map—one showing both position (each node in the chain) and movement (the variations in path each packet could choose)—that this issue became clear to both Byron and his client.

Chapter 3: Different Types of Network Maps

Before the advent of automated mapping tools, administrators manually created a list of devices in a spreadsheet and maintained it with user/device details. For IT pros to have an idea of how network devices were distributed physically, tools like Microsoft® Visio® were available to help create static diagrams. However, once created, a static map doesn't track any changes in either the network or the topology, and it lacks the ability to discover new devices. Moreover, manual effort is needed to update static network maps every time a device is added or removed.

What this boils down to is that static maps are out of date almost as soon as you close the file.

MAP TYPES, PART 1

But even before the question of automatic or static mapping there's the issue of what part of "the network" you intend to map. Do you mean…

Mapping the Physical

Mapping the actual runs of cable, their terminations, etc., may be tantalizing in its concrete-ness. It is, in fact, the closest visual representation of your "true" network environment. But there is a question of depth. Do you need every NIC, whether it has something plugged in or not? How about pin-outs? How about cable types? Cable manufacturers? Backup power lines? And so on. And of course, it's nearly impossible to generate this type of map automatically.

Mapping the Logical

Most network maps fall into this category. It is less interested in the physical layer than the way data connections behave in the environment, and therefore more accurately represents the movement of data even if you can't always tell how the cabling works.

Mapping the Functional

This type of map is the one your users and systems administrators want to see: a map representing the way application traffic logically (but not physically) flows through an environment. That said, as a network map, it's sub-optimal because application servers aren't always physical. The depth of the map is in question, and it's purposely obfuscating the network infrastructure in favor of showing data flows, so its usefulness to network engineers is minimal.

Regardless of the focus of the map, the method with which it is created is still key. And if it wasn't already clear, we're big fans of "automated" whenever possible. All the disadvantages to manual methods have led to the creation of tools for automated network mapping. By automating and easing the mapping process, a significant workload is removed for the network admin. Automation allows maps to be easily updated as new devices are added or topology changes without significant manual intervention. Real-time dynamic network maps go one step further by automatically detecting changes and updating the map accordingly through auto discovery. They help with troubleshooting by creating a layout of connected network devices alongside key performance metrics.

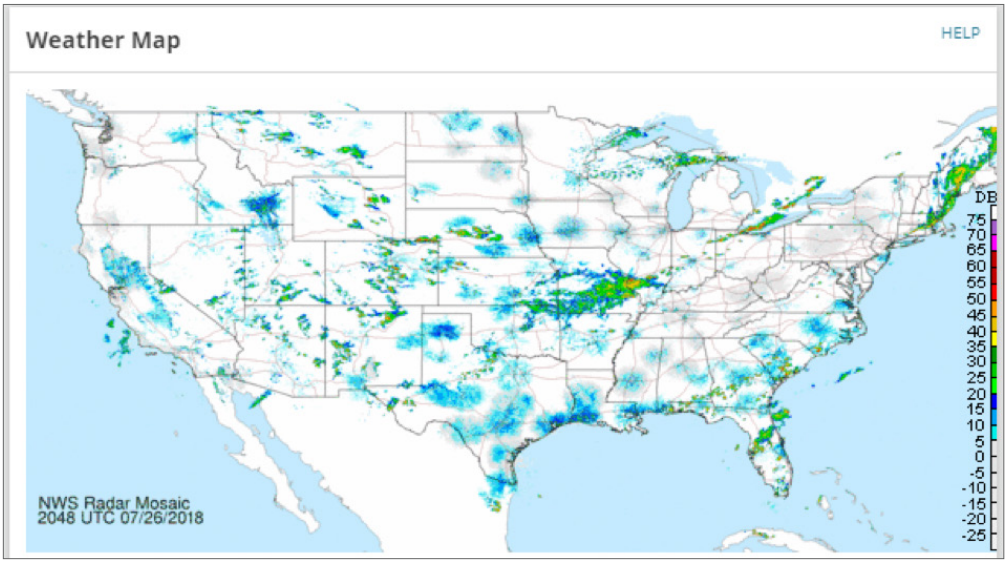
MAP TYPES, PART 2

But not all "automated" maps are equal, so we want to take a moment and describe them at a high level.

Handcrafted Artisanal Maps

Despite having few automated elements, these maps still have a valid use case and are therefore worth mentioning. Creating a map using a manual process similar to a simple, fixed, Visio map, the output that fits into this category (and the tools that create them) require a significant time investment, but, when used correctly, have an equally significant return.

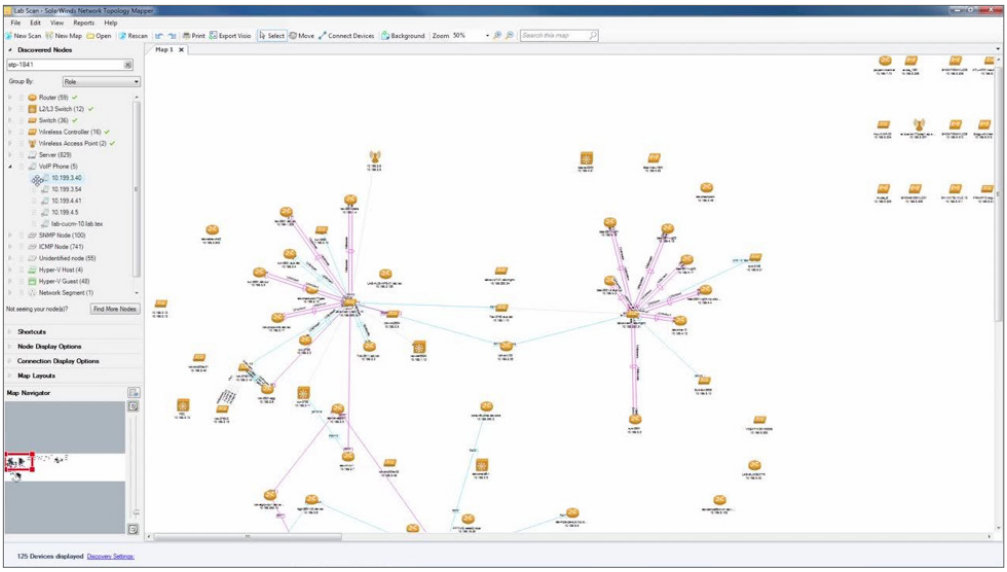
As an example, this technique can be used to create complex nested maps that show a map of the U.S., with the color of each state representing the overall status of all the devices in that region. (Green means everything is "good." Yellow indicates some (but not all) devices have issues. Red means everything is in trouble.) Clicking a state reveals the status of the next lowest level: locations. From there one can drill down through buildings, floors, closets, or data centers, and finally to the devices themselves.



A second use case would be the ability to tie the map to a range of data-fed backgrounds—such as weather maps—which provide a visual clue as to the conditions near the infrastructure.

Semi-Automated

When you can automatically discover new network devices, but still need to interact with the tools to confirm adding those devices to a map (not to mention positioning them in correct relationship to the other objects), you have a semi-automatic process.



The discovery piece relieves staff of the burden of remembering to add equipment, not to mention adding all the relevant sub-elements, but there is still human-based work to be done.

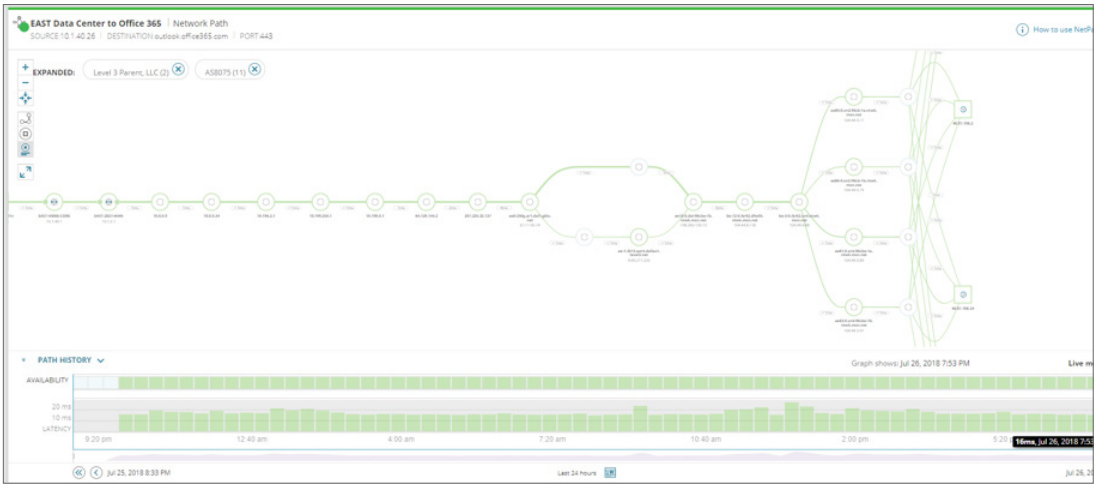
The benefit of this type of mapping is that the repetitive burden of finding, identifying, and adding new devices and sub-elements is removed, while allowing the freedom to control the output.

The downside, as should be obvious, is that it still takes (human) time. It's not reactive to the environment.

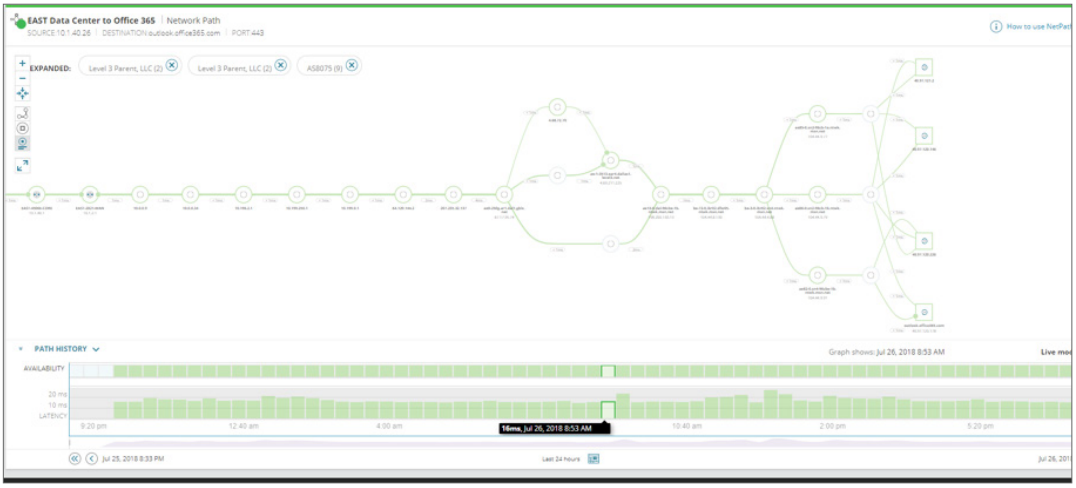
Fully Automated

And this highlights the number one benefit of fully-automated maps: they are responsive to the environment as it changes.

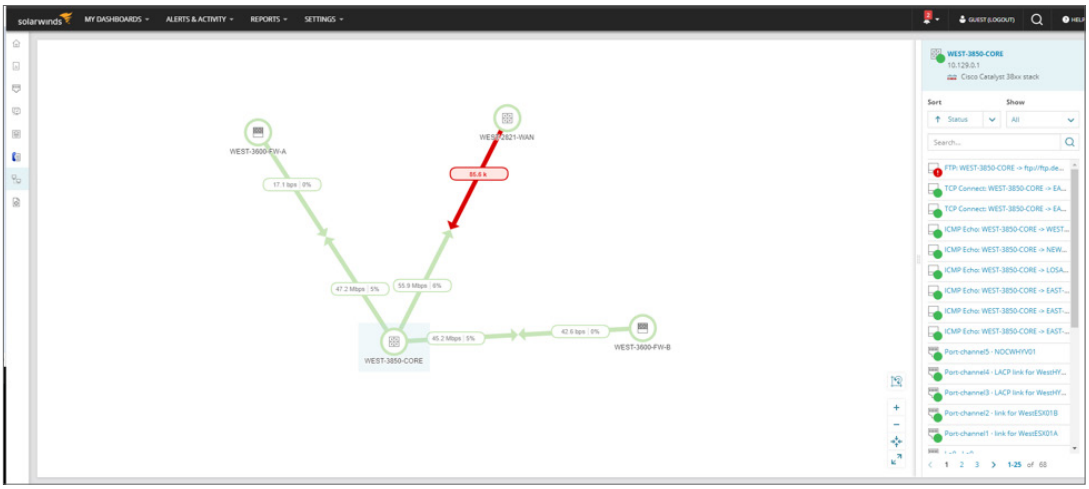
Going back to the mapping example provided earlier by Byron Anderson, a map like this shows all possible CURRENT routes from the origin to the destination.



And when that route changes, those are reflected immediately.



This capability isn't limited to internet paths. Mapping can also reflect both the connectivity between network devices and the performance of those connections.



What's more, associated elements and related devices can be displayed, allowing IT professionals to navigate through their environment and determine the functional as well as the logical flows.

Chapter 4: Standalone vs. Integrated Network Mapping

At this point, it should be clear that on the spectrum of manual-to-automated mapping solutions, each option has its specific benefits and use cases. It's not a question of either-or, but "when is this the right tool to use," in the same way that a chainsaw, circular saw, and coping saw all cut wood, but all are necessary in their own right.

What may not be clear is whether mapping functionality must be fully integrated into the monitoring solution to be viable.

The short answer is "it definitely doesn't hurt."

As networks scale ever larger, enterprises constantly face the challenge of keeping track of network devices. We find that across the industry, network administrators use both standalone mapping tools and tools that are integrated with their network monitoring solution. But the days when firing up a separate tool, generating or updating a map, and then importing it into monitoring are rapidly coming to an end—if the end hasn't already come and gone.

Nobody, not even in small networks, has that kind of time. Mapping tools that don't have at least a degree of both automation and integration represent a significant lost opportunity cost to the business: time the network engineer could have spent on higher value activities.

Mapping tools that integrate with network monitoring solutions provide data on both connectivity and performance of the network devices. Network maps integrated with an NMS reduce back and forth shifting between the maps and monitoring consoles by providing all the statistics in one place. Advanced network monitoring tools integrated with network mapping functionality allow you to drill down from the top-level network map to the device level.

Chapter 5: How Network Mapping Eases Network Troubleshooting

While it should be clear from our earlier descriptions, it's still worth spelling out: network maps—those which are automatically updated and fully integrated into the monitoring solution—are a force multiplier when it comes to improving the speed of resolution of network issues.

To be sure, "monitoring" in the modern sense is never about having a bunch of human eyeballs staring at computer screens waiting for something to turn red. Monitoring is nothing more (and nothing less) than the regular, ongoing, persistent collection and analysis of data coming from devices and their sub-elements around the network. Alerting is the automated notification when an event, condition, or threshold has been breached.

Mapping often comes into play after that. Mapping tells the human responder to the alert, "This is where all the objects are right now. This is where they were moments ago. This is where they could possibly move next."

Position and motion.

Without that map, the IT professional has both data and (sometimes) information. But not necessarily action.

Chapter 6: The Completely Un-Necessary Summary

Whether you manage a small network or a large one, it's best to create a network map to simplify the management of your network. Network mapping has simplified the way administrators manage their networks and helps reduce the time to troubleshoot network issues. Advanced network management systems with dynamic mapping features are capable of extracting, analyzing, and displaying real-time network data and are helpful in scaling, designing, planning, troubleshooting, and documenting your network.

SOLARWINDS SOLUTIONS

From 1,000 to tens of thousands of nodes. Deeper visibility and smarter scalability whether you are covering large environments, critical data centers, or multiple remote locations. Download a free 30-day trial of **Network Automation Manager** today.

TRY IT FREE

Get deeper visibility into your own network. SolarWinds is dedicated to continually bringing you better information about key network gear so you can manage your network, not your network monitoring. Download a free 30-day trial of **Network Performance Monitor** and **Network Configuration Manager** today.

TRY IT FREE

ADDITIONAL RESOURCES

NetPath™

Map key network paths hop by hop, even into the cloud.

PerfStack™

Drag and drop metrics from across your infrastructure onto a common timeline to correlate data and quickly identify the source of trouble on the network.

ABOUT THE AUTHORS

Leon Adato
SolarWinds Head Geek

In a career spanning three decades and four countries, Leon Adato has been an actor, electrician, carpenter, stage combat instructor, pest control technician, Sunday school teacher, and ASL interpreter. He also occasionally worked on computers.

Leon got his start teaching computer classes, worked his way up the IT food chain from desktop support to server support to desktop environment standardization engineer and onward, to systems monitoring, management, and automation. Along the way, he discovered a weird love for taking tests, and picked up an alphabet's worth of certifications, including WPCR, CNE, A+, MCP, MCSE, MCSE+I, CCNA, and SCP.

Leon spent almost 20 years honing his monitoring skills at companies that ranged from big (National City Bank) to bigger (Cardinal Health®) to ludicrous (Nestlé®), becoming proficient with a variety of tools and solutions along the way.

A SolarWinds® software user since 2003, Leon attracted the attention of SolarWinds staff via his impressive participation in THWACK® forums, including providing helpful posts, attending UX sessions, taking part in beta and RC testing, and whining.

It was around that time that Head Geek™ Patrick Hubbard noticed that Leon was long-winded to a fault, and that he lacked any semblance of self-restraint or basic common sense when it came to speaking in front of large audiences. That led to his being offered a position as Head Geek in 2014. Leon has not looked back since, mostly because he's incredibly uncoordinated and would surely run into something.

Follow Leon on Twitter® @LeonAdato, or on THWACK @adatole.

Destiny Bertucci
SolarWinds Head Geek

Destiny Bertucci is a Head Geek at SolarWinds and a Cisco® Certified Network Associate (CCNA®), Master CIW Designer, and INFOSEC, MCITP SQL, and SolarWinds Certified Professional®. In her 15 years as a network manager, she has worked in healthcare and application engineering, and was a SolarWinds Senior Application Engineer for over nine years.

She started her networking career in 2001 by earning CCNA/Security+ certification and launching a networking consultant business. After using SolarWinds tools for many years, she joined the company and continued earning certifications and degrees to expand her professional reach into database development and INFOSEC. Customizing SolarWinds products while working on setups and performance deepened her knowledge of the complete SolarWinds product line. She is now skilled and experienced in network, security, application, server, virtualization, and database management.

Follow Destiny on Twitter @Dez_Sayz, or on THWACK @Dez.

APPENDIX

Dedications

To Debbie

Sometimes you ask me if there's anything you can do to help me, and as a response I ask, "Do you love me?" You give me THAT look and say "Yes." And then I say, "You're doing it." I know it drives you nuts, but I really DO mean it. You loving me is the most awesome, incredible, unbelievable thing anyone has ever done for me. Your love keeps me going. Lifts me up. And on occasion brings me back to my senses. Your love for me bridges every long-distance phone call and every long-hours workweek. And, although you do, if you were to ask ME that question, I have my answer ready: "Forever, and ever, and always, best beloved."

To my husband, Tim

Anyone who knows me understands that I keep pretty crazy hours, have rapidly cascading thoughts, love new challenges, and push my own expectations of myself every day, all day. If not for my husband, who keeps me grounded (without clipping my wings), I would not have been able to attend trainings, earn certifications, or write an eBook in addition to everything else I do. So, I dedicate this to the man who appreciates my geeky self, day in and day out.

About SolarWinds

SolarWinds is a leading provider of powerful and affordable IT infrastructure management software. Our products give organizations worldwide, regardless of type, size or IT infrastructure complexity, the power to monitor and manage the performance of their IT environments, whether on-premise, in the cloud, or in hybrid models. We continuously engage with all types of technology professionals – IT operations professionals, DevOps professionals and managed service providers (MSPs) – to understand the challenges they face maintaining high-performing and highly available IT infrastructures. The insights we gain from engaging with them, in places like our THWACK online community, allow us to build products that solve well-understood IT management challenges in ways that technology professionals want them solved. This focus on the user and commitment to excellence in end-to-end hybrid IT performance management has established SolarWinds as a worldwide leader in network management software and MSP solutions. Learn more today at www.solarwinds.com.