Networks These Days: Boosting Network Visibility in Complex Environments

Whitepaper
# Table of Contents

Introduction ...................................................................................................................................... 3

What is network visibility and why does it matter? ........................................................................ 3

The problem with network blind spots .................................................................................... 3

Why it’s harder than ever .......................................................................................................... 4

Building network visibility ........................................................................................................ 5

Taking stock of networks ......................................................................................................... 5

Quick rules of thumb for ongoing maintenance ........................................................................ 13

N-able N-central ...................................................................................................................... 14
Introduction

Networking used to be simpler. Everyone sat in a single building and connected to the local area network (LAN). Over time, things became more complex but were still manageable.

Then came the explosion of mobile devices, from smartphones to tablets to IoT. Now, new devices are coming onto customer networks without proper management. Beyond that, businesses increasingly adopt software-as-a-service solutions and others are using cloud environments like Microsoft® Azure® for some of their IT infrastructure, adding further complexity to the mix.

Then there’s remote work, which further adds complexity. Each team member who works remotely has their own network with varying settings and devices on it—all of which have different levels of security and could easily have outdated software.

Gaining visibility over these wide-ranging networks is critical for keeping users productive and safe while also keeping customers happy and returning. First, we should start with a definition of network visibility and why it matters.

What is network visibility and why does it matter?

Network visibility refers to the ability to gain a clear understanding of the different components of a network—from devices to applications to traffic to users. This certainly isn’t an exhaustive list, but from a high-level perspective, network visibility involves the practices (and tools) that allow you to monitor and manage your customers’ networks to ultimately help you maintain performance and enhance their security.

Additionally, it’s important to understand that the concept of a corporate network has grown. Yes, you still have a network to design and protect. That’s still your top priority—the on-premises network customers use in the office. But even prior to the shift to more widespread remote work, you had to contend with devices outside the corporate network perimeter that could represent security threats.

Beyond that, your customers increasingly rely on cloud infrastructures and hybrid environments (not to mention SaaS applications). They don’t always draw distinctions about who’s responsible for what. If they can’t access their CRM solution, they’re calling you. You’ll want clear visibility into where that slowdown is, and many network management solutions simply weren’t built for those sorts of challenges. Some modern network visibility solutions were, however—and we’ll cover those.

The problem with network blind spots

Not having full visibility into a network leads to blind spots. These blind spots can come from any number of issues—unmonitored devices or unapproved applications being installed. These blind spots can even come from misconfigurations (especially if the network has grown organically without a plan.)
Network blind spots can bring multiple problems:

- **Performance bottlenecks**: Without clear visibility into traffic flows, you could easily miss areas of the network showing unacceptably slow performance. A good RMM platform that offers strong network visibility lets you set and receive alerts when network performance dips below certain thresholds so you can quickly troubleshoot issues and prevent them from affecting and frustrating customers.

- **Application bandwidth hogs**: Gaining visibility into applications lets you discover which ones wear down your bandwidth. These issues start small, but may add up quickly. This could require additional changes to network configurations and how you prioritize traffic flows to accommodate these changes.

- **Security concerns**: Without clear visibility, criminals can slip in undetected and do untold damage. Monitoring for unusual logins from unexpected countries, for example, can tip you off that someone’s attempting to hack your customer’s network.

**Why it’s harder than ever**

The rise of cloud computing, the increase in mobile devices on the network, and the spread of the network to remote offices have created more blind spots for businesses than ever before. Corporate networks today are a combination of internet-based VPNs, cloud services, MPLS, wired LAN workstations, and mobile workers on the WAN. Because of this, many traditional monitoring tools fall short.

Traditional network monitoring systems aggregate packet flow data from network and security systems like endpoint sensors and firewalls. The introduction of mobile devices and cloud technologies hinders network visibility for many of these network tools.

Why is this the case? For starters, endpoint sensors don’t work on mobile devices. Plus, gaining visibility of traffic passing between cloud datacenters can pose difficulties at the application level. Plus, many monitoring tools struggle to work in the cloud and can exacerbate the problem. Because these tools can obscure data, encryption and network address translation may impact sensors and stifle packet inspection attempts.

Another challenge is that traditional network monitoring tools are often tied to virtual or on-premises hardware. This means each WAN location needs its own individual set of applications that must be appropriately sourced and maintained. This can create serious inefficiencies that put a major anchor on performance (and really drag down your team’s efficiency).

These inefficiencies make it nigh impossible to scale efficiently as networks grow. Organizations juggling multiple applications with differing configurations will become challenging to wrangle. As businesses grow and scale, the complexity will only continue. And frankly, as technology grows, this will still add further complexity. And for MSPs managing a lot of clients, maintaining network visibility without the right tools becomes a recipe for disaster, leading to bad performance or security vulnerabilities.
Building network visibility

So, what do you do to actually gain this network visibility? It comes down to merging the old and the new. You’ll need a mixture of tried-and-true practices and technologies with newer technologies developed for these newer use cases. In this next section, we’ll discuss how to approach thinking about network visibility both when taking on a new client and on an ongoing basis.

Taking stock of networks

For starters, you need to understand the nature of a customer’s network. What technologies do they use? How is the network set up? Who’s connecting to what? What does a typical day look like?

In other words, you need to take a baseline of the network itself when you first take on a new client (and may need to review this on a recurring basis as you continue working them). This is a critical element of network visibility—it allows you to assess the health of a network at the start, make changes to improve network performance and security, and boost customer satisfaction. This helps early on when setting goals to improve their network. But let’s say you’re a few months down the line and there seems to be a major slowdown in the network and it doesn’t correspond with anything on your original baseline—odds are good you’ve found a blind spot and can then act accordingly. The diagnostic value of these baseline assessments cannot be overstated.

When you first take this assessment, you’ll want to focus on the following areas:

- Control implementation
- Availability
- Security
- Issues that could affect regulatory compliance
- Management
- Performance

To perform this initial baseline, you’ll need to do a number of things.
INVENTORY

Take an inventory of their hardware, software, and devices as best you can. You’ll have to do some of this manually, while you can use tools for other portions of it. Some of the important elements here include:

- Servers
- Laptops
- Desktops
- Company-issued mobile devices (including smartphones and tablets)
- IoT devices
- Network devices like routers and switches
- Printers
- Virtual machines and servers

These are just some of the more obvious elements you need to inventory. However, you should also look at the software used by customers. Customers can easily download software to their laptops or devices you may be unaware of, so this can quickly grow out of control. If possible, consider using an application block/allow list solution to control the access people will have on their computers so they don’t introduce potential security concerns to the network.

Additionally, you’ll want a good list of the external software-as-a-service (SaaS) applications your customers rely on. Even if you’re not responsible for these on paper, in practice your customers will get frustrated when any business system faces a slowdown. Don’t let it fall on you. Be aware of what they use—it’s part of the extended network.

Finally, look at any bring-your-own-device (BYOD) policies. If they have one in place, review it carefully and document it. But also, be advised that these can be tricky policies to deal with—using personal devices for work purposes blur the lines between public and private data. If you adopt one, work closely with legal counsel. But if you do have BYOD in place, make sure to document these devices and try to get a handle of the types of devices used, the amount of management required, the bandwidth required, and any potential security issues. The moment you put them under a mobile device management (MDM) tool, you’re accepting potential risk, so don’t do so without legal counsel on board.

However, it is still worth noting that people will bring personal devices to work no matter what. You may want to watch network traffic to get a sense of the unmanaged devices connecting to the network on a given day both to prepare for network bandwidth requirements and for potential security concerns. Also, consider creating a separate “guest” network for employees to use for their personal devices so they don’t slow down the corporate network or introduce security concerns.

There’s a tool we recommend that can make a lot of this network discovery easier.
GET A SENSE OF THE NETWORK TOPOLOGY (AND REWORK AS NEEDED)

Part of gaining visibility into a network means understanding the macrolevel design of the network, and that means understanding its high-level topology. Networks can quickly get complex. And while you can certainly map out a topology by hand, we all know that a real-world, real-time map works better. To make it simpler, we’ve created a feature available within the N-able™ N-central® solution called network topology mapping.

In a very brief overview, network topology mapping scans a network, discovers the devices on it and their relationships and connections, then gives you an up-to-date visual map of the network. Plus, it can automatically detect new devices that connect to a network when it runs a scan (which can be scheduled ahead of time).

You can immediately use this to see how elements of the network are connected and figure out how best to make changes. Typically within seconds, you can see if elements of the network are connected in a suboptimal manner, allowing you to reroute traffic if needed. Plus, as new technicians join your MSP team, having up-to-date diagrams of customer networks can help them hit the ground running fast.

If you’re just taking on a new client, it’s the perfect time to review weak areas and suggest new design changes. Analyze the pros and cons of the current setup, and suggest how you might improve them. Their previous MSP may have set things up in an ad hoc way. Doing everything more deliberately will give them quite a bit more in terms of performance enhancements. You would be surprised how many consultants can skip the network design step. Even just jumping in and being deliberate about this can really set you apart from your competition and improve your time-to-value.
Make sure to focus on developing a clear map of the network, including the structure and layout of the cabling and the physical network (in addition to the logical network provided via network topology mapping). You’ll also want to map out the devices on the network, your IP addressing structure, and any details on network security. We’ll cover some security elements in a later section.

While you’re at this phase, here are a few simple best practices to follow:

- **Be deliberate about the design**: If you’re taking on a small customer, it’s tempting to either run with what you have or simply hook devices up. Optimize now to avoid technical debt later.

- **Plan for the future**: You won’t have a crystal ball, of course, but you should assume the company will grow and things will grow more complex. Work with your customers to figure out where they plan to take the company and consider this in your calculations on what would be the best way to design the networks. For example, if they’re considering opening new locations, you’ll want to factor this into your ideas.

- **Consider security**: Security should be part of your design from day one. We’ll have a brief overview of security later in the piece, but right now, just remember to keep it in mind as part of the design phase. For network design, a good tip here would be to place anything that’s high risk on its own separate network to help prevent it from compromise.

- **Update your design**: You’re never done. Once you’ve finished designing, make sure to regularly update your plans. Set aside time for each client to reconsider network configurations for better performance and security.

**CHECK AND MONITOR PERFORMANCE**

At the outset of your customer relationship, you’ll want to get a baseline on network performance. And of course, you’ll want to continue monitoring this as time progresses to note improvements or deviations from this baseline.

There a few ways to deal with performance monitoring. Please note that these are nonexhaustive.

**SNMP monitoring on the network**

First, SNMP, or simple network management protocol, allows you to gain information on and manage devices on a network. It will give you in-depth metrics, particularly on bandwidth. When taken in aggregate across devices, it can give you a pretty good snapshot of the health of a network at a given time.

SNMP requires you to push an agent to a specific device, which then submits information back to a central station that monitors the devices on the network with an agent. Often, you can use an SNMP scanner to locate SNMP-enabled devices on a network before pushing an agent. Most tools can handle SNMPv1 and SNMPv2, with more comprehensive tools also supporting SNMPv3. Once you’ve pushed agents to devices, you can monitor passively by receiving data on scheduled intervals or monitor actively by polling devices via test packets and using the responses to gather information and troubleshoot.
Let’s be clear about something—SNMP monitoring should absolutely be part of your arsenal for both network monitoring and network visibility. First of all, it’s simple and easy to roll out. With a good RMM tool, it’s likely part of the agent you roll out anyway. Second, it’s efficient. Again, with a good RMM, you can aggregate SNMP-monitored devices into a single report. Third, it’s informative. You can view traffic patterns as they arise via passive monitoring to see if something goes awry. This can be particularly helpful in the event of potential cyberthreats, as noticing bottlenecks could indicate an attack. Finally, SNMP monitoring is just plain effective—you can quickly analyze issues, view them over time, and review to keep them from recurring.

Whatever solution you choose, double check how it allows you to deal with SNMP alerts. Again, remember how complex networks can get—and multiply that over the number of customers you hope to take on for your business—and you’ll see why it’s important to get this part right early. You’ll want something that’s easy to use and offers the ability to create and customize alerts according to your needs. For example, you’ll want something that will let you set alerts based on simple or complex nested trigger conditions, define parent/child dependencies, and map out network topologies to keep you informed of critical network performance.

Unmanaged devices and the extended network

While SNMP must be part of your toolset, there’s a critical missing element that makes it incomplete on its own because it was developed for an older networking and business model. It only offers information on devices with agents on them. Any unmanaged device connected to the main network will remain unseen—and forget about cloud services.

When it comes to the unmanaged device aspect, you can potentially discover issues with tools like ping and find where those issues are with traceroute. Let’s talk a bit about traceroute. It’s a command used in operating systems to trace data packets from their source to their destination. The data typically passes between multiple destinations like routers and switches—each destination known as a “hop.” Traceroute then measures the number of hops the data takes and the amount of time it takes to return. This can give you a sense of whether there are slowdowns in the network or if there’s a ton of additional unnecessary trips. Plus, you can often tell if there’s a hop to an unmanaged device if you refer to your previous inventory (although, this may be impractical unless you’re really trying to look at a particularly thorny issue).

However, traceroute has limitations. For starters, it can’t reach outside your own network. You won’t likely get a response from a slowdown on a critical SaaS application. Also, it’s notorious for only handling a small number of hops. If networks get complex, you’ll quickly run into issues. They don’t even have to get that complex—traceroute is really meant to track hops from point a to point b. Traffic often takes multiple paths in modern networks, so this certainly limits the method. Plus, traceroute tools really aren’t built for visibility into issues—there’s no historical data you’ll get from it. It’s more of a “shoot a signal and see what comes back” diagnostic tool than anything else.

One option we recommend would be to use a tool like NetPath™, available in N-central, which uses advanced network probing to detect a network path from a source server to a destination service, even when traceroute can’t. This works whether you’re working on-premises, in the cloud, or in a hybrid environment. Plus it can track multipath hops, so it overcomes the limitation inherent in traceroute tools—giving you a better, quicker sense of what’s going on in the network at a given time. Beyond that, it offers an easy-to-see visual representation of the network so
you can view slowdowns and bottlenecks. This will save you time compared to running individual traceroute commands on the command line (and will probably save you some eye strain as well).

The NetPath tool can give you insight into off-site services, including SaaS applications like Salesforce® or Microsoft 365™. This way, if a customer wonders why a specific service is running slowly you can confidently let them know whether the issue is with the third-party vendor or due to a slowdown in their own network that you’re currently tackling.

Plus, you can set NetPath up to scan in 10-minute intervals, giving you greater visibility into network performance and offering you historical data you simply can’t get with basic tools like traceroute. With this historical data, you can troubleshoot issues much faster by diagnosing when issues began and having better intel when you start tackling the problem. Also, you can notice issues arising before your customers do, hopefully allowing you to provide a better quality of service.

And let’s be honest for a moment—your customers expect a certain level of service. If a critical application goes down, they’ll be upset. NetPath offers greater visibility so you can see if the issue is something you can handle, if it’s a problem with a cloud vendor, or if it’s an issue with their internet service provider. You shouldn’t have to take the fall for a problem on their ISP’s end—NetPath gives you the visibility to point out where the problem truly lies so you can start helping your customers find a real solution.
REVIEW SECURITY

With the proliferation of cyberattacks across the world, you must consider security while both assessing a network and while running your day-to-day operations.

When you're first taking on a client, you'll want to review the security controls they have in place. It's a good idea to:

- Figure out their firewall situation. Are they using next-generation firewalls or endpoint firewalls? Try to push for more modern next-gen versions if you can, as they can scan encrypted traffic to look for potential threats. This offers increased visibility into the traffic coming into your network so you can help prevent threats. Next-generation firewalls typically have antivirus scanners on them as well, offering an additional checkpoint for incoming network traffic.

- Identify user access and privilege for networks. At the network level, identity and access management plays a crucial role for policing access. Excessive user privileges can grow organically as a company grows—it's not uncommon for early employees to have superuser privileges when their jobs don't require this. Not only does this open you up to malicious insider attacks, but if those accounts get compromised they give cybercriminals carte blanche to the network.

- Make sure there are onboarding and offboarding policies in place for both equipment and accounts. When employees leave, you'll need to shut accounts down quickly so they won't have access to sensitive data (even if they leave on good terms). And to stick to the theme of visibility, make sure you have a system worked out where the company includes you when someone leaves so you can shut down the account as soon as possible. It's an unacceptable risk to leave this undone for too long.

- Use a password manager and turn on multifactor authentication (MFA) for important accounts. This is important for applications and users across the board, but it's especially important for high-risk users with access to sensitive data and high-risk systems that contain sensitive data (or can access sensitive data).

- Consider segmenting the network for extremely sensitive data and requiring a higher level of security to access it. This does two things. First, it helps prevent criminals from getting to the "vault" containing your highest value data. Second, it gives you time to detect an intrusion in the rest of the network before they can reach this vault. In fact, if the organization is large enough, you could even consider breaking the networks into multiple segments to frustrate criminals using lateral movement to attempt recon on the network. Of course, even segmenting the network this way once will add some complexity, and we do mostly want to keep things simple. However, you or your client may decide the risk is worth the benefit of increased security.

- Run a vulnerability scan. This tip really includes several tips, so please don’t skip it. You can run a professional vulnerability scanner or find a free one, but when you first take on a client make sure to at least run an automated vulnerability scan (and preferably run one again while working with the customer). These scans typically find common issues like unpatched software, default passwords, default configurations or misconfigurations, open ports, and other issues that often can be easily exploited (and easily fixed). Vulnerability
scans certainly aren’t as intensive as penetration tests and will never fully replace them, but this is low-hanging fruit to help find things to fix immediately and show value to your customers.

Beyond these tips, make sure not to forget other security layers for managed devices that will connect to the network. You’ll want to make sure they have good antivirus, or preferably an endpoint detection and response tool, DNS filtering, disk encryption, email security and spam filtering, and solid, regular patch management at a minimum. Any endpoint can become an entry point for a cyberthreat to the full network.

REPORTING AND DOCUMENTING AREAS FOR IMPROVEMENT

Finally, it’s extremely important to find a solution that gives you clear visibility into what’s going on in the network at any given time via strong reporting. Getting a good RMM solution that offers a central dashboard to view your entire network helps improve visibility and lets you easily manage elements of the entire system. You’ll be able to receive alerts fast, troubleshoot, and truly deliver on your promises.

But we’re getting ahead of ourselves. If you’re just taking on a new customer, then you should be documenting everything you found while taking an inventory of systems and software, network performance and layout, and security. If you’ve followed that up to now, then you’ll want to put together a list of changes you plan to make to improve your customers’ performance and security. Look for out-of-date operating systems, EOL software to deprecate, security vulnerabilities or misconfigurations, or any network design updates you can make to smooth out workflows.

If you need the customer to make any changes that may be a tad uncomfortable, the start of the relationship is the best time. You have political capital and they believe in your ability to make things better, so asking them to upgrade hardware or to limit some software applications for security or performance purposes should come as part of your initial suggestions.

Once you’ve kicked off the relationship, you’ll want to continue with regular reports on network performance and document any improvements you make. This requires both strong network visibility and an RMM solution with solid reporting. Make sure you’ve chosen an RMM tool with the ability to present historical reports on network performance and security over time.
Quick rules of thumb for ongoing maintenance

When running the day-to-day, you will need to focus heavily on providing sound quality of service (QoS) to customers. This could be a subject of its own white paper, but we’d like to condense some suggestions on what to focus on.

First, let’s define what we mean here. QoS refers to maximizing a network’s bandwidth and performance. This often means prioritizing certain traffic over others to avoid latency and bandwidth issues.

Common QoS technologies or features include:

- Queuing, which allows for traffic prioritization by creating buffers in devices to hold onto the data to be processed
- Classification, which marks traffic so networks know how to prioritize it across the network
- Shaping, which determines a software-determined limit on the rate of bandwidth transmission for a certain class of data
- Policing, which enforces a specific limit on bandwidth that applications can use
- Weighted random early detection (WRED) technology, a queuing discipline that helps prevent congestion by dropping TCP data of a lower priority level
- Link-specific fragmentation and compression techniques, often used on low bandwidth WANs to help prevent high jitter and delays

When trying to maintain and improve QoS, there are a number of things to consider. Here are some best practices:

1. Do a network assessment. If you’ve followed the guide already, you should have completed this step.

2. Identify high-priority network traffic. These will likely be specific to the customer, their business, and the applications they run, so always keep business requirements in mind.

3. Categorize latency-sensitive data flows. This includes voice and video conferencing and many applications essential for running the business, but you’ll also eventually reach some traffic you can classify as nonessential, like general web surfing.

4. Consider eliminating the nonessential flows. This means when congestion occurs, it can drop these flows immediately.

5. Involve business leaders. It’s often overlooked, but run ideas by your customers before you make decisions. It’s not just about getting their clearance—they’ll often have perspectives you won’t think of that will make for a far better experience overall.

6. Apply QoS classes. In other words, start applying classes to traffic to tier and prioritize traffic flows. Also, please remember that less is more here. Keep things simple—networks get complex, but management shouldn’t.
Network visibility and your MSP business

All of this needs to play into your overall strategy for your MSP business. Your customers pay you to make sure their networks perform well and remain secure. So it behooves you to consistently increase the value you provide to them, and look for areas where you can increase your services offerings.

As we mentioned earlier, you should use the early stages of your relationship with them to discuss the changes you plan on making to network configurations and suggest what hardware or software upgrades they may need to make.

Additionally, as you continue working with the customer, make sure to hold quarterly business reviews where you review network performance and suggest additional changes. The visibility you gain into the network will give you strong suggestions on how you can enhance their quality of service for the following quarter. Plus, you can often find new services to expand the account.

N-able N-central

One option to gain a better handle on modern, complex networks is to use N-able N-central. The N-central solution was built to make handling complex networks easier and includes several of the features mentioned in this white paper. Network topology mapping makes it easy to map out networks and view relationships in an easy-to-navigate map. The NetPath tool uses advanced mapping technology to let you upgrade your capabilities from traceroute and other similar tools. It gives you deep visibility into the primary network and helps you troubleshoot issues in the extended network—whether you’re working on-premises, in the cloud, or in a hybrid environment.

Perhaps most importantly, the N-central solution allows you to expand your monitoring capabilities to cover workstations, servers, and devices across multiple operating systems. Whether you want to manage Windows®, Linux®, or Mac®, you can do so confidently from one management console. Also, you can now monitor and remotely manage Microsoft Intune devices using the multitenant capabilities of N-central, extending your capabilities even further.

Learn more by visiting n-able.com/products/n-central.
About N-able

N-able empowers managed services providers (MSPs) to help small and medium enterprises navigate the digital evolution. With a flexible technology platform and powerful integrations, we make it easy for MSPs to monitor, manage, and protect their end customer systems, data, and networks. Our growing portfolio of security, automation, and backup and recovery solutions is built for IT services management professionals. N-able simplifies complex ecosystems and enables customers to solve their most pressing challenges. We provide extensive, proactive support—through enriching partner programs, hands-on training, and growth resources—to help MSPs deliver exceptional value and achieve success at scale. n-able.com