NetBrain®

# State of the Network Engineer: Toward an Automated Future

netbraintech.com

# Executive Summary

Today's enterprises have reached a tipping point when it comes to network management. Networks are growing rapidly and becoming more complex, yet most engineers still use manual processes for managing key IT workflows—network documentation, troubleshooting, change management, and cybersecurity. Collaboration and information sharing are often the difference between quickly diagnosing a problem and hours of frustration and downtime. However, today's processes depend largely on institutional or "tribal" knowledge to diagnose network issues, which can be inefficient and hamper IT's speed to resolution. These issues are only expected to intensify as enterprises increase investments in areas like network security, virtualization, and software-defined networking.

A new survey* from NetBrain Technologies uncovers several areas where network engineers will continue to face challenges in the coming years due to a lack of automated processes. Core requirements such as cross-IT collaboration, network visibility, and the need to streamline tasks are among many areas network engineers acknowledge they are falling short with current methodologies.

NetBrain's survey of more than 200 network engineers, architects, and IT managers from across industries point to automation as the future. Survey results reveal key insights driving toward this outcome:

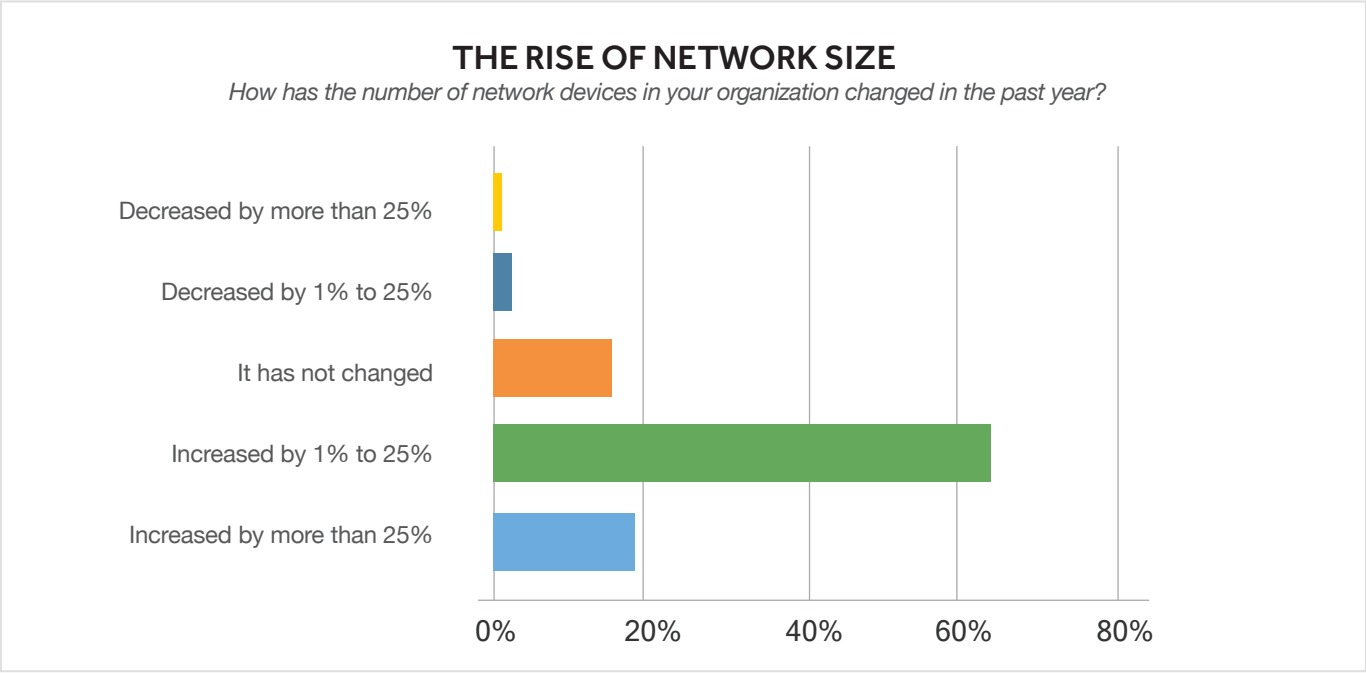
1. **Increasing size and complexity of networks is demanding new skillsets and technologies**
2. **Maintaining accurate network documentation remains elusive**
3. **Current troubleshooting techniques are contributing to longer network downtimes**
4. **"Tribal" knowledge and collaboration gaps are barriers in most enterprises**
5. **Network security is a top priority, but continuously securing the network is difficult**

The research was conducted in April 2017 via an online survey of more than 200 IT professionals with day-to-day oversight and management of enterprise networks within organizations of more than 1,000 employees. Typical respondents had titles such as Network Engineer, Network Security Engineer, Network Architect, Director/Manager of Network Operations, and Director/Manager of IT.

# 1. Increasing Size and Complexity of Networks is Demanding New Skillsets and Technologies

Network management solutions are an enterprise IT priority as networks continue to grow at a rapid rate. In the survey, 49 percent of enterprises with 1,000+ employees have more than 1,000 network devices (e.g., routers, switches, firewalls, etc.), while 21 percent have more than 10,000 network devices. Growth was nearly universal across enterprises, with 83 percent indicating that the size of their networks has increased within the past year.

Combined with this growth are key networking projects that enterprises are investing over the next 12 to 24 months. The top five areas cited by respondents are: network security (64 percent), network hardware refresh/upgrade (40 percent), private/public cloud computing (38 percent), network capacity planning (36 percent), and software-defined networking (20 percent).




These trends are demanding change as traditional network management methods are no longer suited for today's growing networks and complex IT initiatives. Specifically, network engineers cite key technology and skillset investments for the near-term:

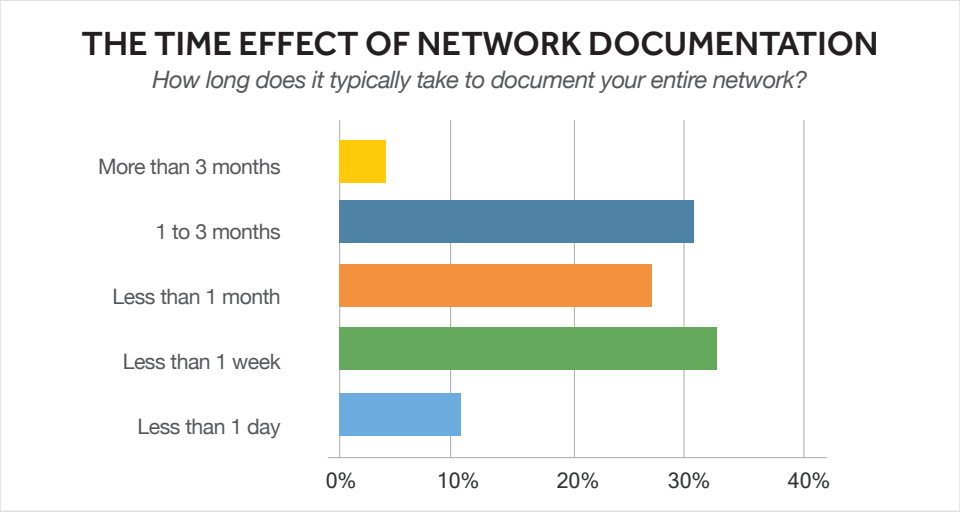
- Nearly 30 percent of respondents cited investing in network automation capabilities
- 53 percent of network engineers said they are required to know programming (beyond just scripting) for their jobs
- Having a single solution for network visualization, management, and analysis is invaluable, cited by 99 percent of respondents

Today's networks are constantly evolving, forcing engineers to consistently adapt and bring new skills to the table. The need for new automated tools to shorten cycles and eliminate time-consuming and tedious tasks has never been higher.

# 2. Maintaining Accurate Network Documentation Remains Elusive

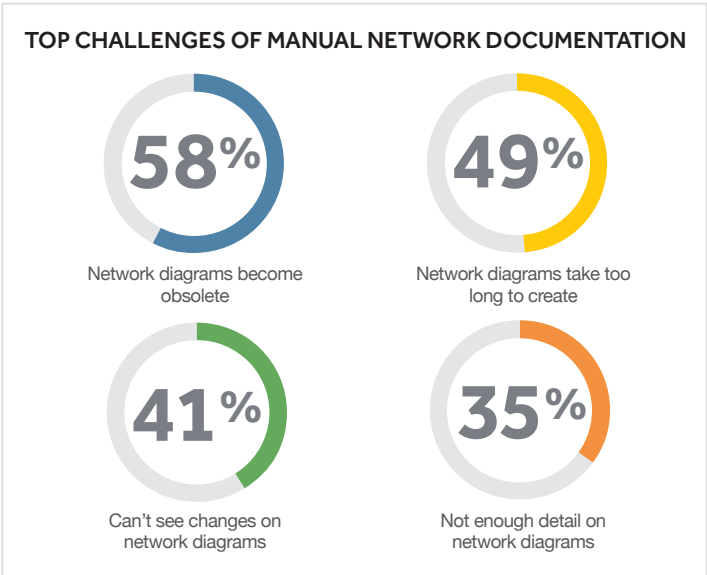
As networks become increasingly complex, gaining clear visibility into these hybrid environments—physical, virtual, and software-defined networks—has become even more difficult. Documentation is one of the network engineer's most important workflows, yet nearly every organization still struggles with this critical task. Today, 87 percent of respondents primarily rely on manual techniques to create and update their network diagrams, whether it's through programs like Microsoft Visio or simply relying on the knowledge of the organization's IT expert.

The time it takes to generate these diagrams and view real-time network details and flows can lead to downstream problems—slower troubleshooting, prolonged security impacts, or lack of compliance. For instance, 49 percent of respondents cited that it takes too long to create network diagrams as a primary challenge, while 33 percent said it would take more than one month to document their entire network given manual methods.




**49%**

**of respondents cited that it takes too long to create network diagrams as a key challenge, while 33% said it would take more than one month to document their entire network given manual methods.**




In addition to the length of time it takes to create a network diagram, obsolescence was cited as another obstacle.

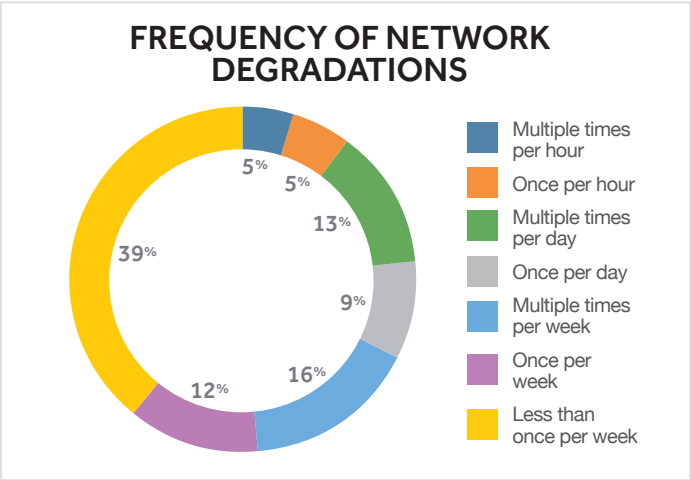
## Fifty-eight percent of network engineers said that network diagrams become obsolete as soon as the network changes, which was the number one documentation challenge cited by respondents.

With diagramming as one of the network team's most time-consuming yet important tasks, having a solution to this ongoing challenge is vital.

**44%** **of respondents respondents indicated that it's been more than one month since they last updated their network diagrams.**

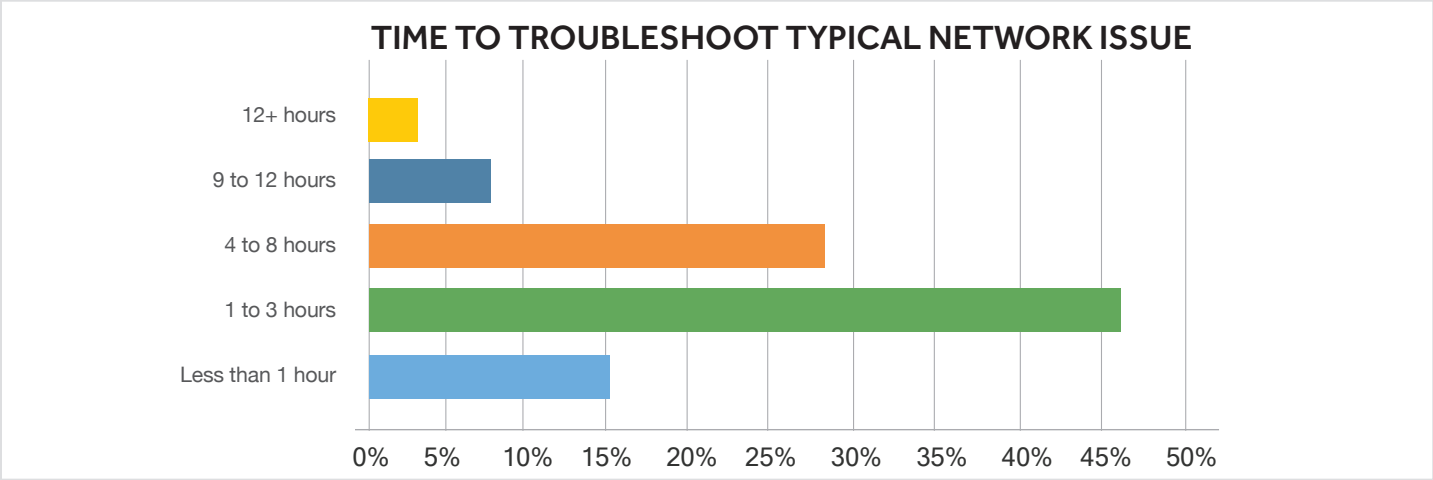
In short, the confluence of challenges brought on by manual techniques continues to keep accurate, up-to-date network documentation in a state of flux. Case in point: 61 percent of engineers say that up to half of their network documentation is out of date, with 44 percent of respondents indicating that it's been more than one month since they last updated their network diagrams.

# 3. Current Troubleshooting Techniques are Contributing to Longer Network Downtimes




Network troubleshooting, another key workflow, primarily relies on engineers conducting multiple manual diagnoses. This leads to longer mean time to repair (MTTR) as they may lack the necessary visibility to quickly identify and mitigate the different network problems. Whether it's a slow application or jittery VoIP connection, the longer they search for the problem, the costlier the impact of a network degradation to the enterprise.

When network issues arise today, 71 percent of engineers said they turn to command-line interface (CLI) as the primary way to troubleshoot problems. During a typical network issue, roughly 40 percent of respondents indicated that it would take more than four hours of troubleshooting time.




**43%**

**said that troubleshooting takes too much time using CLI, while 43% also said that network diagrams are not updated or customized for the specific problem at hand.**

When asked to identify key challenges in troubleshooting workflows today, network engineers responded with significant pain. For instance, 43 percent said that troubleshooting takes too much time using CLI, while 43 percent also said that network diagrams are not updated or customized for the specific problem at hand. This data highlights the belief and frustration among network engineers that relying on manual troubleshooting through CLI is simply not efficient, especially given the growing complexity of physical and virtual network environments.

The bottom line is that increasing network complexity has naturally made troubleshooting more complex. This challenge relies on new approaches where automation can serve as the linchpin technology. Survey results indicated that less than four percent of networking teams are currently applying automation to the network diagnosis and troubleshooting process. For enterprises, automated solutions are imperative to provide improved visibility while streamlining network tasks, helping to drastically reduce, or even eliminate extended and costly diagnostic and repair periods.

# 4. "Tribal" Knowledge and Collaboration Gaps are Barriers in Most Enterprises

**57%**

**of respondents cited that the inability to codify and share best practices was hampering more effective troubleshooting.**

**45%**

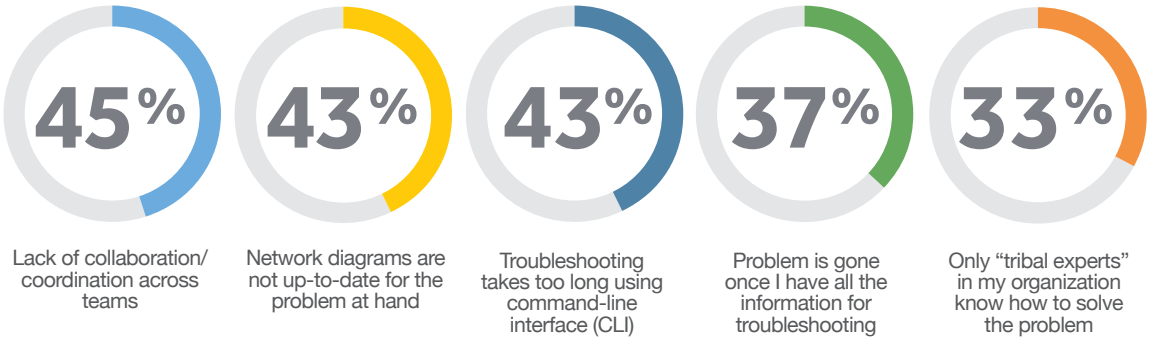
**of network engineers surveyed cited a lack of collaboration as the number one challenge for more effective troubleshooting.**

Survey results also showed that many enterprises continue to rely only on "tribal" knowledge as a key way of managing network problems. Whether it's relying on a network engineer's mental picture to create a network diagram or going to the IT expert to troubleshoot advanced configurations, compartmentalized knowledge is pervasive. The result? Lower efficiency and speed to resolution as technical know how and subsequent learnings are limited to a few individuals. In fact, 33 percent of respondents stated this over-reliance was a key obstacle.

Given this reliance on "tribal" knowledge, 57 percent of respondents also cited that the inability to codify and share best practices was hampering more effective troubleshooting, especially for network security. This is an area of concern as the rate of speed in which cyberattacks can move demands a quick response. Whether it's a denial-of-service attack or the need to harden firewalls to mitigate ransomware threats, the ability to digitize and rapidly disseminate best practices across network and security teams is vital in defending against future attacks. Unfortunately, the time spent searching for the correct persons or procedures can be inefficient and potentially hazardous to network security.

Finally, network engineers cited gaps in cross-IT collaboration as another major pain. This is particularly evident when workflows involve more individuals within the same group (e.g., multiple engineers in the network operations center) or traverse different IT groups (e.g., into the security team and/or application teams). For instance, 45 percent of network engineers surveyed cited a lack of collaboration as the number one challenge for more effective troubleshooting. Change management was another workflow that network engineers cited as needing more collaboration. Specifically, 36 percent of respondents felt that the lack of coordination was creating systematic issues for them when attempting to design and execute network changes.

## TOP CHALLENGES OF NETWORK TROUBLESHOOTING



# 5. Network Security is a Top Priority, But Continuously Securing the Network is Difficult

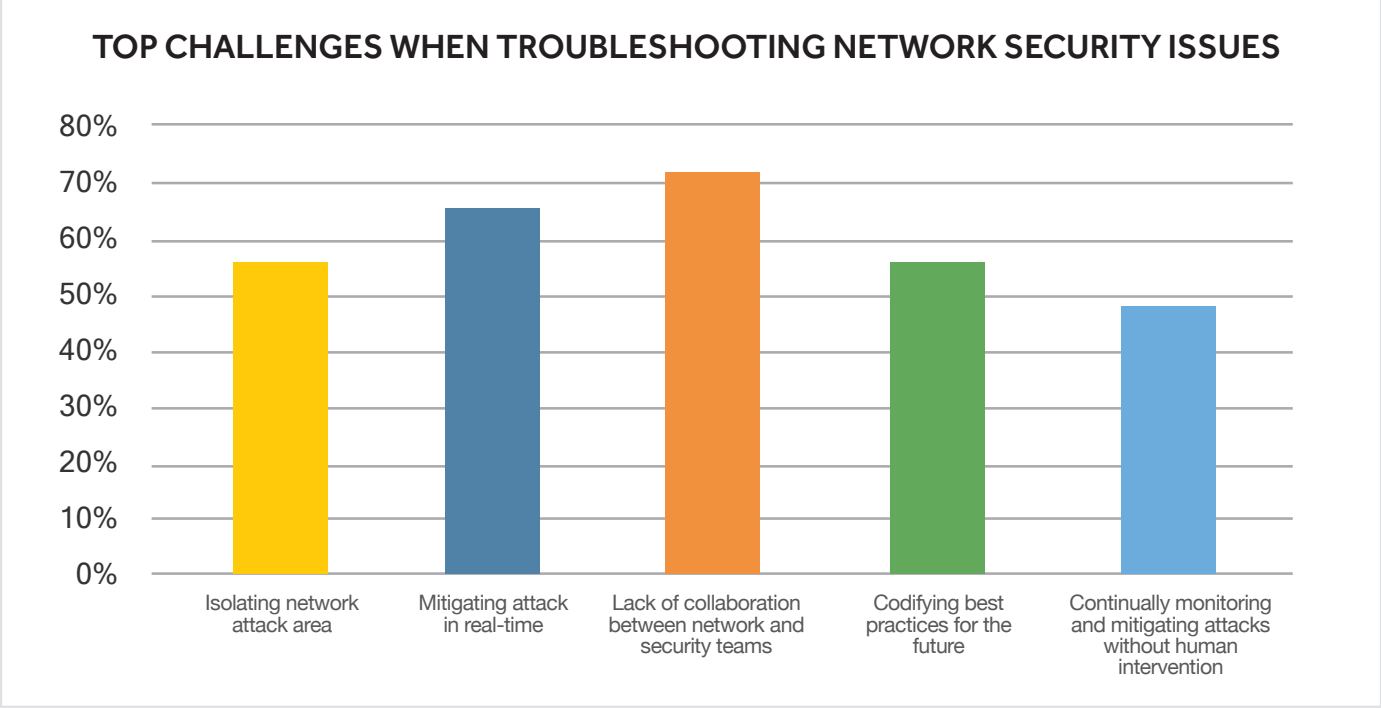
The growth of networks creates additional points of vulnerability that can be exploited for cyberattacks. Today's network security tasks often continue to rely on static playbooks and inaccurate network maps, resulting in sub-optimal knowledge-sharing and collaboration.

In our survey, 64 percent of organizations say they plan to invest in network security within the next 12 to 24 months, making it the number one networking project cited by respondents. While organizations understand the importance of this issue, that doesn't mean network teams necessarily have security under control. For instance, 52 percent of respondents said their response to a security issue is "one part professional, one part hysteria," and seven percent of respondents said it's like "fire in a crowded theater."

In addition, the sheer number of alerts often compounds this situation with false positives generated daily. Today, it has become a physical impossibility for engineers to verify each alert manually given the 24/7 nature of threats. What organizations require is a more proactive approach to mitigating risk to valuable information or long periods of downtime. Unfortunately, current methods of doing so are challenging. For instance, nearly 50 percent of respondents cited the inability to continuously monitor and mitigate attacks without human intervention as a significant issue, while 57 percent of respondents cited an inability to isolate the area of the network where an attack is happening.

Finally, a key problem with troubleshooting network security problems goes back to collaboration.

The number one challenge cited when troubleshooting network security issues was the lack of collaboration between network and security teams in mitigating an attack, selected by 72 percent of respondents.



# Conclusion

NetBrain's survey convincingly highlights that a lack of network visibility, automation, and cross-IT collaboration can inhibit network engineering teams when it comes to day-to-day operations. These issues are exacerbated by networks which are experiencing rapid growth and becoming more hybridized, as enterprises invest in increasingly complex IT projects over the next 12 to 24 months.

At the root cause of the visibility issue remains the reliance on manual processes and tribal knowledge for managing key workflows including network documentation, troubleshooting and change management. Static network diagrams and playbooks (e.g., guides, checklists, etc.) can be time-consuming and challenging to use, requiring network engineers to think beyond the world of CLI to ensure faster MTTR. Moreover, ensuring that network teams are on the same page as their peers in different IT groups– either through joint data capture and subsequent knowledge sharing – is vital for greater efficiency and cross-learning.

The lack of visibility and collaboration goes beyond a matter of efficiency or simple convenience; they can also put the stability of the network at risk. Disruptions to critical network areas prohibit effective IT security and can create vulnerabilities with potentially damaging results. Continuous network security is a must in today's ultra-risky environment, where the need to harden the network and quickly isolate and diagnose the root cause of attacks—before they disappear—is important.

As network engineers turn more toward automation for their daily workflows, they are more able to quickly identify, diagnose, and mitigate problems and threats. Network automation in the linchpin that eliminates the dependence on manual processes, while democratizing the knowledge of the few and providing a level of expertise to the entire team. This ensures that network issues are addressed more quickly, changes can be implemented with confidence, and security is never sacrificed.