BROADCOM

WHITE PAPER

Network Observability Maturity Model

A Roadmap to Achieve Monitoring Excellence and Maximize the Return on Modern Networking and Cloud Investments

TABLE OF CONTENTS

EXECUTIVE SUMMARY

For decades, organizations have continued to expand their usage of diverse networks and networking technologies. In spite of all this dramatic change, many network operations teams are still employing legacy tools and approaches to try and manage the increasingly complex, dynamic networks that critical business services rely upon. This paper offers a detailed look at the nature of the challenges confronting teams today, presenting key findings from a recent industry survey. In addition, this document describes a maturity model that gives teams an effective blueprint for advancing their approaches and capabilities.

KEY CHANGES AND CHALLENGES IN NETWORK OPERATIONS

Today, many business services rely heavily on external networks of internet service providers (ISPs) and cloud providers. In fact, in many organizations, users are now more reliant on external networks than they are on networks running in their company's internal data centers. These new realities, among a wide range of other substantial changes, have all served to fundamentally alter the nature of network operations—and introduce significant challenges as well.

Adoption of cloud technologies, the rise of hybrid work environments, and increased bandwidth demands contribute to a more complex and difficult-to-manage network landscape. In the following sections, we examine how the nature of network operations has undergone fundamental change, and, in the process, introduced a wide range of challenges. These sections feature findings from a recent study performed by Dimensional Data and sponsored by Broadcom.[1]

Modern Networks Introduce Spiraling Complexity

It is now more complex than ever to manage networks and the network delivery experience. Enterprise networks are high scale, virtualized, and made up of multiple vendors' technologies. One user's network path could consist of hundreds or thousands of network elements, with each reliant upon resilient connections. Not surprisingly, 78% of respondents indicated network complexity has grown significantly over the last few years. Several factors contribute to this growing complexity.

Reliance on Distributed, Third-Party Environments

The shift away from centralized data centers to distributed cloud and hybrid work environments creates a much more complex network topology that's harder to monitor and manage. Traditional tools struggle to provide adequate visibility across these diverse environments.

Hybrid Work

The survey found that 95% of respondents support hybrid work environments. Hybrid work has a significant impact on the demands that are placed on modern network operations. As organizations embrace any amount of hybrid work, the network perimeter effectively dissolves, expanding to encompass a vast array of employee devices and home networks. This distributed network environment introduces many new complexities and challenges for network operations teams.

The reliance on internet connectivity for remote workers increases the importance of external network visibility. Unlike a traditional office environment where the network is largely under the organization's control, hybrid work introduces numerous external dependencies, such as home Wi-Fi networks and ISP networks. These dependencies create blind spots for network teams, making it difficult to pinpoint the source of performance issues.

1 Dimensional Research, sponsored by Broadcom, "Cloud and Internet Usage Generates Network Observability Blind Spots," September 2024

Cloud Adoption

Unsurprisingly, our survey found that 98% of companies currently utilize or plan to use cloud infrastructure. Integrating cloud services into the network or consuming SaaS apps for business purposes introduces another layer of complexity for network operations teams. Managing the interconnections between on-premises infrastructure and cloud environments requires new skills and tools.

Reliance on Third-Party Service Providers

The survey also revealed that 65% rely on third parties for network operations. When a third party is responsible for managing part or all of the network delivery path, gaining a complete and unified view of network performance becomes more difficult. Integrating data from various third-party tools and systems into a central monitoring platform can be complex, introducing the potential for blind spots that hinder troubleshooting efforts. This dependence on external providers can limit an organization's direct control over network infrastructure and data collection, making it harder to implement advanced monitoring strategies, such as streaming telemetry and active synthetic monitoring.

Increased Bandwidth Demands

Organizations continue to rely more heavily on bandwidth-intensive applications and services, and the move to AI will only accelerate this trend. Consequently, network operations teams must contend with greater pressure on their infrastructure. This requires more sophisticated traffic management and optimization strategies.

New Technology Adoption

In many companies, teams have implemented new technologies, such as software-defined wide area networks (SD-WAN) and network function virtualization (NFV). These technologies provide an array of advantages to businesses, but they also add a layer of abstraction that introduces complexity and exposes the limitations of legacy network monitoring tools.

Toolsets Are Leaving Teams Ill-Equipped

Broadcom research reveals that 80% of respondents believe that internet and cloud network paths present monitoring blind spots. Traditional monitoring tools often lack the ability to effectively monitor cloud and internet environments, leaving teams contending with visibility gaps and limited control. This is because cloud and internet infrastructures are managed by third-party providers, making it more challenging to collect data and gain insights into performance issues.

Lacking ISP Visibility

Our survey revealed 95% of respondents don't get all of the ISP information they want from their monitoring solutions. Even if a company has robust internal network monitoring, a lack of transparency and information from the ISP can create significant blind spots. ISPs don't provide sufficient data about their infrastructure and performance, making it extremely difficult to pinpoint the root cause of problems, particularly those that lie outside the organization's own network.

This lack of information can lead to long triage times and blame games between internal teams and the ISP. In addition, it hinders efficient resolution and has a negative impact on customer experience. In essence, even with advanced internal monitoring, incomplete ISP information can act as a bottleneck and negate the benefits of those internal systems. This can constrain a company's long-term network strategy and its ability to adapt to changing business needs.

Lacking Cloud Metrics

The survey also found that 95% of individuals surveyed don't get all the metrics they need from cloud providers either. When queried about information needed from cloud providers, data on security incidents and infrastructure performance are tied at 51%, making them the two most needed metrics. Traditional network monitoring tools and skillsets often fall short when contending with cloud infrastructure, leading to a lack of visibility and control. The vast majority of teams struggle to obtain comprehensive information from their cloud providers. This lack of information can hinder troubleshooting, capacity planning, and overall network optimization in cloud environments. The lack of clear visibility may make it difficult for network operations teams to effectively manage cloud-based infrastructure, leading them to defer to cloud teams who may lack experience with broader network operations.

NETWORK OPERATIONS TEAMS CONTENDING WITH SIGNIFICANT IMPLICATIONS

Visibility Gaps Hinder Troubleshooting

Our survey found that only 24% of respondents say they have immediate access to the data they need to troubleshoot issues, which means more than three-quarters of respondents either lack the data they need or experience delays in accessing it. If solutions cannot enable high-scale, multi-vendor, multi-cloud coverage out of the box, teams will lack the correlated data they need to understand global network health. They'll also lack granular metrics like packet loss, latency, and jitter, prolonging triage times.

Teams are Stuck in Reactive Mode

84% of network operations teams regularly learn about network issues from users instead of their monitoring tools. Manual network monitoring practices rely on siloed solutions that lack a comprehensive view of infrastructure health. This leads to long triage and root cause analysis times because teams lack the data to proactively identify and resolve issues. The fact that users often report problems before the network team is aware of them highlights the impact of this lack of visibility. The lack of timely data leads to a reactive approach in which teams are constantly putting out fires reported by users rather than proactively managing network health.

Too Many Network Alarms Prolong Triage Times

Significant percentages of respondents indicate false positive alerts (41%) and alert storms (39%) are making network operations challenging. Fundamentally, too many network alarms are prolonging triage times within many organizations. Modern network infrastructure like software-defined LAN or WAN can produce tens of thousands of events. Level-one network operators then must sift through all these alarms to find the root cause of network performance issues.

Lack of Visibility Slows Resolution

The survey reveals that 76% of network operations teams report that slow or missing data impedes issue resolution times. Reliance on disparate, non-integrated monitoring tools leads to slow triage and lengthy root cause analysis. This emphasizes that the lack of timely and complete data significantly hinders the ability of network teams to quickly identify and resolve issues. Further, missing data will only lead to a lack of confidence in the calculations and predictions a team makes. Therefore, data is the most important ingredient for successful observability practices.

Tools Stifling Adoption of New Technologies

Our data reveals that 64% report that their monitoring tools inhibit the speedy adoption of new network technologies. Further, 80% stated that internet and cloud environments create blind spots. Modern architectures like SD-WAN or secure access service edge (SASE) demand resilient connections at every hop in the network delivery path to deliver on their promise. Without complete observability, adoption of innovative technologies is slowed and potential benefits are eroded.

Skill Gaps Impede Growth

The increasing complexity of network operations contributes to the demand for skilled network professionals. Increasingly, network operations teams will require expertise in cloud technologies, automation, and advanced monitoring tools. As a result, the pool of candidates with the necessary skills will shrink relative to the demand. The more specialized and complex network operations become, the greater the need for individuals with advanced training and experience. This is one reason why difficulties finding qualified candidates present a barrier to the growth of network teams.

Our survey asked respondents what is inhibiting the network team's ability to grow and manage more tasks. Almost half, 48%, indicated growth was being stifled because candidates lack the needed skillsets, and 45% pointed to a lack of available candidates.

KEY REQUIREMENTS FOR ESTABLISHING NETWORK OBSERVABILITY

To address all the challenges outlined above, network operations teams need to employ advanced tools and approaches. In short, they need to establish complete, holistic network observability. Here are the key requirements for making this happen.

Visibility Into Third-Party Environments

To be effective, network operations strategies and processes need to address every network that shapes the delivery experience. This is the only way teams can quickly and easily isolate issues—whether those issues are occurring on networks they're managing or on those run by third parties. The bottom line is that network observability should ensure reliable connections—no matter where a user is or what device or network they are accessing.

A mature network observability solution should provide extended, inside-out, hop-by-hop visibility into third-party cloud and ISP networks. Modern data collection methods, such as streaming telemetry and active monitoring, allow teams to gain real-time insights into network performance, regardless of where the infrastructure resides.

This enables teams to track the end-to-end performance of any network path, no matter where it is located. In this way, you can discover routes that traverse ISP and cloud networks and the devices that support those transmissions. This enables fast isolation of delivery issues that arise in externally managed environments.

Correlated, Scalable SD-WAN Visibility

A mature network observability practice should be able to easily support hundreds of thousands of encrypted tunnels that SD-WAN can produce, correlate multi-vendor underlay and overlay metrics, and provide visibility beyond the internal network and into third-party networks.

Advanced Intelligence and Analytics

A mature network observability practice should employ algorithmic capabilities like event correlation, alarm suppression, root cause analysis, predictive capacity planning, and volatility analytics. These capabilities can eliminate alarm and event noise and quickly reveal which device, process, or user is responsible for an issue, so teams can remediate immediately. A mature network observability solution can help network operations teams adapt to future requirements. These advanced solutions can collect the right data and deliver the right remediation recommendations, while aligning with evolving network architectures and operational procedures. By leveraging an advanced observability solution that can collect more data from every aspect of your network functions, you can gain intelligent insights and efficiently share them with team members.

Active Synthetic Monitoring

The rise of hybrid work underscores the need for real-time data and proactive monitoring. With employees working from various locations and networks, troubleshooting becomes far more complex. Passive monitoring alone is insufficient to address this complexity. Active synthetic monitoring becomes critical for identifying and diagnosing performance bottlenecks across the extended network. While "synthetics" is a term typically defined as web transaction monitoring, a new breed of network synthetics provides better visibility into the layer 2 hops that traffic takes as part of the complete network delivery path.

Streamlined Operations

A mature network observability practice should remove the complexity of managing network operations, offering easy to understand and focused remediation recommendations or automated resolutions, without breaking the budget.

THREE GOALS OF NETWORK OBSERVABILITY

In order to continue to fuel IT and business innovation, observability solutions should enable continuous optimization of network operations center (NOC) workflows, network transformations, and connected experiences. As networks continue to evolve and challenge network operations teams, this continuous improvement will allow the business to stay competitive, deliver innovative new service offerings, and attract and retain customers.

Optimize Network Operations

Too much alarm noise, disparate data sets, and inefficient triage workflows inevitably lead to long triage times. Network operations teams should be able to resolve issues faster, while enabling more predictable, lower-cost IT innovation. By establishing end-to-end coverage, organizations can gain a global perspective of network operations and more rapidly and accurately isolate the cause of issues. With advanced solutions, network operations teams can also leverage historical metric data to calculate future values. This intelligence can deliver actionable insights that enable teams to get ahead of issues—and avoid war rooms and extended firefighting.

Accelerate Network Transformations

When teams lack comprehensive observability, the introduction of new technologies can create dangerous and disruptive blind spots. Consequently, poor observability can stifle the adoption of new technologies. Network operations teams should be providing the visibility and speed needed to deliver modern connections and evolve networks in response to business needs. Effective observability can enable successful transformation because it can support the validation of new network implementations. This visibility leads to the operational consistency that network operations teams need to deliver on business objectives.

NETWORK OBSERVABILITY GOALS

Enhance Connected Experiences

Network operations teams have traditionally focused on tracking uptime based on network faults and performance issues. Today's teams need to tie the network directly to the user experience. To ensure optimal network and application experiences, teams need to validate quality across internal and external networks. With active visibility from the end-user perspective, teams can track private, public, and hybrid cloud connections and gain visibility into internet performance.

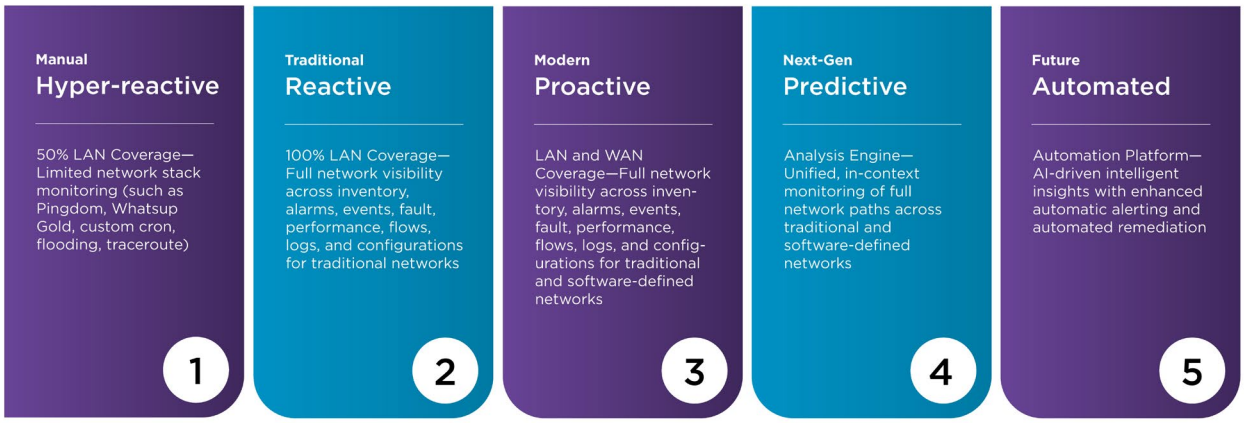
NETWORK OBSERVABILITY MATURITY MODEL

As outlined above, the challenges posed by today's modern networks require new observability techniques. To deliver on the three goals of network observability, network operations teams must advance the maturity of their organization. The following sections outline five stages of maturity and offer a general overview of each level's characteristics. In addition, we detail the network coverage that enables teams to make strides toward each of the three goals described above.

1. Manual

Early network monitoring practices and processes involve solutions from many different vendors. Typically, these tools only offer coverage of a specific system or technology domain. Teams have many siloed solutions that lack comprehensive metric collection and that do not integrate with each other, so teams can't gain a global view of infrastructure health.

At this stage, many teams use a mix of free and open-source tools that provide device-based metrics for a NOC, but introduce data conflicts and false alarms. These stand-alone tools lead to lengthy triage efforts and time-consuming root cause analysis of network performance issues. Teams routinely spend hours, if not days, finding resolutions, which can have an impact on the company's revenue and brand.



This maturity level can be considered the first step to a comprehensive monitoring strategy. To progress, teams need to constantly refine their approaches, and keep adapting as networks continue to grow more complex, fast-changing, and dynamic.

2. Traditional

At this phase, most teams have achieved full network visibility across inventory, alarms, events, fault, performance, flows, logs, and configuration management for their traditional, internally managed networks. However, these teams still rely on some siloed monitoring technologies, such as vendor-specific tools. Given this, the negative effects of swivel-chair monitoring persist. Some of the metrics these siloed tools collect can be correlated and presented to NOC engineers, but other tool sets still collect important network data that gets accessed via separate administrative consoles or internal teams.

This level represents a positive step toward improving the NOC team's visibility into traditional network delivery. However, teams still contend with long triage times and "blame games" that result in poor customer experiences. In many cases, NOC staff have common scripted solutions for recurring issues but tickets remain open, which has a negative impact on mean time to resolution (MTTR). At this stage, given the lack of integration among tool sets, it can be difficult or impossible to establish predictive capacity planning or automate lower-level tasks. This level also does not support modern network technologies like software-defined networking (SDN) and cloud environments. In most cases, the NOC will shift responsibility for cloud operations to cloud teams, who often have very little experience with infrastructure operations.

3. Modern

At this phase, network operations teams have consolidated on a few primary tools with some amount of integration. This enables some correlation of data, which helps teams isolate the root cause of issues. Some teams add active synthetic network monitoring and web testing to their traditional passive monitoring in order to extend their visibility into third-party networks and business-critical applications. With complete visibility into internal and external networks, teams can gain comprehensive, end-to-end coverage of application and network delivery paths.

This level is characterized by an evolution in which teams move from reacting to metrics to proactively analyzing issues. While this is possible in lower tiers of the maturity model, less mature network operations teams don't have visibility into external networks and their tools lack application context.

The addition of more modern data collection methods like streaming telemetry and active monitoring provides real-time insights that pave the way for AI-driven analytics. Streaming telemetry offers real-time data collection services that enable fast and efficient analysis of network performance. With this approach network devices, such as routers, switches, and firewalls, continuously push data related to the network's health to a centralized location. Active monitoring periodically sends test packets over the network and measures response times. This enables teams to objectively measure and track performance of every hop of the network delivery path, whether it traverses internally or externally managed environments.

4. Next Generation

The next-generation stage of maturity begins with efficiently and automatically streaming metrics into a centralized analytics and reporting platform. Data inputs should include the full spectrum of end-to-end network visibility, including across office, home, ISP, transit, backhaul, data center, cloud, and SaaS environments. This stage includes a centralized data lake that provides correlation and AI to analyze metrics. With these capabilities, solutions can provide insights that help level-one and level-two network operations professionals solve more issues, without having to escalate to senior team members.

At this phase, most alerts are actionable, thanks to advanced analytics, suppression of non-critical issues, and correlation of downstream alerts. Anomaly detection, network performance baselining, and root cause analysis provide faster time to insights and reductions in MTTR. Visibility encompasses both internal and external networks.

The next-generation level is the first step into truly predictive network observability and management. At this stage, metrics are layered into advanced traffic engineering, baselining, anomaly detection, and software-defined technologies, helping fuel better digital experiences. By taking an experience-driven approach to the NOC, teams leverage solutions that offer support for SD-WAN, private cloud, and Wi-Fi. With these capabilities, network operations teams can identify and isolate emerging issues and address them before the user experience is affected.

5. Self-Operating and Self-Healing

This final step, and one that admittedly needs more discussion on the broader stage, is the future state of automated networks. At this level, teams build on the AI-driven intelligent insights from previous stages and add more intelligent alerting, external event correlation, and automated remediation. Human-driven, closed-loop automation is still involved due to lingering distrust of full automation.

With new technologies, network operations teams will work as conductors of an orchestra, rather than individual musicians struggling to stay in rhythm. With these capabilities, teams can ensure that all systems work together to ensure network performance and user experience remain optimal. Automated escalation is common, allowing NOC teams to automatically assign tickets, including to internal and external service providers when necessary. At the final stage of the maturity model, teams gain the automation and visibility needed to contend with the inherent difficulties of managing modern networks that feature third-party, cloud, and hybrid work environments.

This level is characterized by automating network functions as much as possible, while enabling human supervision or intervention when necessary. Using predictive insights, baselining data, and other inputs, networks can be set up to change dynamically to match available resources, cost requirements, or performance benchmarks.

PUTTING THE MODEL INTO PRACTICE

To advance network observability maturity, network operations teams need to start by establishing a unified data model that can support the collection of metrics from a multi-vendor network. Next, teams should embrace the advanced and AI-driven features of modern network management solutions, such as alarm noise reduction, event correlation, capacity analytics, and log analysis.

For more than 30 years, Broadcom has delivered patented and foundational capabilities for AI-driven network observability. The team at Broadcom understands the complexity of network operations and continues to deliver solutions that enable true network observability. With the Network Observability by Broadcom solution, enterprise customers have realized a range of benefits, including 95% improvements in triage times, a 50% reduction in operational costs, $1 million in bandwidth savings, outage avoidance that enabled $2.5 million in revenue protection, and a 160% return on investment.

CONCLUSION

Every organization's journey through the five phases of network observability maturity will be different, but there are a few common themes that any organization will encounter. One key aspect is the need to expand network operations sites beyond internal infrastructure and move to external networks. As part of this, it is crucial for teams to move from relying on passive, device-based data and employ active monitoring. While many network operations professionals may see automated remediation as a pipe dream, there are already places within the network that allow automatic decisions, such as with SD-WAN tunnel changes. It's not a stretch to believe more of those instances will arise in the future.

HOW BROADCOM CAN HELP

Broadcom is a company that's uniquely qualified to help organizations advance their network observability maturity. Here's a brief introduction to what sets Broadcom apart from the competition:

- **Solutions**. Network Observability by Broadcom has a long track record of delivering value to customers, with proven capabilities for optimizing network operations. The solution delivers capabilities for managing fault, performance, experience, and flow data in order to optimize network operations. Through the solution, Broadcom can provide unparalleled visibility into internal and external networks.
- **People**. Broadcom has seasoned experts dedicated to supporting network operations initiatives. People in product management, executive leadership, sales, and support have been directly engaged with leaders and delivery teams at top enterprises around the world. Our people have a proven track record of helping businesses achieve network observability maturity.

For more information, please visit our Network Observability by Broadcom page.