BROADCOM

WHITE PAPER

End-to-End Network Operations Coverage

Why It's So Critical and How to Gain the Visibility Required

TABLE OF CONTENTS

OVERVIEW

Today, virtually every critical service and function of every organization relies extensively on digital services and communications. Consequently, it's never been more critical to ensure optimized network delivery and operations at all times.

However, getting a clear and precise view of how the network performs and functions is not easy for the vast majority of network operations teams. A recent survey revealed that only 8.5% of respondents find this task simple, while most face various difficulties.[1]

Modern networks are composed of a broad range of technologies and continue to grow increasingly complex. In these environments, network operations teams struggle to gain the full visibility they need. In response, teams in many organizations have added stacks of network monitoring tools to their arsenal, hoping that more technologies would improve their visibility. A survey revealed that operations teams in a majority of organizations use between 10 and 20 different tools to monitor their networks.[2]

However, this approach has backfired. Rather than helping simplify operations, these tools exacerbate complexity. Teams are now contending with multiple tools from different vendors, and each tool has its own interface, configuration, and data format. This has created more challenges for teams who wanted to enhance their network visibility.

In most organizations today, network operations teams struggle to cope with a deluge of network data and lack the insights they need to truly understand the status of their networks. This represents a vexing problem for organizations, and teams will need to employ new approaches if they're going to fix it.

To overcome these challenges, teams must focus on establishing an effective network observability and management approach that provides end-to-end coverage. Teams need full network visibility across both internally managed networks and network environments that are owned and managed by third parties. Further, they must also have access to a unified topology that shows the interconnections and dependencies among all network elements.

Network operations teams need a robust network observability and management solution that can tackle these critical tasks:

- **Address the demands of multi-vendor, multi-technology environments**. Tool sprawl can create more complexity and risk. Various tools from multiple vendors often use different data taxonomies and architectures, which can complicate analysis. By leveraging a single solution that can handle all types of networks and data sources, teams can realize a number of advantages. These solutions can eliminate the need for multiple tools and platforms, reducing complexity and cost.
- **Eliminate network monitoring blind spots**. Massive volumes of data can create network visibility gaps. By correlating data from multiple sources and applying root cause analysis, advanced solutions enable teams to identify and troubleshoot issues faster and more effectively. Teams can optimize network performance and operational efficiency by more quickly and accurately discovering and eliminating blind spots.
- **Establish unified visibility and control**. Adding more network monitoring tools to the environment increases operational risk and costs. Optimal solutions enable teams to gain full visibility into the health, performance, and availability of all network devices and services. These solutions enable teams to track performance from an end-user perspective, regardless of where users are located or who owns the networks that services are reliant upon.

1 Enterprise Management Associates, "**Network Observability: Delivering Actionable Insights to Network Operations**," Shamus McGillicuddy and Robert Gates, October 2022:

2 Enterprise Management Associates, "**Network Observability: Delivering Actionable Insights to Network Operations**," Shamus McGillicuddy and Robert Gates, October 2022:

ADDRESSING THE DEMANDS OF MULTI-VENDOR, MULTI-TECHNOLOGY ENVIRONMENTS

Applications are increasingly deployed across various data centers, edge locations, and public clouds as digital transformation and cloud migration initiatives expand in organizations. This intensifies network observability and management challenges in today's multi-vendor, multi-technology environments, where different devices, protocols, standards, and technologies coexist. Many network teams rely on specialized monitoring tools for various components, but different network monitoring tools are designed to monitor distinct aspects of a network. While these tools can provide valuable insights into the performance and availability of specific parts of the network, they can also create gaps in understanding end-to-end network performance and service quality. This is because each tool provides a limited view, making it challenging to correlate data from different tools to get a complete picture of the network.

A large financial services firm struggled with managing their network, running various components from different vendors and technologies. They had different monitoring tools for their data centers, multi-cloud, and endpoints, but none of them could provide a complete picture of the end-to-end network performance. When various monitoring tools only cover specific parts of the network, it could lead to visibility gaps. As a result, some problems can go unnoticed if they happen outside of different teams' respective domains. Ultimately, the firm experienced a significant slowdown in application performance, which took tens of minutes instead of a few seconds to refresh. End users were frustrated as their services were degraded. The problem was caused by 5% packet loss on Azure ingress, but none of the monitoring tools could determine it by themselves. They all showed a "green" status, implying that everything was fine. This shows how having disjointed network monitoring tools, especially in multi-technology environments, can create gaps in visibility and diagnosis, resulting in poor network performance and experience.

Multi-Vendor and Multi-Technology Support

Network operations teams need a network observability and management solution that can work with different vendors and technologies, including across the data center, the edge, and the cloud. NetOps by Broadcom is an integrated solution that meets this need. The solution combines DX NetOps and AppNeta to deliver a complete solution that provides end-to-end network visibility, from the site to the cloud. To illustrate how these products work together, let's revisit our previous example. By using the powerful combination of DX NetOps and AppNeta, the teams at the financial services firm can gain the complete visibility they need to quickly isolate the network segment where packet loss happened, which is the cloud domain in this scenario. Here's how each solution helped:

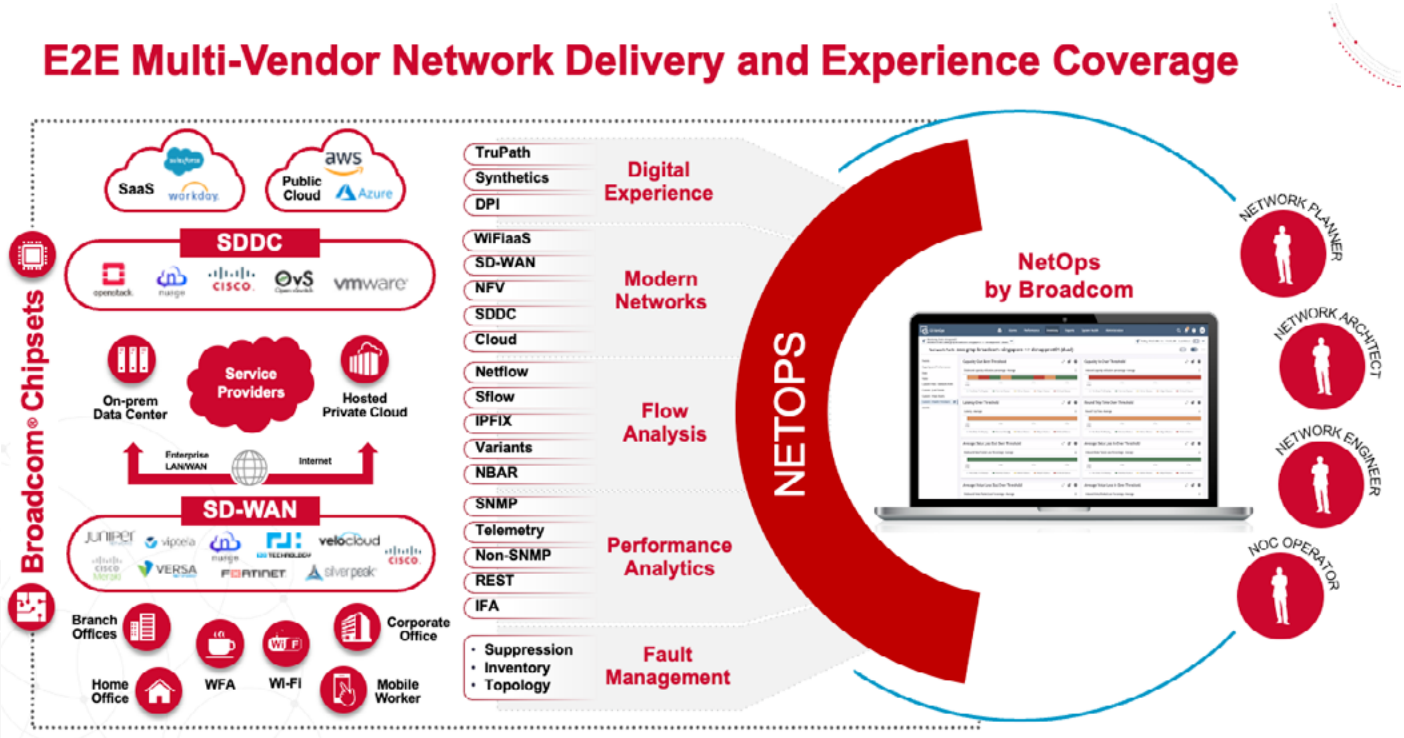
- **DX NetOps**. DX NetOps offers scalable network monitoring capabilities that span traditional and modern architectures. The solution converts inventory, topology, device metrics, faults, flow, and packet analysis into actionable intelligence.
- **AppNeta**. AppNeta delivers active, continuous monitoring. AppNeta gives teams end-to-end visibility of network delivery paths, even those that span third-party internet service provider (ISP) networks, cloud networks, and hybrid work environments.

With the solution, teams can collect, store, analyze, and display detailed information from various sources, such as SNMP MIB requests, streaming telemetry, flow protocols, and third-party APIs. The solution provides a technology certification portal that displays all the vendor and metric families that are supported out of the box. Here's a list of the wide range of vendors the solution supports:

3Com	F5	Motorola
Adtran	Foundry Networks	NetScaler
Alcatel	Dell	Lucent
Avaya	HP	Mitel
Avocent	Foundry Networks	Nokia
Blue Coat Systems	Hitachi	Nortel
Calix Networks	IBM	Palo Alto
Cedar Point Communications	InnoMedia	Siemens
Cisco (including Meraki)	Juniper	TrendPoint Systems
DataPower Technology		VMware

The solution provides monitoring points that can monitor WAN and cloud traffic. To do so, teams can deploy monitoring points using a SPAN/mirrored port or by placing them inline in the network path. Teams can also use Global Monitoring points that Broadcom owns and manages, giving them vital outside-in perspectives of the network, helping them reduce the time needed to deliver value (MTTV). By using deep packet inspection (DPI), these monitoring points can measure the traffic volume of different applications and application categories. Monitoring points can also capture traffic flow records in real-time for bandwidth analysis. Further, the solution simplifies the discovery and monitoring of software-defined network devices across various technologies, such as Cisco ACI, Juniper 128T, Meraki, Nokia Nuage, SilverPeak, Versa, Viptela, and VMware.

The solution enables teams to manage Wi-Fi access points as part of the standard device inventory and monitor metrics like radio signal strength for Cisco, Juniper, and Aruba wireless systems. Network operations teams can also get data on wireless controllers and clients. Further, in software-defined wide area network (SD-WAN) environments, the solution can track the performance of both overlay and underlay networks, across remote sites. In this way, the solution helps teams ensure users of web-based applications have an optimal experience, whether applications are hosted in the cloud or on premises.



The Broadcom solution unifies the capture and analysis of device health, network traffic, and digital experience monitoring (DEM), without requiring teams to implement additional solutions. With these broad integration capabilities, the solution can monitor the performance of end-to-end network paths, including those that span externally managed networks, which is traditionally a blind spot for internal monitoring solutions.

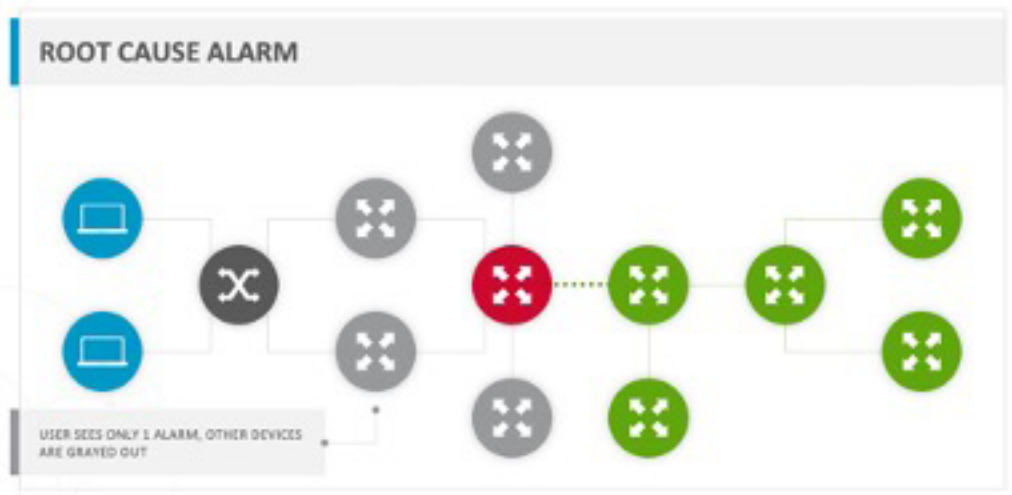
Layer 2 and Layer 3 Device and Topology Discovery for Multi-Vendor Technologies

A comprehensive and accurate network topology is essential for making smart decisions about the network and infrastructure. To gain end-to-end coverage of all network components, teams need to do an inventory of both internally and externally managed devices. However, many teams struggle to maintain an accurate inventory of their network assets. Due to a lack of visibility, teams often delay in replacing their old equipment for several years, exposing themselves to greater risks of outages and performance issues. A simple question like "Do you know where your outdated devices are located?" can prove to be difficult for teams to answer.

To achieve end-to-end network visibility, teams need to have multi-vendor device and topology discovery. This discovery process needs to identify and map the network devices and links at layer 2 (data link) and layer 3 (network) of the OSI model. This discovery can generate a complete and accurate picture of the network topology, with details such as device attributes, interfaces, IP addresses, MAC addresses, VLANs, subnets, routing protocols, neighbors, and more. It can also display the network topology in a graphical or tabular format or export it to other tools for further analysis.

NetOps by Broadcom can discover and map layer 2 and layer 3 devices and topologies. With the solution, teams can easily see an accurate depiction of the network infrastructure, including devices from different vendors, and how they are connected logically and physically. The solution can scan the network using various protocols, such as SNMP, LLDP, CDP, ARP, BGP, and more. It can gather information about devices, such as hostname, IP address, model, OS version, serial number, and interface details. The solution can also find the links between devices, such as port-to-port connections, VLANs, subnets, and routing tables. The solution can also discover software-defined topology via API. This enables teams to gain full visibility of both traditional and modern networks. By building a detailed and interactive network map that displays the devices and their relationships, teams can easily identify the scope of the issue for faster problem resolution.

The Broadcom solution offers multi-vendor discovery of level 2 and 3 devices and topologies. With the solution, teams can establish a comprehensive view of their network devices and configurations. The solution can also detect changes or anomalies in the network topology and notify teams immediately, so they can more quickly identify the root cause and impact of network issues and resolve them.



ELIMINATING NETWORK MONITORING BLIND SPOTS

The increasing complexity of IT environments makes network visibility crucial for ensuring optimal performance and high-quality connected experiences. However, many network operations teams struggle to achieve a comprehensive view of their entire network infrastructure. This is particularly challenging given the reliance on networks that are owned, operated, and maintained by third parties, including cloud service providers, ISPs, home Wi-Fi networks, and more.

These externally managed networks pose significant challenges for network operations teams, as they introduce blind spots, making risks hard to detect and mitigate. Further, if teams can't monitor these external networks, they can't prove their network's innocence or hold their service providers accountable. Without evidence, it is hard to show that ISPs, vendors, and technology partners are failing to meet their SLAs.

Network operations teams have had to contend with explosive growth in new technology adoption, complexity, and network traffic flowing beyond the edge of the data center. All these factors have created unprecedented visibility gaps. A global survey by Dimensional Research, for example, reveals that 81% of organizations report network monitoring blind spots. [3] Another study shows 67% of network operations teams cite internet and cloud network paths as monitoring blind spots.[4] Faced with reduced visibility into the networks that deliver applications to users, teams are forced to reference vendor status pages and support tickets in order to determine whether an outage affects end users.

To address the challenges posed by externally managed networks, some organizations have started adopting DEM tools. These are software applications that help organizations measure the performance of their digital services, which typically run in the cloud. These tools provide insights into how users actually experience these digital services.

DEM tools can provide insights into how users interact with websites, mobile apps, cloud services, and other digital platforms. In addition, they can reveal how these platforms perform in terms of speed, availability, reliability, and security. However, DEM alone is not enough because it only provides limited visibility into the end-to-end network delivery chain and the underlying infrastructure that supports it.

What's needed is to "operationalize" the internet and cloud provider environments that most users' network paths now traverse. Teams can achieve this by feeding user experience metrics into their standard operating procedures and workflows and establishing complete visibility, from the client to the cloud. In this way, teams can gain expanded visibility across network performance, fault, flows, and user experience—and in the process eliminate blind spots in their network visibility.

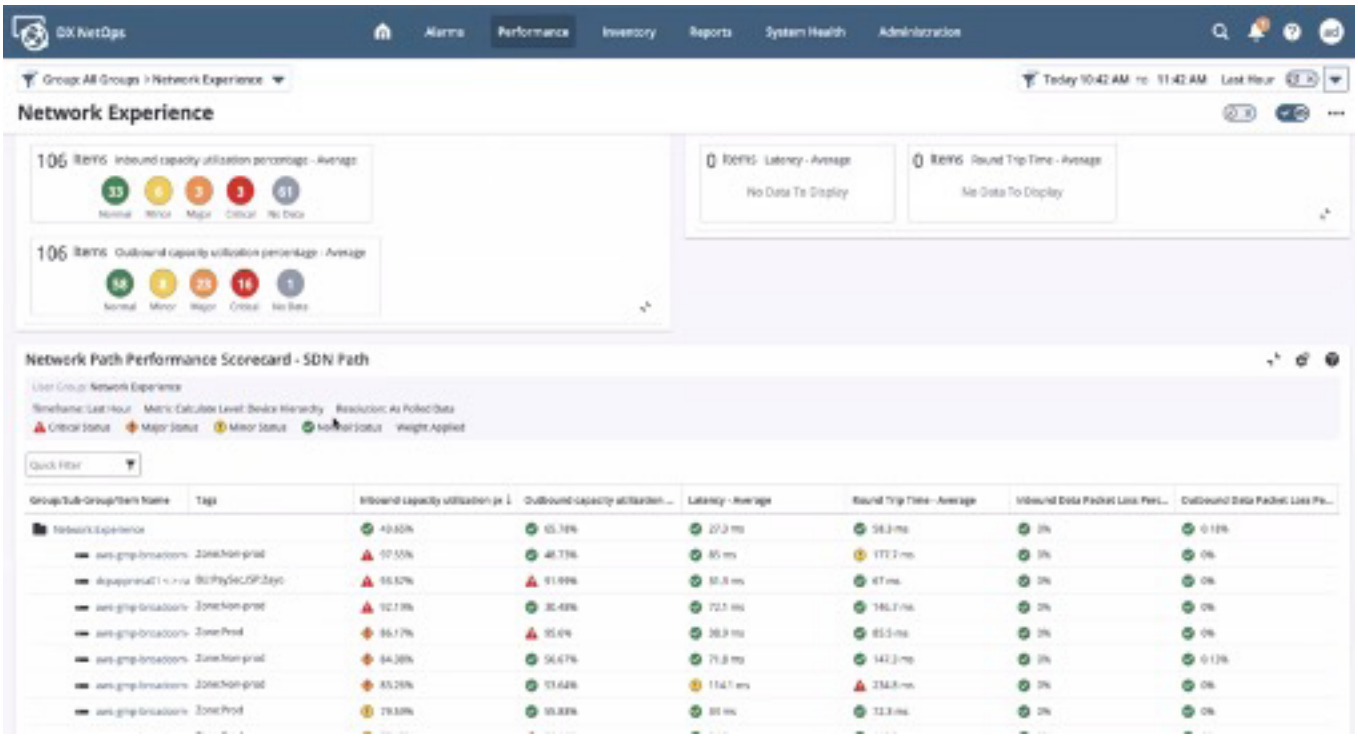
Experience-Driven Approach to Network Operations

Broadcom offers an industry-leading experience-driven approach to network observability and management. NetOps by Broadcom enables teams to operationalize the modern network, bringing user experience insights directly into the network operations center (NOC).

The solution feeds user experience metrics into the NOC's standard operating procedures to create continuous feedback, reduce blind spots, and enable more efficient event triage. The solution can leverage synthetic testing of web applications, which provides an accurate picture of end-user experience. When problematic network delivery paths are identified, the solution can provide automated diagnostics and enable deep-dive analysis through a single click, all from within a unified portal. The solution goes beyond real user monitoring (RUM) and other reactive monitoring methods. It can measure the network experience proactively and help teams find and fix issues before the user experience gets impacted. As a result, the solution helps improve end-user satisfaction, while optimizing resource utilization and reducing operational costs.

3 Dimensional Research, "**Are Networks Ready for Massive Scale Increases and New Technology?**" February 2022

4 Intelligent Tech Channels, "**Spire Solutions signs with Gigamon to accelerate response times**," Mark Bowen, July 29, 2019



The solution helps organizations to establish a unified NOC across various network environments, such as private and public networks, and modern network architectures like SD-WAN, secure access service edge (SASE) and software-defined data center (SDDC), and ISP networks. With the solution, organizations can extend the NOC by incorporating network experience metrics provided by AppNeta into DX NetOps.

The integrated solution provides unified alarm management, applying patented network alarm noise reduction technology to AppNeta path events and alarms to quickly determine the root-cause of the alarm and not just the symptoms of the issue. For instance, by consolidating performance events from multiple sites into a single ticket about a cloud application outage, teams can solve the problem faster. The solution also provides unified dashboards that reflect views of multiple technology domains, which can help teams perform critical operation workflows across multi-vendor network technologies to avoid blind spots. Within the single network management platform, teams can have the insights they need to identify the source of the network problem and its impact on end users.

Data Collection Services

A major challenge for network observability and management is collecting and analyzing different types of data that indicate the state and behavior of the network. Some of the common data types include:

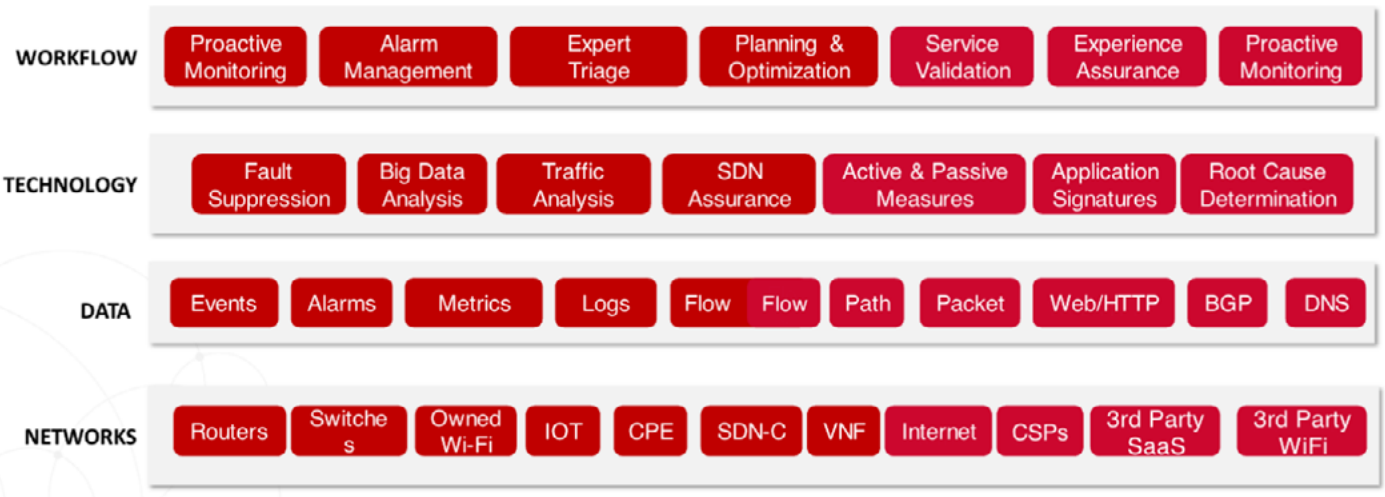
- **Metrics**. These are values that represent the performance or status of a network component like CPU utilization, memory usage, packet loss, latency, throughput, etc. Metrics can be aggregated, averaged, or plotted over time to show trends and patterns.
- **Logs**. Logs are textual records that capture the events or actions that occur within the network, such as configuration changes, errors, warnings, and alerts. Logs can be searched, filtered, or parsed to extract relevant information or insights.

- **Traces**. Traces are sequences of events representing the flow of requests or transactions across the network, such as HTTP requests, database queries, and RPC calls. Traces can be used to measure the latency, performance, or reliability of a network service.
- **Events**. These are discrete occurrences that indicate a change or anomaly in the network, including failures, faults, incidents, alerts, and so on. Events can be used to trigger notifications, actions, or remediation.
- **Packets**. Packets are units of data that travel over a network containing information like sender and receiver IP addresses, capture time, and protocol used. Network operations teams can use packet data to get a detailed view of network traffic to help them solve network problems and measure performance.
- **Flow data**. This data provides information about traffic patterns throughout the network. Teams can use flow data to understand the normal behavior and performance of the network. By analyzing flow data, teams can track the frequency and timing of user information access and optimize the allocation of resources.
- **Streaming telemetry**. This is an emerging technique for real-time network data collection, allowing teams to receive continuous and granular data from their network devices, without relying on traditional polling or SNMP protocols.

NetOps by Broadcom offers data collection capabilities that can gather data from various technologies, supporting multiple protocols and telemetry formats, such as events, logs, configs, user experience, and more. The solution also collects flow data, giving teams a real-time enterprise view of the network traffic composition. This includes support for packet capture/DPI, NetFlow, IPFIX, sFlow, and proprietary implementations like NBAR and J-Flow, and more.

As network data collection shifts from SNMP to network telemetry, the solution supports gNMI-based telemetry time series data. This enables teams to collect data for devices that are moving away from SNMP-based management or for larger devices where SNMP polling adds performance overhead to critical network equipment functions. This also allows teams to obtain new metrics that are added to telemetry APIs, which provide deeper insights into vendor specific technologies and use cases. With the Broadcom solution's end-to-end coverage of multi-technology data collection, network operations teams can get the comprehensive view of network health, performance, and experience they need to quickly and effectively identify and troubleshoot issues.

Broadcom's *Network Visibility Anywhere* Architecture



Integrated Flow and Traffic Analysis

NetOps by Broadcom provides deep visibility into network traffic and offers capabilities for proactive capacity planning, anomaly detection, and problem solving. The solution delivers flexible dashboards and reports that unify all aspects of monitoring. Equipped with intuitive visualizations and customizable dashboards, network specialists can easily interpret complex data, identify potential issues, and manage network resources more consistently and effectively.

With the solution, teams can see the traffic composition on every link in their network and spot potential threats before they cause outages. Teams can easily find the root cause of performance issues, assess the impact of network changes, and optimize WAN investments. Understanding what is consuming resources is as important as understanding resource usage itself. By using the solution's app-aware flow monitoring capabilities, teams can determine what apps are being used and how they are consuming resources, and spot usage trends that are related to other performance indicators and events.

Armed with these app usage insights, teams can effectively prioritize and balance critical app performance with available network resources. In addition, the solution provides a unified portal that shows the relevant information for each device, site, or location in context. With the solution, teams can make more informed decisions about cost saving opportunities, capacity planning, troubleshooting, and network traffic analysis across the enterprise.

Highly Scalable Monitoring, Support for the Largest Global Networks

NetOps by Broadcom can scale from the smallest remote site to the fastest 100 Gbps data center. The solution can monitor more than 500,000 network devices, over 8 million interfaces, and over 300,000 SD-WAN tunnels. It can also monitor cloud environments with more than 10,000 locations using purpose-built appliances that measure network experience with high-frequency testing and low overhead. This way, the solution provides complete visibility without affecting network performance and experience. One of the most scalable monitoring platforms in the market, the solution monitors more than 2.4 million objects for the third largest telecommunications provider in North America.

This solution uses a distributed server architecture to enable the load balanced management of portions of a large-scale network. Using such an architecture, customers can create a unified representation of the network infrastructure. These views can incorporate multiple domains, with each composed of the models, associations, attributes, values, alarms, events, and statistics belonging to a specific management server.

ESTABLISHING UNIFIED VISIBILITY AND CONTROL

The reality is that network operations teams lost visibility and control when workloads started moving to cloud and SaaS environments. Teams must also contend with increasingly complex network architectures in their data centers and remote locations. SD-WAN technologies continue to be adopted at a rapid rate. These technologies are complex and dynamic, changing constantly due to evolving business demands. This leads to a number of challenges, such as long triage times, poor capacity planning, and increased operational costs.

Moreover, teams must deal with the fact that network delivery paths increasingly span externally managed networks, including those of ISPs, cloud providers, and SaaS environments. Without visibility into these environments, teams encounter such problems as lengthy troubleshooting efforts and multi-vendor blame-game scenarios. When teams can't identify and address delivery issues, the end-user experience suffers. The main question for network operations teams is how to troubleshoot something they can't see?

Limited network visibility can have a significant impact on mean-time-to-resolution (MTTR) metrics. When teams lack full network visibility, MTTR increases, which can lead to costly downtime for the business. One survey found that, in almost half of firms (44%), the costs of an hour of downtime can be between $1 million and $5 million.[5]

5 TechChannel, "**The Cost of Enterprise Downtime**," Laura DiDio, September 30, 2021

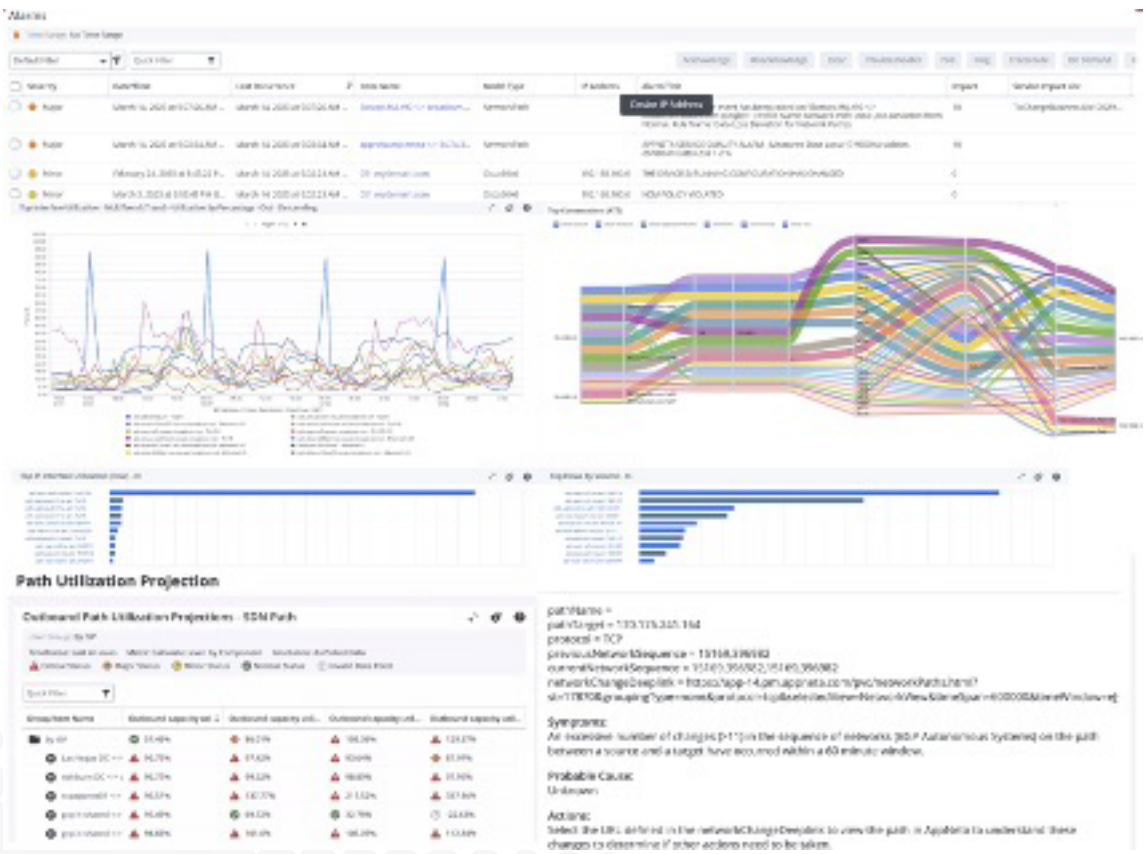
To reduce MTTR, network operations teams need end-to-end visibility and control over their IT networks and resources. They need to be able to monitor the user experience from end to end, with the ability to check every hop, every step, and every transaction—all in an intuitive and easy-to-use interface. This way, they can quickly identify where issues are occurring and isolate the root cause of the problem. For example, with this visibility, an operator can determine that the user's home network, ISP, and transit networks are fine, but that the cloud service provider's environment is experiencing an outage. As a result, they can quickly prove the innocence of the internal network, and take details about the issue to the cloud provider to escalate resolution. In addition, they can seek to find a workaround to establish the required connectivity for users.

To regain full network monitoring visibility and control, teams need to collect, correlate, and analyze network and user experience data from all networks—regardless of who owns the infrastructure. This means having unified views of physical infrastructures, virtual machines, and containers, including across different generations of network infrastructure. Teams need this visibility, even if these systems are hosted in ISP, cloud, and SaaS environments.

Unified Portal

NetOps by Broadcom provides a single unified portal that visualizes and transforms inventory, topology, device metrics, logs, configurations, faults, and flows into actionable insights for network operations teams. The solution provides end-to-end network visibility by correlating data from various sources, delivering a unified and holistic view of the network's health and performance at a glance. This makes it easier to track issues, analyze trends, and collaborate efficiently across teams.

The solution can route end-user experience metrics through the standard operating procedures and workflows that network specialists depend on. By leveraging comprehensive analytics, network operations teams can triage easily, find root causes quickly, escalate to engineers or architects, and open trouble tickets. Ultimately, teams can efficiently isolate and resolve the network delivery issues that degrade user experiences.



Maximizing Standard Operating Procedures

Modern network operations teams face the challenge of scaling up internet connectivity in a fast and cost-effective way. To achieve this, many organizations are adopting SD-WAN/SDDC solutions that offer flexibility and efficiency. At the same time, wireless technologies have continued to proliferate and are now the de facto standard for hybrid work, enterprise LAN, and campus environments. SD-WAN/SDDC and Wi-Fi are key components of modern networks, but they also add complexity for network operations teams. To manage the modern network effectively, teams need to be more diligent in adhering to standard operating procedures and leverage automation where possible.

NetOps by Broadcom provides standardized workflows and processes to cover both traditional network monitoring for the data center, and new areas such as the connectivity path to cloud, SaaS, enterprise sites, and campus or branch Wi-Fi networks. Ultimately, equipped with intuitive visualizations and customizable dashboards, network specialists can easily interpret complex data, identify potential issues, and manage network resources more consistently and effectively.

The solution provides proven insights that can help teams achieve efficiencies in their standard operating procedures and workflows. The solution's tested and simple workflows enable level 1 and 2 operations staff to do quick troubleshooting. This means that a level 1 NOC operator can access enough insights, intelligent data, and simple troubleshooting workflows to identify and isolate end-user experience issues, without needing to escalate to a network engineer or architect. Further, level 3 experts can get detailed visibility into performance, fault, and flow, across traditional and software-defined environments, as well as networks they do not control, such as ISP and cloud environments.

The Broadcom solution collects metrics from different networks and devices, regardless of their technology or vendor. With embeddable dashboards and APIs, users can easily rollup and integrate their network metrics with other visualization tools for reporting. For example, network operations directors can see the status of each site group in their region on a SharePoint dashboard, while a network engineer can use a Grafana dashboard to dive deeper into the performance of all servers. Operators can adjust the dashboards and views to fit their needs and use predefined workflows to streamline operations. These features give teams the most efficient way to gain visibility and control over their network-based services.

CONCLUSION

When network operations teams are reliant upon multiple, redundant tools to monitor network performance, it introduces significant inefficiencies and challenges, and those challenges only continue to grow more pronounced.

With disparate tools in place, teams contend with higher costs, the complexity of maintaining multiple products, and inconsistent or conflicting data and alerts from different sources. Further, these siloed tools leave teams with gaps in visibility, which makes it difficult to identify the root cause of issues and resolve them quickly.

Further, today's modern environments are increasingly reliant upon externally managed networks of cloud providers and ISPs, which threatens to further diminish the visibility and control of network operations teams. Therefore, now is the right time to review your network observability and management strategies, and find ways to establish end-to-end coverage and gain full network visibility and control.

In today's digital world, ensuring that end users consistently receive quality experiences is vital. It's critical to track the user experience, and to have the capabilities required to ensure responsive, reliable services are delivered consistently. By establishing this visibility with a single solution, teams can significantly streamline their standard procedures and workflows.

Broadcom delivers advanced solutions that enable teams to validate whether users are experiencing reliable, responsive connectivity. With NetOps by Broadcom, teams can enjoy the efficiency benefits of standardizing on a single solution, and gain unified visibility of both internal and externally managed networks.

DIVERSIFIED FINANCIAL SERVICES FIRM RATIONALIZES TOOLS AND REDUCES COST

The network operations team in a leading financial services institution needed to establish full visibility of internal and externally managed networks, without having to rely on multiple network monitoring tools.

In prior years, they had been contending with tool sprawl, which continued to create increasing complexity and cost. Their previous network monitoring tools offered limited coverage. This limited visibility grew more acute as the organization continued to employ software-defined networking and modern wireless technologies. Ultimately, in spite of all the tools employed, they only had visibility of approximately 60% of all the objects and interfaces the business relied upon.

By adopting NetOps by Broadcom, the financial services firm enhanced its network coverage from end to end. The network operations team eliminated network monitoring blind spots and regained control by integrating end-user experience metrics into their standard procedures and workflows. With a unified view of both internal and externally managed networks, the team was able to rationalize its tool sets. By retiring unnecessary and redundant network monitoring tools, the team realized significant savings, reducing its software licensing, maintenance, and operational costs.

WHY BROADCOM

For many network operations teams today, network observability and management is extremely challenging and costly. These teams are struggling to use and maintain multiple tools, while contending with blind spots and a lack of control.

Broadcom offers a highly scalable, comprehensive solution that can help you overcome these challenges. NetOps by Broadcom offers end-to-end network visibility, providing complete coverage of the networks you manage, and even those you don't. Our solution enables you to manage your network with a flexible and comprehensive solution that works with any vendor, technology, or protocol.

The solution can collect and analyze different network metrics from any point, from the client to the cloud. The solution can track diverse metrics, including utilization, throughput, latency, jitter, packet loss, errors, congestion, quality of service, and end-user experience. This end-to-end visibility of your network can help you quickly and accurately detect and fix any problems and improve network performance and operational efficiency.

With NetOps by Broadcom, you can gain unified visibility across your internal and externally managed environments, reduce operational and software costs, minimize downtime, improve service quality, and enhance the user experience.

BROADCOM
connecting everything®

For more information, visit our website at: www.broadcom.com

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

end-to-end-coverage-wp-2024-01-18 January 18, 2024