

WHITE PAPER

Tame the Complexity of Software-Defined WANs and Hybrid Networks

TABLE OF CONTENTS

Challenge	2
Best Practices	3
Unified Observability Across Vendors and Technologies	4
Managing Multi-Vendor Infrastructures	4
Monitoring Multi-Edge Infrastructure.....	7
Streamlined Operational Workflows	10
Managing Overlay and Underlay Performance	10
Automating the Triage of Issues	15
Automated Root Cause Identification	16
Anomaly Detection	16
Experience-Driven Triage	16
Integration with ITSM Tools	16
Unbiased Deployment Validation	17
Validating Against Pre- and Post-Deployment Baselines.....	17
Validating Against End-User Experience.....	21
Conclusion	24
Service Provider Boosts Monitoring Scale by 50%.....	24
Telecom Company Increases Operational Efficiencies by 70%.....	25
Why NetOps by Broadcom	25

CHALLENGE

As organizations around the world increase their dependence on cloud-based service models like software-as-a-service (SaaS), storage-as-a-service, and unified communications, they add pressure on their wide area network (WAN) infrastructure. These infrastructures contend with increasing traffic as users access distributed services from various third-party providers. These networks must also support the traffic flows generated by users located in remote branch offices. Traditional network infrastructures rely on private links that backhaul traffic through the data center. As the reliance on cloud-based service models continues to grow, these networks can quickly become a performance bottleneck.

Because of these realities, software-defined wide area networking (SD-WAN) technology is being broadly adopted. Decision-makers primarily choose SD-WAN because it enables their organizations to build higher performance WANs using lower cost and commercially available Internet access. SD-WAN technology is also ideally suited to the distributed networking environment that supports cloud transformation. However, the number of failed SD-WAN deployments is surprisingly high. In fact, one survey found that just 38% of IT professionals believed their SD-WAN implementations have been fully successful.¹

The main reason for this lack of success is that shifting from traditional WAN to SD-WAN technologies introduces a new set of challenges:

- **Increased complexity.** Organizations continue to grow less reliant on data centers to secure and route internet-bound traffic from remote offices and branches. Given this move, performance monitoring must increasingly occur at every branch location. As a result, network operations can rapidly be overwhelmed as they grapple with managing the growing number of tunnels connecting remote branches to critical cloud applications.
- **Limitations of native monitoring tools.** Most SD-WAN platforms offer native capabilities to monitor some aspects of application and network performance. However, these offerings only monitor from network edge to network edge, and can only support one specific SD-WAN vendor technology. Consequently, network teams face challenges in maintaining visibility into multi-vendor landscapes and identifying and addressing performance issues that occur along network delivery paths.
- **Dynamic traffic patterns.** Organizations continue to adopt unpredictable transports, such as internet broadband connections that are used in place of MPLS. This leaves organizations more exposed to latency and routing issues. While SD-WAN tools offer some visibility into the overlay, they often lack insight into the underlay network, especially circuits operated by third-party providers. This limits network teams' ability to pinpoint the root cause of performance degradation, which makes it difficult to hold internet service providers (ISPs) and cloud providers accountable.
- **Skill gaps.** Many organizations lack the internal skills required to deploy SD-WAN effectively. Consequently, teams increasingly rely on service providers to handle their implementations or fully outsource network management. However, the service provider may not have the business and domain expertise needed to understand the organization's specific applications and requirements.

SD-WAN is a cost-effective and flexible alternative to traditional WANs, but the high rate of failed deployments indicates that achieving a successful implementation is not as straightforward as it seems. To deploy SD-WAN effectively, IT and network operations teams must be prepared to address these challenges and embrace new approaches to network management. By doing so, organizations can dramatically increase their chances of successfully deploying SD-WAN and fully leveraging the significant benefits this technology offers.

In this white paper, we discuss how organizations usually address the challenges of WAN modernization and we examine best practices that can help network operations teams manage SD-WAN and its associated complexity.

¹ EMA Research, "WAN Transformation with SD-WAN: Establishing a Mature Foundation for SASE Success," Shamus McGillicuddy, April 2023

BEST PRACTICES

Companies often struggle to find and retain skilled personnel for network deployment, management, and support, hindering their ability to adapt to the ever-changing digital landscape. Consequently, it is not surprising to see recent findings showing that 66% of IT organizations prefer to consume SD-WAN as a managed service.²

However, if managed SD-WAN has tangible advantages, it also has some shortcomings. Since a critical portion of the network is operated by a third party, it can be difficult for teams to customize deployments to meet their business' unique requirements. Introducing yet another outsourced silo can also thwart the flexibility promised by SD-WAN and ultimately reduce business agility. Even if teams choose to outsource SD-WAN administration, they will still need a network performance monitoring system that can help ensure their SD-WAN deployment addresses their organization's performance requirements.

Actually, many organizations mix and match SD-WAN capabilities to create customized solutions that better meet their needs. Different vendors may excel in distinct areas, such as integrated security, advanced cloud connectivity, intelligent routing, or SD-Branch. But working with multiple vendors introduces more complexity. Each vendor offers management capabilities in their SD-WAN equipment, however these technologies are typically incompatible with other vendors' solutions. This leads to gaps in visibility and limited control over the network.

Network professionals typically follow a set of standard operating procedures to triage network performance issues. They may issue a ping command, do a traceroute, open trouble tickets, and escalate issues to engineers or architects. Typically, they have to use multiple tools and administrative consoles from distinct vendors to work through each step of the triage process. Moreover, many IT teams continue to focus solely on network performance data, rather than starting investigations with application and end-user experience metrics. As a result, teams spend the bulk of their time firefighting up/down issues, with no insight into the impact on the digital experience.

Finally, another important aspect of SD-WAN implementation is preparing and planning for deployment. These efforts require a deep understanding of the applications running in production, their traffic characteristics, and the quality of service required from the network. This latter step is a crucial one because the service level delivered by the network ultimately translates into the quality of the end-user experience. In many organizations, teams fail to plan adequately for deployments. As a result, teams don't achieve the desired traffic shaping—and that, in turn, has a negative impact on the overall digital experience. In the worst case, in organizations that cannot reap the benefits of their SD-WAN implementation, leaders might decide to roll back to their legacy WAN infrastructure.

To manage SD-WAN effectively and establish a reliable and efficient environment that meets the demands of the modern WAN, teams need to adhere to these key best practices:

- **Establish unified observability** across SD-WAN vendors and the other traditional networking technologies that make up today's enterprise networks.
- **Create streamlined operational workflows** that bring efficient SD-WAN management within reach of NOC teams.
- **Employ unbiased deployment validation** to objectively gauge the success of SD-WAN implementations.

The following sections offer a detailed look at each of these best practices.

² EMA Research, "WAN Transformation with SD-WAN: Establishing a Mature Foundation for SASE Success," Shamus McGillicuddy, April 2023

UNIFIED OBSERVABILITY ACROSS VENDORS AND TECHNOLOGIES

Many organizations are adopting a multi-vendor approach to SD-WAN for a couple key reasons. First, using different vendors may provide access to specialized capabilities that meet specific requirements. For example, teams at large office campuses or remote industrial sites may require different vendors and specialized hardware in order to fulfill their unique needs for bandwidth and security. 43% of companies now use multiple SD-WAN vendors to address the needs of connecting different kinds of sites.³ Second, within large organizations, multiple business units can have distinct technology strategies and requirements, which also results in the adoption of multiple vendors.

Real-Life Challenges Reported by IT Professionals

“I have to use two or three tools to troubleshoot an issue. As an experienced network engineer, it’s easy for me to correlate that data across tools, but if I present that data to a non-expert, he would have a hard time correlating it.”⁴

Incorporating monitoring of different SD-WAN vendors into unified network management workflows is a must to reduce silos, optimize post-deployment operations, and ensure robust infrastructure monitoring. Here are some key requirements for establishing holistic visibility across the WAN infrastructure and enabling NOC teams to handle the complexity of SD-WAN environments.

Managing Multi-Vendor Infrastructures

One of the primary hurdles for managing multi-vendor SD-WAN landscapes is the inherent complexity that arises from dealing with various toolsets from different vendors. Each vendor typically has its proprietary protocols, management interfaces, and feature sets, making it challenging to achieve seamless interoperability and consistent network policies across the entire network.

Overall, 87% of companies are experiencing at least one significant problem with SD-WAN. Typically, there are two major issues: network team skills gaps and a lack of defined processes and best practices.⁵ Multi-vendor SD-WAN also requires network teams to develop expertise with different vendors and technologies, which exacerbates the skill shortage being experienced in many organizations. While devices may have some similar capabilities, the depth of knowledge required varies from one vendor’s solution to another. Some SD-WAN platforms might be fully managed using a centralized user interface, while some others might still need access to configuration files and a command line interface (CLI).

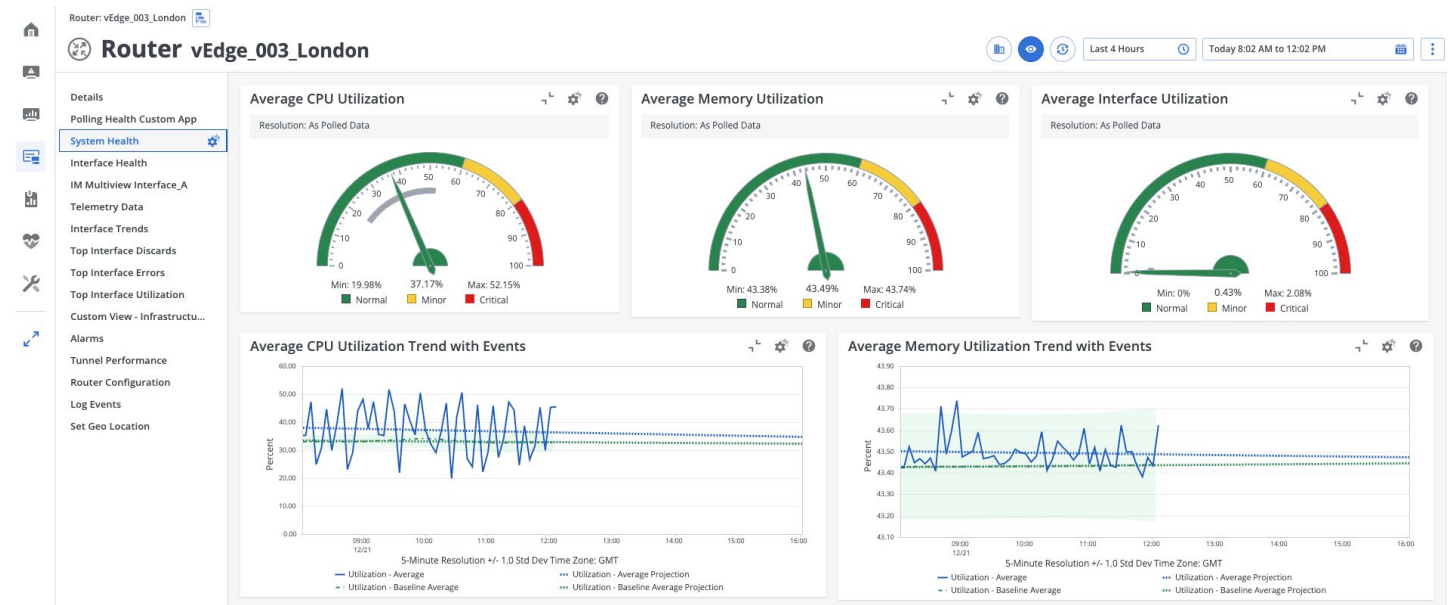
³ EMA Research, “WAN Transformation with SD-WAN: Establishing a Mature Foundation for SASE Success,” Shamus McGillicuddy, April 2023

⁴ EMA Research, “Network Management Megatrends 2022: Navigating Multi-Cloud, IoT, and NetDevOps During a Labor Shortage,” Shamus McGillicuddy, April 2022

⁵ EMA Research, “WAN Transformation with SD-WAN: Establishing a Mature Foundation for SASE Success,” Shamus McGillicuddy, April 2023

When it comes to managing technologies from multiple SD-WAN vendors, a best practice is to establish holistic network observability. To do so, teams need a solution that can provide insights into the entire network, including across multiple SD-WAN platforms.

NetOps by Broadcom offers unified, scalable, and comprehensive monitoring of multi-vendor SD-WAN and legacy WAN technologies. The solution extends the native management capabilities of SD-WAN controllers. The solution delivers multi-vendor indicators that enable NOC users to monitor alarms, identify the cause of issues, and create operational dashboards.



NetOps by Broadcom delivers cross-vendor metrics that enable NOC users to leverage unified monitoring dashboards.

Access to multi-vendor metrics enables NOC teams to gain insights into the performance of each component in the network and simplifies day-to-day operations. This data facilitates proactive optimization, allowing for the adjustment of configurations and policies to ensure optimal performance across the entire SD-WAN ecosystem.

The solution delivers cross-vendor metrics and inventory, providing holistic visibility that allows IT teams to monitor and analyze network performance comprehensively. The following table details the coverage provided:

	JUNIPER (128T)	CISCO MERAKEI	FORTINET	NOKIA NUAGE	HPE ARUBA (SILVER PEAK)	VERSA	CISCO VIPTELA	VMWARE VELOCLOUD
Sites	X	X	X	X	X	X	X	X
Controller	X	X	X	X	X	X	X	X
Routers/Devices	X	X	X	X	X	X	X	X
CPU	X	X	X	X	X	X	X	X
Memory	X		X	X	X	X	X	X
Storage			X	X			X	X
Interfaces/Links	X	X	X	X	X	X	X	X
Packets In	X	X	X	X	X	X	X	X
Packets Out	X	X	X	X	X	X	X	X
Bytes In				X	X	X	X	X
Bytes Out				X	X	X	X	X
Speed					X	X	X	X
Tunnels	X	X	X	X	X	X	X	X
Jitter	X	X	X	X	X	X	X	X
Latency	X	X	X	X	X	X	X	X
Packet Loss	X	X	X	X	X	X	X	X
Capacity	X	X	X	X	X	X	X	X
Bytes In			X		X		X	X
Bytes Out			X		X		X	X
Speed					X			X
Apps/SLA paths	X		X	X	X	X	X	X
Jitter	X		X	X	X	X	X	
Latency	X		X	X	X	X	X	
Packet Loss	X		X	X	X	X	X	
Quality								X
Alarms/Events	X	X	X	X	X	X	X	X

As network teams continue to be stretched thin, Broadcom enables users to leverage their existing skills and operational processes in managing multi-vendor SD-WAN infrastructures, enabling improved economics and service assurance.

Monitoring Multi-Edge Infrastructure

As organizations adopt SD-WAN to optimize connectivity across distributed networks, the number of possible communication paths continues to multiply, introducing complexities in monitoring and managing network traffic. When moving to multi-edge networks, teams need to partner with trusted monitoring vendors who can help them harness all the potential of their SD-WAN deployments.

The sheer number of SD-WAN tunnels can overwhelm teams using traditional monitoring solutions, making it difficult to identify specific issues affecting network performance. Additionally, the dynamic nature of SD-WAN, where tunnel settings are established or modified in response to changing network conditions, requires adaptation in real-time.

To understand the scope of the challenge, it is important to recognize the number of possible communication paths data can take to be delivered across an SD-WAN infrastructure:

SD-WAN star topology example

$200 \text{ (sites)} \times 2 \text{ (data centers)} \times 2 \text{ (edge routers)} = 800 \text{ models (tunnels)}$

$800 \text{ Tunnels with 4 defined SLAs} = 800 \times 4 = 3200 \text{ models (SLAs)}$

SD-WAN full mesh topology example

$200 \text{ (sites)} \times 200 \text{ (sites)} \times 2 \text{ (edge routers)} = 80,000 \text{ models (tunnels)}$

$80,000 \text{ tunnels with 4 defined SLAs} = 80,000 \times 4 = 320,000 \text{ models (SLAs)}$

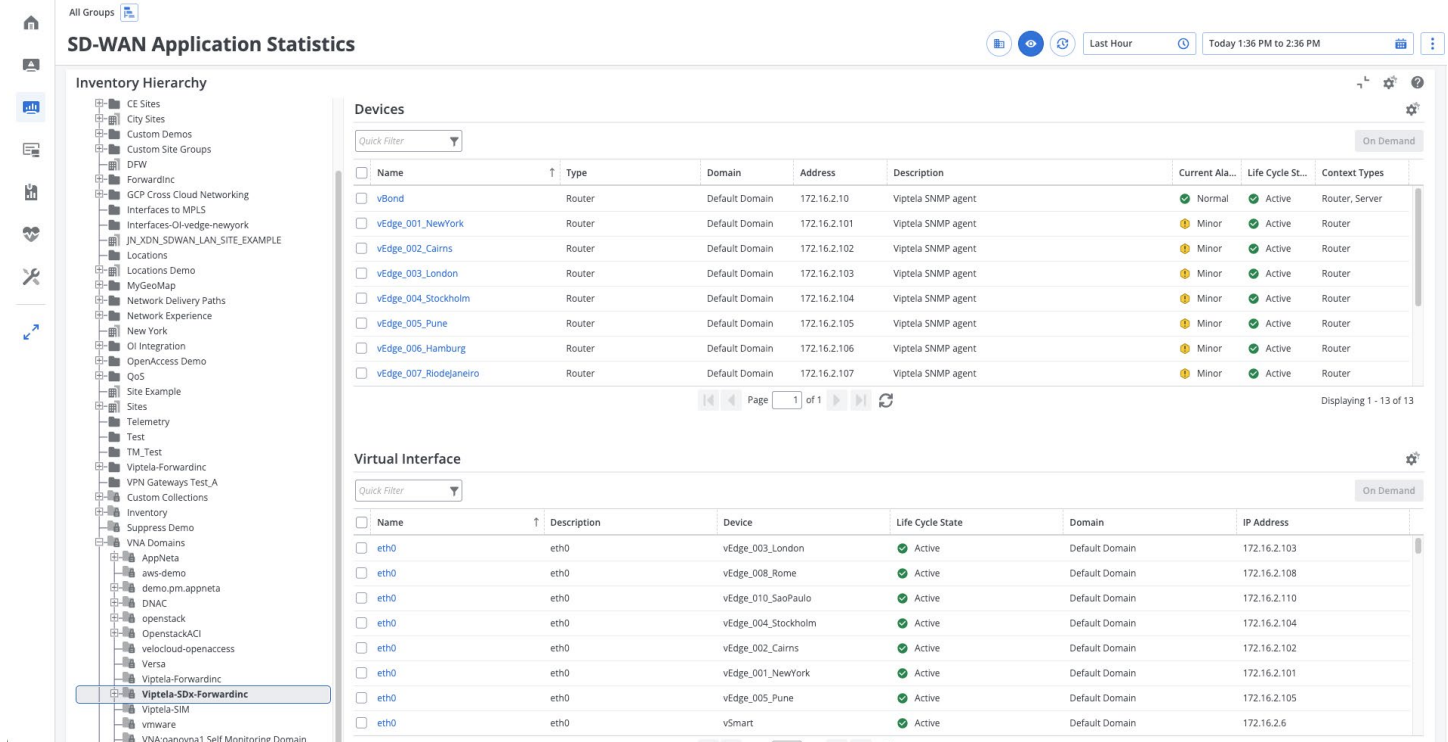
SD-WAN introduces a significant increase in the number of elements requiring management, particularly for extensively distributed organizations. Within the overlay network alone, the number of tunnels may surpass one hundred thousand. Furthermore, when considering the underlay, the potential communication paths multiply with each ISP network the packets traverse. Ultimately, the lack of visibility in between the enterprise network's edges can result in a lack of control for the network operations team. However, this issue will be further explored in subsequent sections of this white paper.

NetOps by Broadcom is based on a distributed architecture, making it one of the most scalable network monitoring platforms on the market. With the solution, network teams can manage large-scale SD-WAN deployments that feature thousands of sites with hundreds of thousands of tunnels. The solution incorporates all associated edge devices. The solution can include both primary and secondary systems in device inventories and offer views by location.

Here are some of the key elements of the environment:

- **Folders.** The solution creates folders that are specific to each type of technology.
- **Sites.** The solution creates sites automatically by discovering the SD-WAN landscape.
- **Groups.** Site groups represent source and destination targets. When communicating with controllers, the solution polls edge routers. All devices can be coalesced into site groups.
- **Geolocation.** Upon device discovery, the solution assigns longitude and latitude, making it easy to group elements by region and to view devices on a map.

The use of folders makes it easy to drill down into all devices in a particular domain. For example, a user can create a filter in order to see only controllers from a specific SD-WAN vendor. This visibility can provide powerful insights. For example, a user can view utilization metrics for a specific region and quickly see numbers for a specific interface are extremely high.



SD-WAN Application Statistics | Last Hour | Today 1:36 PM to 2:36 PM

Inventory Hierarchy

- CE Sites
- City Sites
- Custom Demos
- Custom Site Groups
- DFW
- Forwardinc
- GCP Cross Cloud Networking
- Interfaces to MPLS
- Interfaces-Oi-vedge-newyork
- JN_XDN_SDWAN_LAN_SITE_EXAMPLE
- Locations
- Locations Demo
- MyGeoMap
- Network Delivery Paths
- Network Experience
- New York
- Oi Integration
- OpenAccess Demo
- QoS
- Site Example
- Sites
- Telemetry
- Test
- TM_Test
- Viptela-Forwardinc
- VPN Gateways Test_A
- Custom Collections
- Inventory
- Suppress Demo
- VNA Domains
- AppNeta
- aws-demo
- demo.pm.appneta
- DNAC
- openstack
- OpenstackACI
- velocloud-openaccess
- Versa
- Viptela-Forwardinc
- Viptela-SDx-Forwardinc**
- Viptela-SIM
- vmware
- VNA-coanovm1 Self Monitoring Domain

Devices

Name	Type	Domain	Address	Description	Current Ala...	Life Cycle St...	Context Types
vBond	Router	Default Domain	172.16.2.10	Viptela SNMP agent	Normal	Active	Router, Server
vEdge_001_NewYork	Router	Default Domain	172.16.2.101	Viptela SNMP agent	Minor	Active	Router
vEdge_002_Cairns	Router	Default Domain	172.16.2.102	Viptela SNMP agent	Minor	Active	Router
vEdge_003_London	Router	Default Domain	172.16.2.103	Viptela SNMP agent	Minor	Active	Router
vEdge_004_Stockholm	Router	Default Domain	172.16.2.104	Viptela SNMP agent	Minor	Active	Router
vEdge_005_Pune	Router	Default Domain	172.16.2.105	Viptela SNMP agent	Minor	Active	Router
vEdge_006_Hamburg	Router	Default Domain	172.16.2.106	Viptela SNMP agent	Minor	Active	Router
vEdge_007_Riodejaneiro	Router	Default Domain	172.16.2.107	Viptela SNMP agent	Minor	Active	Router

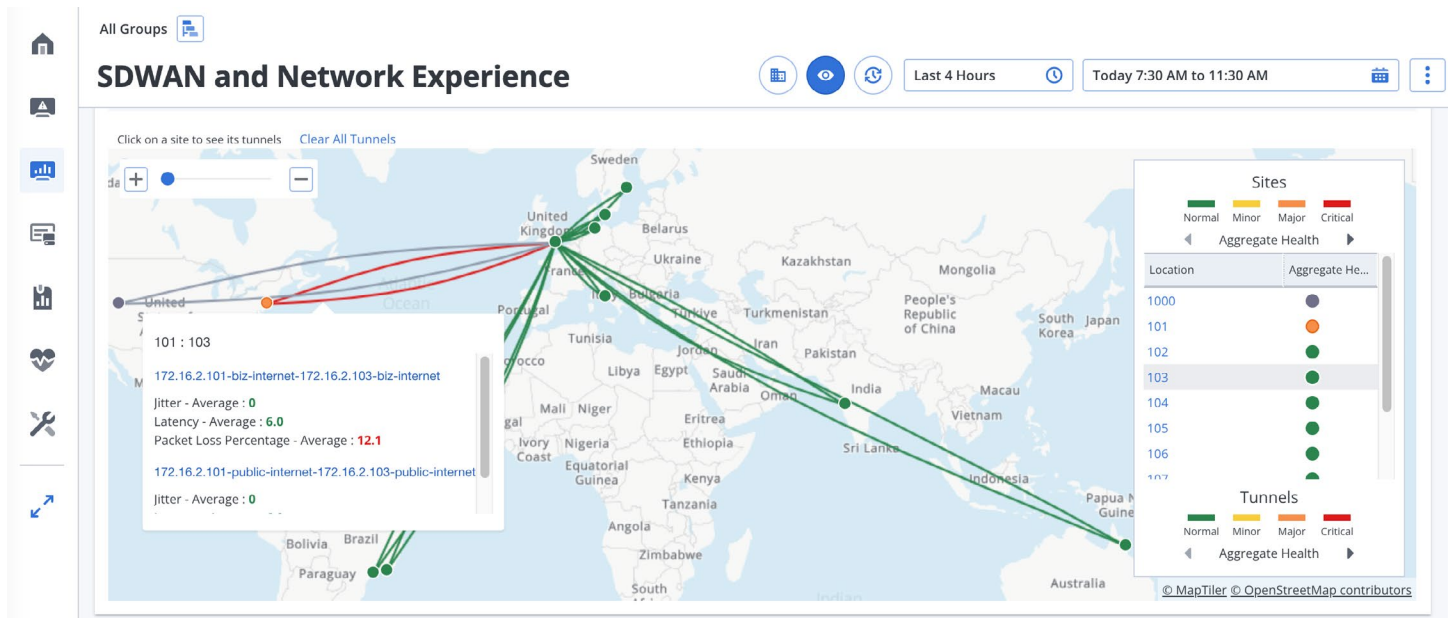
Page 1 of 1 | Displaying 1 - 13 of 13

Virtual Interface

Name	Description	Device	Life Cycle State	Domain	IP Address
eth0	eth0	vEdge_003_London	Active	Default Domain	172.16.2.103
eth0	eth0	vEdge_008_Rome	Active	Default Domain	172.16.2.108
eth0	eth0	vEdge_010_SaoPaulo	Active	Default Domain	172.16.2.110
eth0	eth0	vEdge_004_Stockholm	Active	Default Domain	172.16.2.104
eth0	eth0	vEdge_002_Cairns	Active	Default Domain	172.16.2.102
eth0	eth0	vEdge_001_NewYork	Active	Default Domain	172.16.2.101
eth0	eth0	vEdge_005_Pune	Active	Default Domain	172.16.2.105
eth0	eth0	vSmart	Active	Default Domain	172.16.2.6

NetOps by Broadcom uses groups to organize network items into logical categories.

The solution also provides map views that allow NOC teams to see the physical and logical topology of the SD-WAN network at a glance. These views deliver insights into the current network paths between different locations. This is particularly useful for understanding how well traffic is being delivered across the network and whether transmissions are aligned with defined policies. In the event of network issues, having a visual representation of the SD-WAN infrastructure can significantly speed up the troubleshooting process. Network specialists can pinpoint the location of problems and take corrective actions more efficiently.



The solution monitors devices from a wide range of SD-WAN vendors and provides holistic maps and dashboards from a single console.

As organizations embrace SD-WAN for enhanced network connectivity, the resultant surge in communication paths presents increased monitoring and management challenges. Broadcom delivers a robust platform that is capable of addressing the scalability demands posed by large-scale SD-WAN deployments and empowering network teams to efficiently navigate the complexities of these environments.

STREAMLINED OPERATIONAL WORKFLOWS

Traditional network management is highly manual in nature, requiring skilled engineers who can perform management tasks using a command line interface or proprietary tools. With fewer personnel available and infrastructures experiencing constant growth and flux, there are not enough experts to efficiently manage and troubleshoot configurations and issues. This leaves organizations exposed to the increased risk of operational disruptions.

This situation is exacerbated by the influx of events generated by all the diverse devices and tools in place, which can routinely flood users with alerts. This event volume makes it difficult to sift through every alert and identify genuine problems that require attention. As a result, in the average IT organization, end users still detect and report 31% of all service problems before network operations teams are aware of them.⁶

Real-Life Challenges Reported by IT Professionals

“We’re doing a good job of keeping the network up and running, but the number of pending tickets for low-impact incidents is usually around 1,000. We need to develop automation focused on dealing with those.”⁷

Here are some key requirements for establishing workflows that can help NOC teams to manage SD-WAN environments more efficiently.

Managing Overlay and Underlay Performance

One of the more exciting features of SD-WAN is its ability to decouple the data plane from the control plane, which creates the notion of overlay and underlay. The underlay refers to the physical infrastructure, including routers, switches, and various transports (such as MPLS, internet broadband, and wireless). The underlay handles the actual data transmission and routing between the different network locations. On the other hand, the overlay is an abstracted layer that operates on top of the underlay. The overlay is managed and orchestrated by SD-WAN controllers and enables intelligent traffic steering, path selection, and prioritization.

SD-WAN platforms typically provide a degree of visibility for the overlay, but they offer only limited or no insight into the underlay network, especially for circuits operated by third-party providers. This makes network teams ill-equipped to determine the root cause of performance degradation. In other words, those teams struggle to infer whether the corporate network, an ISP, or a cloud provider should be held accountable as the source of a problem. As a consequence, the biggest issue reported by network teams is a lack of end-to-end insight across the SD-WAN overlay and underlay.⁸ The native capabilities of SD-WAN tools leave visibility gaps that NetOps by Broadcom can address, as outlined in the table below.

6 EMA Research, “Network Management Megatrends 2022: Navigating Multi-Cloud, IoT, and NetDevOps During a Labor Shortage,” Shamus McGillicuddy, April 2022

7 EMA Research, “Network Management Megatrends 2022: Navigating Multi-Cloud, IoT, and NetDevOps During a Labor Shortage,” Shamus McGillicuddy, April 2022

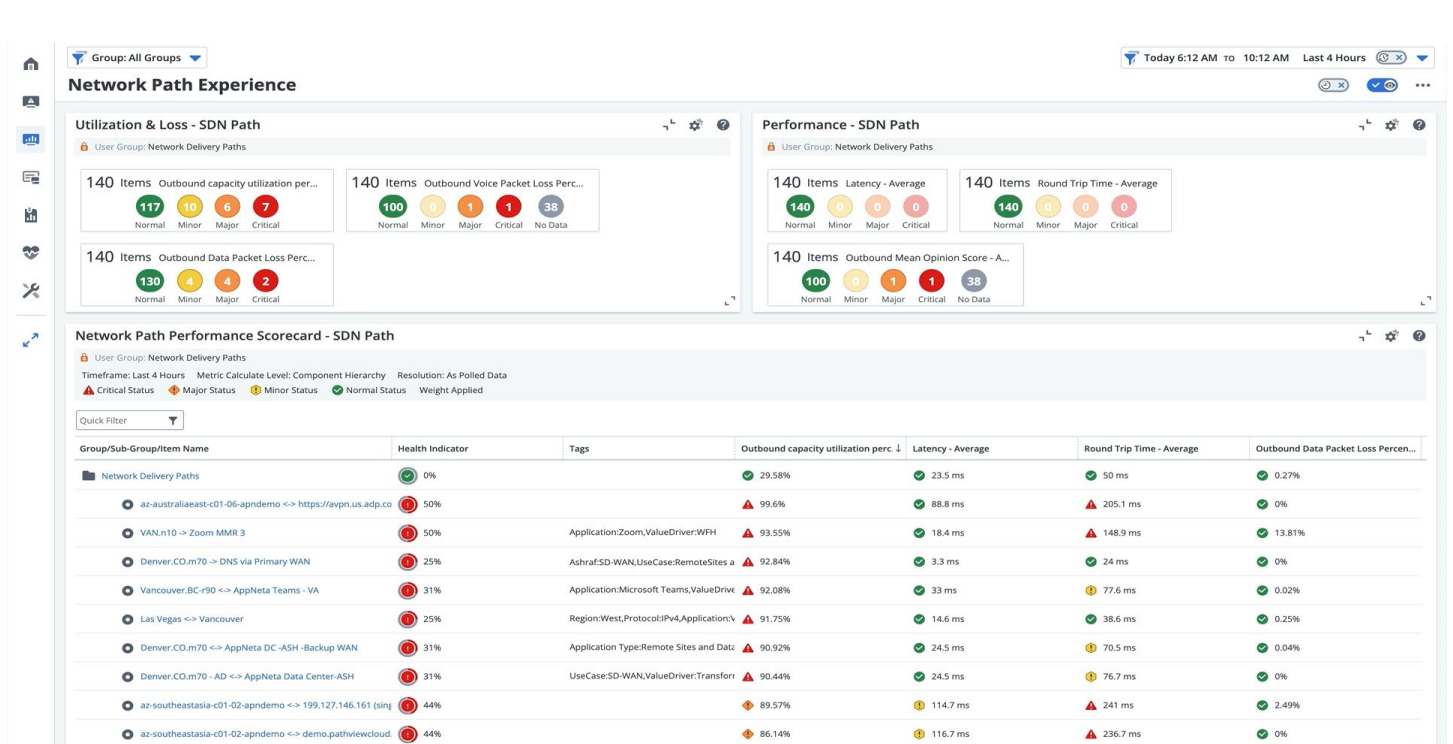
8 EMA Research, “WAN Transformation with SD-WAN: Establishing a Mature Foundation for SASE Success,” Shamus McGillicuddy, April 2023

SD-WAN NATIVE MONITORING CAPABILITIES

BROADCOM ADDITIONAL CAPABILITIES

Edge-to-Edge	End-to-End
Overlay	Underlay
Tunnel Performance	Hop-by-Hop Performance
SLA Path Performance	End User Experience
Site-to-Site	Site-to-Cloud, Cloud-to-Cloud
SD-WAN Infrastructure	Enterprise Infrastructure

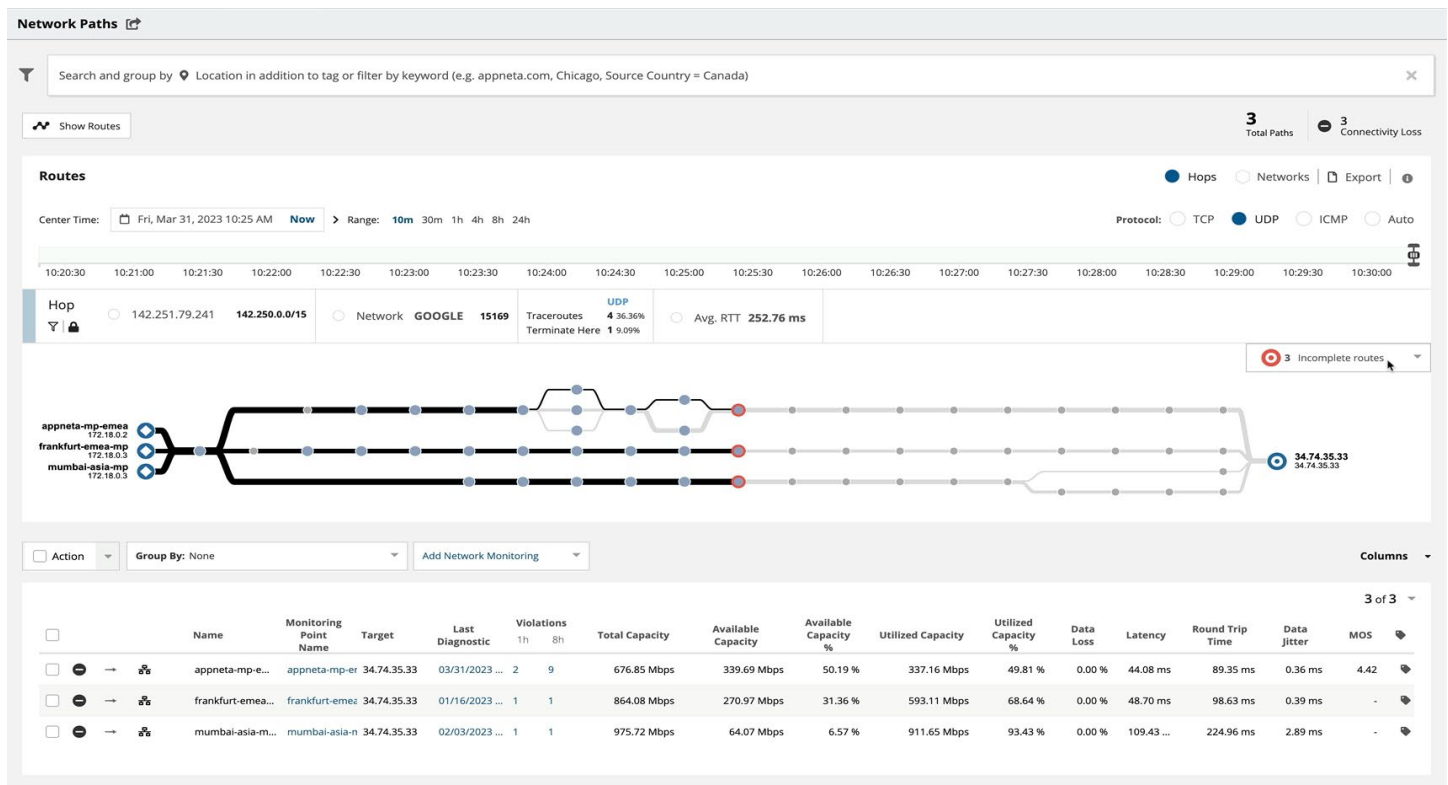
The Broadcom solution enables NOC teams to eliminate the monitoring roadblocks presented by SD-WAN platforms. The solution delivers the correlated intelligence that enables teams to effectively track, manage, and optimize their SD-WAN and legacy environments. With holistic visibility and effective baselines, the solution can distinguish between optimal and suboptimal performance of the overlay. At the same time, it can provide an end-to-end view of the underlay's performance, no matter where users or critical business applications may be. This enables network teams to expedite the identification of the root cause of software-defined infrastructure issues.



NetOps by Broadcom provides dashboards that help users to understand the overall health of network delivery across the SD-WAN infrastructure.

The solution offers rich statistics and performance metrics by collecting data about network devices and their performance, harnessing both SNMP and specific controller APIs supported by various SD-WAN platforms. By using controller APIs, network specialists can gain more valuable insights into interface statistics, CPU usage, memory utilization, SLA policies, and more.

The solution's overlay visibility is supplemented by the ability to monitor each hop of the underlay across ISPs and cloud service providers (CSP). These capabilities equip NOC teams with a true end-to-end perspective and also give SD-WAN specialists the ability to use actual network conditions to validate control plane measurements.



The Broadcom solution delivers hop-by-hop network analysis and troubleshooting through MPLS, SD-WAN pairings, CASB services, and directly over an ISP

The solution enables the visualization of the performance of the underlying network and determines where network problems are occurring. It uses continuous lightweight path analysis to determine if there are network problems and automatically initiates diagnostic tests to help pinpoint the cause. The analysis involves periodically sending out small bursts of packets to user-determined network targets and collecting timing data about the packets after they traverse the network. These capabilities help teams answer these types of questions:

- Where across the end-to-end network path is the problem occurring?
- Are there particular routes that are slow?
- What routes are down and when did they go down?
- How much capacity am I being provided by my ISP?
- How much of the available capacity am I using?

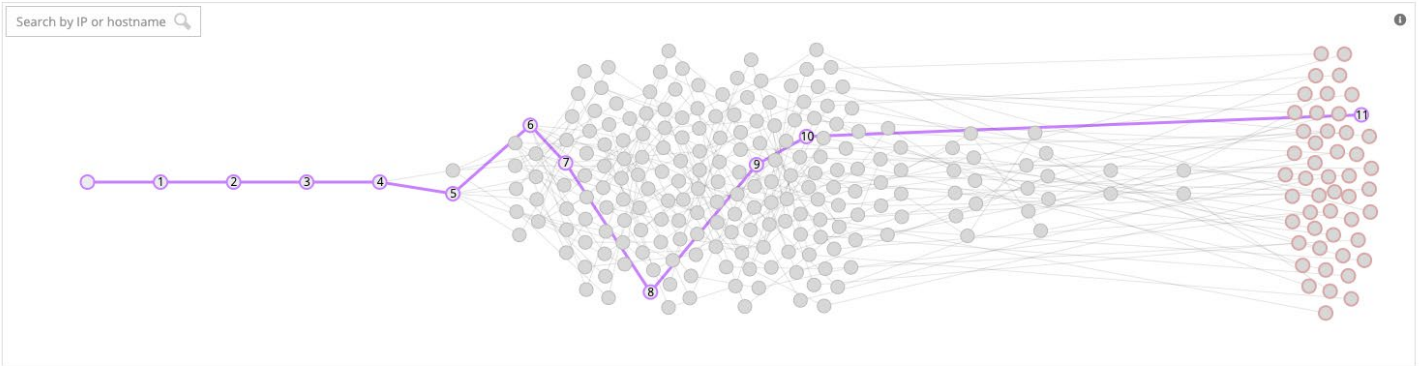
The solution can continuously monitor network paths—all the hops between a source and a target. To do so, the solution uses monitoring points that can act as the source, the target, or both endpoints. There are basically four types of monitoring points:

- Physical monitoring points. These are used for general monitoring and for monitoring in wireless networks and environments requiring high performance.
- Virtual monitoring points. These points are virtual machines that run in KVM or VMware virtual environments.
- Container-based monitoring points. These points can be run in environments that support Docker.
- Native monitoring points. These points run as an application on various operating systems.

Depending on the use case, monitoring points can be user managed and owned, user owned but Broadcom managed, and owned and managed by Broadcom.

TruPath is Broadcom's patented network performance monitoring technology. Implemented in monitoring points, TruPath represents the heart of the solution's network path monitoring. With minimal network load or impact, TruPath enables continuous monitoring, problem detection, and the discovery of changes. This technology probes a network using short bursts of packets ("packet trains") and waits for the replies. The solution can directly measure key network performance metrics, using information like the time the packets take to go from a source to a target and back, the delay between packets on their return, the reordering of packets, and the number of packets lost.

TruPath employs two distinct instrumentation modes: Continuous Path Analysis (CPA) and Deep Path Analysis (DPA). CPA mode runs continuously. Every 60 seconds, it sends 20-50 packets over the network to the target and analyzes the replies. If a network issue is detected, TruPath automatically shifts to DPA mode and runs a diagnostic test that probes not only the target but all intermediate devices on the network path between the source and the target. In this mode, no more than 400-2000 packets are sent in a series of packet trains in order to delve into the cause of the performance issue. Therefore, the overall load on the network is kept very low, typically averaging 2 Kbps for CPA and only 10-200 Kbps during a DPA diagnostic test. For very slow links or networks with other restrictions like small maximum MTU size, TruPath automatically adjusts its traffic loads to minimize network impact even further.

Route Details


Hop	IP Address	Host Name	RTT
1	2604:b040:1:2::1	2604:b040:1:2::1	0.29 ms
2	2001:668:0:3:ffff:2:0:21b9	xe-1-1-3-300.cr1-ren1.ip6.gtt.net	0.23 ms
3	2001:668:0:2:ffff:0:5995:b486	2001:668:0:2:ffff:0:5995:b486	7.04 ms
4	2001:668:0:3:ffff:2:0:1092	2001:668:0:3:ffff:2:0:1092	7.07 ms
5	2a01:111:2000:2:8000::731	2a01:111:2000:2:8000::731	13.0 ms
6	2603:10b0:b10:8101::a	2603:10b0:b10:8101::a	7.34 ms
7	2603:10b0:b10:8001::276	2603:10b0:b10:8001::276	7.37 ms
8	2603:10b0:b10:8305::142	2603:10b0:b10:8305::142	7.47 ms

The solution can retrieve and display a specific route based on accumulated route analysis records.

With fingers being pointed at the network whenever an application becomes slow, efficient issue identification is more important than ever. By using the Broadcom solution, network teams obtain comprehensive visibility and can readily demonstrate that performance issues occur within environments owned by ISPs and third-party providers. This allows them to resolve issues faster, eliminating the need to spend hours searching for the “needle in the haystack.” As a result, teams can reduce operational costs, while ensuring optimal performance throughout the enterprise network.

Automating the Triage of Issues

Tackling incidents in SD-WAN infrastructure poses several challenges due to the complexity of these dynamic networks. The infrastructure managing diverse types of network traffic and the constant adjustments to changing conditions make incident triage an intricate task. Featuring limited visibility, coupled with variability in policies and potential security implications, these environments demand a skilled workforce with expertise in troubleshooting. Vendor-specific nuances only add more layers of complexity to effective incident triage.

These challenges are compounded by the fact that many network operations teams have a shortage of SD-WAN experts available. When issues arise, front-tier operators often lack the insights they need, which means scarce, highly paid SD-WAN experts are routinely brought in to triage issues. This leads to lengthier troubleshooting efforts and proliferating costs. Further, given these limitations, teams are constantly wading through overwhelming numbers of tickets and are left reacting to issues rather than managing service levels proactively.

To overcome these limitations and successfully manage SD-WAN, teams need correlated intelligence and effective baselines, so they can distinguish between optimal and suboptimal performance. In addition, gaining an end-to-end understanding of network performance is paramount to identify emerging issues and address them before critical services are affected.

NetOps by Broadcom provides easy and intelligent workflows that enable level-one and level-two operations staff to accelerate triage. The solution provides level-one NOC operators with enough intelligence, insights, and data, so they can identify and isolate SD-WAN issues, without systematically escalating to a specialist or an architect. Further, the NOC team can identify issues that are occurring in networks they do not own, such as ISP and cloud environments.

The screenshot displays the 'Alarm Console' interface. At the top, there are filters for 'Group: All Groups' and a time range of 'Today 6:11 AM to 10:11 AM Last 4 Hours'. Below this is a table of alarms with columns for Severity, Date/Time, Last Occurrence, Item Name, Model Type, IP Address, Alarm Title, Impact, and Number of Occurrences. One alarm is selected, showing details for 'appneta-mp-emea <-> 34.74.35.33 (single)'. The details include a table for 'Alarm Details' and a text area for 'Event Details'.

Severity	Date/Time	Last Occurrence	Item Name	Model Type	IP Address	Alarm Title	Impact	Number of Occurrences	Service Impact List
Major	March 31, 2023 at 10:30:1...	March 31, 2023 at 10:30:1...	frankfurt-emea-mp <-> 34.74.35.33 (s...	NetworkPath		APPNETA SERVICE QUALITY ALARM - Connectivity has been lost (Could not connect to target)	10	1	TixChangeBusiness (0x10...
Major	March 31, 2023 at 10:29:4...	March 31, 2023 at 10:29:4...	appneta-mp-emea <-> 34.74.35.33 (s...	NetworkPath		APPNETA SERVICE QUALITY ALARM - Connectivity has been lost (Could not connect to target)	10	1	TixChangeBusiness (0x10...
Major	March 31, 2023 at 10:29:4...	March 31, 2023 at 10:29:4...	mumbai-asia-mp <-> 34.74.35.33 (sin...	NetworkPath		APPNETA SERVICE QUALITY ALARM - Connectivity has been lost (Could not connect to target)	10	1	TixChangeBusiness (0x10...
Critical	March 31, 2023 at 10:29:0...	March 31, 2023 at 10:29:0...	tixchange-appneta	IP Device	34.74.35.33	DEVICE HAS STOPPED RESPONDING TO POLLS	1	1	
Critical	March 30, 2023 at 4:19:16...	March 30, 2023 at 4:19:16...	R100.mydomain.com	Cisco3640	192.168.1...	DEVICE HAS STOPPED RESPONDING TO POLLS	1	1	
Minor	March 29, 2023 at 10:47:2...	March 31, 2023 at 10:02:2...	CE1.mydomain.com	Cisco3640	192.168.1...	THE DEVICE(S) RUNNING CONFIGURATION HAS CHANGED	0	96	
Major	March 29, 2023 at 10:43:5...	March 31, 2023 at 10:29:1...	mumbai-asia-mp <-> 34.74.35.33 (sin...	NetworkPath		APPNETA EXCESSIVE NETWORK CHANGES	10	2	
Major	March 29, 2023 at 10:43:2...	March 31, 2023 at 10:29:4...	frankfurt-emea-mp <-> 34.74.35.33 (s...	NetworkPath		APPNETA EXCESSIVE NETWORK CHANGES	10	2	

Alarm Details	Severity	Event Details
Impact: Management Lost	Major	A "apnSqevent" event has occurred, from NetworkPath device, named appneta-mp-emea <-> 34.74.35.33 (single). A trap to indicate that an SqeEvent has occurred.
Impact: Symptoms	Date/Time: March 31, 2023 at 10:29:45 AM Eastern Daylight Time	eventDetails = Connectivity has been lost (Could not connect to target)
Neighbor Topology	Item Name: appneta-mp-emea <-> 34.74.35.33 (single)	eventid = 5487765
Interfaces	IP Address	eventTime = 2023-03-31 14:29:00 UTC
Events	Model Type: NetworkPath	eventType = sqEvent
Log Events	Acknowledged: No	monitoringPointIp = 34.175.108.248
	Contact Person	pathGroup = appneta-mp-emea
	Troubleshooter: None	pathGroup = 35227
	Trouble Ticket ID: None	pathGroupName = Ticket Exchange
	Number of Occurrences: 1	pathEventDeliveryTime = 2023-03-31 14:29:45 UTC
	Impact: 10	pathId = 305206
		pathName =
		pathDesc = Auto-generated for web path
		pathTarget = 34.74.35.33
		pathTargetType = Auto
		sqMeasuredParameter = connectivityLoss

NetOps by Broadcom brings user-experience metrics into standard operating workflows for triage and root-cause identification.

AUTOMATED ROOT CAUSE IDENTIFICATION

The solution delivers unique root cause analysis capabilities. The solution automates troubleshooting by correlating and interpreting a set of symptoms and events, pinpointing the underlying cause, and generating an actionable alarm. These root cause analysis capabilities take advantage of patented inductive modeling technology, using a sophisticated system of models, relationships, and behaviors to create a digital representation of the infrastructure. The relationships that are established among the models provide a context for collaboration. This enables the solution to correlate symptoms with events or changes, suppress unnecessary alarms, and track the impact on users, customers, and services.

ANOMALY DETECTION

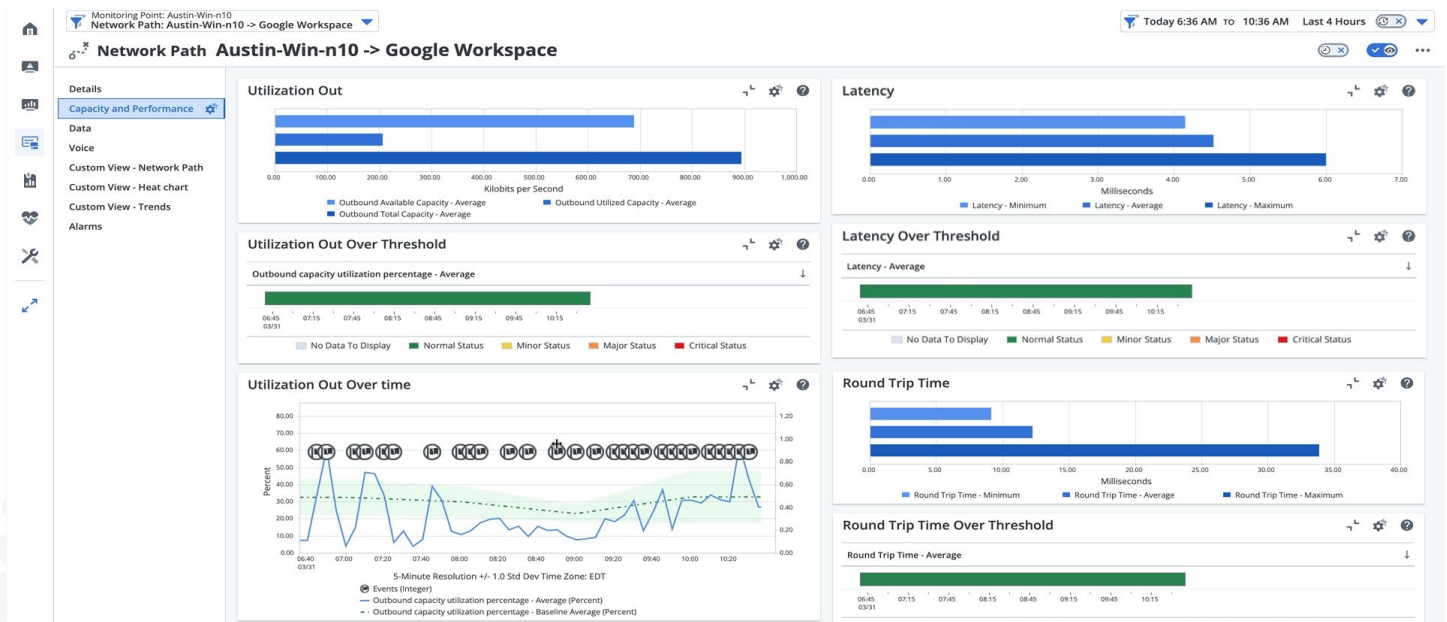
The Broadcom solution uses historical data and statistical analysis to establish a baseline of normal behavior, enabling the detection of anomalies that could be indicators of problems. The solution analyzes historical data to identify patterns, using a mix of device metrics, network traffic, user experience, error rates, and other relevant metrics. As more network data is collected, metrics are compared to established baselines. Any deviation that falls outside of an expected range is flagged as an anomaly and can trigger an alert.

EXPERIENCE-DRIVEN TRIAGE

The solution applies patented event correlation to network path performance and end-user experience alarms. This brings a new level of correlation to existing network and infrastructure alarms, helping NOC teams to understand how outages and performance issues are affecting actual application delivery and end-user experience. With these insights, network teams can prioritize remediation efforts based on actual business impact, rather than simply on alarm duration or severity.

INTEGRATION WITH ITSM TOOLS

The solution offers integration with third-party help desk ticketing systems. With this integration, events and alarms originating in the solution can populate ticketing systems with relevant device information and, in many cases, update and close the ticket once remediation is completed. The solution is directly integrated with CA Service Desk Manager, and it also natively supports third-party service desk applications, such as BMC Remedy, OpenText Service Manager, and ServiceNow. This allows NOC teams to get automated, real-time updates on the status of problems as they are triaged and resolved.



The Broadcom solution enables the definition of event rules that use standard deviation to compare the poll results to the baseline, for any path, device, or component.

Network operations teams have both a people problem and a technology problem. Broadcom's approach to network management eliminates both challenges, removing the technology and skills bottlenecks that prevent success. By bridging operational domains, the solution helps teams to better understand and manage the performance of digital services. By providing easy triage workflows that take the complexity out of finding the root cause of SD-WAN performance issues, the solution also helps reduce operational costs and improve service levels.

UNBIASED DEPLOYMENT VALIDATION

A comprehensive validation approach is required to ensure correct network delivery in the context of an SD-WAN migration. Gaining the right visibility before, during, and after SD-WAN deployment empowers network teams to budget more predictably and ensure they meet their scheduling goals. These capabilities even enable teams to deliver more cost-effective connectivity at remote locations.

According to one report, 57% of companies are updating their SD-WAN policies multiple times a year.⁹ However, most network organizations still lack adequate tooling for validating these changes—especially from the end-user experience perspective. At the same time, application delivery is getting more complex as it grows increasingly reliant on third parties, such as ISPs and CSPs. To gain a comprehensive understanding of the digital experience, network teams must establish accurate visibility of performance from the end-user perspective.

Real-Life Challenges Reported by IT Professionals

“Everyone was affected across the board, including our headquarters and our refineries. Those sites were going down and up on a recurring basis. The network team was literally running around and putting out fires every day. It was chaotic.”¹⁰

Here are some key requirements for effectively validating new deployments and configuration changes, ensuring SD-WAN operations do not have a negative impact on business activities.

Validating Against Pre- and Post-Deployment Baselines

In order to objectively gauge the success of SD-WAN implementations, it is important for teams to monitor and measure performance and establish effective baselines to be used before, during, and after their rollout. Here are some key activities for each phase of deployment:

- **Day 0 (Before).** Determine performance baselines against existing transports, remote location connectivity, and applications. Assess global connectivity needs, such as bandwidth and capacity.
- **Day 1 (During).** Apply continuous testing of network performance to identify issues causing bottlenecks and determine mitigation measures before full deployment.
- **Day 2 (After).** Verify network performance against initial baseline measurements and expected outcomes, especially for changes related to service level policies.

⁹ EMA Research, “WAN Transformation with SD-WAN: Establishing a Mature Foundation for SASE Success,” Shamus McGillicuddy, April 2023

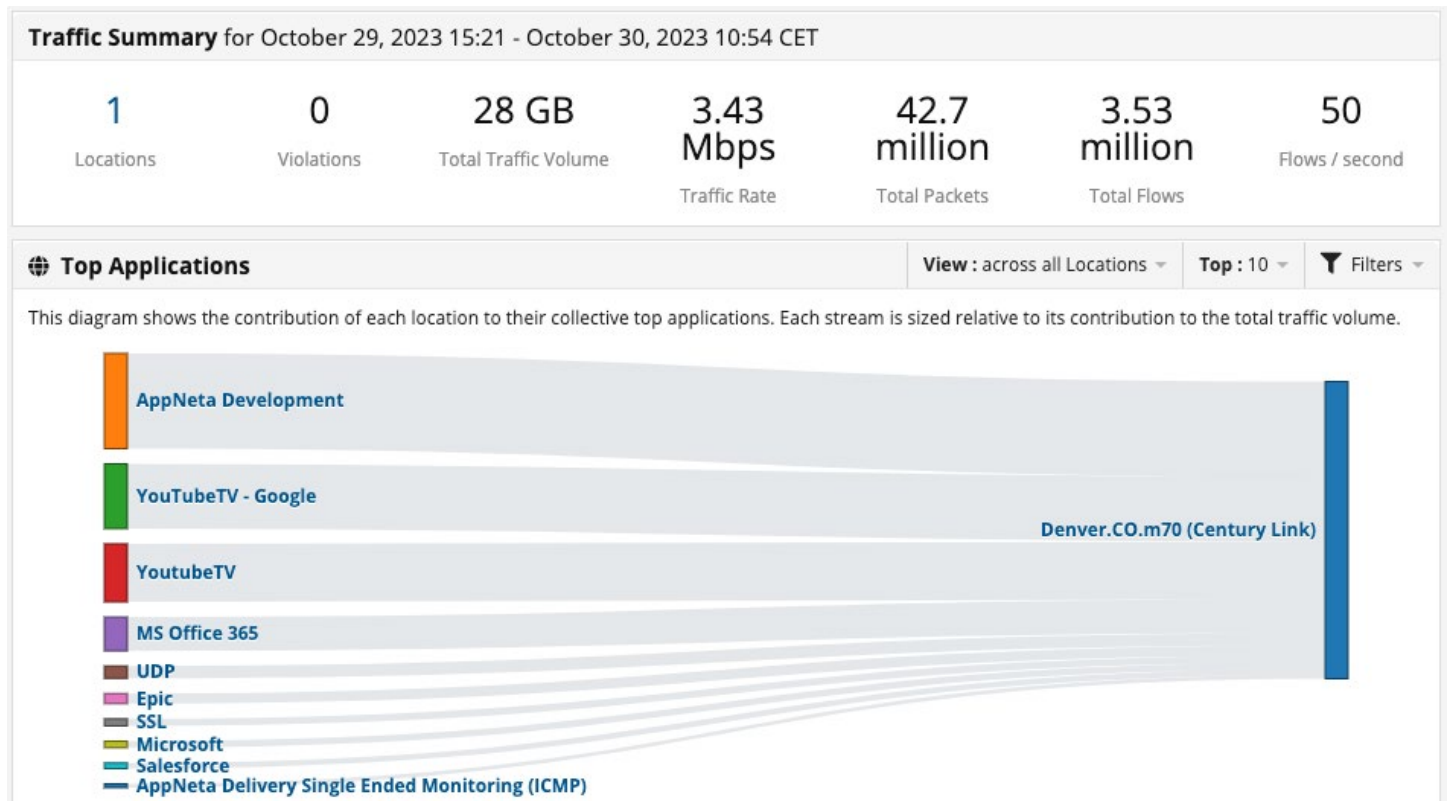
¹⁰ EMA Research, “Network Management Megatrends 2022: Navigating Multi-Cloud, IoT, and NetDevOps During a Labor Shortage,” Shamus McGillicuddy, April 2022

It is critical to realize that SD-WAN deployment isn't just a checkbox on the WAN modernization journey. SD-WAN is a dynamic and adaptive technology that needs continuous, end-to-end monitoring to provide the agility and resilience that business users and executive management expect. Also, SD-WAN technology doesn't run in isolation; it interoperates with the rest of the network. Given this, holistic visibility is the key to maintaining adequate performance levels. With NetOps by Broadcom, teams can effectively track the effectiveness of their WAN before, during, and after their SD-WAN rollout. The solution delivers the vital intelligence teams need to track, manage, and quantify the success of their deployments.

The solution enables network teams to see how bandwidth at a given location is being devoted to particular applications, hosts, and users. It monitors the traffic on a link to determine which applications are being used and who is using them. With the solution, teams can answer these types of questions:

- Which applications are being used at a given location?
- How much bandwidth is consumed by which application?
- How is traffic distributed over time and across locations?

The solution features an innovative approach that combines the strengths of deep packet inspection (DPI) and NetFlow analysis. That combination delivers powerful synergy, fueling comprehensive network visibility. With the solution, teams can ingest and analyze multiple types of NetFlow data generated by compatible network devices in the corporate network. Additionally, the DPI capabilities of monitoring points located at the edges of the network enable the capture and measurement of traffic volume information for the cloud services and web applications being used, as well as for the hosts that are accessing those applications.

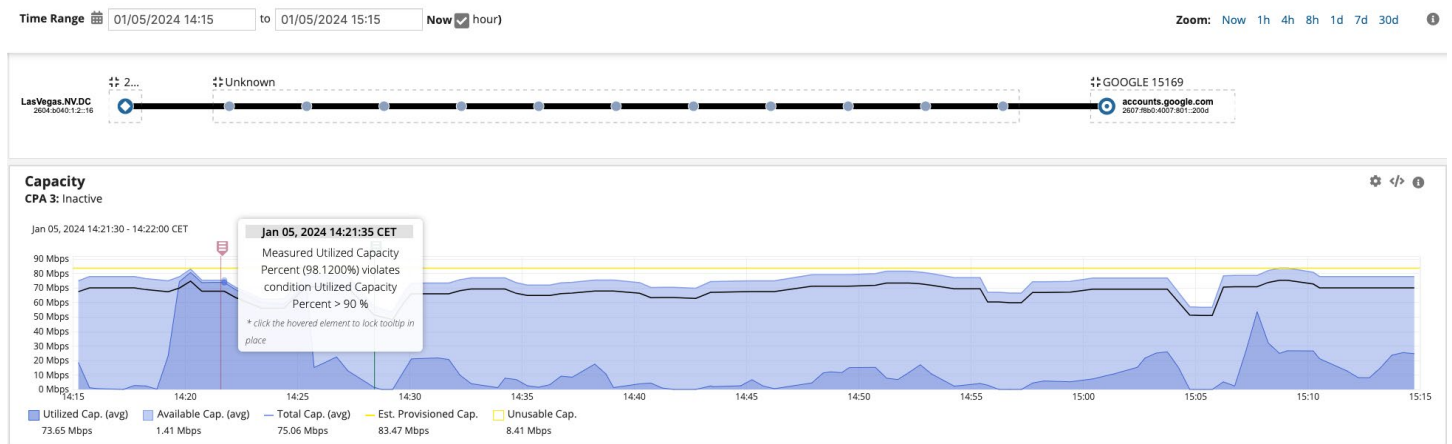


NetOps by Broadcom uses a combination of DPI and NetFlow to provide categorized traffic details, helping users understand which applications are traversing the network.

There are a number of capacity-related metrics that are delivered by the solution. They are derived from measurements made with TruPath. The solution does numerous test iterations that contain various packet patterns:

- **Total capacity.** The peak transmission rate observed in the last three hours by TruPath. The calculation takes into account variations in latency and cross-traffic.
- **Available capacity.** The part of the total capacity that is available for use.
- **Utilized capacity.** The part of the total capacity that is in use. It is calculated as total capacity minus available capacity.

It is important to understand that bandwidth and capacity are related concepts in network communication, each addressing different facets of a network link's capabilities. On the one hand, bandwidth refers to the maximum data transfer rate of a link. Bandwidth is typically the number an ISP specifies for its internet connections. It's akin to the width of a pipe, indicating the quantity of data that can simultaneously flow through the link. On the other hand, capacity is a more comprehensive term considering the link's overall ability to manage diverse types of traffic and support multiple concurrent connections. Capacity is an end-to-end measurement and is determined by the most constricted part of the path, from source to target. Given this, the bandwidth number is typically higher than capacity. Capacity, however, is a better representation of how application data is handled by the network. Understanding both bandwidth and capacity is crucial for effective network planning and management, and for ensuring optimal performance and responsiveness in diverse operational scenarios.

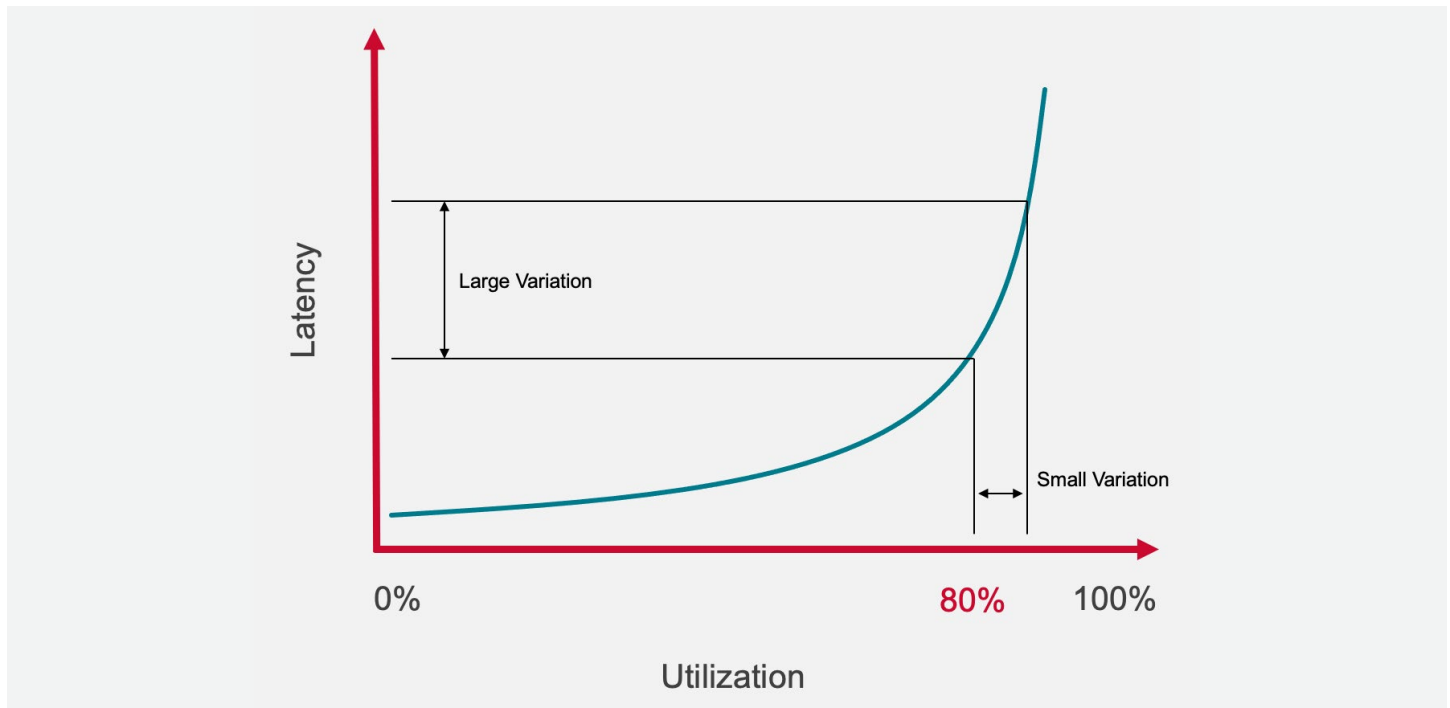


The Broadcom solution measures capacity and capacity utilization for any network path in real-time.

In order to provide continuous measurements with minimal impact, TruPath uses packet dispersion analysis to calculate capacity rather than saturating the path, which is what a tool like Speedtest would do. To understand how this works, imagine two packets of equal size are sent back-to-back with no other traffic on the line. Packet dispersion focuses on the distance between those packets by the time they reach the target. Specifically, packet dispersion is the time between the arrival of the last byte of the first packet and the last byte of the second packet, which allows these real-time calculations of capacity:

- **Total capacity.** Calculates packet size (in bits) divided by the dispersion (in seconds). The dispersion value used is the minimum dispersion observed over a series of packet trains.
- **Available capacity.** Measures the average dispersion of a series of packet trains, factoring lost packets into the calculation.
- **Utilized capacity.** Represents total capacity minus the available capacity.

When implementing SD-WAN, defining the right bandwidth needs is crucial. The main reason for that is latency, the time delay between the initiation and completion of a data transfer. Latency is not a linear function of utilization. While it might be tempting to assume there is a linear relationship between network utilization and latency, the reality is more nuanced due to the nature of network protocols, queuing mechanisms, and congestion dynamics. This nonlinearity is particularly influenced by the well-known phenomena observed in such models as queuing theory. At low levels of utilization, the network may operate efficiently with minimal latency. But when utilization approaches or surpasses certain thresholds (commonly 80%), the probability of congestion and packet contention rises, leading to a non-linear increase in latency.



As referenced in theoretical models, latency is actually not a linear function of utilization.

Such behavior of a network link under heavy demand explains why latency can become highly volatile, affecting network service performance and the quality of experience. In essence, the relationship between network utilization and latency is intricate and influenced by various factors that interact in a non-linear manner. Understanding and monitoring this dynamic is crucial for network administrators and engineers to effectively manage and optimize SD-WAN performance across different utilization scenarios.

Baselines are foundational mechanisms that empower IT teams to make informed decisions throughout SD-WAN planning, deployment, and operational phases. Broadcom provides a comprehensive understanding of the performance of the existing WAN, serving as a benchmark for evaluating the impact of SD-WAN implementation. This knowledge is instrumental in capacity planning, enabling network teams to anticipate and scale the SD-WAN infrastructure according to historical traffic patterns and usage demands. Additionally, they serve as a reference point for optimizing the network, managing user experience, and detecting anomalies. By regularly comparing post-deployment metrics to established baselines, the solution helps fine-tune configurations and policies to maintain optimal network efficiency and responsiveness.

Validating Against End-User Experience

Legacy, private MPLS connectivity is costly, and so increasingly being replaced by cheaper public internet connections. As a result, the quality of the communications delivered by the enterprise network is no longer being governed by service level agreements (SLAs). The internet is a diverse and unpredictable transport mechanism, which makes branch users vulnerable to latency and other routing issues that degrade the quality of the experience. Network teams are often the first to be blamed when there is a drop in performance. Given that, these teams are now seeking real-time visibility on user experience.

However, network teams are still over-dependent on end users to detect application issues at remote locations. They lack visibility into the end-user experience. When users complain, network teams have no way to determine whether it's a legitimate complaint, and, if so, what changes may be responsible for the issue. Teams' focus, time, and resources are largely dedicated to firefighting rather than focusing more on strategic endeavors related to SD-WAN deployments.

SD-WAN deployment validation must involve testing and monitoring to ensure that the infrastructure meets the expected criteria for end-user satisfaction. This includes evaluating application response times, latency, and overall network performance under various conditions. By closely examining the end-user experience during validation, organizations can confirm that the SD-WAN effectively prioritizes and delivers critical applications. A comprehensive validation process considers both technical metrics and real-world user interactions. This helps ensure that the SD-WAN deployment aligns with business objectives and provides the intended benefits in terms of performance and user satisfaction.

NetOps by Broadcom provides insight into how the network is performing from a user or client application perspective. In order to provide an unbiased evaluation of the quality of the service delivered to the end-user, the solution uses Apdex (Application Performance Index) and MOS (Mean Opinion Score) indicators, which are industry-recognized metrics used to assess and quantify the quality of user experience.

Apdex is a standardized measure that evaluates the responsiveness of applications based on user satisfaction. It considers response time thresholds, categorizing three levels of satisfaction (satisfactory, tolerable, or frustrating). This allows network teams to gauge application performance in a user-centric manner. On the other hand, MOS is a metric used to assess audio quality in communication networks. It quantifies user perception of call quality on a scale from 1 to 5, with higher scores indicating better call quality. Together, Apdex and MOS play an important role in understanding the user experience on the network. These metrics address the quality of experience related to both applications and communications.

Application QoE		Communication QoE	
Apdex		MOS	
Reference Time	T	5	Excellent
Satisfied	≤ T	4	Good
Tolerating	≤ 4T	3	Fair
Frustrated	> 4T or failed	2	Poor
		1	Bad

$\text{Apdex } \tau = (\text{Satisfied Count} + (\text{Tolerating Count} / 2)) / \text{Total Measurements Count}$	<p><i>Estimated using quality models as a function of latency, jitter, packet loss and codec</i></p>
---	--

NetOps by Broadcom uses Apdex and MOS to assess and quantify the quality of the user experience.

Broadcom uses synthetic monitoring to feed the Apdex score, a modern way to see trends in the usage and performance of SaaS and web applications. This approach uses scripting to emulate the paths and actions that end users take as they use an application. The workflows are run at regular intervals from monitoring points that can be strategically located in the enterprise network and also around the world. Each time a script is executed, the monitoring point measures the amount of time taken by the browser, the network, and the server running the application. It also breaks down the measurements by milestone within the workflow. All measurements are collected and stored for analysis and presentation. In addition, teams can set alerts so they are notified whenever performance is outside of acceptable limits.

Enterprise Web App Performance Current range: January 1, 2024 4:04 PM - Now
Zoom: 1h 4h 8h 1d 7d 30d

Web App Groups	Apdex	Workflow Completion Time	Outages	Alerts
Google Workplace: Google Workspace Navigation	50%	38.1s	0 events	0 events
Broadcom Box: Untitled	100%	1.2s	0 events	0 events
0365 Apps - Direct: Excel Workflow	70%	38.0s	0 events	3 events 5 days 4 hours 17 min...
Web Paths				
Las Vegas, US - LasVegas.NV.DC (Auto) to https://login.microsoftonline.com	70%	46.1s	0 events	3 events 5 days 4 hours 17 min...
Vancouver, CA - Vancouver.BC-r90 (Auto) to https://login.microsoftonline.com	72%	17.9s	0 events	0 events
Denver, US - Denver.CO.m70 (eth0 - 10.) to https://login.microsoft...	68%	44.7s	0 events	0 events
Las Vegas, US - LasVegas.NV.DC (eth0 - 130.) to https://login.micros...	69%	43.5s	0 events	0 events
Microsoft Teams: Open	100%	8.3s	0 events	13 events 5 hours 50 minutes
Broadcom Zoom: Homepage test	100%	3.3s	0 events	0 events
SAP HANA: SAP Load	99%	9.0s	0 events	2 events 39 minutes

The solution rates every application path using the Apdex score, offering an overview of the quality of experience delivered to end users.

The MOS metric was traditionally calculated through subjective methodologies involving human listeners, who provided opinions on the quality of audio signals. In these tests, listeners were exposed to various audio samples, such as voice calls, and asked to rate the perceived quality on a numerical scale. The individual scores were then averaged to compute the MOS. However, in today's digital world, it is not possible to have human listeners rating every communication on every network link, so the Broadcom solution estimates the MOS using quality models. Monitoring points compute the MOS as a function of latency, jitter, packet loss, and the type of codec.

Monitor suspects latency violated - Failed at 01/08/2024 14:44



▼ Denver to Ashburn (Denver.CO.m70 -> Ashburn.VA.DC) →

Hop	Severity	IP Address	Host Name	Voice Loss (%)	MOS	Latency (ms)	Voice Jitter (ms)			RTT (ms)		QoS	
							Avg	Max	Min	Avg	Max	Set	Measured
1	✓	10.1.1.1	AppNetaDenver	0.00	4.4	0.05	0.03	0.63	0.10	0.15	0.77	46	46
2	ⓘ	192.1.1.1	192.1.1.1	0.20	4.4	0.10	0.03	0.69	0.21	0.22	0.26	46	46
3	✗	170.39.139.1	1-139-39-170.versone...	76.40	1.0	3.53	55.67	294.85	7.26	11.55	49.75	46	46
4	⊖	10.1.1.1	10.1.1.1	-	-	-	-	-	-	-	-	46	-
5	✓	38.122.238.45	te0-0-1-1.nr11.b0044...	0.00	4.4	4.02	0.59	10.27	8.42	8.84	15.30	46	46

The solution uses MOS to report on the quality of audio communication experiences and delivers hop-by-hop diagnostics.

Network organizations need to continuously validate SD-WAN performance by correlating it to the actual end-user experience. The Broadcom solution equips network teams with the right level of insight into end-to-end network delivery and the quality of experience. Whether they are looking to validate new deployments or some change in existing infrastructures, teams are better equipped to operationalize SD-WAN to drive the success of WAN modernization initiatives.

CONCLUSION

Adopting SD-WAN is a cost-effective and flexible alternative to investing in traditional MPLS networks, but the modest rate of successful deployments makes clear that implementing such a technology is not straightforward. SD-WAN introduces increased complexity, making it more difficult and more critical to track and manage network performance. To ensure consistent performance, NetOps by Broadcom helps network operations teams take an approach that allows holistic, correlated visibility into the performance of the underlay and overlay, both for networks they own and those of external service providers.

USE CASE	BROADCOM	NATIVE SD-WAN TOOLS
Multi-Vendor	Yes	No
End-to-End Path Monitoring	Yes	No
End-Point Monitoring	Yes	No
Application Synthetic Testing	Yes	No
Traffic Analysis	Yes	Yes
Digital Experience	Yes	No
Validation	Yes	No

Networks continue to evolve and the Internet is now effectively the new enterprise network. In this new paradigm, network teams are responsible for services they have less and less control over. Native SD-WAN monitoring tools fill some basic needs but leave significant gaps in visibility, lacking coverage of multi-vendor networks and end-user experience. By gaining insights into end-to-end network delivery, network teams will be better equipped to validate and operationalize SD-WAN deployments. As a result, organizations can dramatically increase their chances of successfully deploying and fully leveraging the significant benefits of SD-WAN.

Service Provider Boosts Monitoring Scale by 50%

The network teams of a large infrastructure services provider had previously relied upon traditional monitoring approaches and native tools from technology vendors, including SD-WAN vendors. With these tools, teams were left with blind spots, and couldn't track the end-to-end delivery paths of user connections. Further, the team has been contending with spiraling volumes of alarms.

NetOps by Broadcom has enabled the team to effectively scale to meet the monitoring demands of a large, and rapidly growing SD-WAN estate. While native monitoring tools lacked the scale and underlay/overlay correlation the team needed, the Broadcom solution enabled the team to boost monitoring scale by 50%. With the Broadcom solution, the service provider is able to correlate individual device performance with end-to-end network monitoring, across both internal environments and externally managed networks. As a result, the solution helps the network operations team intelligently focus triage efforts and confidently validate SD-WAN performance.

Telecom Company Increases Operational Efficiencies by 70%

This telecom company has traditionally offered managed network services using single-vendor technology. However, over the years, the team has recognized the need for providing multi-vendor capabilities. Using multiple network vendors typically presents any service provider with a challenge regarding the use of multiple monitoring tools and the lack of a consistent portal for visibility and reporting. The network team recognized the pitfalls of utilizing and managing multiple monitoring solutions, including lack of integrations, increased effort, time-consuming data correlation, skilled resources needed to operate all tools, and limited end-to-end reporting capabilities.

With NetOps by Broadcom, the company can now discover and reconcile all of its SD-WAN networks. Through a single operational experience, the solution provides insights into the health and performance of all SD-WAN deployments, across any vendor technology. Network teams can identify when and why route changes are occurring to validate that SLA policies are providing expected results, while appropriately leveraging the various WAN connectivity options and technologies available. Ultimately, the Broadcom solution enabled the company to confidently deliver high quality services and meet service guarantees.

Why NetOps by Broadcom

NetOps by Broadcom offers unified, scalable, and comprehensive capabilities for monitoring multi-vendor SD-WAN and legacy WAN technologies. The solution extends the SD-WAN controllers' native management capabilities by delivering end-to-end visibility into the WAN overlay and underlay infrastructure, including third-party networks.

This is one of the only solutions that offers both network monitoring and digital experience monitoring. On a continuous basis, the Broadcom solution helps teams validate deployments as well as routing and forwarding decisions made by the SD-WAN. The solution correlates user experience issues with the offending network components or carrier providers, removing the complexity inherent to troubleshooting in SD-WAN environments.

As they continue to struggle to manage services over which they have limited control, network teams' time and resources continue to be stretched thin. The Broadcom solution empowers these teams to scale operations, improve service assurance, and boost cost efficiency.