WHITE PAPER

Addressing the Monitoring Imperatives of Software-Defined, Cloud, and ISP Networks

TABLE OF CONTENTS

CHALLENGE

The data center has traditionally been the central spine of enterprise IT strategy. For decades, the data center has been the core hub for applications, routing, firewalls, processing, and more. However, a number of trends—such as the increased move to hybrid, cloud, and work-from-anywhere models—have upended everything.

Now, the enterprise is highly reliant upon distributed workplaces, cloud-based resources, and third-party operated networks. In this context, conventional networking models that backhaul traffic to the data center are seen as slow, resource-intensive, and inefficient. Now the Internet is the new enterprise network.

As organizations continue to adapt their IT strategies and transform traditional working practices into new digital approaches, IT and network operations teams are facing new challenges:

- **Infrastructure diversity.** Modern networks encompass more diverse infrastructures, including on-premises, internet and communication service providers (ISP, CSP), managed service providers (MSPs), cloud providers, and wireless networks. Teams are now responsible for end-to-end service delivery, including services that run across networks they own and those they do not.
- **Network growth.** Networks continue to expand, featuring more devices, end points, and network components. With the proliferation of IoT devices, mobile devices, and interconnected systems, networks must accommodate more entities, and operations teams must contend with the added demands of managing and maintaining these expanding environments.
- **Multi-vendor environments.** Most organizations use networking equipment and solutions from multiple vendors to meet their specific requirements. Managing and integrating different vendor technologies, configurations, workflows, and protocols can complicate network operations and troubleshooting, which leads to an increase in mean-time-to-resolution (MTTR) metrics and a decrease in user satisfaction.
- **Software-defined and virtualized networks.** The adoption of virtualization technologies and software-defined networking (SDN) introduces new complexities in network management and configuration. Integrating and managing these multi-layer virtual, logical, and physical topologies requires expertise in multiple technologies and protocols.
- **Distributed workforce.** With the rise of distributed teams and hybrid workers, operations teams need to ensure employees working from various locations have secure remote access and reliable connectivity. This creates additional requirements when designing the network, managing security, and optimizing performance.

Now, operations teams are responsible for the performance of the entire connectivity path, regardless of who owns or operates the underlying networks. Interestingly, EMA recently published their Megatrends report, which noted "99% of enterprises have adopted public cloud, but only 18% described their tools as very effective at monitoring the cloud."[1]

Most organizations have adopted some form of cloud computing, offloading infrastructure deployment tasks to an external provider. Organizations rely on a range of offerings, from simple software-as-a-service (SaaS) subscriptions to platform - or infrastructure-as-a-service (PaaS or IaaS) offerings. As cloud offerings continue to mature, many businesses now rely upon a multi-cloud approach. Managers look to match workloads to the attributes of specific cloud provider offerings. In addition, they deploy to a separate cloud environment in order to ensure availability in the event of an outage in an on-premises site or at another cloud provider environment. However, moving workloads between clouds or to and from on-premises infrastructure can create network visibility gaps.

Integrating legacy and cloud workloads over Internet connections brings performance challenges into sharp focus. The Internet wasn't designed to deliver enterprise applications the way LAN and MPLS networks do. Many applications feature bandwidth intensive and reliably performant protocols that may perform fine in a data center, but experience significant latency, loss, and/or jitter when run over the Internet. Benefits of cloud computing come with the increased challenge of ensuring network reliability in an environment where entire applications may be in transit across networks that operations teams do not own.

[1] EMA Research, "Network Management Megatrends 2022: Navigating Multi-Cloud, IoT, and NetDevOps During a Labor Shortage," Shamus McGillicuddy, April 29, 2022

Finally, there is the growing impact of SDN. SDN is rapidly gaining in popularity, as it promises the agility and flexibility of decoupling network deployments from the underlying hardware. As organizations move to converged or hyper-converged infrastructure, networks will be able to grow, shrink, and redeploy on-demand. Featuring multi-layered virtual, logical, and physical topologies, these environments dramatically increase operational complexity, however.

Because of these rapid advances in networking technology coupled with increasing business demands, operations teams often find themselves with a multiplicity of tools, each designed to manage or monitor a single aspect of the enterprise network and application performance. Today, large toolsets are the norm: In organizations with 5,000 or more network devices, nearly all teams are using 11 or more tools.[2]

Perhaps the biggest problem created by this fragmentation is a lack of end-to-end visibility into the network infrastructure. This visibility gap obscures knowledge about critical applications.[3]

A lack of resources is also a significant problem. Further, as network teams add more tools, they become less effective at network problem detection and their networks become less stable.

Operations teams will need to implement new approaches in order to understand and manage the performance of digital services running across software-defined and hybrid infrastructures. These approaches should bridge network silos and extend monitoring reach into edge services and multi-cloud and SaaS environments. Further, teams must establish the visibility needed to see every potential degradation point across the end-to-end delivery path.

Network teams need a way to establish unified operations. This begins with comprehensive visibility provided by a platform that delivers visibility into these areas:

- **Software-defined data center.** Virtualized, hyper-converged networking infrastructures are dynamic and highly complex, making them difficult to monitor.
- **ISP and cloud networks.** Traditional network monitoring tools can’t measure the performance of today’s hybrid cloud environments.
- **Digital experience.** Enterprises typically have thousands of applications and data-producing devices competing for network bandwidth. It is vital to be able to objectively measure the user experience.

[2] EMA Research, “Network Management Megatrends 2022: Navigating Multi-Cloud, IoT, and NetDevOps During a Labor Shortage,” Shamus McGillicuddy, April 29, 2022

[3] Dimensional Research, “Are networks ready for massive scale increases and new technology?” February 2022

VISIBILITY INTO THE SOFTWARE-DEFINED DATA CENTER

Software-defined data centers (SDDC) have emerged as an important concept in next-generation computing because they are aimed at reducing sourcing complexities and accelerating resource provisioning. SDDC refers to a virtualized data center that leverages software-driven tools to centrally manage computing, storage, and network resources.[4]

However, implementing SDDC is not a simple or risk-free process. As organizations continue to embrace virtualization and software-defined technologies, traditional network monitoring tools fall short in providing holistic insights. This is particularly true when issues involve various domains, such as microservice architectures and virtual data center environments, such as Cisco ACI or VMware NSX-T. In these scenarios, operations teams must have the right visibility to correlate intelligence and resolve problems.

Unlike traditional data centers, where physical components are predominantly fixed and visible, SDDCs are characterized by dynamic, software-driven architectures that abstract and virtualize networking resources. This abstraction introduces new layers of complexity, making it challenging to manage the performance of the data center environment.

To track and optimize performance of software-defined infrastructures, teams need insights into the interactions between legacy network components, controllers, virtual machines, virtual networks, and applications. Network professionals often do not have a single monitoring solution for managing these multi-layered environments. This means teams have to dig into distinct silos of information, which is extremely time consuming and takes operators away from more productive tasks.

Comprehensive visibility into the SDDC and overall network infrastructure is now paramount for operations teams. It is only with this visibility that these teams can track resource deployments, detect abnormal performance, optimize workloads, and proactively address performance and capacity needs. Without advanced monitoring and issue detection, the agile and dynamic nature of the SDDC makes it virtually impossible for operations teams to maintain the service levels that modern applications and services require.

Real-Life Challenges Reported by IT Professionals

Network equipment and servers with factory settings generate alarms for all measurable events, resulting in information overload and little actionable insights. Network switches and routers often come configured in a way in which a simple upstream error can often cascade into a series of thousands of alarms. These alarms did nothing to help point to the root cause of a technical issue, resulting in reduced productivity for network and help desk professionals.[5]

Here are some key requirements for establishing comprehensive visibility and seamless operations for the SDDC.

[4] Wikipedia, "Software defined data center," Quote: "In a software-defined data center, all elements of the infrastructure — networking, storage, CPU and security – are virtualized and delivered as a service."

[5] Forrester, "The Total Economic Impact Of Experience-Driven NetOps By Broadcom," October 2022

Visibility Into Cisco ACI

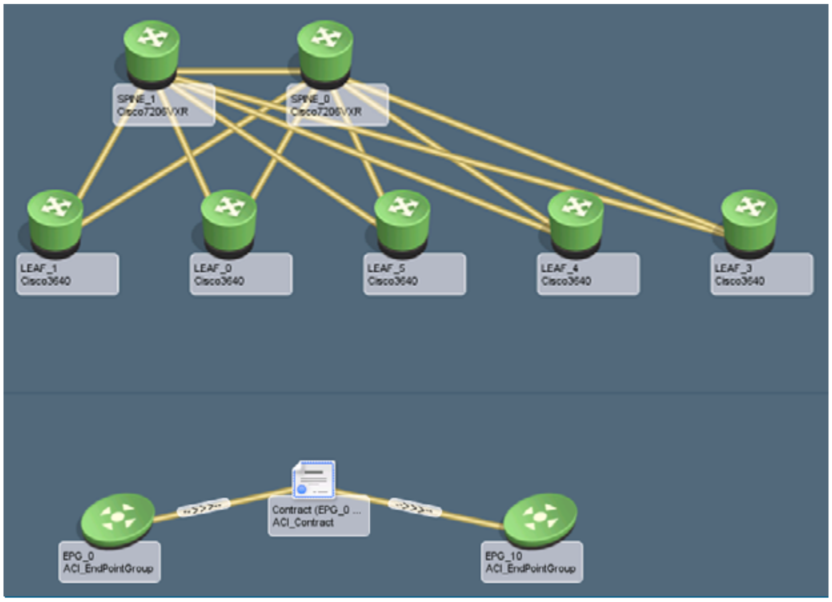
As a software-defined networking solution designed for data centers, Cisco ACI enables network infrastructure to be defined based upon flexible network policies. This offers greater flexibility, dynamism, and automation. However, these environments introduce constant changes that can't be tracked with traditional networking monitoring tools. Abstracting the physical network into a number of virtual and logical entities also means a lot of additional alarm noise for operations teams. ACI technology features more than 20,000 predefined events, with hundreds of unique messages and alarms. That many events and faults can flood the network operations center (NOC) and impede the operations team's ability to troubleshoot efficiently.

Cisco APIC is a centralized management system that is perfectly suited to the network engineers designing and deploying the network. However, this system doesn't provide NOC staff with easy operational troubleshooting workflows and triage scenarios. On the other hand, traditional network monitoring tools fall short in several key ways:

- They can't scale to meet the monitoring needs of highly dynamic SDNs.
- They are unable to monitor both traditional and new SDN-enabled architectures together in one operational user interface.
- They can't unravel ACI abstraction layers, which means teams can't verify and understand the relationships and dependencies established after deployment. As a result, teams can't validate service activation success, and visualize and monitor all the layers within the ACI architecture.

NetOps by Broadcom provides visibility into the components and infrastructure that comprise SDDCs. Using Cisco ACI northbound REST APIs, the solution automatically discovers leaf switches and application profiles, and it provides visibility into which leaf switches are servicing a particular application profile.

The ability to understand how logical entities in the ACI fabric affect or are affected by physical infrastructure is a key value that the solution provides. When using OpenStack or vSphere with ACI, the solution provides views into how an entity related to the underlying physical or virtual computing infrastructure may be causing degradation to the application experience. This information helps operations teams isolate problems on a layer or component of the stack, such as high CPU, memory, or interface usage on a virtual machine, vSwitch, hypervisor, or ACI leaf switch.



NetOps by Broadcom displays connections between leaf and spine switches and shows how contracts and end point groups are associated with a tenant.

The solution automatically discovers the inventory of the ACI fabric and collects components' performance metrics, such as utilization rate and health score. Here are some of the components and metrics covered:

Inventory	Performance Metrics
ACI interfaces ACI tenants ACI virtual routing and forwarding (VRF) APIC controller APIC interfaces Application profiles (AP) Bridge domains Contracts End points End point groups (EPG) L2/L3 EPGs Subnets Switches (leafs and spines) IP Route Paths (IPV4 and IPV6)	Health score Incoming/outgoing traffic CPU utilization Disk utilization Memory utilization Scalability Policy capacity/usage

Using the solution's out-of-the-box dashboards, operations teams can view performance of ACI leaf and spine switches, including such metrics as CPU, memory, interface, health score, and fault counts. Additionally, the dashboards are specifically designed to apply in the context of role-based workflows. Following is an overview of the roles and tasks supported:

System Administrators	Tenant Administrators
• Gain visibility across the fabrics, VMs, and the relationships between entities. • Use the ACI inventor to track the number of entities in the ACI environment. • Track the performance of APs and EPGs on context pages	• Understand VM relationships to the AP, EPGs, computing resources, and the fabric. • Monitor health score and faults within the tenant. • Track the performance of APs and EPGs.
Application Owners	**Fabric Administrators**
• Understand VM relationships to the AP, EPGs, computing resources, and the fabric. • Monitor computer and storage utilization per VM, and top VM utilization.	• Understand fabric relationships to APs and EPGs and the relationships of fabric nodes to computing resources. • Monitor health score and faults within the fabric. • Track the performance of the Nexus 9000 switches.

With the Broadcom solution, the NOC can extend monitoring beyond the physical layer, and gain a holistic understanding of the relationships between ACI-based virtual and logical components as well as legacy network devices. The solution centralizes monitoring visibility, delivering a highly scalable operations monitoring portal that offers visibility across the entire network infrastructure.

The solution delivers a unified view of Cisco ACI deployments, including the overlay and underlay. Through discovery processes, the solution delivers views that are also connected to the rest of the legacy network. The solution offers coverage of the entire ACI deployment, providing visibility into inventory, alarms, status, and performance. By leveraging the solution's network event correlation and alarm noise reduction, NOC teams can efficiently check, update, and track issues that have an impact on service delivery.

Visibility Into VMware NSX-T

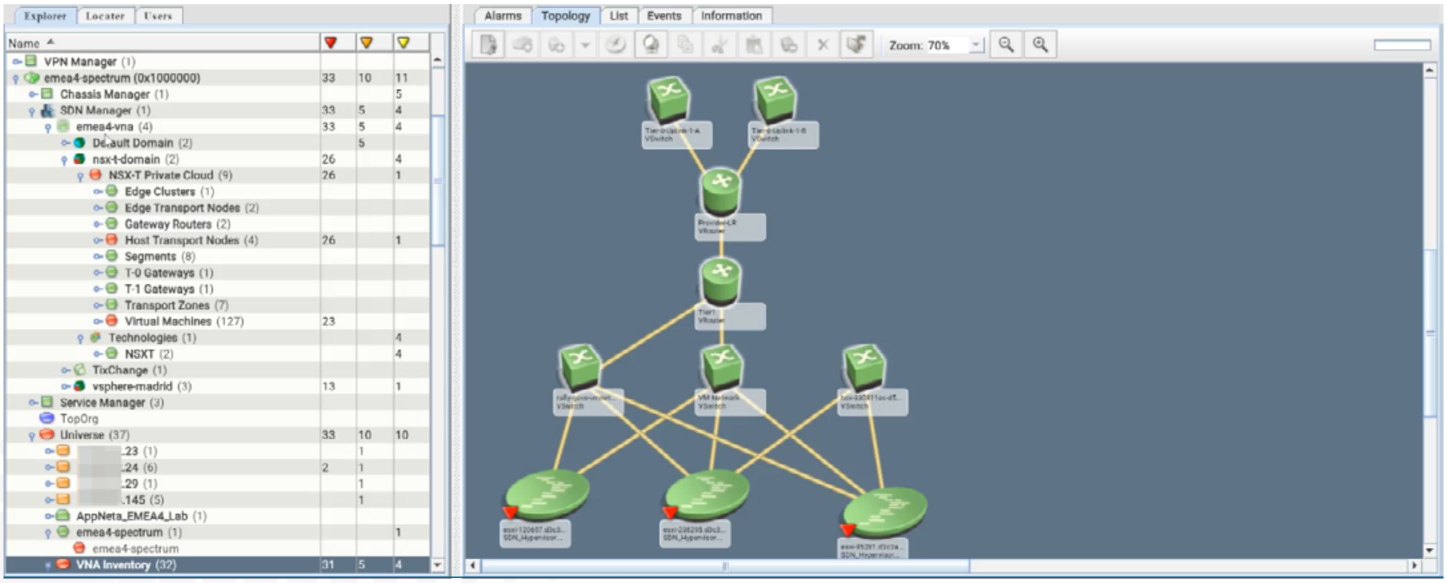
VMware NSX-T virtualizes networking and security services, decoupling them from physical hardware and enabling dynamic, policy-driven network provisioning. The VMware platform abstracts a complete set of networking services, such as switching, routing, firewall protection, and quality-of-service mechanisms. The system consists of several components that operate across three different planes: management, control, and data.

This approach to data center networking can provide greater agility but it also introduces more complexity. Traditional network monitoring tools were typically designed to provide north-south visibility on connections between physical devices. These tools become irrelevant in a software-defined infrastructure, where most of the traffic flows east-west, between VMs or containers, and does not traverse physical links. As a result, pinpointing the root cause of network issues in NSX-T environments can be significantly delayed when teams are using inefficient point tools, especially across a complex service delivery path. Native monitoring capabilities in NSX-T can help by providing granular visibility, but will fail to address the following challenges:

- Handling the integration gaps between the underlay and the overlay networks, leaving blind spots that inhibit visibility and troubleshooting.
- Delivering effective provisioning and deprovisioning, given collaboration between network operations teams is hampered by the diversity of tools.
- Providing single source-of-truth dashboards and unified visibility for teams managing siloed physical and virtual network tools.

NetOps by Broadcom can collect inventory data, alarms, and performance metrics from VMware NSX-T Data Center. The solution collects intelligence via the REST API of NSX-T Manager. By simplifying monitoring and reducing the learning curve for NOC operators, the solution helps teams maximize the return on their SDDC technology investments. The solution provides fast access to insights across software-defined and traditional network infrastructures, offering a single portal that correlates overlay and underlay performance issues.

The Broadcom solution provides unified monitoring capabilities and consistent visibility across a range of technologies, including VMware NSX-T, Cisco ACI, and Cisco DNAC. As a result, teams can leverage standard operating procedures across multiple vendors and technologies.



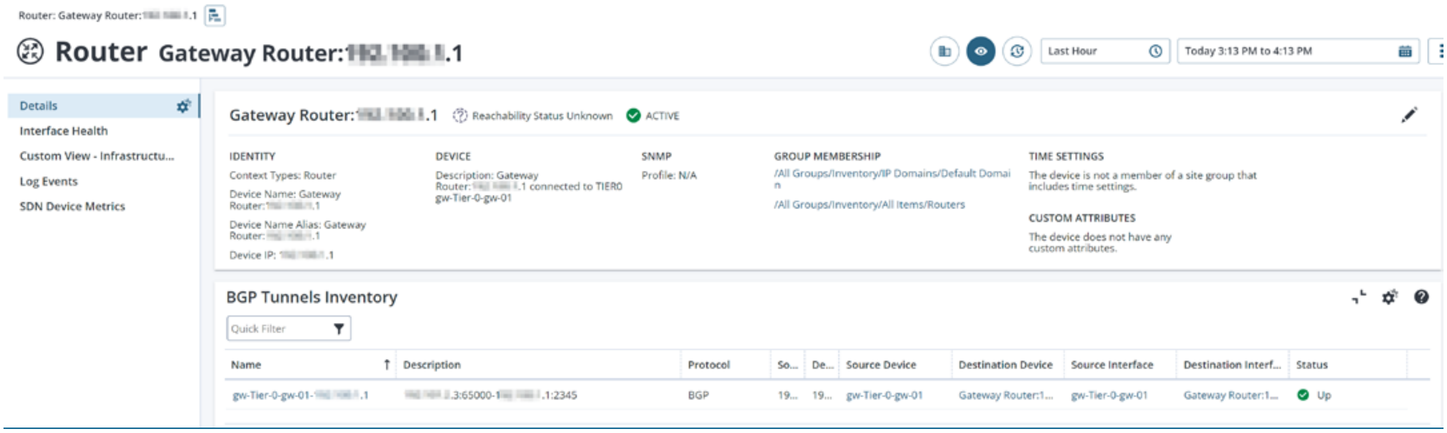
Name ▲	▼	▼	▼
VPN Manager (1)			
emea4-spectrum (0x1000000)	33	10	11
Chassis Manager (1)			5
SDN Manager (1)	33	5	4
emea4-vna (4)	33	5	4
Default Domain (2)		5	
nsx-t-domain (2)	26		4
NSX-T Private Cloud (9)	26		1
Edge Clusters (1)			
Edge Transport Nodes (2)			
Gateway Routers (2)			
Host Transport Nodes (4)	26		1
Segments (8)			
T-0 Gateways (1)			
T-1 Gateways (1)			
Transport Zones (7)			
Virtual Machines (127)	23		
Technologies (1)			4
NSXT (2)			4
TixChange (1)			
vsphere-madrid (3)	13		1
Service Manager (3)			
TopOrg			
Universe (37)	33	10	10
[redacted].23 (1)		1	
[redacted].24 (6)	2	1	
[redacted].29 (1)		1	
[redacted].145 (5)		1	
AppNeta_EMEA4_Lab (1)			
emea4-spectrum (1)			1
emea4-spectrum			
VNA Inventory (32)	31	5	4

NetOps by Broadcom provides an overview of the NSX-T environment, including topology and component status, as well as drill-down links.

The solution automatically discovers and updates the topology and the relationships within the NSX-T infrastructure. This enables easy mapping of all the software-defined components for every cluster, transport node, gateway router, virtual machine, and more. The solution also collects performance metrics and alarms related to the components listed below.

Inventory	Performance Metrics	Alarms
NSX-T Manager cluster and nodes	CPU utilization	Certificate
Transport zones	Memory utilization	CNI health
Host transport nodes	Disk utilization	DHCP
Edge transport nodes	Availability	Distributed firewall
Transport node interfaces	Incoming/outgoing traffic	DNS
Transport node tunnels	BGP session details	Edge health
Edge clusters	Packet drop details	Endpoint protection
Virtual machines	Collisions	Federation
Virtual machine interfaces		High availability
Border routers		Infrastructure communication
BGP connections (BGP sessions)		Infrastructure service
Segments		Intelligence communication
Tier-0 and Tier-1 gateways		Intelligence health
Logical switches		License
Logical routers		Load balancer
		Manager health
		NCP
		Node agent health
		Password management
		Routing
		Transport node
		VPN

By bridging the integration gaps between underlay and overlay networks, the solution enables NOC teams to take a holistic approach to NSX-T management. Once it collects inventory data, the solution populates NSX-T Overlay to Underlay dashboards. These dashboards map tier 0 routers to the border gateway routers they are connected to. From these dashboards, users can drill down to BGP sessions that are connecting these routers.



Router: Gateway Router:[redacted].1

Router Gateway Router:[redacted].1

Last Hour | Today 3:13 PM to 4:13 PM

Gateway Router:[redacted].1 Reachability Status Unknown ACTIVE

IDENTITY
Context Types: Router
Device Name: Gateway Router:[redacted].1
Device Name Alias: Gateway Router:[redacted].1
Device IP: [redacted].1

DEVICE
Description: Gateway Router:[redacted].1 connected to TIER0 gw-Tier-0-gw-01

SNMP
Profile: N/A

GROUP MEMBERSHIP
/All Groups/Inventory/IP Domains/Default Domain
/All Groups/Inventory/All Items/Routers

TIME SETTINGS
The device is not a member of a site group that includes time settings.

CUSTOM ATTRIBUTES
The device does not have any custom attributes.

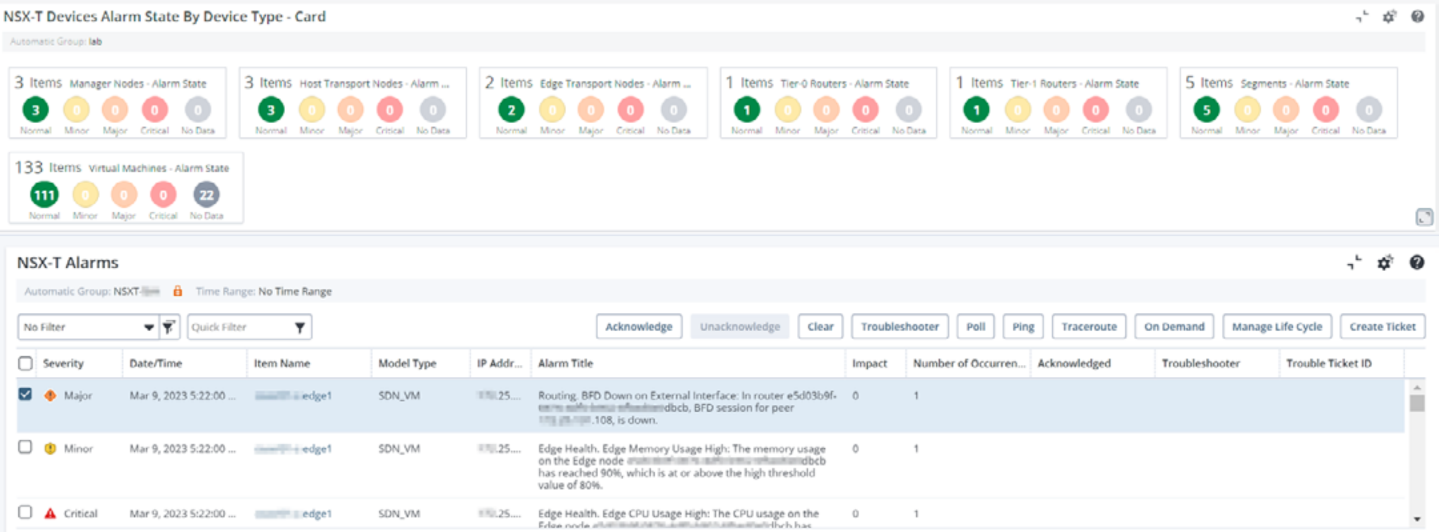
BGP Tunnels Inventory

Quick Filter

Name	Description	Protocol	So...	De...	Source Device	Destination Device	Source Interface	Destination Interf...	Status
gw-Tier-0-gw-01-[redacted].1	[redacted].3:65000-[redacted].1:2345	BGP	19...	19...	gw-Tier-0-gw-01	Gateway Router:1...	gw-Tier-0-gw-01	Gateway Router:1...	✓ Up

The Broadcom solution drills down into BGP sessions and their status for NSX-T Gateway routers.

The solution delivers unified visibility that eliminates blind spots and simplifies infrastructure troubleshooting. By minimizing the need to rely on disparate point tools, the solution helps operations teams establish standardized processes and enhance collaboration. With the solution, teams can more effectively and confidently manage service levels, even in SDDC environments in which resources are constantly being provisioned and deprovisioned.



NSX-T Devices Alarm State By Device Type - Card

Automatic Group: lab

Items	Card	Normal	Minor	Major	Critical	No Data
3 Items	Manager Nodes - Alarm State	3	0	0	0	0
3 Items	Host Transport Nodes - Alarm ...	3	0	0	0	0
2 Items	Edge Transport Nodes - Alarm ...	2	0	0	0	0
1 Items	Tier-0 Routers - Alarm State	1	0	0	0	0
1 Items	Tier-1 Routers - Alarm State	1	0	0	0	0
5 Items	Segments - Alarm State	5	0	0	0	0
133 Items	Virtual Machines - Alarm State	111	0	0	0	22

NSX-T Alarms

Automatic Group: NSXT-[redacted] Time Range: No Time Range

No Filter | Quick Filter

☐	Severity	Date/Time	Item Name	Model Type	IP Addr...	Alarm Title	Impact	Number of Occurren...	Acknowledged	Troubleshooter	Trouble Ticket ID
☑	Major	Mar 9, 2023 5:22:00 ...	[redacted]edge1	SDN_VM	[redacted].25....	Routing. BFD Down on External Interface: In router e5d03b9f-[redacted]dbcb, BFD session for peer [redacted].108, is down.	0	1			
☐	Minor	Mar 9, 2023 5:22:00 ...	[redacted]edge1	SDN_VM	[redacted].25....	Edge Health. Edge Memory Usage High: The memory usage on the Edge node [redacted]dbcb has reached 90%, which is at or above the high threshold value of 80%.	0	1			
☐	Critical	Mar 9, 2023 5:22:00 ...	[redacted]edge1	SDN_VM	[redacted].25....	Edge Health. Edge CPU Usage High: The CPU usage on the Edge node [redacted]dbcb has	0	1			

The Broadcom solution provides NSX-T Health dashboards that enable users to quickly identify issues and to drill down to related items for further troubleshooting.

The Broadcom solution aggregates data from various sources, presenting a consolidated view that transcends the silos of physical and virtual networks. The solution streamlines access to actionable information, simplifies management, and empowers the NOC team to do proactive issue detection and resolution. With the solution, organizations can realize the full potential of their NSX-T environments.

VISIBILITY INTO ISP AND CLOUD NETWORKS

Enterprise networks typically connect multiple geographically dispersed locations. Having insights into remote locations helps ensure smooth data transmission and timely issue resolution. Until recently, network operations teams had complete visibility into their WANs and remote locations. Network specialists could effectively ensure end users weren't meaningfully affected by performance issues, while also thinking about how to plan for the future.

However, today's IT landscape is increasingly interconnected and cloud-centric. By 2025, 40% of all enterprise locations will use Internet access as their only WAN transport, compared with fewer than 20% in 2021.[6] The adoption of unpredictable transports, such as Internet broadband connections for replacing MPLS, introduces higher risk of latency and routing issues. Traditional network monitoring tools often lack insights into the underlay network, especially circuits operated by third-party providers. This limits the NOC's ability to pinpoint the root cause of performance degradation, and makes it difficult to hold ISPs and CSPs accountable for the levels of service they provide.

For years now, network operations teams have been contending with complex network architectures within the four walls of their data centers and within each of their remote locations. Further, these teams' challenges are now being compounded by the fact that their scope of responsibility has expanded to networks they do not own, such as ISP, CSP, and SaaS environments. This results in lengthy troubleshooting efforts, multi-vendor blame-game scenarios, and a lack of visibility across large portions of the network. As a result, teams can't quickly identify and resolve network delivery issues, and the end-user experience is degraded.

These days, it seems whenever an application or a service becomes slow, fingers are pointed at the network. Consequently, obtaining comprehensive visibility is more important than ever. Network operations teams need to readily demonstrate their innocence when performance issues occur within environments owned by ISPs and other third-party providers. This results in faster MTTR as the evidence can be taken to the ISP or SaaS provider to escalate the issue for resolution, while the NOC can find a workaround to establish the required connectivity.

Real-Life Challenges Reported by IT Professionals

Public Internet and cloud services that weren't monitored properly, if at all. Teams lacked tools to monitor the performance of services, such as VoIP, that traversed public and private networks. While there were many tools for monitoring private networks, network engineers had fewer tools for tracking performance of services across the public Internet. To monitor networks connecting to public clouds, interviewees had to rely on analytics from their providers.[7]

Here are some key requirements for establishing visibility into networks managed by third parties, such as ISPs and CSPs.

[6] Gartner, "Optimize WAN Architectures for Workloads That Span the Hybrid Cloud and the Multicloud," Simon Richard, Sumit Rajput, December 2022

[7] Forrester, "The Total Economic Impact Of Experience-Driven NetOps By Broadcom," October 2022

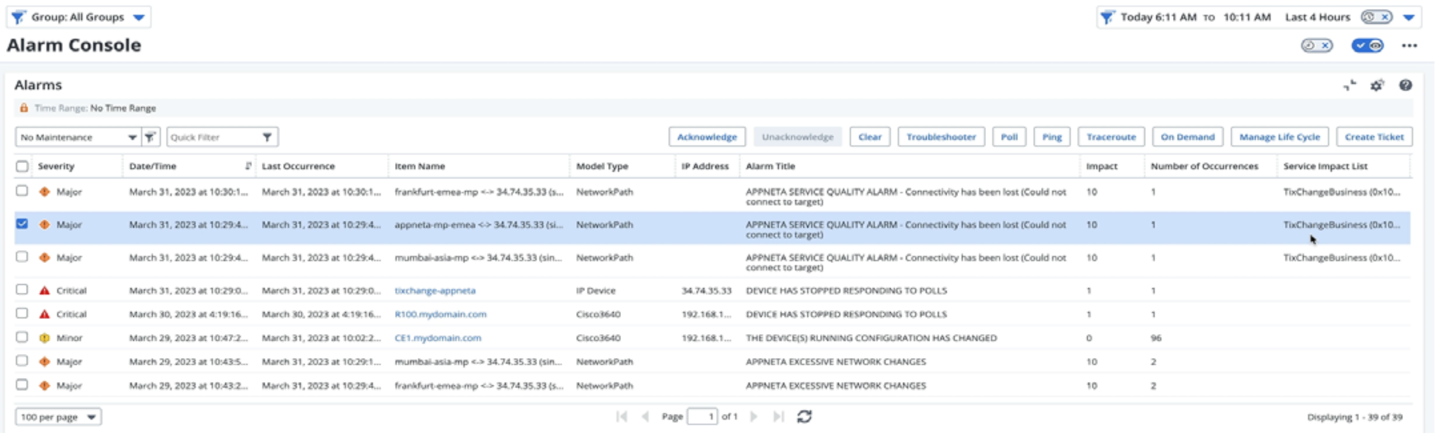
Visibility Into ISP Networks

While operations teams may have basic, binary insight into whether a device is able to connect to a cloud or other remote network or whether an application is being successfully delivered from one end of the network to the other, they won't necessarily be able to identify all of the handoffs between ISPs and other providers. This leaves operations teams unable to identify the owner of a degraded hop, and ill-equipped to quickly remediate the issue. This problem is compounded when a team has to manage hundreds of global locations, and is unfamiliar with typical ISP connections or peering relationships.

The scope of responsibility for the NOC team has expanded significantly. Now, these teams are often held accountable when there is a unified communication service glitch or an application performance issue. These teams now find themselves in a defensive role, where the assumption of guilt prevails until the network is proven innocent. This explains why a metric called mean time to innocence (MTTI) has gained increasing prominence.[8] Without effective solutions to assist them, operations teams face challenges in reducing MTTI and proving their innocence when issues arise outside of the networks they control.

NetOps by Broadcom provides real-time, actionable insight into how third-party networks affect application performance. With the solution's patented TruPath™ technology, operations teams can gain the visibility required to evaluate the state of the networks that application data travels through.

TruPath is based on the monitoring principle of sending and receiving many varied short sequences of packets—called packet trains—and measuring the end-to-end performance. Application data travels back and forth through the network between a source (for example, a user workstation) and a target (for example, an application running in the cloud). The solution monitors the network path between the source and target, including all the network devices or "hops" it passes through. The solution measures the time packets take to go from a source to a target and back, the delay between packets on their return, packet reordering, and the number of packets lost. These measures enable the solution to report on key network performance metrics, such as round-trip time (RTT), latency, jitter, and data loss. It also uses this data to infer other metrics like total capacity, utilized capacity, and mean opinion score (MOS).

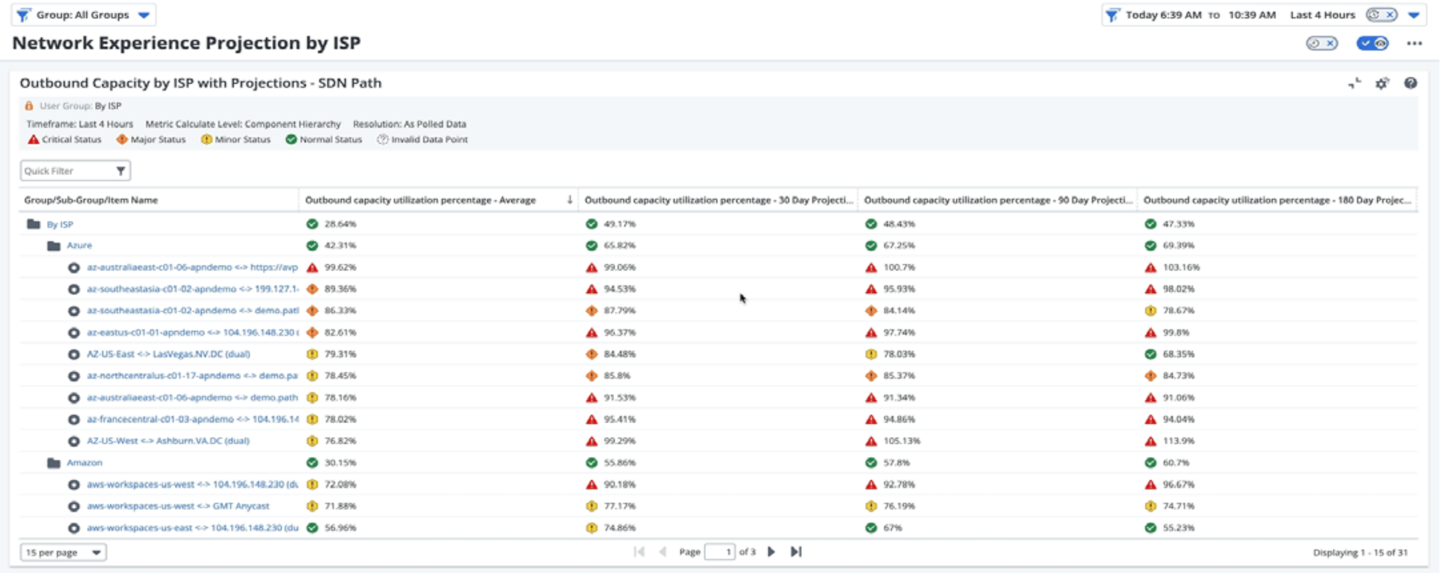


□	Severity	Date/Time	Last Occurrence	Item Name	Model Type	IP Address	Alarm Title	Impact	Number of Occurrences	Service Impact List
□	Major	March 31, 2023 at 10:30:1...	March 31, 2023 at 10:30:1...	frankfurt-emea-mp <-> 34.74.35.33 (s...	NetworkPath		APPNETA SERVICE QUALITY ALARM - Connectivity has been 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 (si...	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	

NetOps by Broadcom brings network delivery experience metrics into the NOC's standard operating workflows, including triage and root-cause identification.

[8] MTTI: Mean Time To Innocence (or Mean Time To Identify), is how long it takes for the networking organization to prove it is not the part of the network they own causing the degradation.

To achieve this visibility, you deploy physical or virtual monitoring end points. TruPath can be employed in either a single-ended or dual-ended configuration. In the single-ended configuration, ICMP echo requests are sent to the target and ICMP echo replies are returned. In the dual-ended configuration, UDP packets are used for monitoring. The advantage of dual-ended paths is they provide a more accurate picture of network performance. That's because independent measurements are taken from source to target and from target to source.



Network Experience Projection by ISP

Outbound Capacity by ISP with Projections - SDN Path

User Group: By ISP

Timeframe: Last 4 Hours   Metric Calculate Level: Component Hierarchy   Resolution: As Polled Data

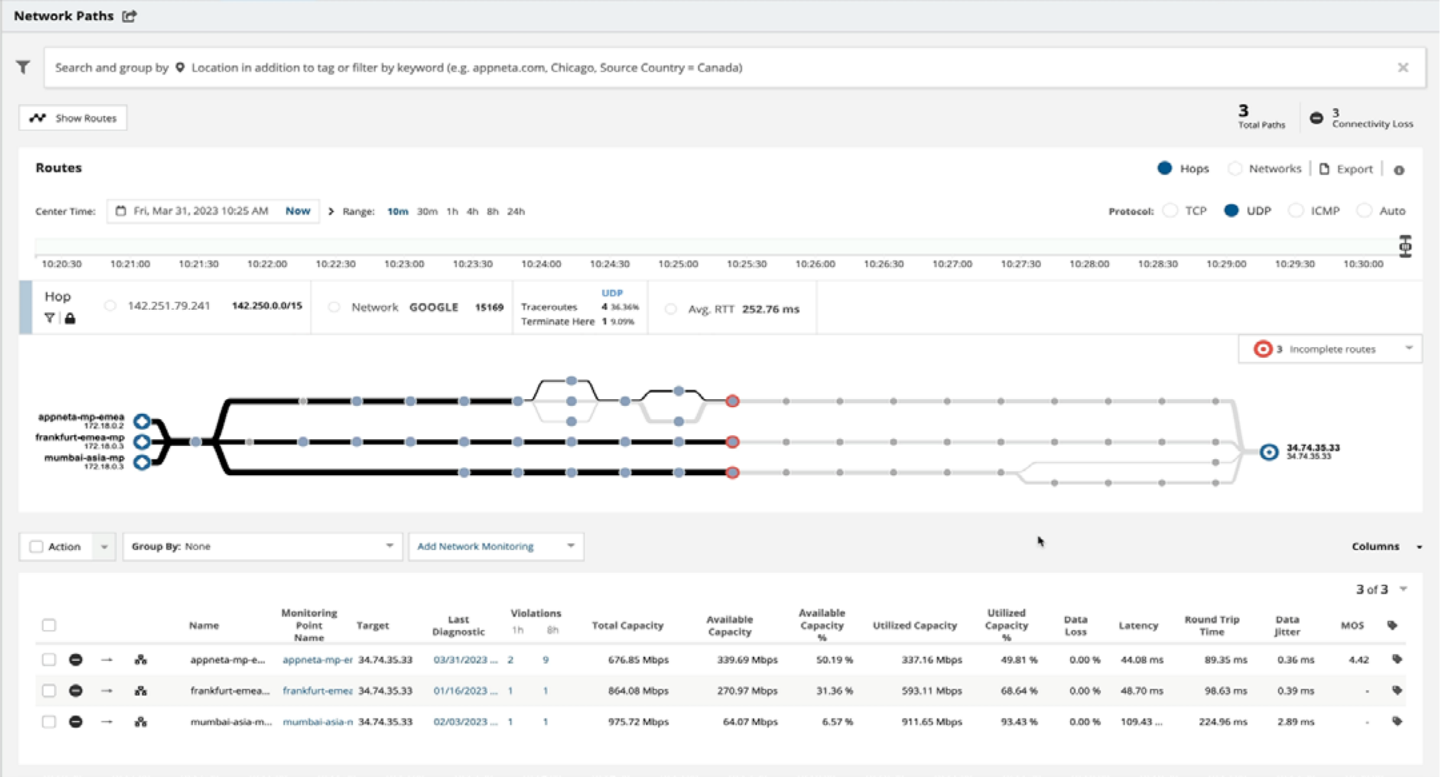
▲ Critical Status ◆ Major Status ! Minor Status ✓ Normal Status ? Invalid Data Point

Group/Sub-Group/Item Name	Outbound capacity utilization percentage - Average ↓	Outbound capacity utilization percentage - 30 Day Projecti...	Outbound capacity utilization percentage - 90 Day Projecti...	Outbound capacity utilization percentage - 180 Day Projec...
By ISP	✓ 28.64%	✓ 49.17%	✓ 48.43%	✓ 47.33%
Azure	✓ 42.31%	✓ 65.82%	✓ 67.25%	✓ 69.39%
az-australiaeast-c01-06-apndemo <-> https://avp	▲ 99.62%	▲ 99.06%	▲ 100.7%	▲ 103.16%
az-southeastasia-c01-02-apndemo <-> 199.127.1-	◆ 89.36%	▲ 94.53%	▲ 95.93%	▲ 98.02%
az-southeastasia-c01-02-apndemo <-> demo.patl	◆ 86.33%	◆ 87.79%	◆ 84.14%	! 78.67%
az-eastus-c01-01-apndemo <-> 104.196.148.230 (	◆ 82.61%	▲ 96.37%	▲ 97.74%	▲ 99.8%
AZ-US-East <-> LasVegas.NV.DC (dual)	! 79.31%	◆ 84.48%	! 78.03%	✓ 68.35%
az-northcentralus-c01-17-apndemo <-> demo.pa	! 78.45%	◆ 85.8%	◆ 85.37%	◆ 84.73%
az-australiaeast-c01-06-apndemo <-> demo.path	! 78.16%	▲ 91.53%	▲ 91.34%	▲ 91.06%
az-francecentral-c01-03-apndemo <-> 104.196.14	! 78.02%	▲ 95.41%	▲ 94.86%	▲ 94.04%
AZ-US-West <-> Ashburn.VA.DC (dual)	! 76.82%	▲ 99.29%	▲ 105.13%	▲ 113.9%
Amazon	✓ 30.15%	✓ 55.86%	✓ 57.8%	✓ 60.7%
aws-workspaces-us-west <-> 104.196.148.230 (du	! 72.08%	▲ 90.18%	▲ 92.78%	▲ 96.67%
aws-workspaces-us-west <-> GMT Anycast	! 71.88%	! 77.17%	! 76.19%	! 74.71%
aws-workspaces-us-east <-> 104.196.148.230 (du	✓ 56.96%	! 74.86%	✓ 67%	✓ 55.23%

15 per page   Page 1 of 3   Displaying 1 - 15 of 31

The solution provides network delivery dashboards that offer views of the overall health of network paths across third-party providers, such as ISPs or CSPs.

Today's networks handle many different traffic types. Given this, the solution employs a quality-of-service mechanism to handle packets appropriately, based on traffic criticality. By specifying DSCP markings on test packets sent by TruPath, teams can determine how traffic that uses those markings is treated by the network. In this way, teams can see if traffic with unmarked packets has different performance metrics. They can also determine if any hops are changing the markings.


Network Paths

Search and group by Location in addition to tag or filter by keyword (e.g. appneta.com, Chicago, Source Country = Canada)

Show Routes

3 Total Paths | 3 Connectivity Loss

Routes

● Hops ○ Networks | Export

Center Time: Fri, Mar 31, 2023 10:25 AM Now > Range: 10m 30m 1h 4h 8h 24h

Protocol: ○ TCP ● UDP ○ ICMP ○ Auto

Hop ○ 142.251.79.241 142.250.0.0/15 | ○ Network GOOGLE 15169 | UDP Traceroutes 4 36.36% Terminate Here 1 9.09% | ○ Avg. RTT 252.76 ms

3 Incomplete routes

□ Action | Group By: None | Add Network Monitoring | Columns

3 of 3

□			Name	Monitoring Point Name	Target	Last Diagnostic	Violations 1h	Violations 8h	Total Capacity	Available Capacity	Available Capacity %	Utilized Capacity	Utilized Capacity %	Data Loss	Latency	Round Trip Time	Data Jitter	MOS	🏷
□	⊖	→	appneta-mp-e...	appneta-mp-er	34.74.35.33	03/31/2023 ...	2	9	676.85 Mbps	339.69 Mbps	50.19 %	337.16 Mbps	49.81 %	0.00 %	44.08 ms	89.35 ms	0.36 ms	4.42	🏷
□	⊖	→	frankfurt-emea...	frankfurt-emea	34.74.35.33	01/16/2023 ...	1	1	864.08 Mbps	270.97 Mbps	31.36 %	593.11 Mbps	68.64 %	0.00 %	48.70 ms	98.63 ms	0.39 ms	-	🏷
□	⊖	→	mumbai-asia-m...	mumbai-asia-n	34.74.35.33	02/03/2023 ...	1	1	975.72 Mbps	64.07 Mbps	6.57 %	911.65 Mbps	93.43 %	0.00 %	109.43 ...	224.96 ms	2.89 ms	-	🏷

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

TruPath is lightweight enough to monitor the network continuously, down to every second on networks up to 100 Gbps. In addition, the solution can get a complete picture of end-to-end network performance very quickly—often in just seconds. The solution regularly traces the route for each network path, hop-by-hop, from source to target. This information can be used to confirm whether traffic is traveling through expected hops and networks.

With these capabilities, the Broadcom solution enables the NOC team to see beyond the boundaries of the private network. With the solution, teams can track how routes change over time, review connectivity failures, track capacity variations, and determine which ISP should be held accountable for issues.

Visibility Across Cloud Networks

As organizations continue to accelerate their digital transformations, they continue to grow increasingly reliant upon cloud services. Therefore, it is not surprising that a vast majority of companies now report using at least two distinct cloud providers. By 2024, nearly 88% of enterprises will be multi-cloud.[9] However, the way IT organizations are sourcing their infrastructure and applications is not radically different from their approaches of ten years ago. The reality is that selecting a cloud vendor is generally a functionality-based approach. By evaluating capabilities, performance, and reliability, teams choose the cloud technology that fits the best with their business' requirements and expectations. These technical and functional reasons are often why teams quickly come to adopt multiple cloud vendors. It is less common that teams choose multiple cloud vendors because of economic imperatives or to avoid the risk of vendor lock-in.

For operations teams, the impact of these transitions has been significant, introducing mounting challenges. Traditional monitoring software practices, like analyzing SNMP data, NetFlow records, packet captures and logs, worked great for the on-premises data center. However, these approaches fail completely in a public-cloud environment. This is one reason why users in only 24% of organizations are fully satisfied with their multi-cloud network monitoring and observability capabilities.[10]

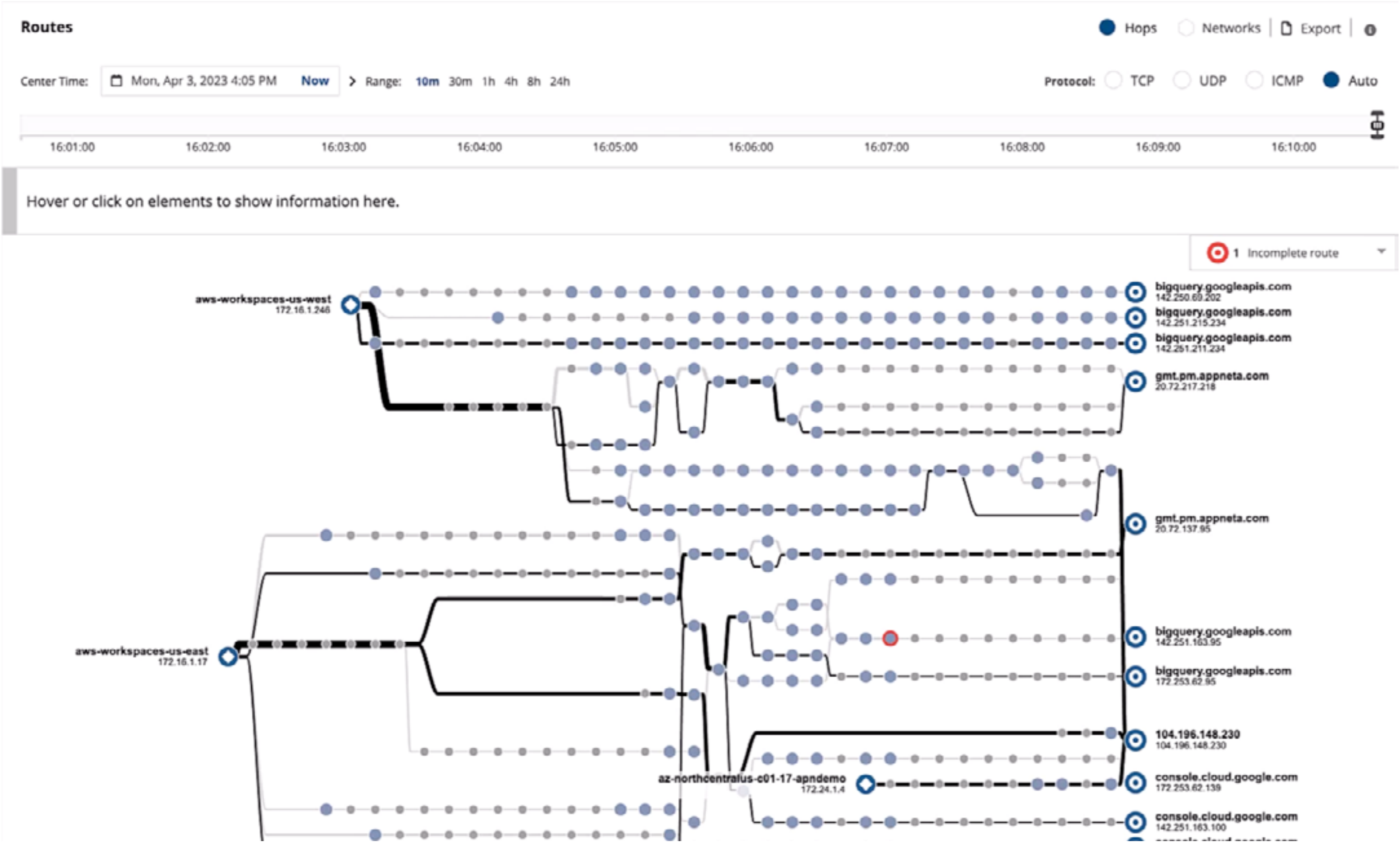
Monitoring hybrid infrastructures consisting of internal computing resources, PaaS, and SaaS introduces increased complexity. Network operations teams must typically first contend with so-called "north-south" dependencies. These dependencies are associated with scenarios in which users are accessing applications or services that are located in the cloud. However, as the use of the cloud evolves, teams must also contend with managing network connections between different cloud environments, which is referred to as "east-west" traffic. In either case, the NOC is often involved in troubleshooting issues that arise.

Given the increasing number of workloads shifting to the cloud, the landscape of corporate networks sees fundamental changes. However most operations teams still fail to effectively understand the performance impact of the unmanaged networks that now deliver critical applications. All major cloud service providers offer optimized services that connect companies, offices, and data centers to their virtual private clouds (VPCs). This includes such services as Direct Connect from AWS, ExpressRoute from Azure, and Dedicated Interconnect from Google Cloud. However, all these services prioritize the network connection on the cloud provider side; they don't provide visibility into a significant portion of the application delivery path, including the corporate network and the Internet.

NetOps by Broadcom provides complete, end-to-end visibility for all the different ways organizations rely upon access to the cloud. The solution tracks data-center-to-cloud connections, region-to-region transmissions within a single cloud provider, and cloud-to-cloud connections in multi-cloud environments. In addition, in cases where cloud resources are integrated with external SaaS offerings, the solution can track cloud-to-SaaS connections.

[9] EMA, "Multi-Cloud Networking: Connecting and Securing the Future," Shamus McGillicuddy and Robert Gates, January 2023

[10] EMA, "Multi-Cloud Networking: Connecting and Securing the Future," Shamus McGillicuddy and Robert Gates, January 2023



Routes

● Hops ○ Networks | Export

Center Time: Mon, Apr 3, 2023 4:05 PM Now > Range: 10m 30m 1h 4h 8h 24h

Protocol: ○ TCP ○ UDP ○ ICMP ● Auto

Hover or click on elements to show information here.

1 Incomplete route

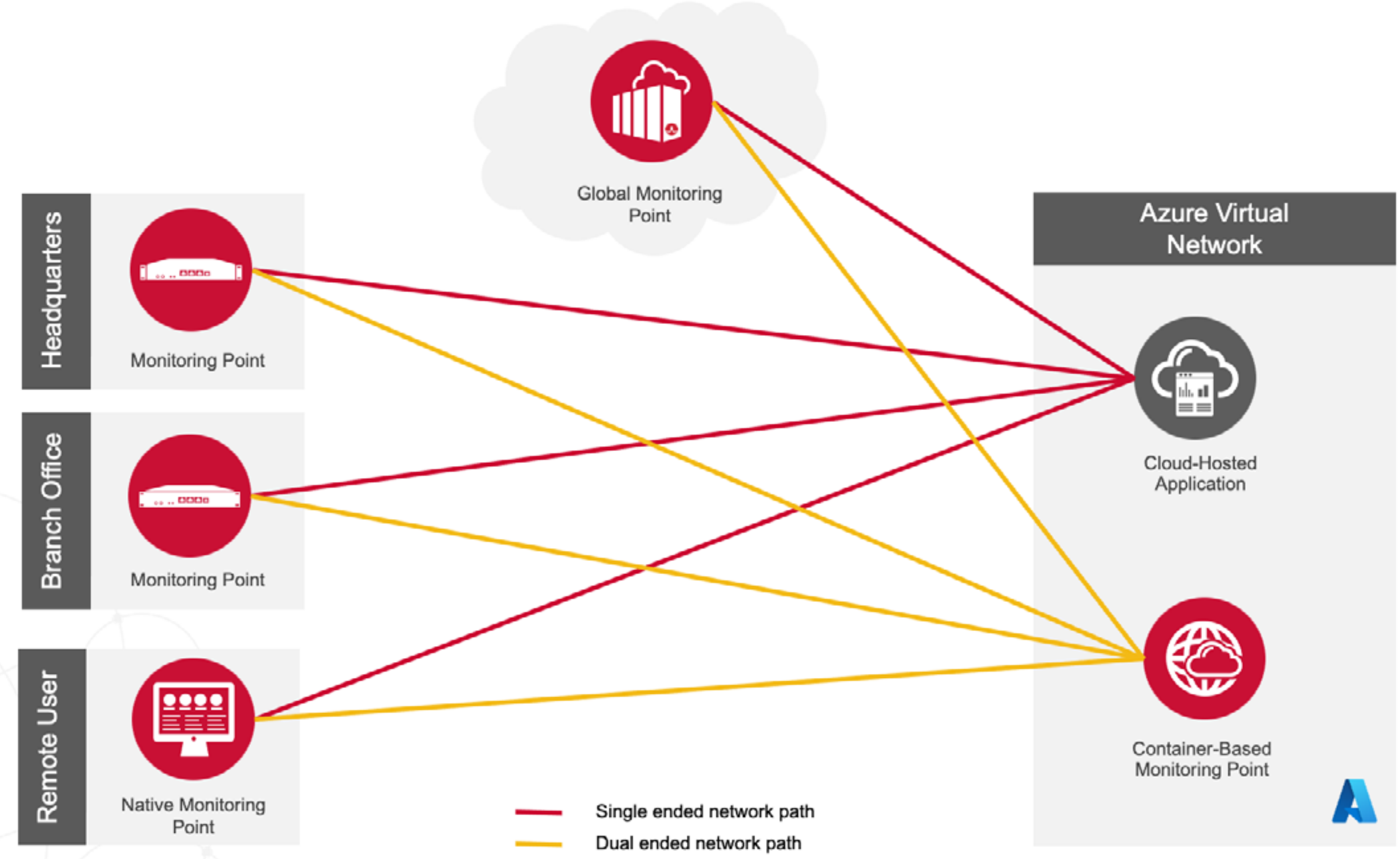
NetOps by Broadcom can be deployed in environments of major cloud providers, including AWS and Google, and it can measure connectivity between these providers.

To provide full visibility in a variety of cloud-based use cases, Broadcom delivers a solution that is network device and deployment agnostic. The solution uses active monitoring technology from purpose-built monitoring points. The solution provides performance monitoring for any cloud architecture and over any network by using managed global monitoring points or by placing enterprise monitoring points inside containers, virtual hosts, end-user workstations, or next to the application code. The monitoring points measure key network performance metrics, such as round-trip time (RTT), latency, jitter, and data loss. The solution also uses this data to infer other metrics like total capacity, utilized capacity, and MOS. It can provide these measurements across various cloud locations, third-party networks, and corporate network segments.

One of the advantages of the Broadcom solution is the vendor-neutral and flexible approach to monitoring from any IP target. This approach makes it is possible to reduce the reliance on traditional testing methods, like IPSLA performance tests, which can strain network capacity. The solution's lightweight and continuous monitoring approach minimizes any negative impact on network performance.

There are three categories of monitoring points:

- Enterprise monitoring points are owned and managed by an organization's network operations team. There are four types of these monitoring points: hardware, virtual, container-based, and software. These points can be deployed in locations that operations teams control.
- Global monitoring points are owned by an organization's network operations team, but are managed by Broadcom. These container-based monitoring points are installed in global cloud provider locations, enabling teams to monitor network and web applications from locations in which active users are based. Operations teams can establish the visibility they need, without having to bear the burden of deploying, monitoring, and maintaining these monitoring points.
- Global monitoring targets are highly available targets owned and managed by Broadcom and installed in cloud provider locations worldwide. These targets allow teams to monitor remote sites and application connectivity to specific regions around the globe.



The Broadcom solution is typically deployed across headquarters, branch offices, and remote user locations, with monitored network paths connecting to monitoring points and hosts located in virtual private clouds.

In order to successfully leverage cloud services, teams need to have reliable network connections across a range of environments. The Broadcom solution helps teams achieve these objectives. The solution can actively monitor end-to-end network performance, including east-west and north-south traffic. The solution delivers complete cloud observability, covering all critical components across the most distributed architectures, from offices and data centers to cloud providers. With the offering, teams can quantify and improve performance, even when services run on infrastructure outside of their control.

VISIBILITY INTO THE DIGITAL EXPERIENCE

Business-critical applications are not served or used in a single location anymore. This is compounded by the trend of enterprise decentralization. Now most enterprises have a global web of remote locations, including home offices, rather than a smaller network centered tightly around hardware at central headquarters. As a result, network teams need to zero in on the digital experience of any user, no matter which application they run, where they're based, or what network they use.

Additionally, many teams continue to focus solely on network performance, rather than tracking application experience metrics. Analysts at EMA believe that network operations teams are at a crossroads in their cloud journeys. Most are struggling as the public cloud, SaaS applications, and cloud-native application architectures begin to drive IT strategy. According to EMA analysts, "They need to modernize their tools. Today's toolsets are bloated, inefficient, and disconnected. They contribute to manual errors that degrade the network, and they are producing too many false alerts."[11]

When organizations hand over their ownership of enterprise applications to cloud and SaaS solution providers, operations teams lose a lot of visibility—both on the network and the application side. This hinders their ability to quickly spot issues and find the root cause of problems. This is problematic because these teams are still held fully responsible for supporting digital transformation and ensuring user satisfaction across the organization. As a result, teams need solutions that deliver full visibility across all network environments. It is only with this visibility that teams can ensure users have the best possible experience with business-critical applications, wherever they're hosted.

Real-Life Challenges Reported by IT Professionals

Teams that used a variety of tools, some of which were only partially implemented. Several interviewees reported using dozens of different tools for specific purposes, and that many of these tools were only partially implemented. Conversations between teams using different tools challenged problem-solving because each group had different data pointing to different issues, resulting in longer MTTR.[12]

Here are some key requirements for establishing visibility into digital experience across private and public networks.

[11] EMA, "Network Management Megatrends 2022: Navigating Multi-Cloud, IoT, and NetDevOps During a Labor Shortage," Shamus McGillicuddy, April 29, 2022

[12] Forrester, "The Total Economic Impact Of Experience-Driven NetOps By Broadcom," October 2022

Visibility Into End-User Experience

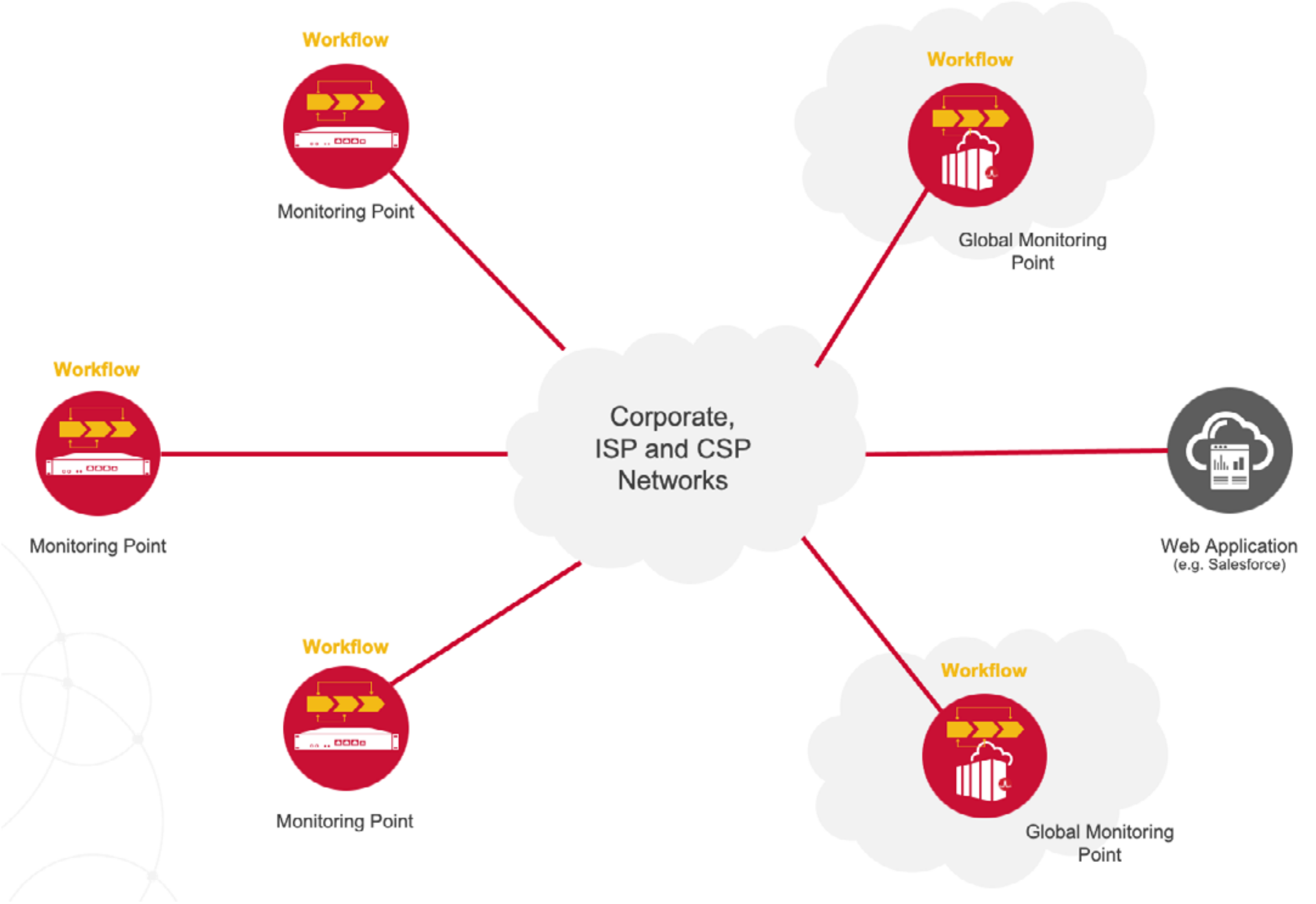
As enterprise networks undergo cloud, SaaS, and Internet transformations, it is crucial for network operations teams to maintain a superior end-user experience. However, it is no longer just about keeping networks and applications up and running. To achieve successful transformation initiatives, network teams must ensure they can contend effectively with applications they do not have full control over. The key to validating experience is to monitor applications from where users are located. Running tests throughout the day on a consistent interval allows baseline performance to be monitored, so when issues occur, there is an opportunity to spot and fix the problem before users complain.

However, many operations teams are still over dependent upon end users to detect application issues at remote locations. When problems are encountered, users quickly lose confidence in the quality of services provided. Too often, operations teams only find out about issues and start trying to troubleshoot after there's been a significant impact on user productivity. It's no surprise then that end users will be quick to blame network teams whenever performance issues arise, no matter where the issue occurs or which team or service provider is actually responsible.

Because network operations teams lack visibility into the user experience, they have no way to determine where the problem is located when users complain—or even if it's a legitimate complaint. When issues arise, teams can't tell whether they're occurring within their own network domain, within an application owned by another team, or on the network of a third-party service provider. Teams' focus, time, and resources are largely dedicated to "firefighting," rather than focusing on higher value, more strategic endeavors.

Synthetic monitoring is 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. Tests are run periodically, and if performance degradation is detected, the NOC is alerted. These scripting strategies can take various forms, though, and vary widely in sophistication and complexity.

NetOps by Broadcom can monitor applications synthetically from behind the firewall by running live scripts against any application. This is one of the rare solutions that can do active network testing and synthetic web experience monitoring, and provide deep packet visibility. The only other way to gain these combined monitoring capabilities is by employing an array of tools that deliver fragmented visibility—and add significant administrative burden for the network operations team.

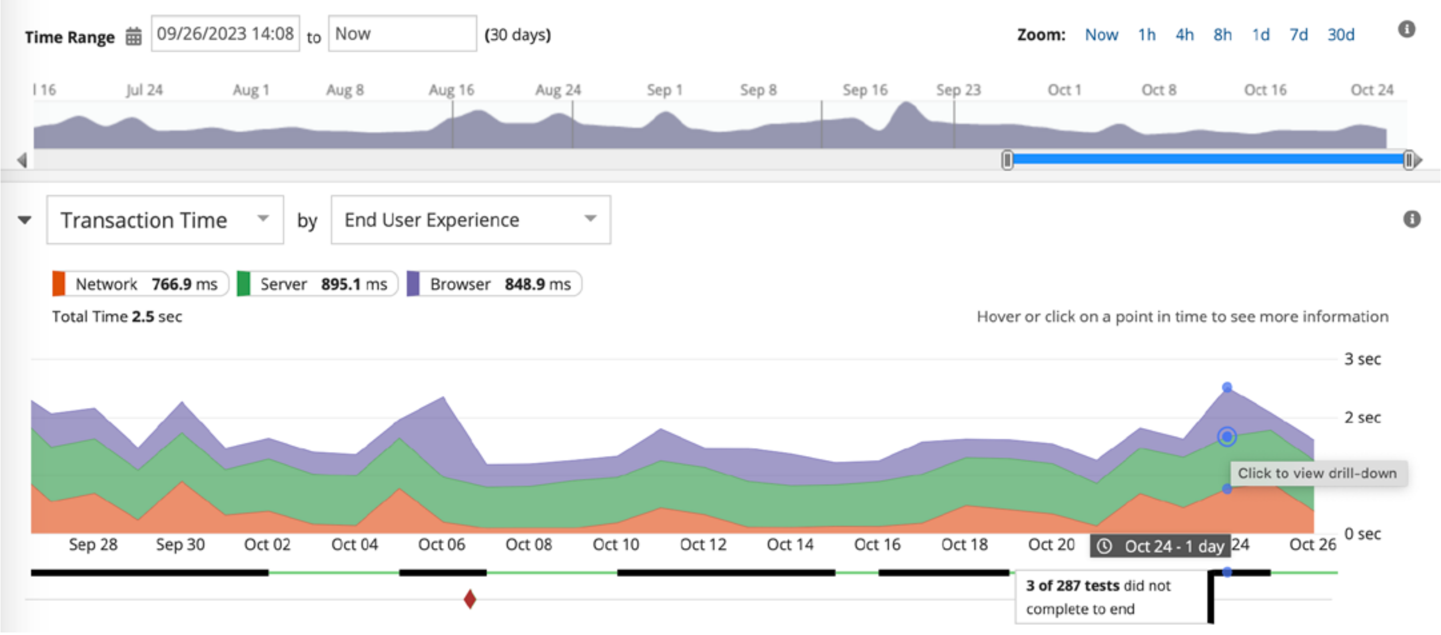


NetOps by Broadcom enables teams to deploy monitoring points at the same location as end users, and run workflows interacting with a web application.

The solution provides insight into how web applications are performing from a user or client application perspective. Monitoring points execute transactions that emulate user or client interactions with an application. Transactions can be generated by two different types of workflows:

- **Browser workflows.** Browser workflows are primarily used to monitor HTML-based web apps. These scripted synthetic transactions emulate an end user's interactions with a web page through a browser. The solution utilizes Selenium, an open-source framework for automating web browsers and testing web applications. The solution can conduct scripted, user-like interactions and deliver precise performance insights.
- **HTTP workflows.** HTTP workflows are primarily used to monitor web service APIs. These workflows generate direct HTTP requests that emulate interactions with a web service, using commands such as GET, PUT, or POST. Monitoring points generate HTTP requests and send them to a target application's API. By measuring the roundtrip time between the request and the response, the solution enables operators to track a web application's availability and responsiveness.

The workflows are run at regular intervals from monitoring points strategically located in the enterprise network and also from monitoring points that can be located 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 the application experience is outside of acceptable limits.



Time Range 09/26/2023 14:08 to Now (30 days)

Transaction Time by End User Experience

🟥 Network 766.9 ms 🟩 Server 895.1 ms 🟪 Browser 848.9 ms

Total Time 2.5 sec

Hover or click on a point in time to see more information

Click to view drill-down

Oct 24 - 1 day

3 of 287 tests did not complete to end

The Broadcom solution breaks end-user experience measurements down to network, server, and browser response times, and enables operators to drill down into incidents.

To accurately report on the status of web applications, Broadcom uses Apdex. Apdex is an industry-standard method for reporting on and comparing applications in terms of the end-user experience. The Apdex rating is based on converting performance measurements into user satisfaction insights and counting the number of “satisfied,” “tolerating,” and “frustrated” user interactions. This is calculated based on a reference maximum satisfactory time (T) and a maximum tolerating response time (4T). Any response time above this latter threshold is given a rating of frustrated.

APDEX Measurements

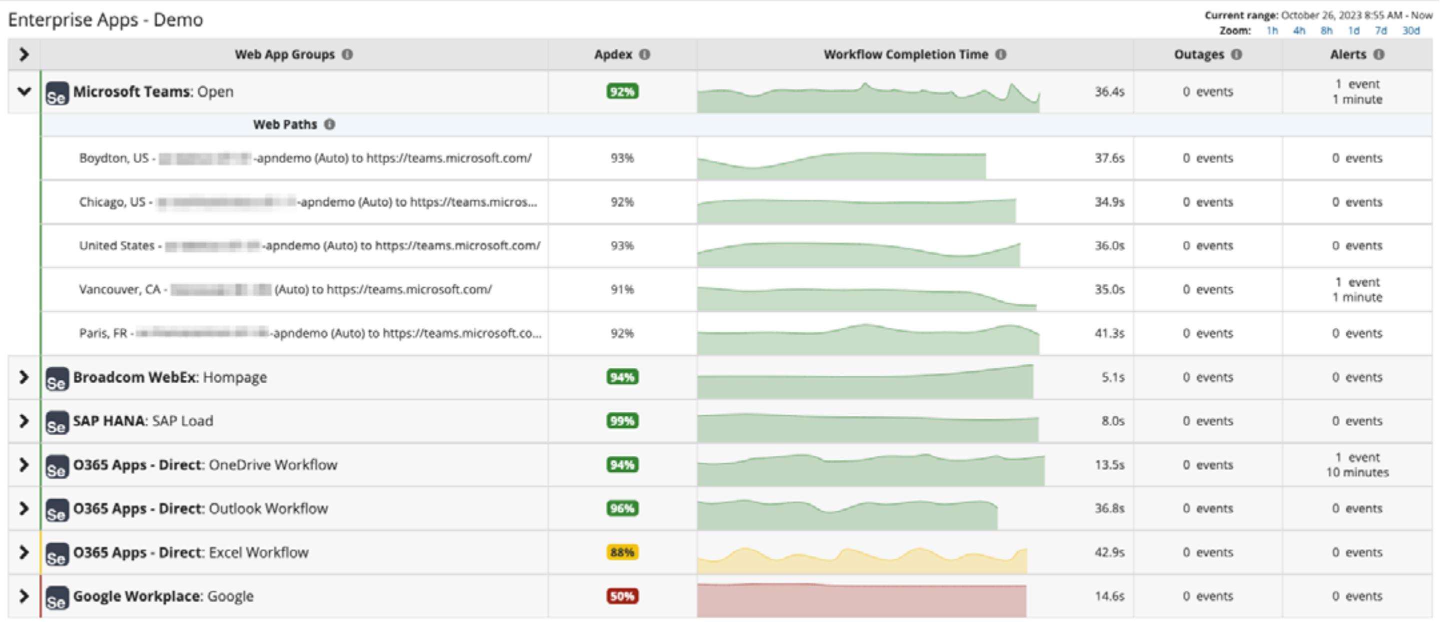
Reference Time	T
Satisfied	<= T
Tolerating	<= 4T
Frustrated	> 4T or failed

The Broadcom solution computes the Apdex score as a ratio of satisfied and tolerated page-load response times to the total number of requests made. Each page load rated as satisfied is counted as 1. Each tolerating page load is counted as 1/2. All others that take longer than the tolerating threshold, and those that fail, are counted as 0.

Here's the Apdex formula used in the solution:

$$\mathit{Apdex}_T = (\mathit{Satisfied\ Count} + (\mathit{Tolerating\ Count} / 2)) / \mathit{Total\ Measurements\ Count}$$

As a result, the Apdex score is equivalent to a weighted average of the three types of interaction counts. In the solution's dashboards and reports, the Apdex score is converted from a value between 0.0 and 1.0 into a percentage from 0% to 100% to provide improved readability.



Enterprise Apps - Demo

Current range: October 26, 2023 8:55 AM - Now
Zoom: 1h 4h 8h 1d 7d 30d

Web App Groups	Apdex	Workflow Completion Time	Outages	Alerts
Microsoft Teams: Open	92%	36.4s	0 events	1 event 1 minute
Web Paths				
Boydton, US - [redacted] -apndemo (Auto) to https://teams.microsoft.com/	93%	37.6s	0 events	0 events
Chicago, US - [redacted] -apndemo (Auto) to https://teams.micros...	92%	34.9s	0 events	0 events
United States - [redacted] -apndemo (Auto) to https://teams.microsoft.com/	93%	36.0s	0 events	0 events
Vancouver, CA - [redacted] (Auto) to https://teams.microsoft.com/	91%	35.0s	0 events	1 event 1 minute
Paris, FR - [redacted] -apndemo (Auto) to https://teams.microsoft.co...	92%	41.3s	0 events	0 events
Broadcom WebEx: Hompage	94%	5.1s	0 events	0 events
SAP HANA: SAP Load	99%	8.0s	0 events	0 events
O365 Apps - Direct: OneDrive Workflow	94%	13.5s	0 events	1 event 10 minutes
O365 Apps - Direct: Outlook Workflow	96%	36.8s	0 events	0 events
O365 Apps - Direct: Excel Workflow	88%	42.9s	0 events	0 events
Google Workplace: Google	50%	14.6s	0 events	0 events

The solution delivers dashboards that display the status of selected web application groups, which are sorted by Apdex scores over time.

Within most enterprises today, end users are highly reliant upon third-party SaaS apps and APIs to perform critical tasks. The solution offers the visibility needed to track and manage these critical services. The solution provides flexible monitoring capabilities that range from simple HTTP requests to multi-step synthetic scripting. In addition, it offers automated alerts for when performance degrades or isn't meeting acceptable thresholds. With these capabilities, teams can better ensure service vendors are meeting their SLAs. For network operations teams who too often are at the receiving end of finger pointing, this visibility is now critical, especially for those applications that the business is reliant upon, but no longer run on internal networks.

Visibility Into Network Utilization

The explosive growth in SaaS applications, cloud services, mobile devices, and video traffic has placed unprecedented demands on networks—and created new challenges for network operations teams. At any given time, a wide range of traffic traverses the network; some of it is lower priority, some is business critical. Further, some traffic may be illegitimate or malicious. Being able to distinguish these different types of traffic is critically important today. It's the only way teams can start to proactively manage quality of service for the most critical applications—while minimizing the cost and damage of illegitimate and malicious traffic.

Understanding network traffic that spans remote offices is critical to ensuring quality end-user experiences. In the past, it made sense to deploy technologies like NetFlow in the data center. However, with increased usage of SaaS applications and broadband Internet, fewer packets are actually traveling through the data center.

Armed with basic network management tools, many operations teams lack the visibility and control they need to optimize their network infrastructure. Further, with the increase in bandwidth-intensive, delay-sensitive network traffic, many organizations have to contend with ballooning infrastructure costs just to meet the service-level expectations of end users. To minimize network infrastructure costs, while ensuring service levels are optimized for high-priority applications and services, operations teams need to understand who is consuming network resources, where they're going, what they're doing, and what kinds of service levels they're receiving.

Packet inspection and flow analysis are two distinct yet complementary technologies that are crucial for assessing network traffic utilization. While both play vital roles for network management, they employ different approaches to achieve their objectives. On the one hand, packet inspection involves the detailed examination of individual packets, scrutinizing various aspects of the payload as it travels through the network. This approach provides granular insights into network utilization but can be data-and resource-intensive.

On the other hand, flow analysis focuses on data aggregated in flow records, which represent summarized information about traffic patterns, such as source and destination IP addresses, ports, and byte counts. The synergy between these two approaches is invaluable in comprehensive network management. Packet inspection excels at catching traffic details, while flow analysis offers a high-level view of overall network behavior. By integrating these methods, network operations teams can gain a holistic understanding of network utilization, swiftly detect and address issues, and plan future operations based on reliable information.

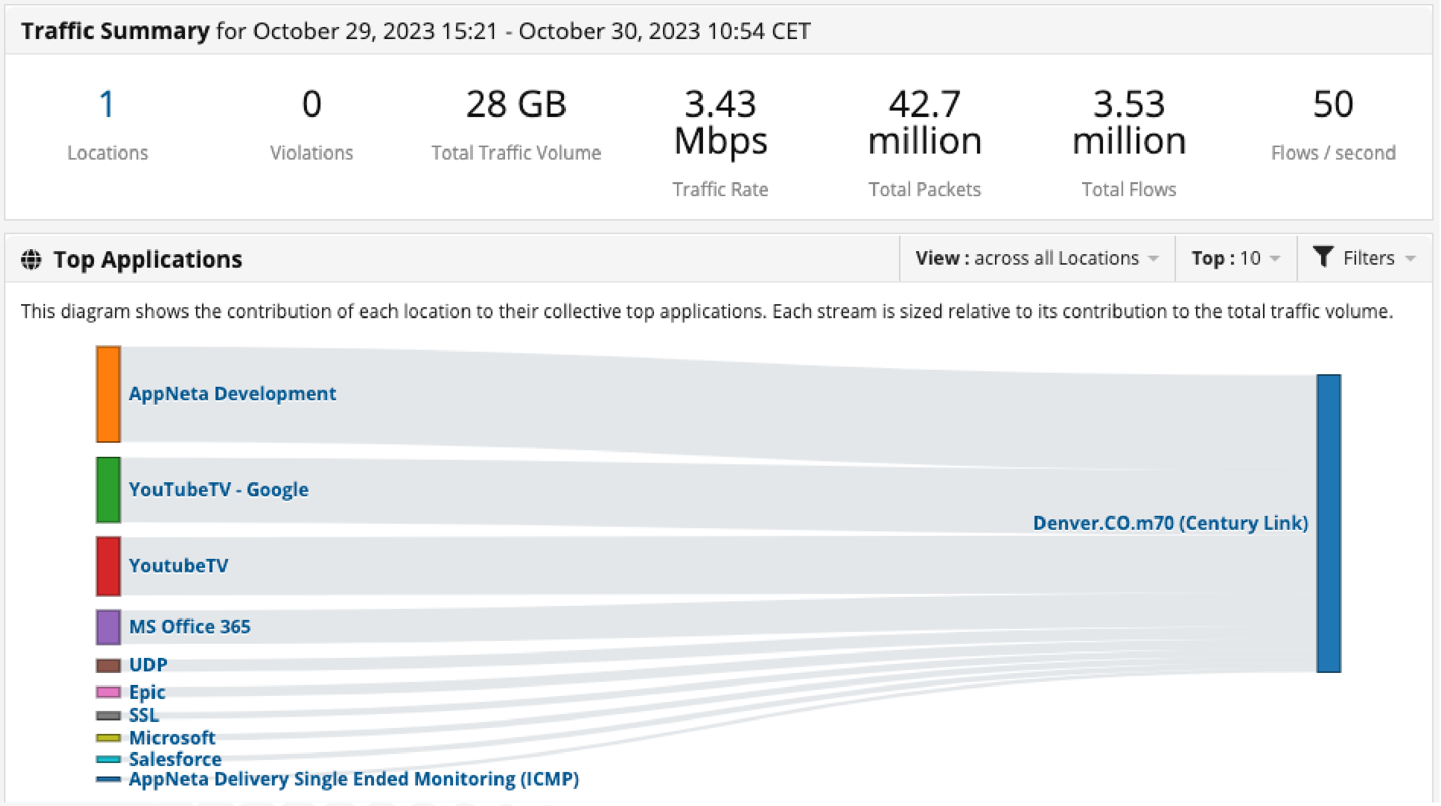
NetOps by Broadcom provides a unique combination of packet inspection and flow analysis. The solution delivers an enterprise-wide view into the composition of traffic on every link and helps teams detect threatening traffic patterns in the making. By providing comprehensive and timely insights into application traffic, the solution helps mitigate the risks of planned changes and unexpected events. With automated baselining, alerting, and investigation capabilities, the solution can speed response when potential performance issues arise. With the solution, NOC teams can identify and resolve problems faster, maximizing service levels of critical applications and services.

NetFlow-enabled devices, such as routers and switches, generate metadata at the interface level and send the information to a flow collector, where the flow records are stored and analyzed. NetFlow is commonly used to refer to multiple types of flow records, such as IPFIX, J-Flow, and sFlow. However, while NetFlow may have sufficed in the past, strategies that leverage only passive traffic analysis simply are not sufficient to meet the monitoring needs of modern networks that extend into ISP and CSP infrastructures. By combining the strengths of both deep packet inspection (DPI) and NetFlow approaches in an effective and scalable platform, the solution helps teams address the requirements of traditional and modern networks. The table below offers an overview of key usage considerations.

	NetFlow (IPFIX, sFlow, J-Flow)	DPI
Use Case	Ideal for monitoring inside the corporate network, with easy setup on devices that operate at layer 3.	Ideal for monitoring at the edge of the network, where applications piggyback on other protocols.
Application Identification	NetFlow sources are port-based, so many popular web applications will only be identified as port 443/HTTPS.	Access to the raw packets can identify far more applications than engines using standards like NBAR2.
Overhead	On average, NetFlow requires 10% overhead on network capacity, and significant CPU utilization on network devices.	Uses purpose-built monitoring devices, so there is no additional traffic and processing overhead on network devices.
Packet Insights	NetFlow is metadata from the packets, not the packets themselves. Additional packet capture might be needed for troubleshooting.	No limit to what is captured, helping to paint a complete picture of performance and enable faster troubleshooting of issues.

The Broadcom solution features an innovative approach that combines the strengths of DPI and NetFlow analysis. As a result, the solution creates a powerful synergy for comprehensive network visibility. The solution provides these key capabilities:

- Ingest and analyze multiple types of NetFlow data generated by compatible network devices in the corporate network, providing actionable intelligence and real-time visibility into network behavior.
- Leverage DPI capabilities of monitoring points at the edges of the network to capture and measure traffic volume information on the cloud services and web applications being used, as well as for the hosts that are accessing those applications.



Traffic Summary for October 29, 2023 15:21 - October 30, 2023 10:54 CET

1	0	28 GB	3.43 Mbps	42.7 million	3.53 million	50
Locations	Violations	Total Traffic Volume	Traffic Rate	Total Packets	Total Flows	Flows / second

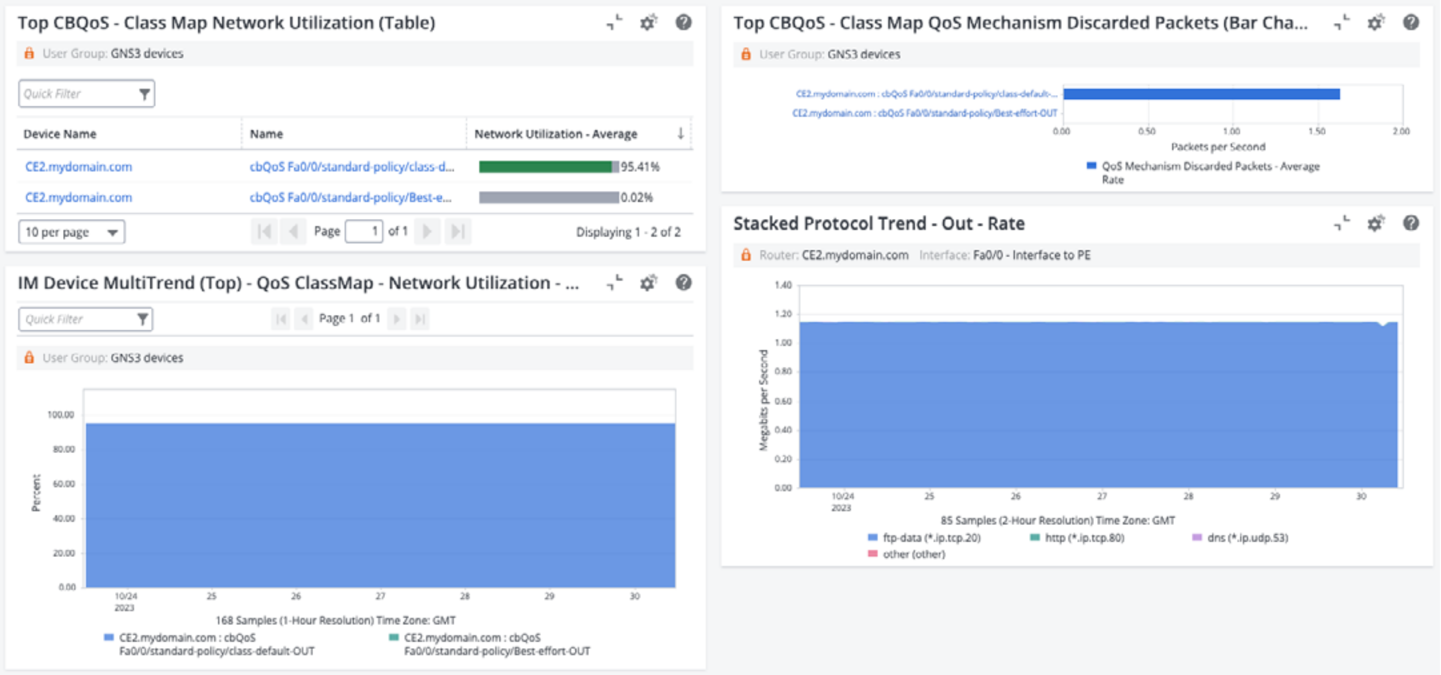
Top Applications

View : across all Locations | Top : 10 | Filters

This diagram shows the contribution of each location to their collective top applications. Each stream is sized relative to its contribution to the total traffic volume.

NetOps by Broadcom uses DPI to help understand what applications are traversing the network edges with location-by-location comparisons and categorized traffic details.

With these holistic analysis capabilities, network operations teams can gain real-time visibility into traffic across all enterprise services. The solution provides an enterprise-wide view into the composition of traffic on every link. This helps teams detect threatening traffic patterns in the making, quickly identify the source of performance problems, validate the impact of planned and unplanned changes within the network, and avoid unnecessary WAN costs.



Top CBQoS - Class Map Network Utilization (Table)

User Group: GNS3 devices

Quick Filter

Device Name	Name	Network Utilization - Average
CE2.mydomain.com	cbQoS Fa0/0/standard-policy/class-d...	95.41%
CE2.mydomain.com	cbQoS Fa0/0/standard-policy/Best-e...	0.02%

10 per page | Page 1 of 1 | Displaying 1 - 2 of 2

IM Device MultiTrend (Top) - QoS ClassMap - Network Utilization - ...

Quick Filter | Page 1 of 1

User Group: GNS3 devices

100.00
80.00
60.00
40.00
20.00
0.00
Percent
10/24
2023
25
26
27
28
29
30
168 Samples (1-Hour Resolution) Time Zone: GMT
CE2.mydomain.com : cbQoS Fa0/0/standard-policy/class-default-OUT
CE2.mydomain.com : cbQoS Fa0/0/standard-policy/Best-effort-OUT

Top CBQoS - Class Map QoS Mechanism Discarded Packets (Bar Cha...

User Group: GNS3 devices

CE2.mydomain.com : cbQoS Fa0/0/standard-policy/class-default-...
CE2.mydomain.com : cbQoS Fa0/0/standard-policy/Best-effort-OUT
0.00
0.50
1.00
1.50
2.00
Packets per Second
QoS Mechanism Discarded Packets - Average Rate

Stacked Protocol Trend - Out - Rate

Router: CE2.mydomain.com Interface: Fa0/0 - Interface to PE

The Broadcom solution delivers valuable insights into applied policies and patterns across different classes of traffic, enabling the NOC team to make more informed decisions.

The Broadcom solution offers comprehensive capabilities for discovering and measuring application traffic, both within the corporate network and across public networks, such as those managed by ISPs and CSPs. The solution enables operations teams to gain much deeper insight into which applications are running in their networks and their traffic characteristics. Leveraging layer 3-7 information, the solution identifies applications and consolidates traffic data for management and reporting. With these capabilities, teams can establish much more intelligent control over network usage and take the steps necessary to fix problems and improve overall network performance.

CONCLUSION

Network operations teams today are facing a technological inflection point. Networks everywhere are being re-architected to support cloud migrations, software-defined transitions, increasing business demands, and high user experience expectations. Meanwhile, teams struggle to keep pace with a constant influx of software-defined technologies in the data center, the increased stress on the WAN due to the growing number of highly sensitive applications, and the pressures to demonstrate high levels of network reliability.

Exacerbating matters is the fact that traditional monitoring solutions, which have been in use for years, were not designed to handle the accelerated pace of change, the interdependent layering of SDN, and the transient, dynamic nature of modern environments and services. Ultimately, teams need to align network delivery and application performance. The ultimate KPI is not network performance anymore, it is the user experience.

What teams need is a network management solution that combines contextual diagnostic abilities with visibility into the actual user experience. They need analytics that can search through monitoring data and handle high-scale correlations. They need solutions that help navigate the maze of interdependent network layers, and provide a unified approach that supports traditional infrastructures, while offering expert views into modern SDNs.

Software Company Improves MTTR by 65%

A global software corporation had adopted Cisco ACI, and sought to migrate all their worldwide data centers to a modern SDDC architecture. They also were planning to use OpenStack as their infrastructure provider. However, the introduction of SDN completely changed the IT management landscape, introducing trade-offs on operational visibility and supportability. Due to new complexities, alarm storms delayed triage times, and teams could not establish relationships between the underlay and overlay, which made it difficult to determine the root cause of issues.

NetOps by Broadcom has helped the company by delivering a unified view of Cisco ACI deployments, including the overlay and underlay. With the solution, network operations teams can extend monitoring beyond the physical layer, and gain a holistic understanding of the relationships between virtual and logical components as well as legacy network devices. As a result, the team improved their MTTR by 65%.

FinTech Company Speeds Triage by 95%

This well-established FinTech institution has grown increasingly reliant on cloud services, which means they're also increasingly reliant upon ISP and cloud providers' networks. Lacking visibility into these externally managed environments, the IT operations team had to set up bridge calls and war rooms to diagnose issues. To ensure quality operations and high service levels, it was increasingly essential for the network operations team to establish end-to-end visibility across all the networks users relied upon.

With NetOps by Broadcom, teams are able to correlate individual device performance and end-to-end network path health, including across internal and externally managed environments. Now they can pinpoint the root cause of any degradation that affects end-user services, whether it arises in internally or externally managed networks. This enables the operations team to identify and resolve any network issue much faster. In fact, with the Broadcom solution, the team was able to speed triage by up to 95%.

Why Broadcom

NetOps by Broadcom delivers the unified, end-to-end network visibility teams need to understand, manage, and optimize the performance of digital services running on traditional and modern SDN architectures. Broadcom extends network operations teams' monitoring reach into edge services, multi-cloud environments, and ISP networks. With the solution, operators can spot every communication path and degradation point, from the core network to the end user.

With its advanced analytics, the solution improves network operations teams' readiness to manage emerging requirements for next-generation network technologies. With a single platform, teams can gain end-to-end, holistic awareness across domains and vendor technologies. This helps teams break down monitoring data silos and reduce operational complexities.

The Broadcom solution uniquely integrates both network monitoring and user experience monitoring, offering the most comprehensive visibility into every aspect of modern networks. As a result, the solution helps teams align network management strategies with key business outcomes, so they can become a better partner in enabling accelerated digital transformation.

BROADCOM®
connecting everything®

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

Broaden-Visibility-White-Paper_BC-NO-2024_CE-4061_v4 February 27, 2024