

WHITE PAPER

3 Keys to Maximizing Operational Consistency in Modern Networking Environments

TABLE OF CONTENTS

Challenge	03
Single Source of Truth	05
Heterogenous Support across Vendors and Technologies.....	06
Unified Visibility across all Network Technologies	07
Integration of Third Party Technologies	09
Ability to Track Device Configuration Changes	12
Automated Discovery and Inventory Management	13
Configuration Management.....	15
Continuous Validation of the Connected Experience	18
Standard Operating Procedures and Workflows	21
Cross Technology and Domain Operations Workflows	22
Integration with ITSM and Collaboration Tools	24
Conclusion	26
MSP Reduces Total Cost of Ownership by 75%.....	26
Financial Services Achieves Eight-Fold Scale in Visibility	27
Why Broadcom.....	27

CHALLENGE

In order to manage increasingly large, complex, and dynamic network environments, it is vital for network operations (NetOps) teams to establish consistent operational approaches. Through consistent network management operations, teams can ensure that networks—and the business services that rely upon these networks—continue to function seamlessly and effectively.

Operational consistency is essential in enabling teams to effectively mitigate disruptions, improve performance, and ensure optimal resource utilization. To achieve operational consistency in network management, teams must establish an effective mix of people, process, organization, governance, architecture, tools, and technology.

However, NetOps teams in a lot of enterprises struggle to achieve this mix. According to an EMA Research Report, the percentage of teams that are successful at managing operations is in steep decline, dropping from 49% in 2016 to 27% in 2022.¹ Operational inconsistencies play an important role in this plummeting success rate. These inconsistencies can have a negative impact across the business. Here are a few of the repercussions:

- **Downtime.** Inconsistency in network management can cause network performance issues or downtime. These issues can have a significant impact on an organization's productivity and service delivery, resulting in revenue losses and brand damage.
- **Security risks.** Inconsistent network operations can leave gaps in security that can be exploited by malicious entities, leaving the business exposed to cyberattacks, data breaches, and reputational damage.
- **Poor performance.** Inconsistent network operations can result in degraded network performance, which can lead to slower application response time, reduced employee productivity, and diminished customer experience.
- **Increased costs.** Inconsistent operations often result in inefficient use of resources, which can lead to higher costs. These increased costs can stem from excess capacity, frequent outages requiring emergency repairs, and increased labor costs due to contending with preventable issues.
- **Compliance issues.** Many industries have regulations around data security and availability. Inconsistent network operations can leave a business exposed to hefty fines and legal exposure associated with compliance breaches.
- **Ineffective change management.** Without consistent operations, network changes, such as software updates or new device implementations, can be poorly managed, causing disruptions or incompatibilities.
- **Delayed decision making.** Lack of consistency in network management may also lead to inaccurate or unreliable network data, which can impede decision-making processes related to IT investments, resource allocation, and strategic planning.
- **Reduced customer satisfaction.** For customer-facing businesses, network inconsistencies lead to service interruptions, which can have a negative impact on customer satisfaction and loyalty and the company's reputation.
- **Scalability issues.** Without consistent operations, it becomes difficult to scale the network infrastructure in order to meet demands associated business growth and change.
- **Overdependence on IT personnel.** When network operations are inconsistent and frequently problematic, businesses become overly reliant on their IT personnel. This might lead to increased burnout and turn over, and the associated loss in knowledge capital. Further, this can introduce gaps in workflows and procedures and diminish the team's ability to focus on strategic initiatives.

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

To avoid these business problems and boost network management success, it is critical that teams prioritize operational consistency with unified practices. Extending reach across all network technologies from a single tool can simplify SOPs, enable L1 Ops to solve more problems, and to decrease MTTR and MTTI. In this white paper, we will discuss one of the key areas that can fuel enhanced consistency: the tooling used in network operations management. In this paper, we examine how these tools can support people, process, and governance.

When it comes to tooling, there are three practices at the core of consistent and effective NetOps management:

- Maintaining a single source of truth across the infrastructure.
- Tracking changes and their impact on network delivery.
- Streamlining standard operating procedures and associated workflows.

SINGLE SOURCE OF TRUTH

Large enterprises often have disparate, siloed technology stacks composed of various technologies from a range of vendors. Typically, these stacks are managed by separate teams and different tools. Within most organizations, teams often use somewhere between three and 10 different network monitoring tools in various environments.² However, business services typically rely upon more than one environment as the technical foundation, meaning that it is difficult to triage and troubleshoot any issue affecting these services. Often, multiple teams need to be engaged, and a number of tools and operating procedures have to be employed. Senior network engineers or service reliability engineers might be able to triage across multiple environments and tools, but troubleshooting becomes more difficult.³ This effort also requires knowledge of and familiarity with multiple diverse solutions, which only the most skilled personnel possess. This is also the reason that most teams are able to solve and close high-priority incidents, but struggle to resolve the hundreds or thousands of low-priority incidents that arise; resolution simply takes too much time.

In the context of network monitoring, the concept of a “single source of truth” refers to the practice of maintaining a centralized and authoritative repository of network-related data and information. By consolidating network data into a central location for analysis, organizations can ensure greater consistency in their network management efforts.

Standardizing on one network management platform allows for better collaboration and knowledge sharing among different teams. This consistency helps to ensure that the knowledge operational teams acquire can be most fully leveraged, and universally applied across vendors and technologies. Network operators, network engineers, and security specialists can access a single set of accurate data, fostering a collaborative and uniform approach to network management. Ultimately, this shared visibility serves to improve operational consistency for the NetOps organization.

Real-Life Challenges Reported by IT Professionals

No single view of network performance. With a mix of cloud providers, SaaS applications, and network providers, and without a single tool to correlate network issues and other systems, finding the root cause of an issue was often difficult.⁴

Here are some key requirements for successfully establishing a single source of truth that provides a comprehensive and up-to-date view of network status.

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

³ Triage and troubleshooting are two different processes. In the context of problem-solving, triage is used to determine the priority of the problem based on its severity, impact, and urgency. Troubleshooting is the process of analyzing or diagnosing a problem to the point of determining a solution. It involves identifying the root cause of the problem and finding a way to fix it.

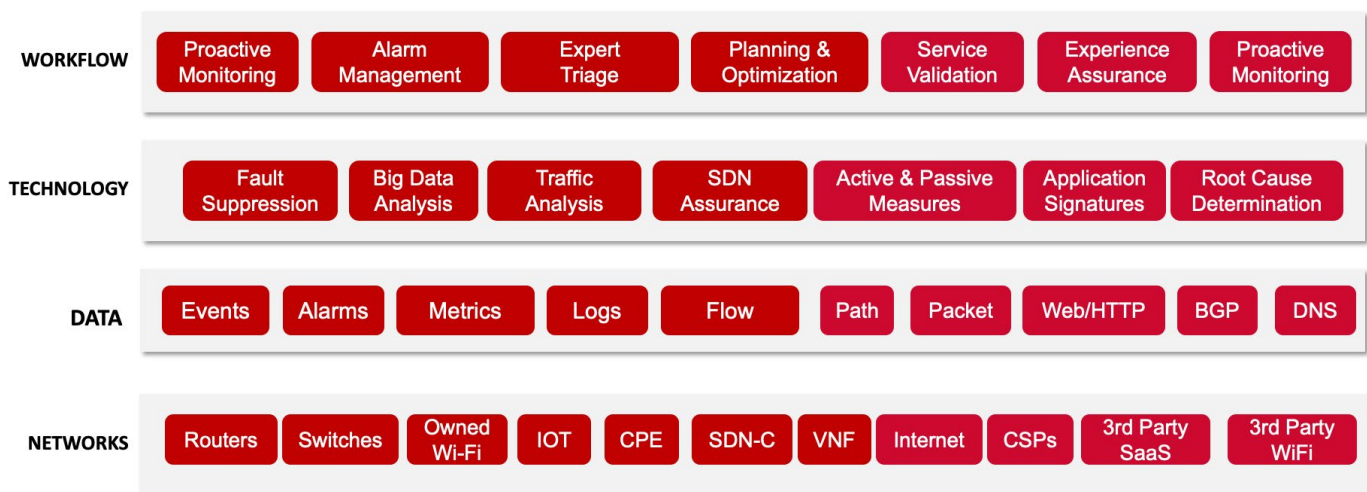
⁴ Forrester, “The Total Economic Impact Of Experience-Driven NetOps By Broadcom,” October 2022

Heterogenous Support across Vendors and Technologies

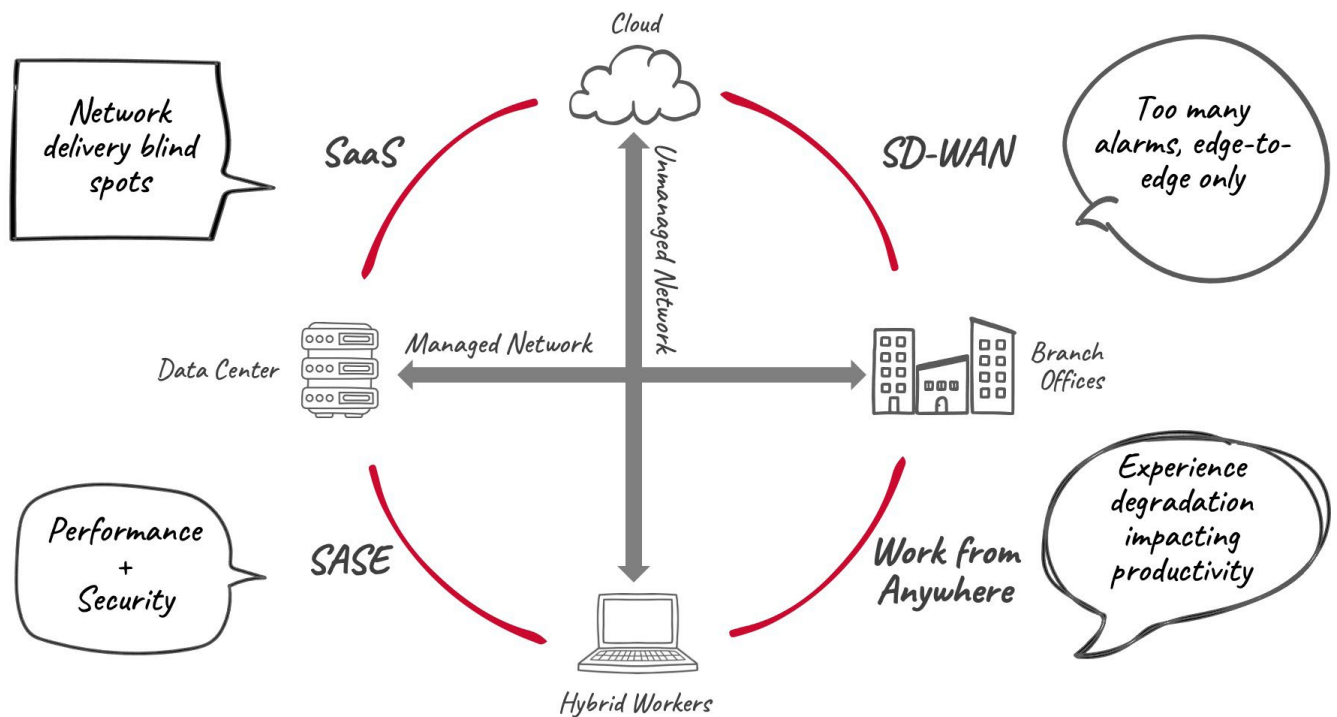
Modern networks incorporate a mix of networking devices—such as routers, switches, firewalls, load balancers, and servers—from various vendors. Each device typically runs embedded operating systems and protocols. Additionally, organizations may be running a diverse array of technologies, including wired or wireless networks, software-defined or virtualized infrastructure, and cloud-based services. By leveraging a unified solution that provides vendor-agnostic support and protocol flexibility, NetOps teams can be empowered to efficiently manage their networks, regardless of the diverse mix of vendors and technologies involved.

NetOps by Broadcom offers a range of advanced features and is one of the most scalable monitoring platforms on the market. The solution can manage up to five million objects at 500,000 metrics per second. With the solution, the third largest telecommunications provider in North America manages more than 2.4 million objects.

Broadcom monitors, stores, analyzes, and displays detailed information to assess performance across large, complex, multi-technology, and multi-vendor network infrastructures. The solution features a distributed server architecture that enables the load balanced management of portions of a large-scale network. With this architecture, customers can establish a unified representation of the network infrastructure, which is composed of multiple domains composed of the models, associations, attributes, values, alarms, events and statistics belonging to a specific management server. Finally, in a cloud environment, the solution offers purpose-built appliances that can monitor more than 10,000 locations.



With the solution, teams can employ monitoring points between remote locations. This enables to gain visibility into the health of both overlay networks (such as SD-WAN tunnels and performance policies) and underlay networks (including CPE and PE across both MPLS and Direct Internet). Teams can monitor the connected experience to a SaaS application or to an enterprise web application. The health of the SD-WAN network is measured using single-ended network paths to the same targets, while the health of the underlay network is measured through a dual-ended network path, that is, with monitoring points employed at both ends.



NetOps by Broadcom delivers total visibility over managed and unmanaged networks.

NetOps by Broadcom unifies the capture and analysis of device health, network traffic, and digital experience monitoring, without a requirement to implement additional solutions. With its broad environment coverage and integration, Broadcom unique solution that enables performance monitoring of end-to-end network paths, including those that span external, third-party managed networks, which are traditionally a blind spot for internal network monitoring solutions.

Unified Visibility across All Network Technologies

While it is important for network management tools to offer technology-agnostic data collection, they must also be able to combine data from various sources into comprehensive dashboards and reports. The goal of unified visualizations is to provide NetOps teams with a holistic view of the network's health and performance at a glance, making it easier to track issues, analyze trends, and collaborate efficiently across teams.

NetOps by Broadcom delivers advanced scalability and features that enable network teams to effectively monitor and manage complex, multi-vendor networks—including traditional, software-defined, and edge infrastructures. The solution provides a single visualization portal that converts inventory, topology, device metrics, logs, configurations, faults, and flows into actionable insights for NetOps teams.

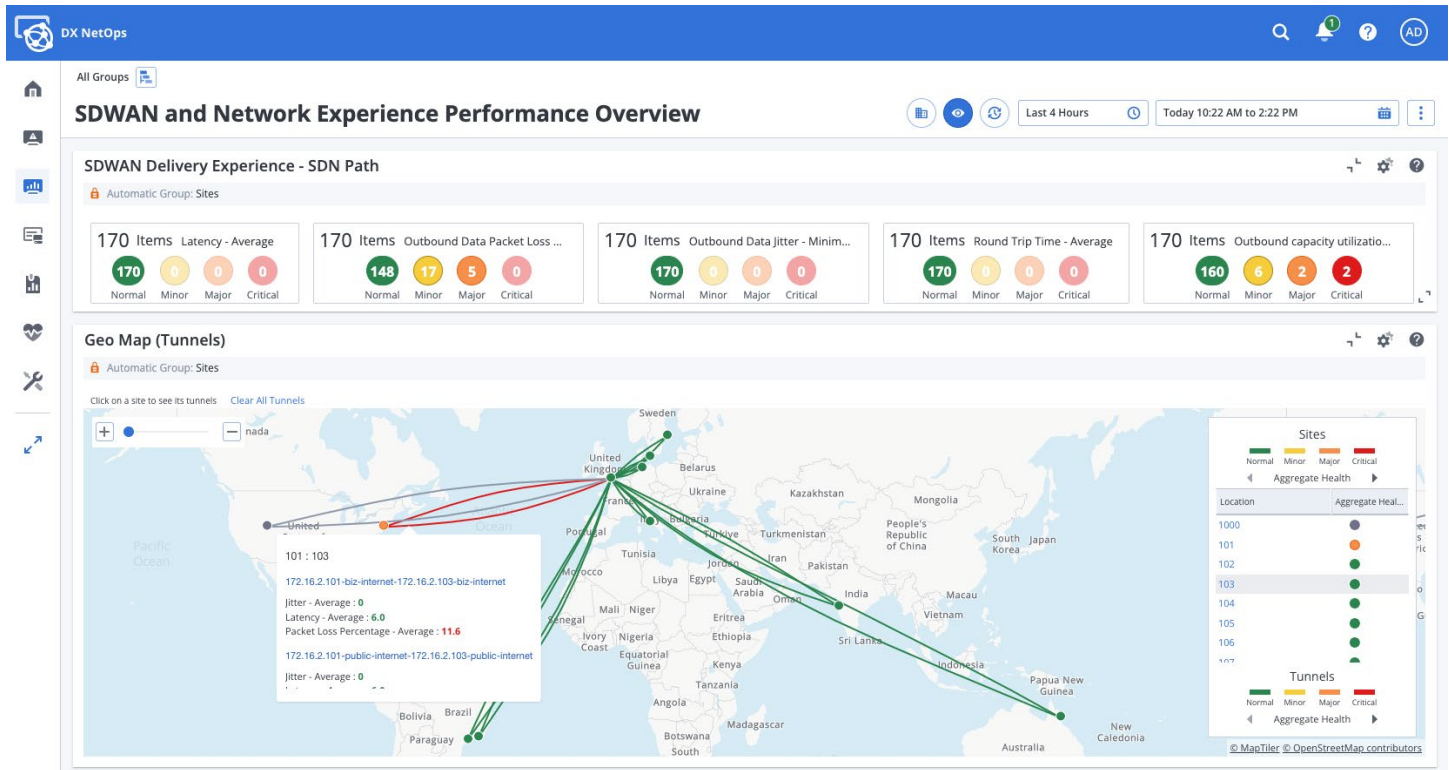
Most importantly, the solution can route end-user experience metrics through the standard operating procedures and workflows that network specialists depend on. With the solution's comprehensive analytics, network teams can more simply and rapidly manage triage, find root causes, escalate to engineers or architects, open trouble tickets, and resolve the network delivery issues that degrade user experiences.



NetOps by Broadcom delivers actionable insights for a variety of network data sources.

NetOps by Broadcom unifies the capture and analysis of device health, network traffic, and digital experience monitoring, without a requirement to implement additional solutions.

NetOps by Broadcom collects, stores, analyzes, and displays massive amounts of performance data, offering holistic visibility across complex network infrastructures. The solution delivers deep visibility into network traffic. With its flexible, intuitive dashboards and reports and unified monitoring visibility, the solution makes it easier for network specialists to interpret complex data, identify potential issues, and manage network resources more consistently and effectively. Ultimately, by leveraging this advanced, unified solution, NetOps teams can maximize operational consistency.



NetOps by Broadcom provides visualizations that enable isolating performance degradations quickly.

Integration of Third Party Technologies

Overall, broad, multi-vendor and multi-technology coverage is crucial for network management tools. This coverage enables seamless data workflows and collaboration among various infrastructures and teams. In today's quickly evolving network landscape, it is indeed challenging for any tool to comprehensively cover every vendor's devices and every emerging technology. This is why the ability to integrate data with third-party technologies can be so vital.

Managing the network from a single platform provides valuable insights and streamlines operational processes. In addition, integrating network operations data into external platforms can play a crucial role in enabling teams to better understand how the network affects overall IT operations. This is particularly true in the context of operational practices, such as Site Reliability Engineering (SRE).⁵ These practices require that IT operations professionals fine-tune service level indicators (SLIs).

SRE principles prioritize proactive management and automation to ensure reliable IT services. By incorporating real-time network data into their operational processes, SRE teams can create more consistent, data-driven procedures and more intelligent automated workflows. This results in a more dynamic and self-adjusting environment that helps minimize downtime and accelerate incident resolution.

⁵ Site Reliability Engineering (SRE) is a set of principles and practices that applies some aspects of software engineering to IT infrastructure and operations.

Ultimately, network management tools need to integrate with external data sources to bridge the gap between native capabilities and the unique requirements of some specific network environments. This approach empowers teams to adapt to their organization's distinctive technologies, while still meeting their network management standardization objectives.

NetOps by Broadcom delivers various integration capabilities that allow NetOps teams to connect network management with other IT systems and tools. The solution features a comprehensive set of APIs, enabling teams to create customized integrations that enhance fault management and performance management processes. This enables teams to take a cohesive approach to building an operations ecosystem and managing networks.

INTEGRATION POINTS

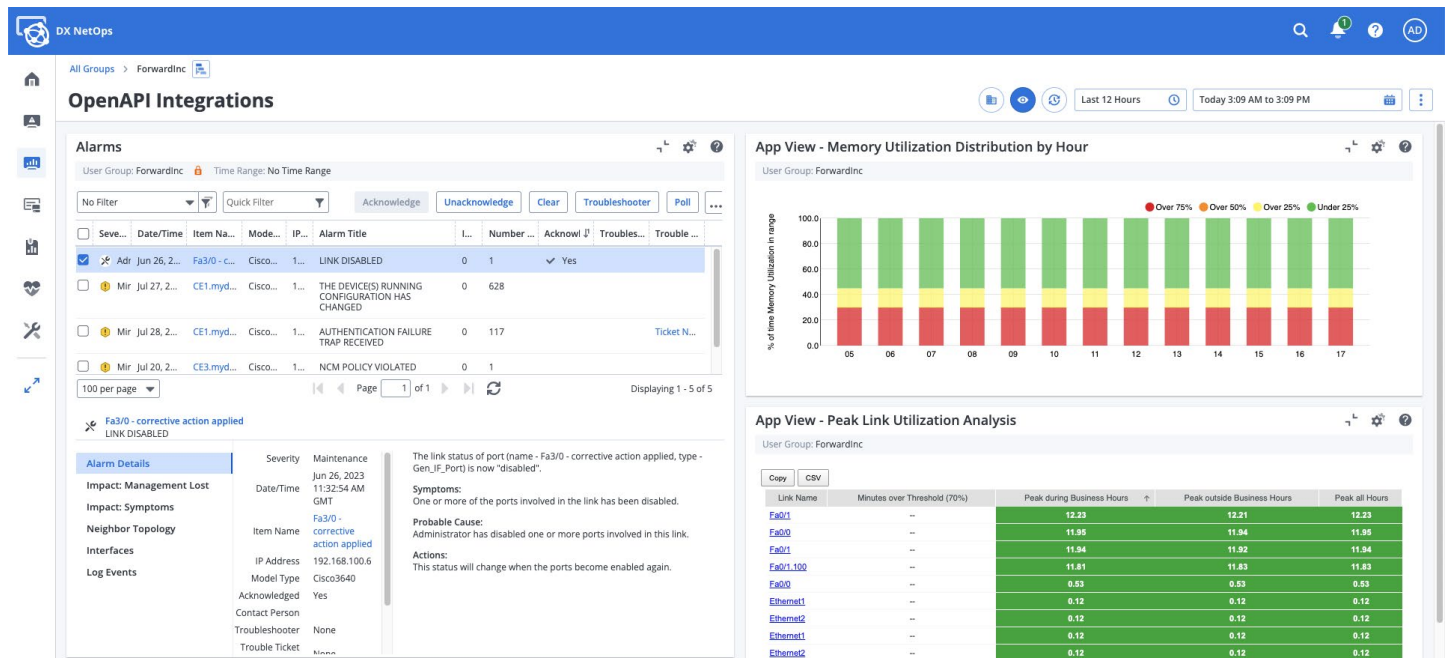
Broadcom is offering several integration points for ingesting or exporting data, enabling teams to create customized integrations. Here are the integration points available:

Integration	Module	Description	Use Case	Technology
WS API	Fault	Read/write access to devices, models, relationships, attributes, actions, and alarms	<ul style="list-style-type: none"> Extract data to third-party apps Bulk administration operations 	Web Service
Alarm Notifier	Fault	Extracts alarms for notifications or actions	<ul style="list-style-type: none"> Implement alarm notifications and actions (SANM) ITSM, emails, scripts Send traps to third-party tools, such as Splunk 	Scripts
Southbound Gateway	Fault	Ingest alerts from third-party sources	<ul style="list-style-type: none"> Use the solution as a master NMS to view all alerts 	Traps / XML
Modeling Gateway	Fault	Import and export network topology data	<ul style="list-style-type: none"> Non discoverable devices (ATM, FR, Wireless) Migrate large landscapes from legacy tools 	XML
CLI	Fault	Unix, Linux, or Window CLI to manipulate configuration data	<ul style="list-style-type: none"> Background actions and bulk administration tasks 	Script
Extension	Fault	Advanced development toolkit	<ul style="list-style-type: none"> Develop product extensions 	Corba ORB
WS API	Perf	Automate tasks that are manually performed in the NetOps portal	<ul style="list-style-type: none"> Set devices in maintenance (lifecycle) Manage groups and members Manage devices and discovery 	REST Web Service
Open API	Perf Flow	Extract data to integrate with external applications	<ul style="list-style-type: none"> Export inventory and performance data Extend native data visualization in the solution's portal 	OData 2.0 / JavaScript
Streaming Export	Perf Flow	Stream data to third-party application	<ul style="list-style-type: none"> Streaming performance data Streaming flow data 	Kafka
Bulk Data Export	Perf	Export data at the frequency of the polling rate	<ul style="list-style-type: none"> External reporting tool Auditing 	CSV
Mediation Manager	Perf	Ingest external performance data	<ul style="list-style-type: none"> Integration of non-SNMP metrics 	Device Pack

OPENAPI APPS

OpenAPI is a flexible interface that can be used to extract performance data from NetOps by Broadcom.⁶ When used with the integrated QueryBuilder, it is possible to extract and explore performance data and create custom URLs for queries. These URLs return customized data in the requested format, so it is easy to view the data in a browser or process it in a custom web application. These capabilities enable seamless integration between Broadcom and any third-party reporting tool or application.

In addition, OpenAPI-enabled apps use the flexibility of OpenAPI queries to deliver and present data in a highly customizable way. OpenAPI enables teams to serve custom content to OpenAPI app views on dashboards and context pages presented in the solution's portal. It is possible to build OpenAPI apps from scratch or to select a specific capability from various available apps. After deployment, the new apps are displayed directly in the portal console.



Alarms

User Group: Forwardinc | Time Range: No Time Range

Buttons: Acknowledge, Unacknowledge, Clear, Troubleshooter, Poll

Seve...	Date/Time	Item Na...	Mode...	IP...	Alarm Title	L...	Number ...	Acknowl ↓	Troubles...	Trouble...
✓	Jun 26, 2...	Fa3/0 - c...	Cisco...	1...	LINK DISABLED	0	1	✓	Yes	
ⓘ	Mir Jul 27, 2...	CE1.myd...	Cisco...	1...	THE DEVICES RUNNING CONFIGURATION HAS CHANGED	0	628			
ⓘ	Mir Jul 28, 2...	CE1.myd...	Cisco...	1...	AUTHENTICATION FAILURE TRAP RECEIVED	0	117			Ticket N...
ⓘ	Mir Jul 20, 2...	CE3.myd...	Cisco...	1...	NCM POLICY VIOLATED	0	1			

100 per page | Page 1 of 1 | Displaying 1 - 5 of 5

Alarm Details

Severity: Maintenance
Date/Time: Jun 26, 2023 11:32:54 AM GMT
Impact: Management Lost
Impact: Symptoms
Neighbor Topology
Interfaces
Log Events

Item Name: Fa3/0 - corrective action applied
IP Address: 192.168.100.6
Model Type: Cisco3640
Acknowledged: Yes
Contact Person
Troubleshooter: None
Trouble Ticket

The link status of port (name - Fa3/0 - corrective action applied, type - Gen_IF_Port) is now "disabled".
Symptoms: One or more of the ports involved in the link has been disabled.
Probable Cause: Administrator has disabled one or more ports involved in this link.
Actions: This status will change when the ports become enabled again.

App View - Memory Utilization Distribution by Hour

User Group: Forwardinc

Time Range: Last 12 Hours | Today 3:09 AM to 3:09 PM

Legend: Over 75% (Red), Over 50% (Yellow), Over 25% (Green), Under 25% (Light Green)

App View - Peak Link Utilization Analysis

User Group: Forwardinc

Buttons: Copy, CSV

Link Name	Minutes over Threshold (70%)	Peak during Business Hours	Peak outside Business Hours	Peak all Hours
Fa0/1	--	12.23	12.21	12.23
Fa0/0	--	11.95	11.94	11.95
Fa0/1	--	11.94	11.92	11.94
Fa0/1_100	--	11.81	11.83	11.83
Fa0/0	--	0.53	0.53	0.53
Ethernet1	--	0.12	0.12	0.12
Ethernet2	--	0.12	0.12	0.12
Ethernet1	--	0.12	0.12	0.12
Ethernet2	--	0.12	0.12	0.12

NetOps by Broadcom dashboards can mix out-of-the-box components such as alarms lists, with custom OpenAPI Apps views.

NetOps by Broadcom delivers various integration capabilities that allow NetOps teams to connect network management with other IT systems and tools.

⁶ The OpenAPI specification, previously known as the Swagger specification, is a standard for a machine-readable interface definition language.

ABILITY TO TRACK DEVICE CONFIGURATION CHANGES

NetOps teams are responsible for managing complex, often fragile environments. As a consequence, teams are fearful of delivering the level of agility required by new digital initiatives, because of concerns around potential network disruptions. However, networking technology has followed the same path as data center trends. Programmable, software-defined, and cloud-based network environments have made agile networks a reality through the use of infrastructure-as-code and automation.

The problem is that many teams' fractured toolsets lead to poor overall visibility into network configuration. Also, a large toolset tends to result in teams having poor processes and policies around change controls. That's because these tools tend to have overlapping capabilities around network changes, making it difficult, if not impossible, to institute change controls. These changes can create performance problems or leave an organization exposed to potential security breaches. Further, these overlapping toolsets also make solving issues more difficult.

By tracking changes, teams can quickly identify modifications and undo potentially problematic changes. It is especially useful when network experience issues can be associated with changes, giving teams an opportunity to fix problems early—before they have an actual impact on business activities. Also, in regulated industries, organizations might be required to control and document all network changes for auditing purposes.

As organizations are pressured to increase the agility of network operations processes, traditional practices can be a roadblock to accelerated network transformations. It is for these reasons that teams need configuration management and pre- and post-change validation of network delivery. Without these capabilities, risk-averse network teams will be wary of managing a larger volume of changes more quickly, given all the potential exposure these changes can introduce. All of this points to the need to consolidate disparate network management tools, and establish a unified platform capable of accurately tracking and visualizing the effects of changes.

Real-Life Challenges Reported by IT Professionals

No comprehensive inventory of network equipment and the devices that connect to it. Knowing the topography of a network—which devices were connected to each other and in what order—was a challenge. The process for creating and updating inventory databases was time consuming and error prone.⁷

Here are some key requirements for establishing a successful network change management strategy across modern network environments.

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

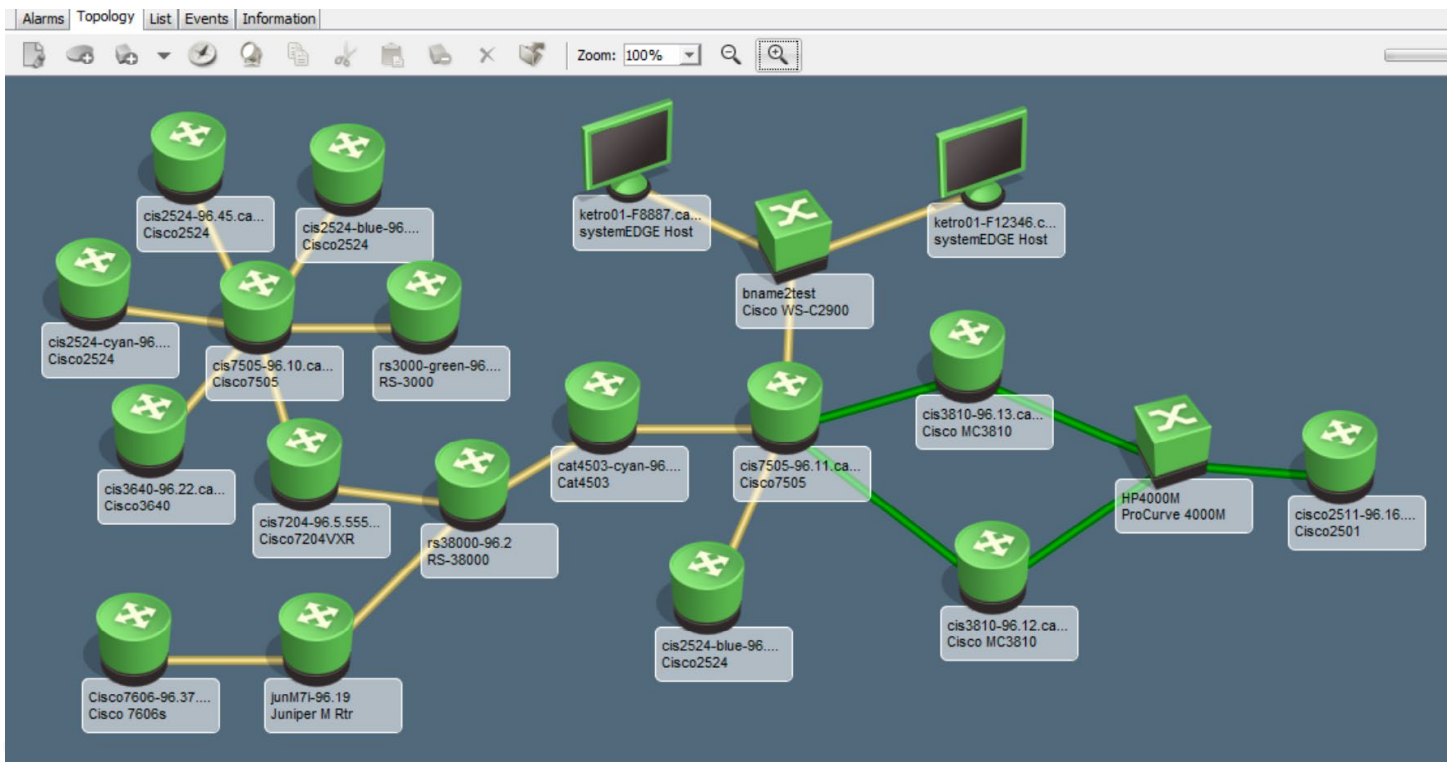
Automated Discovery and Inventory Management

Creating and maintaining an up-to-date inventory of network assets, devices, and virtual resources, and doing so with minimal manual intervention, is a fundamental requirement for effective network management today. These capabilities play an essential role in enabling proper change management. To automate the discovery process, teams often need specialized software that can scan the network, collect relevant information, and create a comprehensive map of the network's topology.

However, these specialized discovery tools typically lack integration with other network management tools, such as those for configuration management and performance monitoring. This reduces the overall efficiency of network management processes. With modern networks incorporating traditional, SDN, and NFV elements, network tools must be in a continual state of discovery. These tools must constantly look for new elements being created and for the hypervisor-driven migrations of elements and workloads.

NetOps teams need a centralized analytics engine that brings together monitoring and topology data. This can enable more accurate root cause identification, network self-healing, and service-to-infrastructure correlation, while equipping teams with consistent insights across dynamic infrastructures.

NetOps by Broadcom automatically discovers networks and device configurations, creates a model of the environment, and maps the topology down to individual ports and paths. The solution's modeling technology generates an accurate topology map that is automatically updated as devices are changed, added, or deleted. The modeling offers support for the highly dynamic nature of hypervisor-based and software-defined entities, endpoints, and virtual machines (VMs). The solution also captures device configurations during discovery. This allows network operators to use change awareness as an aspect of root cause analysis, so they can spot when updates cause outages or performance issues.

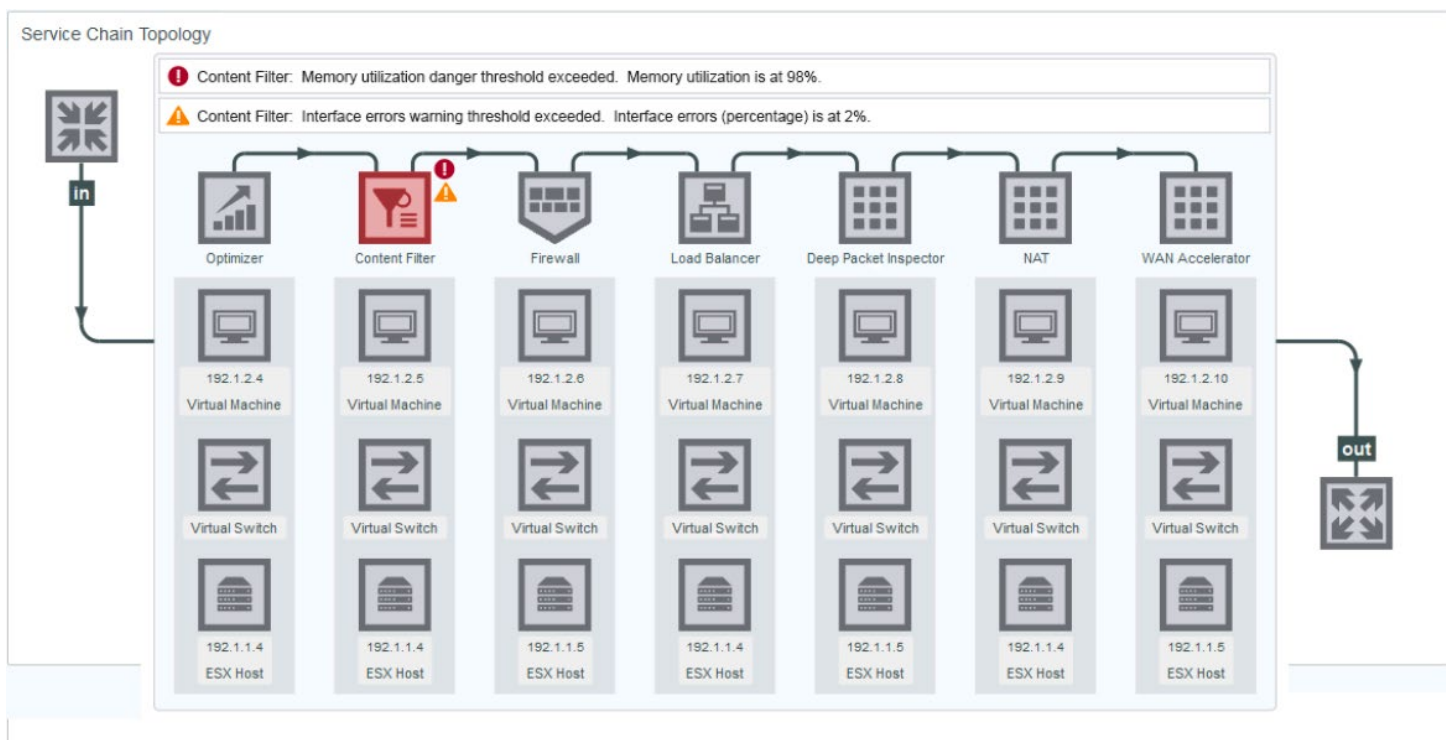


NetOps by Broadcom modeling technology creates accurate network maps with dependencies.

The solution also supports discovery and modeling of wireless LAN controllers (WLCs) and connected access points. With the solution, teams can confidently deploy wireless networking and support their organization's increased reliance on wireless wearables, mobile phones, laptops, smart meters, scanners, point-of-sale systems, IoT, and more.

At the core of NetOps by Broadcom is the ability to model SDN and NFV environments as a multi-layer stack. By applying this model to the collection, normalization, presentation, and analysis of data, the solution can adapt to the dynamic nature of components in these types of networks. This tracking is accomplished through a component-level, relationship-mapping approach that can maintain an updated network stack, while the smallest components expand, contract, relocate, transform, and so on.

NetOps by Broadcom uses a uniform data model that represents the multi-layer stack. The data model also contains relationship IDs for each associated layer. If a VM changes, a new relationship ID for the VM layer will be created and sent upstream to the other subscribers. This is a scalable way to track granular changes in dynamic SDN and NFV networks.



NetOps by Broadcom enables teams to model and visualize the building blocks of SDN and NFV service chains.

Broadcom supports service chaining and presents collection data, inventories, and performance in a service chain view. The solution visualizes logical VNF connections as well as the building blocks that support the chain, helping improve NetOps teams' operational knowledge and troubleshooting. As a result, NetOps groups can easily discover, model, monitor, and manage the relationships between the network infrastructure and business services.

The solution offers patented discovery and topology mapping that fuels effective root cause analysis and fault isolation. By providing comprehensive coverage across traditional, software-defined, and wireless networking technologies, Broadcom provides essential capabilities for efficiently managing modern networks.

Configuration Management

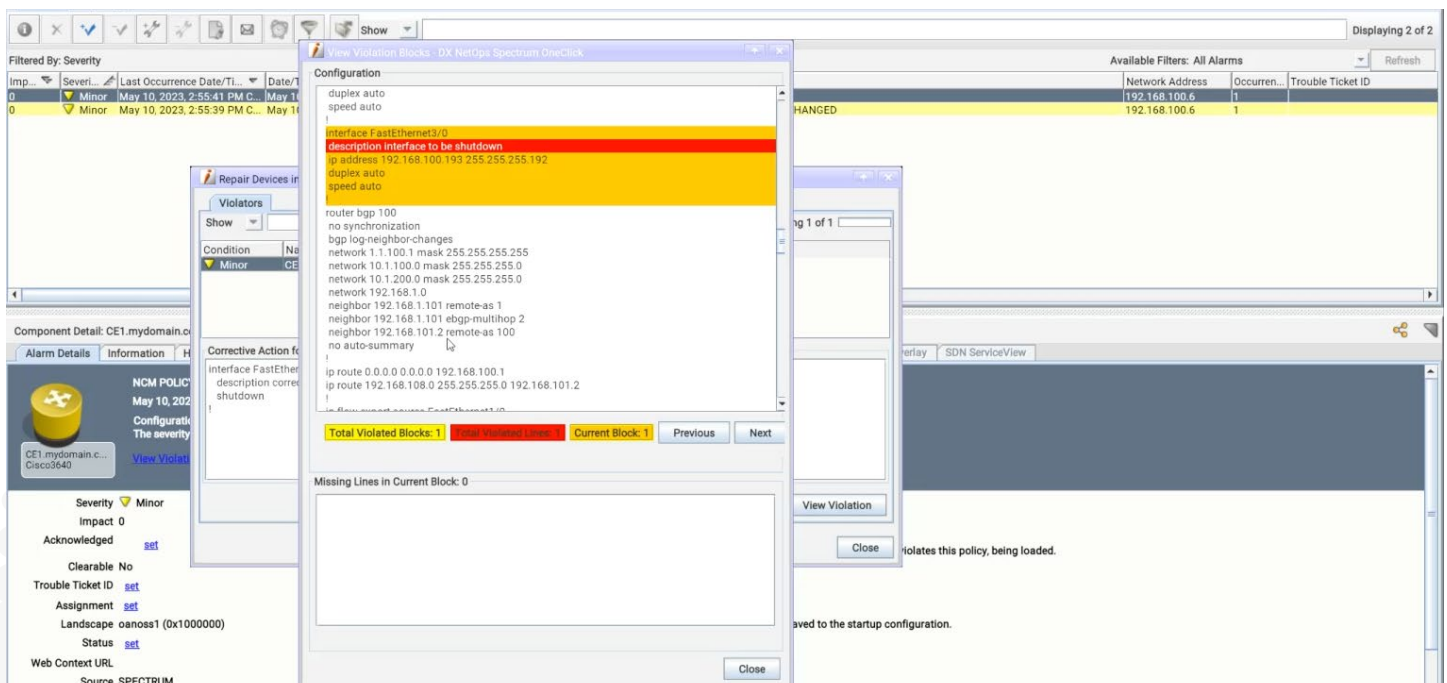
Network configuration management involves tracking and updating configuration settings for routers, switches, firewalls, load balancers, and other physical or virtual network devices. The primary goal is to ensure network devices are configured consistently to avoid the risks of misconfigurations that can lead to performance issues, downtime, and security vulnerabilities. Configuration management and automated discovery should work hand in hand to facilitate the maintenance of an accurate, up-to-date, and consistent picture of the network infrastructure.

Configuration management helps to maintain a version history of configuration files. It serves as a safety net for network teams, allowing them to roll back to a previous configuration in the event that problems arise after a change. It also enforces a structured and consistent approach to making changes to the network by supporting the establishment of configuration policies that serve as reference points when auditing configurations over time.

Automated remediation and configuration management should work together to ensure a stable network environment. When a device configuration deviates from predefined rules and policies, the configuration manager restores the device to its last known good configuration automatically. This tight integration helps maintain consistency and compliance while minimizing the manual intervention required by network teams.

NetOps by Broadcom offers integrated configuration management capabilities that minimize the complexity of managing network device configuration changes. The solution enables teams to manage the capture of configurations, modifications, loads, and verifications for thousands of network devices from virtually any vendor. With the solution, each configuration is time stamped and identified by the revision number. Configuration comparisons can be scheduled to run automatically, and teams can be notified immediately if any unauthorized changes are detected. The solution delivers this comprehensive set of capabilities:

- Capture and store device configurations
- Perform firmware uploads
- Generate alarms based on policy violations
- Report globally on policy compliance
- Provide an audit trail of changes
- Automate remediation of configuration issues



The screenshot displays the NetOps by Broadcom interface, which is used for managing network configurations and detecting violations. The interface is divided into several sections:

- Top Left:** A table showing filtered violations by severity. The table has columns for 'Severity', 'Last Occurrence Date/Time', and 'Date/Time'. A row shows a 'Minor' violation on 'May 10, 2023, 2:55:41 PM C...'.
- Bottom Left:** A panel for 'Component Details' for 'CE1.mydomain.c...'. It includes fields for 'Severity' (Minor), 'Impact' (0), 'Acknowledged' (set), 'Clearable' (No), 'Trouble Ticket ID' (set), 'Assignment' (set), 'Landscape' (oanoss1 (0x1000000)), 'Status' (set), and 'Web Context URL' (Source SPECTRUM).
- Center:** A 'View Violation Blocks' dialog box showing a configuration snippet for 'interface FastEthernet2/0'. The configuration includes:


```

duplex auto
speed auto

interface FastEthernet2/0
description interface to be shutdown
ip address 192.168.100.193 255.255.255.192
duplex auto
speed auto

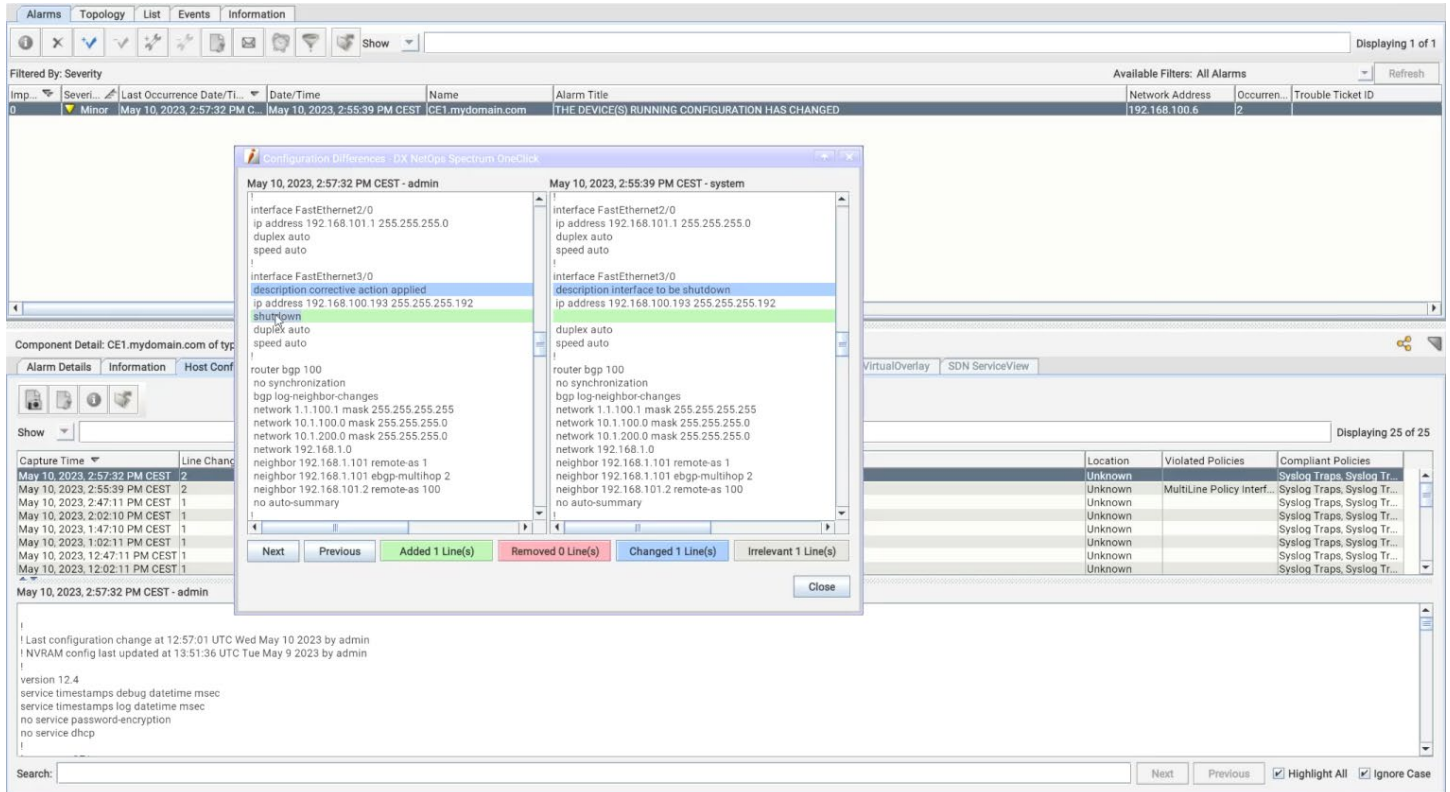
router bgp 100
no synchronization
bgp log-neighbor-changes
network 1.1.100.1 mask 255.255.255.255
network 10.1.100.0 mask 255.255.255.0
network 10.1.200.0 mask 255.255.255.0
network 192.168.1.0
neighbor 192.168.1.101 remote-as 1
neighbor 192.168.1.101 ebgp-multihop 2
neighbor 192.168.101.2 remote-as 100
no auto-summary

ip route 0.0.0.0 0.0.0.0 192.168.100.1
ip route 192.168.108.0 255.255.255.0 192.168.101.2
      
```

 The dialog also shows 'Total Violated Blocks: 1' and 'Current Block: 1'.
- Right:** A table showing available filters and a list of violations. The table has columns for 'Network Address', 'Occurren...', and 'Trouble Ticket ID'. A row shows '192.168.100.6' with '1' in the 'Occurren...' column.
- Bottom Right:** A 'View Violation' dialog box with a 'Close' button and a message: 'violates this policy, being loaded.'

NetOps by Broadcom uses policies to detect and report configuration violations.

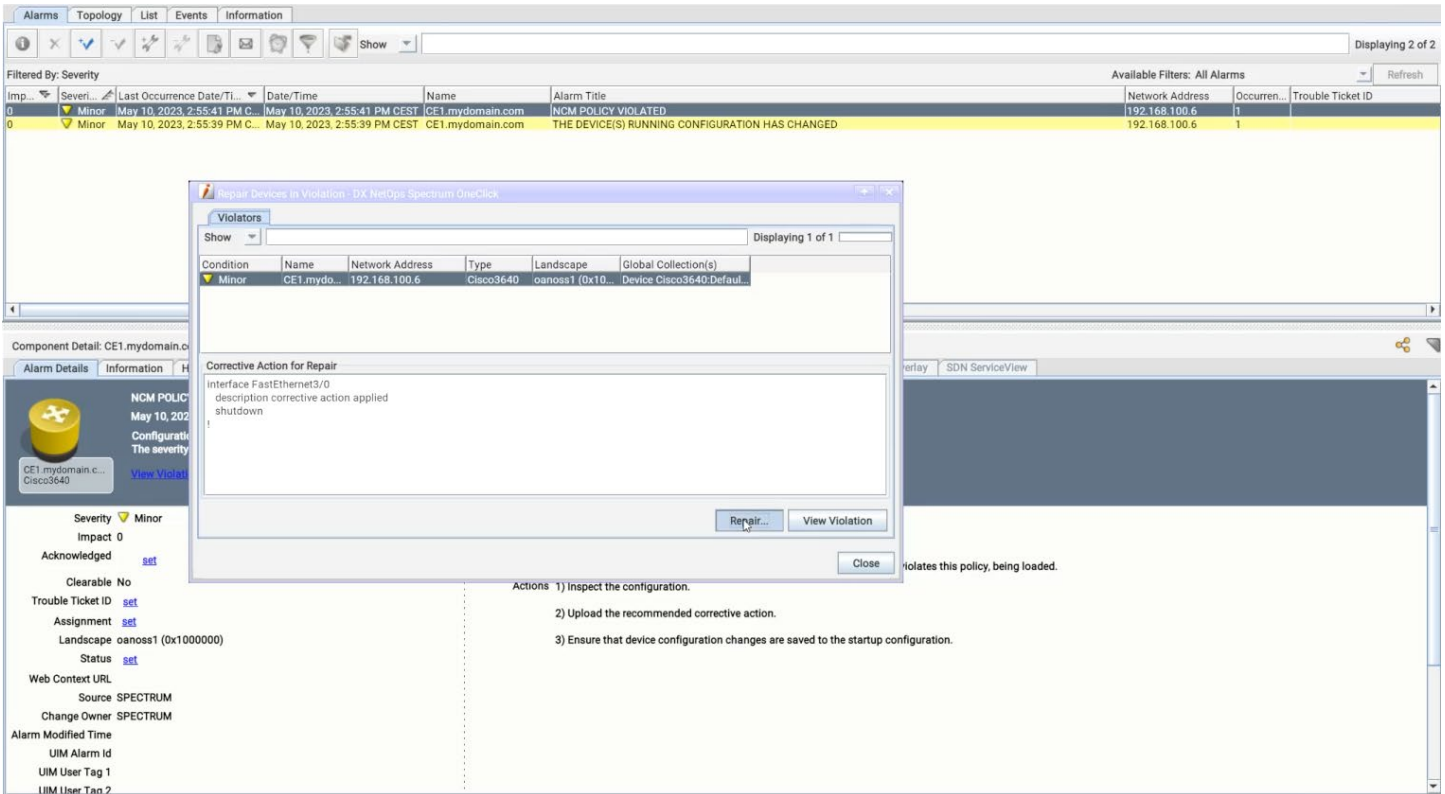
Integration of fault management and network configuration management enables correlation of network events with configuration change activity. The solution can also provide a configuration audit trail of any selected network device, capturing the history data typically retained by fault management tools. As a result, Broadcom delivers a change-aware root cause analysis solution.



NetOps by Broadcom keeps a history of configuration versions and enables searching for differences.

Configurations can be uploaded to multiple devices simultaneously, and any changes are automatically tracked. Teams can schedule automated configuration captures. The solution can then notify appropriate individuals of any unauthorized or policy-violating changes.

NetOps by Broadcom offers integrated configuration management capabilities that minimize the complexity of managing network device configuration changes.



NetOps by Broadcom detects policy-violating device configurations and enables manual or automated repair.

By providing a single network management platform that incorporates network configuration intelligence, teams can realize a range of benefits:

- Uniform configurations can become routine, reducing the likelihood of human error, which results in less downtime and degradation.
- Regular automated capture of configurations and comparison against an organization's configuration policies can pinpoint changes that may lead to availability or performance issues, before users are affected.
- Associating device configurations and configuration changes as part of automated root cause of any fault will result in faster issue identification and resolution.
- Integrated network service, fault, and configuration management intelligence can help teams improve administrative and cost efficiency. This reduces the manual tasks that prevent IT staff from tackling more interesting and strategic projects.

Continuous Validation of the Connected Experience

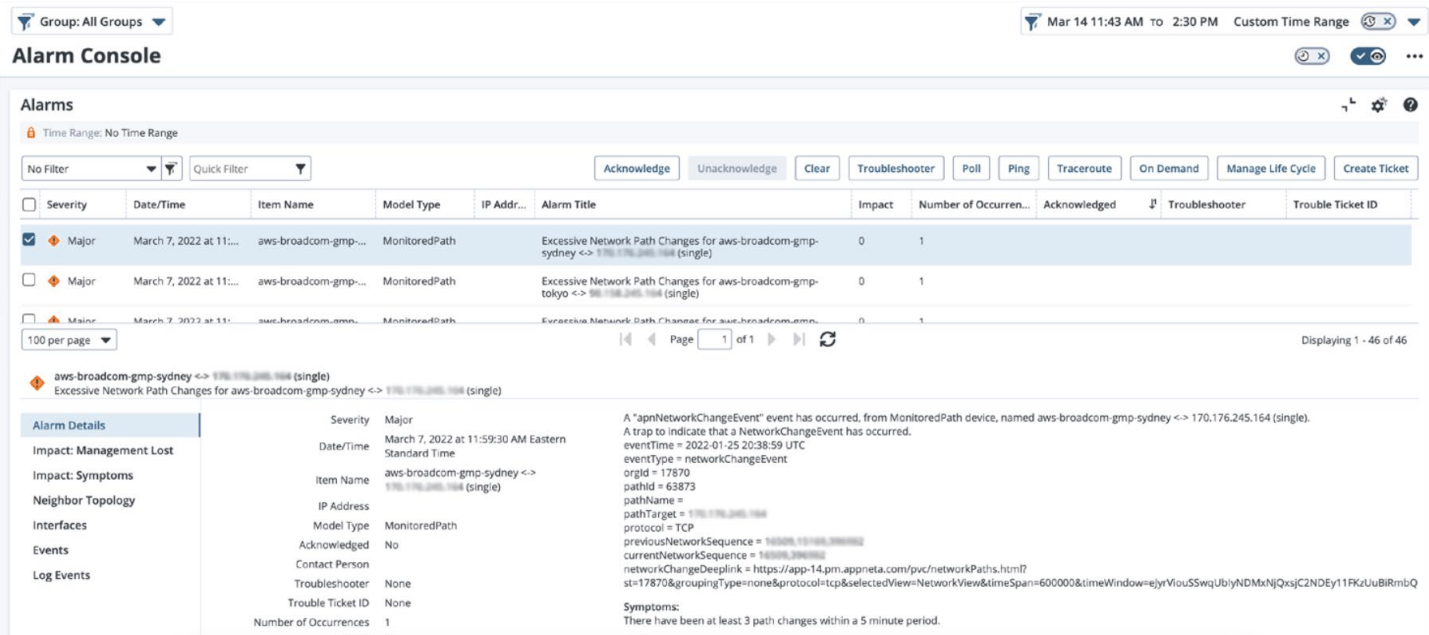
When implementing changes to the network, such as infrastructure upgrades, configuration adjustments, or new device implementations, it is essential to ensure that the user experience is not negatively impacted. However, this gets more difficult as teams move application workloads from traditional data centers to multi-cloud platforms and co-located data centers. These transformations have introduced third-party performance dependencies and reduced visibility. Since traffic is delivered over multiple networks that reside outside of the enterprise data center, network teams are blind to around 75% of the network delivery path.

Traditional passive monitoring relies on aggregating metrics drawn from owned devices, using SNMP or flows as primary ways to capture performance data. This creates a fundamental challenge considering the dynamic aspect of software-defined and internet-based infrastructures. When the network topology can change several times a day, validating network delivery requires different ways to measure performance. By gathering Border Gateway Protocol (BGP) data from public sources and using active monitoring that periodically sends test packets over the network (whether owned or third party), teams can begin to understand the actual performance being delivered.

Ultimately, by integrating continuous monitoring and configuration management, teams can take a proactive approach to network management and deliver a consistent user experience, while accelerating network transformations.

NetOps by Broadcom enables teams to gain vendor-agnostic, end-to-end connection visibility from the perspective of the end user. The solution offers coverage that spans across all networks, regardless of technology, location, or ownership. With the solution's capabilities for active testing and synthetics, teams can gain deep insights into the network delivery experience. This includes key insights into hop-by-hop performance across ISPs and cloud networks. With this solution, NetOps teams are equipped to validate the performance of the network paths that connect end users and systems to applications and services, within and beyond the four walls of the data center.

By integrating change, events, and performance data into a single platform, teams can gain a seamless operations experience and leverage industry best practices and best-in-class triage and alarm correlation workflows. With Broadcom, network operations center (NOC) personnel can easily triage outages and end-user experience issues across the entire path of network transactions.



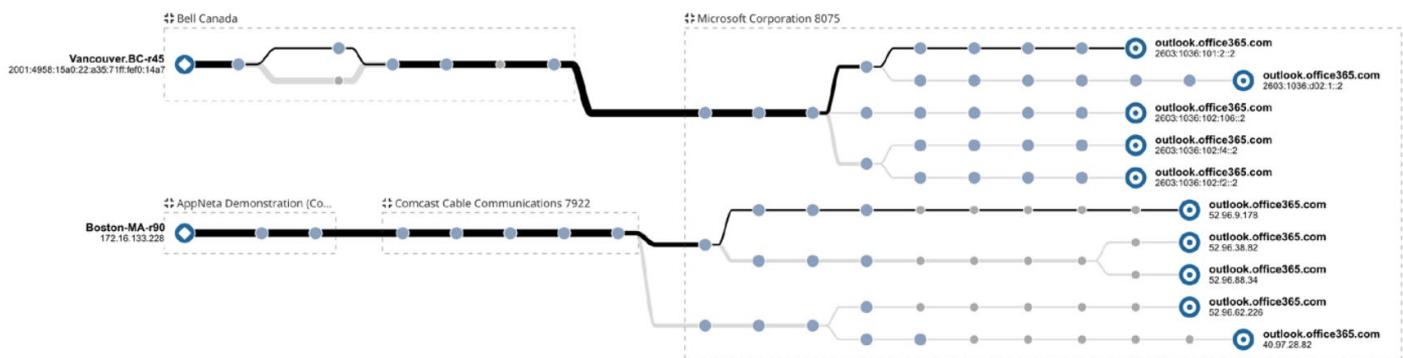
The screenshot shows the 'Alarm Console' interface. At the top, there's a filter for 'Group: All Groups' and a time range selector set to 'Mar 14 11:43 AM to 2:30 PM'. Below this is a table of alarms. The first alarm is selected, showing details for 'aws-broadcom-gmp-sydney <-> 170.176.245.164 (single)'. The alarm title is 'Excessive Network Path Changes for aws-broadcom-gmp-sydney <-> 170.176.245.164 (single)'. The impact is 'Management Lost'. The severity is 'Major'. The date/time is 'March 7, 2022 at 11:59:30 AM Eastern Standard Time'. The item name is 'aws-broadcom-gmp-sydney <-> 170.176.245.164 (single)'. The IP address is '170.176.245.164 (single)'. The model type is 'MonitoredPath'. The alarm is not acknowledged. The number of occurrences is 1. The alarm details section provides a description: 'A "apnNetworkChangeEvent" event has occurred, from MonitoredPath device, named aws-broadcom-gmp-sydney <-> 170.176.245.164 (single). A trap to indicate that a NetworkChangeEvent has occurred. eventTime = 2022-01-25 20:38:59 UTC eventType = networkChangeEvent orgId = 17870 pathId = 63873 pathName = pathTarget = 170.176.245.164 protocol = TCP previousNetworkSequence = 142091.17140.299992 currentNetworkSequence = 142091.299992 networkChangeDeepLink = https://app-14.pri.apprieta.com/pvc/networkPaths.html?st=17870&groupingType=none&protocol=tcp&selectedView=NetworkView&timeSpan=600000&timeWindow=eyJrYiYUyNDMxNjQxSjC2NDEy11FKzUuBIRmBQ Symptoms: There have been at least 3 path changes within a 5 minute period. Actions: ...'

NetOps by Broadcom detects a BGP routing change and delivers path degradation alarms that pinpoint the ISP network responsible for the performance issue.

NetOps by Broadcom provides route visualization that helps users get a big-picture view of network performance. This feature allows users to see how DNS, content delivery networks, and BGP work together to deliver content to users. Importantly, users can quickly identify when things aren't working as expected and drill down to the cause.

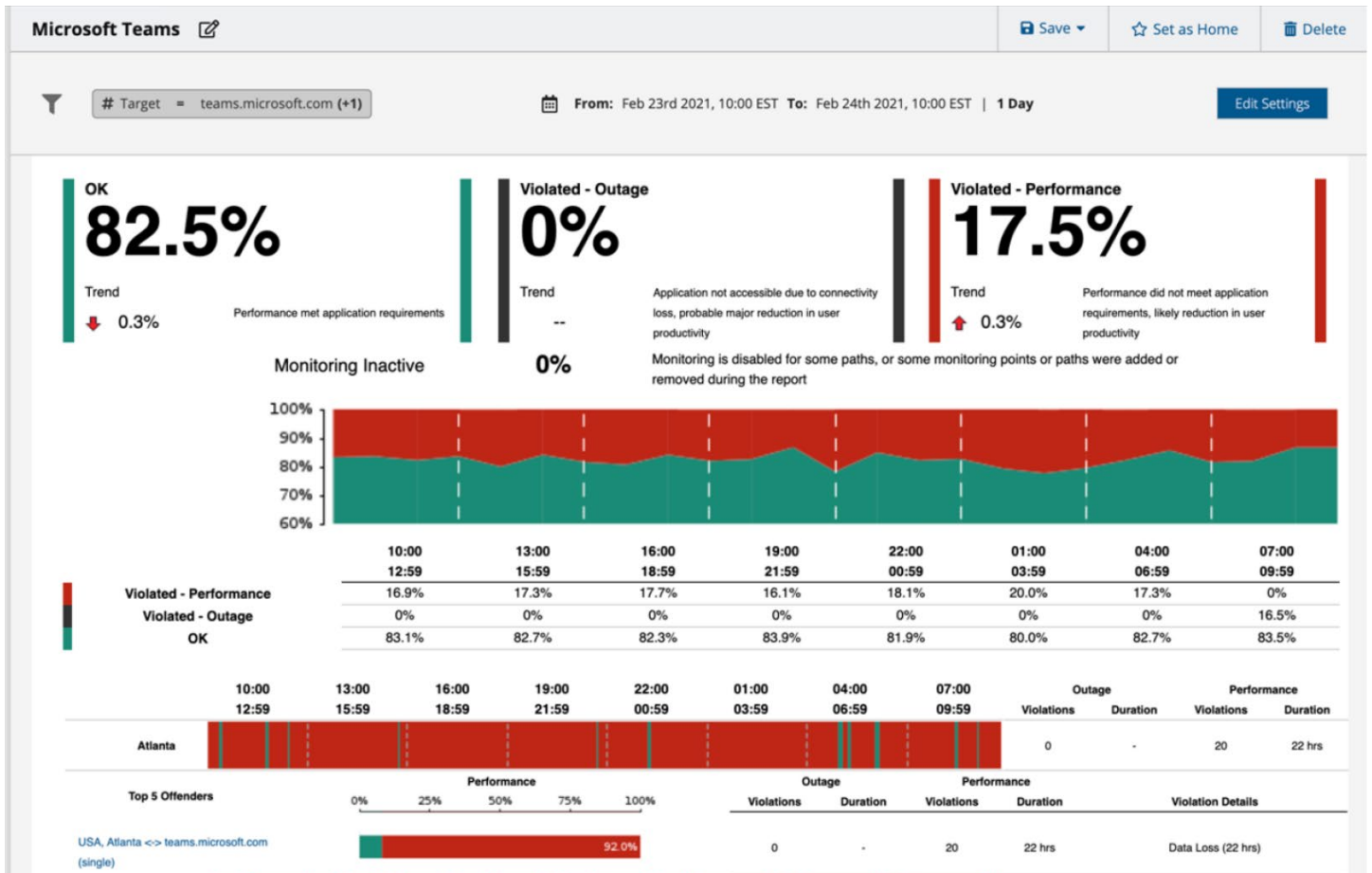
Here are some of the specific BGP monitoring features of the network management platform:

- **BGP Autonomous System overlay.** This overlay presents public networks traversed between office locations and the applications in use. Because this is based on BGP routing data, views reflect real-time changes in routing.
- **Search.** The solution's search capability enables users to do instant comparisons of routing across many locations and applications. Operators can quickly isolate which applications or locations are affected by changes and what routers and networks they have in common.
- **Historical views.** Users can view routes over time and analyze the effect of routing changes by seeing all active routes in a single view. The solution can present up to a year of routing history, helping teams identify long-term trends, gradual degradations, and intermittent issues.



NetOps by Broadcom can visualize routing differences detected between multiple locations over time for a cloud-based or SaaS application, such as Office365.

Software-defined infrastructure controllers make automated changes based on performance, NetOps by Broadcom provides continuous, low impact, and active testing of network delivery, enabling teams to keep pace with these dynamic environments. In addition, the solution gathers data more frequently when issues are detected to help speed root cause analysis. The solution routinely gathers high-resolution data every minute and, in degraded conditions, this interval is reduced to every 15 seconds. This significantly increases the NetOps team's reaction time when changes are having an impact on applications and the end-user experience.



NetOps by Broadcom uses active testing to track network experience variations over time.

Active testing helps validate that automated changes do not have a negative impact on the end-user experience and it also helps operations teams adhere to their SLOs and SLAs. Additionally, the solution offers continuous monitoring that can correlate performance variations with configuration changes. This enables network specialists to return to prior intervals and look at what was happening before and after events have occurred.

STANDARD OPERATING PROCEDURES AND WORKFLOWS

In many organizations, NOC groups face a skill shortage, which is due to several factors. As networks continue to see the addition of new technologies and become increasingly complex, teams need expertise in various fields, and it can be hard to find qualified candidates that possess these skills. This is often exacerbated by the fact that executive leadership prefers to keep lean teams and operating budgets. Consequently, training and development resources are scarce, and internal staff are relatively inexperienced. For these reasons, it is generally becoming increasingly difficult to ensure teams stay current with advanced, rapidly evolving technologies and best practices.

Traditional network management tools have failed to help teams navigate these disruptive digital changes and skills shortages. Across the industry, automation levels have remained low. It is estimated that only 35% of network activities are automated today.⁸ NOC personnel lack tools that enable them to standardize on the same workflows and processes, while gaining coverage of new areas, such as connectivity paths to cloud, SaaS, enterprise sites, and campus or branch Wi-Fi networks. As a result, teams have to contend with a higher level of manual intervention, further exacerbating the skills shortage problem.

When organizations have teams using multiple, disconnected network management tools, they experience a higher percentage of problems resulting from manual errors. If a large number of tools are employed, it typically leads to suboptimal processes and policies because each tool will have overlapping capabilities, making it difficult, if not impossible, to enforce consistent controls. To reduce the associated risks, there is a compelling need to consolidate network management tools as much as possible. This consolidation is vital in limiting errors and improving overall network management practices.

Real-Life Challenges Reported by IT Professionals

Teams used a variety of tools, some of which were only partially implemented. Several interviewees reported using dozens of different tools for specific purposes that were often only partially implemented. Conversations between teams using different tools posed challenges, because each group had different data that pointed to different issues. This resulted in longer MTTR.⁹

Here are some key requirements for establishing successful processes and workflows that can span across NOC teams and infrastructures.

⁸ Gartner Report, "Market Guide for Network Automation Tools," Andrew Lerner, Ted Corbett, February 2022

⁹ Forrester, "The Total Economic Impact Of Experience-Driven NetOps By Broadcom," October 2022

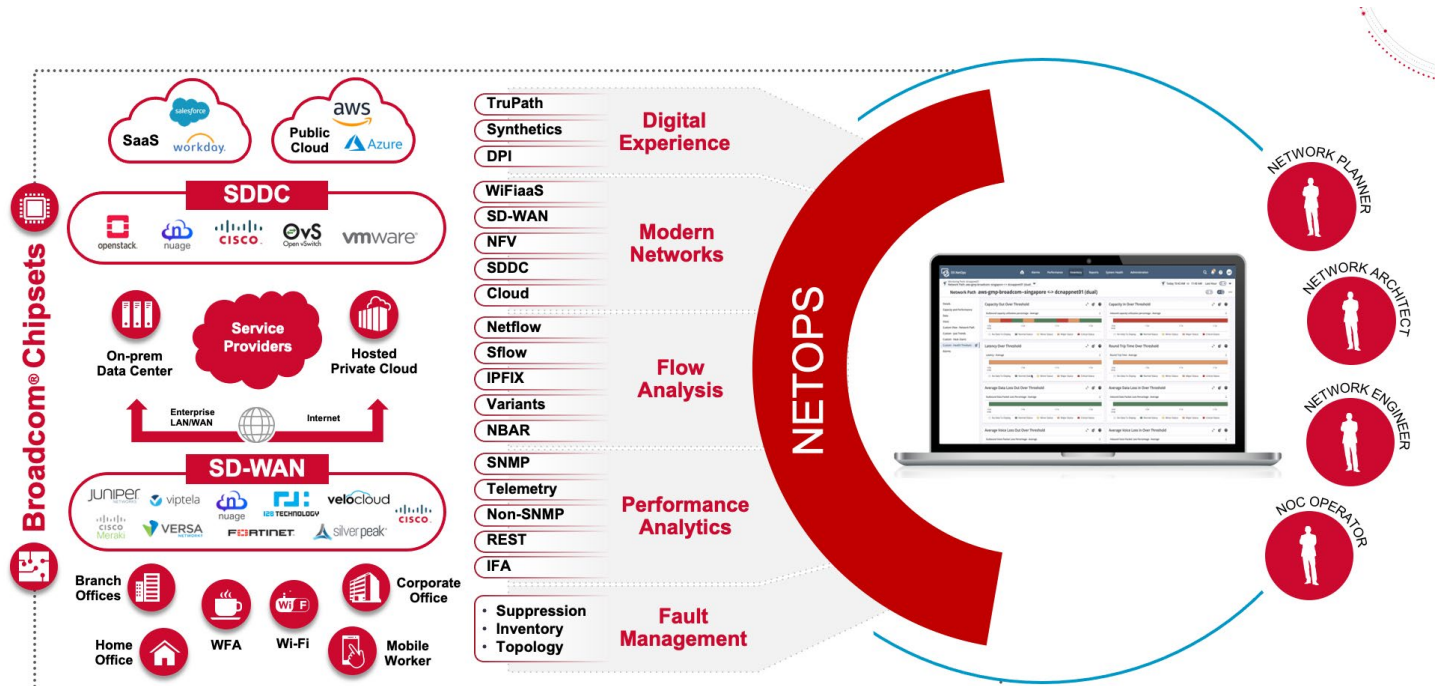
Cross Technology and Domain Operations Workflows

Most network tools are designed to manage certain aspects of networks, but they are not engineered to handle enterprise networks holistically. This multiplicity of tools has led to swivel-chair management and the need to extract data from one system and manually enter it into another. Beyond the obvious problems of duplication of effort and increased possibilities for human error, teams are fundamentally ill-equipped to stay in control. Without a comprehensive approach to managing traditional and software-defined environments, NetOps teams can't get the extended visibility they need to help ensure better performance and minimize service disruptions.

The result is that only 25% of network personnel's typical workday is spent on value-added activities, such as building out new services.¹⁰ Employing legacy approaches, NetOps professionals devote a significant amount of time to firefighting and generating reports and less time on strategic projects. In contrast, those working in a cross-domain operations center tend to spend less time on mundane tasks and more time focusing on strategic projects.

Today, teams are contending with a diverse range of networking services, from the LAN to the WAN, and across multiple types of services, increasingly including wireless. Consequently, NetOps teams have to stay on top of constantly evolving environments. To do so, they need tools that can help them establish network management processes that extend end-to-end across network delivery paths.

NetOps by Broadcom provides easy and intelligent workflows that enable level-one and level-two operations staff to do fast triage. The solution also provides level-three visibility, offering granular visibility into performance, fault, and flow; along with coverage that spans traditional, software-defined, and cloud architectures. What this means is that even a level-one NOC operator has enough intelligence, insights, and data, as well as easy triage workflows, so they can identify and isolate end-user experience issues without having to escalate to a network engineer or architect. Further, the NOC can identify issues that are occurring in networks they do not own, such as ISP and cloud environments.



Network Management by Broadcom enables cross-domain workflows that empower NOC staff and network specialists.

¹⁰ EMA Research, "Network Management Megatrends 2022: Navigating Multi-Cloud, IoT, and NetDevOps During a Labor Shortage," Shamus McGillicuddy, April 29, 2022

EXPERIENCE-DRIVEN TRIAGE

NetOps by Broadcom applies patented event correlation and inductive modeling technologies to paths 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.

AUTOMATED ROOT CAUSE IDENTIFICATION

NetOps by Broadcom delivers unique root cause analysis capabilities. The solution automates troubleshooting by correlating and interpreting a set of symptoms and/or 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, enabling the solution to correlate symptoms with events or changes, suppress unnecessary alarms, and track the impact on users, customers, and services.

ANOMALY DETECTION

NetOps by Broadcom 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.

SD-WAN VALIDATION

NetOps by Broadcom monitors the SD-WAN overlay in addition to each hop of the underlay, including across owned and unowned network infrastructure, for any vendor and technology. By providing unified, cross-environment coverage the solution enables teams to compare the perceived performance of the SD-WAN from the controller's perspective as well as performance from the application and end-user perspective. As SD-WAN controllers make automated changes based on performance. To ensure visibility remains current in these environments, the solution uses continuous testing of network delivery. This helps teams instantly validate that changes do not have a negative impact on the end-user experience.

END-TO-END PERFORMANCE

NetOps by Broadcom extends the traditional monitoring reach into edge services, multi-cloud environments, and ISP networks. The solution makes it possible to see every communication path and potential degradation point, from the core network to the end user, whether they are employees working in a corporate office or hybrid work environments.

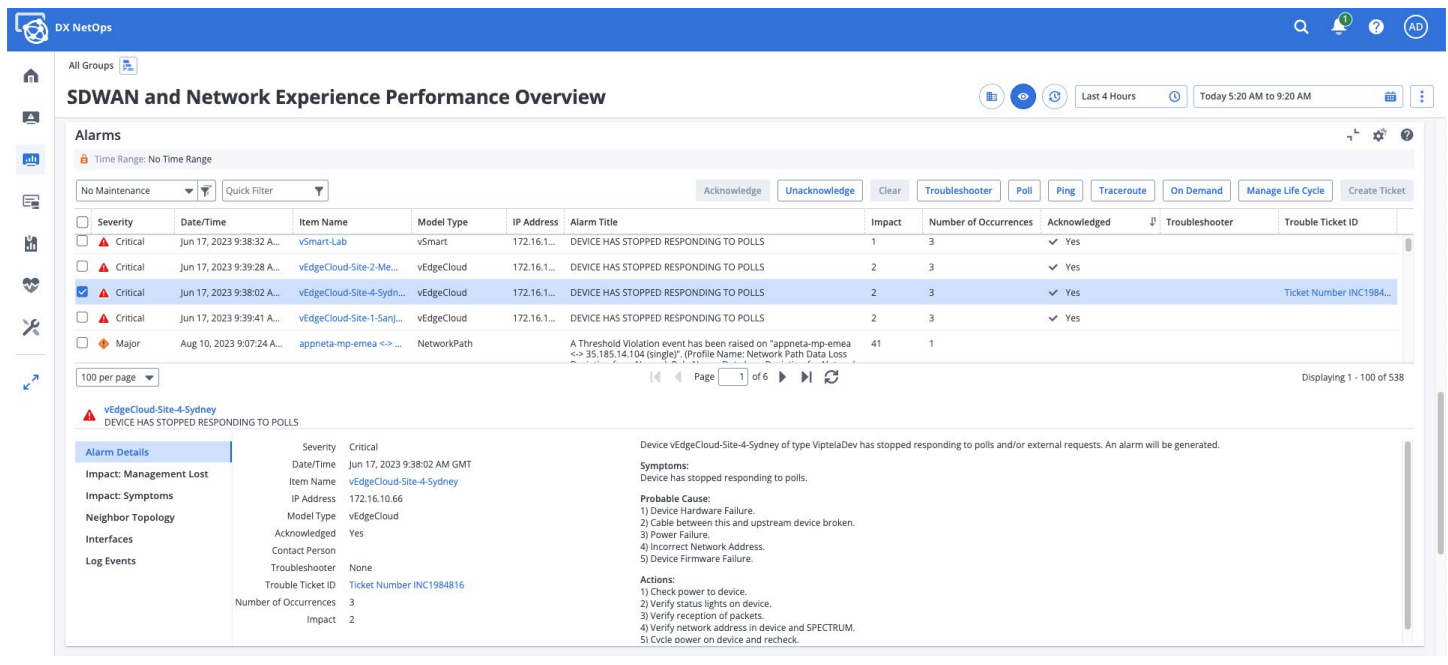
Integration with ITSM and Collaboration Tools

For teams looking to enhance their network operations and service management, integrating network management with the service desk is a strategic imperative. By connecting performance monitoring data and events with the incident management processes in ITSM platforms, NetOps teams can swiftly respond to and resolve issues, so they minimize any potential impact on end-users.

This integration facilitates proactive incident management. Performance-related alerts can trigger automated incident creation and receive immediate attention from support teams. The result is a more efficient incident management lifecycle, with improved response times and better service levels. Ultimately, integrating network tools with ITSM solutions enables better coordination and communication between network teams and other IT functions, and ensures more consistent operations.

NetOps by Broadcom can integrate with numerous third-party help desk trouble-ticket systems to ensure that 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.

While the solution is directly integrated with CA Service Desk Manager, it also natively supports third-party service desk applications, such as BMC Remedy, OpenText Service Manager, and ServiceNow. This allows teams to get automated, real-time updates on the status of problems as they are triaged and resolved.



DX NetOps

SDWAN and Network Experience Performance Overview

Alarms

Time Range: No Time Range

No Maintenance | Quick Filter

Acknowledge | Unacknowledge | Clear | Troubleshooter | Poll | Ping | Traceroute | On Demand | Manage Life Cycle | Create Ticket

Severity	Date/Time	Item Name	Model Type	IP Address	Alarm Title	Impact	Number of Occurrences	Acknowledged	Troubleshooter	Trouble Ticket ID
Critical	Jun 17, 2023 9:38:32 A...	vSmart-Lab	vSmart	172.16.1...	DEVICE HAS STOPPED RESPONDING TO POLLS	1	3	✓ Yes		
Critical	Jun 17, 2023 9:39:28 A...	vEdgeCloud-Site-2-Me...	vEdgeCloud	172.16.1...	DEVICE HAS STOPPED RESPONDING TO POLLS	2	3	✓ Yes		
Critical	Jun 17, 2023 9:38:02 A...	vEdgeCloud-Site-4-Sydn...	vEdgeCloud	172.16.1...	DEVICE HAS STOPPED RESPONDING TO POLLS	2	3	✓ Yes		Ticket Number INC1984...
Critical	Jun 17, 2023 9:39:41 A...	vEdgeCloud-Site-1-Sanj...	vEdgeCloud	172.16.1...	DEVICE HAS STOPPED RESPONDING TO POLLS	2	3	✓ Yes		
Major	Aug 10, 2023 9:07:24 A...	appneta-mp-emea <-> ...	NetworkPath		A Threshold Violation event has been raised on "appneta-mp-emea <-> 35.185.14.104 (single)", (Profile Name: Network Path Data Loss	41	1			

100 per page | Page 1 of 6 | Displaying 1 - 100 of 538

vEdgeCloud-Site-4-Sydney
DEVICE HAS STOPPED RESPONDING TO POLLS

Alarm Details

Severity	Critical
Date/Time	Jun 17, 2023 9:38:02 AM GMT
Item Name	vEdgeCloud-Site-4-Sydney
IP Address	172.16.10.66
Model Type	vEdgeCloud
Acknowledged	Yes
Contact Person	
Troubleshooter	None
Trouble Ticket ID	Ticket Number INC1984816
Number of Occurrences	3
Impact	2

Impact: Management Lost

Neighbor Topology

Interfaces

Log Events

Symptoms:
Device has stopped responding to polls.

Probable Cause:
1) Device Hardware Failure.
2) Cable between this and upstream device broken.
3) Power Failure.
4) Incorrect Network Address.
5) Device Firmware Failure.

Actions:
1) Check power to device.
2) Verify status lights on device.
3) Verify reception of packets.
4) Verify network address in device and SPECTRUM.
5) Cycle power on device and recheck.

NetOps by Broadcom delivers two-way integration with ServiceNow, enabling operators to access tickets with a simple click.

The ServiceNow integration supports two-way communication and notifications can be sent to Broadcom when a ticket that is associated with the alarm changes. These notifications update the alarm that is associated with a ticket to reflect changes that occurred on the ServiceNow side. The integration can be configured to generate an automatic notification when a ticket is closed. When the solution receives this notification, it will clear the associated alarm. Similarly, when a ticket has been transferred, a notification can be generated that causes Broadcom to update the troubleshooter information for the associated alarm.

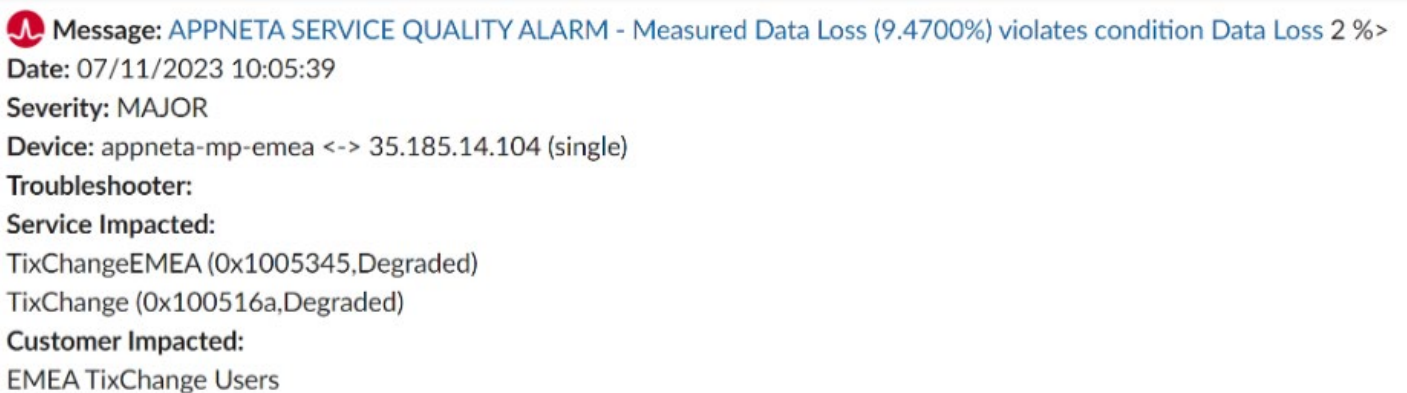
By leveraging the real-time communication afforded by instant messaging platforms, NOC teams can improve collaboration and responsiveness. With these platforms, teams can establish dedicated channels to monitor incidents or projects. These channels enable operations teams to be quickly informed of incidents, share updates, and collectively work towards solutions. Routing incident notifications to specific channels ensures that critical issues reach the right team members promptly, facilitating rapid incident response that is aligned with standardized escalation procedures.


In many organizations, NOC teams continue to be increasingly geographically dispersed, which can make it harder to engage in discussions, share insights, and collaboratively troubleshoot network issues. As a result, instant messaging is emerging as an essential capability. By integrating monitoring tools with messaging platforms, such as Slack and Google Chat, teams can streamline communication and maintain a comprehensive record of incident-related discussions. Ultimately, this results in more effective and consistent interactions between team members.

Instant messaging platforms have become increasingly popular. Today, many organizations use these platforms as the primary interaction point for the NOC. Teams can easily integrate NetOps by Broadcom with these platforms by using the alarm notifier integration point described earlier in this white paper.

The alarm notifier acts as a gateway for outbound integrations and makes it possible to create a policy that decides what alarms will be sent to Slack, Google Chat, or both, for subsequent processing or action. Once these policies are established, relevant alarms will be sent as messages to the instant messaging tool.

By integrating Broadcom with instant messaging platforms, teams can collaborate more effectively and react faster to network events.



 **Message:** APPNETA SERVICE QUALITY ALARM - Measured Data Loss (9.4700%) violates condition Data Loss 2 %>
Date: 07/11/2023 10:05:39
Severity: MAJOR
Device: appneta-mp-emea <-> 35.185.14.104 (single)
Troubleshooter:
Service Impacted:
TixChangeEMEA (0x1005345,Degraded)
TixChange (0x100516a,Degraded)
Customer Impacted:
EMEA TixChange Users

NetOps by Broadcom integrates with Slack through the alarm notifier. Messages can feature hyperlinks that let users connect directly to the portal console.

CONCLUSION

According to many industry analysts, NetDevOps is among the most highly touted innovations in networking.¹¹ Successful NetDevOps initiatives can yield fully automated environments. These environments enable deployment and testing of configuration changes across networks, so they're ready to be consumed in a DevOps style manner throughout the continuous integration/continuous delivery (CI/CD) pipeline. At the same time, SRE approaches continue to gain increased adoption, offering also a solution for operations teams looking to deliver greater agility. Network Reliability Engineering (NRE) approaches are also seeing increased adoption.¹² NRE incorporates SRE practices into network management, offering a way to maintain reliability, while achieving the benefits of accelerated innovation.

In the near future, these approaches will become increasingly mainstream. Agile network teams will have to guarantee consistent operations and reliable digital experience on a continuous basis, under the strain of an increasing volume of changes. However, most potential adopters still lack adequate tooling, such as standardized workflows, automation, and continuous validation. Therefore, now is the right time to review network management strategies and establish approaches for improving operational consistency and getting prepared for the next round of transformation. Broadcom can help teams navigate this journey. With its solutions, Broadcom helps organizations collaborate more effectively, and work seamlessly with third parties, such as ISPs and cloud providers. The following sections offer some examples of how customers have benefited from Broadcom solutions.

MSP Reduces Total Cost of Ownership by 75%

The NetOps team of a managed service provider is responsible for the management of highly complex customer environments with thousands of devices, such as routers, switches, firewalls, load balancers, and more. Broadcom has helped the team improve operational consistency and efficiency by streamlining incident management processes, while improving visibility into the data that matters. The team has also enhanced network configuration management processes, establishing a repository for tracking known-good configurations, viewing changes, and doing compliance auditing. Further, the team gained the insights needed to retire redundant toolsets. As a result, their NOC realized a 75% reduction in total cost of ownership.

¹¹ Gartner, "Paving the Path from ClickOps to NetDevOps," Andrew Lerner, October 2022

¹² Similar to the SRE and DevOps culture, the NRE and DevNetOps culture values an allowance for failure, enabling teams to make quick fixes and learn lessons. [Source: Juniper Networks, "What is an NRE?"]

Financial Services Achieves Eight-Fold Scale in Visibility

A NetOps team within a financial services company lacked a single source of truth for all their network monitoring intelligence, which meant groups from different domains had to rely on their own tools. As a result, troubleshooting was inconsistent, labor-intensive, and costly. Executives weren't able to get the insights they needed, which meant staff spent a significant amount of time providing reports and chasing down status updates. As their environment continued to grow in scope and complexity, the network team needed to implement even more tools, which further reduced operational consistency and left them struggling with lengthy remediation efforts. Broadcom solutions enabled the company to realize dramatic improvements in visibility and operational consistency. Monitoring scale was increased by eight-fold, enabling the team to go from supporting 30,000 to 260,000 objects, while optimizing collaboration and improving agility across multiple teams.

Why Broadcom

For today's enterprises, successful transformation relies extensively on networks. Transformation is not just about technological change—it's about operational change too. NetOps by Broadcom converts inventory, topology, metrics, faults, flow, and experience into actionable intelligence for network operations teams. The solution provides out-of-the-box, single-pane-of-glass dashboards and workflows that are ready to use, without having to learn a new network management tool.

With its leading solutions, Broadcom eliminates prevalent visibility gaps and delivers a comprehensive network management solution designed with tomorrow in mind. Network teams benefit from consistent workflows and a unified approach to managing traditional and software defined environments, while offering extended visibility into end-to-end network operations. With Broadcom, NetOps teams gain the operational consistency and agility they need to accelerate their network transformations.