BROADCOM

WHITE PAPER

Rapid and Accurate Isolation of Issues in Modern Networks: Key Challenges and Critical Requirements

TABLE OF CONTENTS

OVERVIEW

For decades, organizations have continued to expand their usage of diverse networks and networking technologies. In response, network operations (NetOps) teams have continued to adopt disparate tools to manage these networks. This growth in network usage and siloed tools, as well as the adoption of software-defined technologies, has served to create a dramatic proliferation in event and alarm volumes. With so many events and alarms to sift through, troubleshooting takes too much time and effort.

To date, tools employed within many organizations can only offer support for a narrow set of products and vendors—and the number of distinct technologies employed only continues to grow. Given this, NetOps teams continue to contend with lengthy triage efforts, inefficient root cause analysis, and inadequate governance of configuration changes. Organizations therefore keep being more exposed to the incidence of outages and performance issues.

This spiraling complexity creates an increasingly untenable situation for NetOps teams—and the organizations they support. After all, slow is the new down. Outages, even slow performance, are ever more devastating for organizations. In an always-on digital world, corporate clients and consumers are increasingly unwilling to put up with downtime or lagging performance, and today's digitized services make it easier to switch to another vendor at any time.

The only way to combat these issues is by investing in an advanced network monitoring and management solution that provides:

- **A highly scalable, unified data model.** Every piece of multi-vendor network data needs to be collected by one solution. This one solution must be able to collect, normalize, and correlate disparate data sets from across the organization's multi-vendor, -technology, and -protocol network environments. This data needs to be presented in intelligent, unified views of network health, delivering the "one source of truth" that eludes many NetOps teams today.
- **Advanced analytics.** Advanced and patented analytics must be applied to this collected data. Teams need analytics that correlate network fault, performance, and flow data. These analytics enable teams to uncover patterns, identify issues faster, and anticipate how changes will affect the user experience or network health.
- **Intelligent triage workflows.** The results of the collected data and analytics must be presented to the operator in easy-to-understand troubleshooting workflows. The solution must minimize alarm noise, so NetOps teams can quickly diagnose issues and get to the root cause. This solution must also enable teams to quickly dive into a specific technology domain in order to get the details required.

These three areas do not work in isolation, but together provide the observability needed to manage today's complex networks. For example, if you need to look at the logs on a specific device you are troubleshooting, you should not have to connect into that device in order to get your answers. An advanced network monitoring and management solution should have already collected those logs, analyzed those logs, found any patterns or anomalies, and revealed the root cause in easy triage workflows. Further, these workflows should be integrated with standard operating procedures that minimize the number of clicks needed to resolve issues.

HIGHLY SCALABLE, UNIFIED DATA MODEL

NetOps teams need various types of data to intelligently manage modern, multi-vendor networks, including logs, flow information, configuration details, and more. Too often, this data is held in disparate locations and managed by different tools. This means each team needs to toggle between its unique set of tools and multiple interfaces when issues arise, which leads to inefficiency and complexity, and ultimately slows triage.

Within many organizations, teams rely on logs or scripts to gather the information they need from the various tools they've employed. In other cases, teams have deployed an AIOps solution. While AIOps products can be helpful in many scenarios, they don't always work in a network management context. Because networking data is complex, rich, and high-volume, many AIOps tools can only consume a small portion of data. Consequently, they may miss essential topology, configuration, or flow analytics that are critical in rapid network issue resolution.

DX NetOps offers teams a complete, domain-agnostic, multi-vendor network management solution to counter these challenges. DX NetOps delivers high-scale monitoring that enables fast data collection for a variety of networking data types. Further, network teams need a solution to deliver the high scalability required to aggregate and correlate the massive volumes of data today's networks generate. DX NetOps provides a highly scalable data model that collects, cleans, correlates, and normalizes data from disparate vendors, technologies, and protocols to provide an enterprise-wide view of network health. Unlike other data repositories, DX NetOps data model has been fine tuned to work with the largest networking data sets.

With DX NetOps, teams can consolidate data from multiple sources and establish a unified view of all the data that matters, so they can operate with maximum intelligence and speed. DX NetOps Portal is a single portal that leverages inventory, events, alarms, topology, device metrics, configurations, faults, and flows to deliver actionable insights and easy-to-understand troubleshooting workflows. It is the only place for Network Operation teams for troubleshooting and reporting fueling more extensive usage, identifying issues quickly and optimizing operations.

NetOps unified data model is the bridge needed to expose insights from disparate data sources, contextualize that information and serve as the foundation upon which to more purposefully apply advanced analytics.

NetOps unified data model design principles consist of the following:

- **Flexible and network-agnostic.** Understand complex properties and relationships within and across multiple data types, including logical and physical networks and the large volume and variety of data consumed and generated by monitoring and SDN systems.
- **Post-deployment-extensible.** Future-proof the organization by enabling new technologies and data types to be quickly incorporated within the model without enforcing the need to manually identify and tag elements. As networks and technologies evolve, our unified data model is prepared to capture and correlate new data types.
- **Multi-dimensional.** Reconcile elements from multiple layers and with multiple facets into unified models with relationships and highly contextual data. Every new layer of information provided by a data source increases understanding and enables the users to consume relevant data from multiple dimensions in a single pane of glass.

NetOps unified data model consists of a Data Collection layer and a Data Aggregator Engine. The Data Collection layer retrieves raw data from disparate data sources and performs expressions on it to normalize it into meaningful metrics and models. These calculations are driven by our Data Aggregator Engine and leverage Metric Families and Vendor Certifications in order to normalize the data to be consumed in our unified data model. Then, data is transmitted to the Data Aggregator engine via high available buses, and here, data is reconciled in order to consolidate multiple data sources into a single model. The Data Aggregator is also responsible for baselining performance metrics in order to facilitate the creation of advanced analytics. Finally, correlated models and metrics are stored in a highly available backend database, capable of managing millions of monitored elements.

This consolidation is critical for rapid and accurate isolation of issues. It enables NetOps users to consume events, metrics, flows, logs and topology all in the context of a single model from a single pane of glass. Some design principles of our data model are:

- **Flexible and network-agnostic.** Be capable of understanding the complex properties and relationships within and across multiple data types, including logical and physical networks and the large volume and variety of data consumed and generated by monitoring and SDN systems.
- **Post-deployment-extensible.** Future-proof the organization by enabling new technologies and data types to be quickly incorporated within the model without enforcing the need to manually identify and tag elements. As networks and technologies evolve, our unified data model is prepared to capture and correlate new data types.
- **Multi-dimensional.** Reconcile elements from multiple layers and with multiple facets into unified models with relationships and highly contextual data. Every new layer of information provided by a data source increases understanding and enables the users to consume relevant data from multiple dimensions in a single pane of glass.

This unified data model enables NetOps to represent a digital twin of constantly changing network environments and serves as the foundation for standardizing operational procedures and surfacing smart actionable insights.

ADVANCED ANALYTICS

Across regions and industries, many IT organizations are struggling to retain seasoned, qualified personnel. Often, industry veterans move to rapidly growing sectors, such as cloud services and cyber security, where they have the potential to see increased salaries and benefits.

At the same time, diagnosing network issues and managing performance continues to get more complex. For teams short on resources and expertise, locating the source of network outages and performance issues is increasingly akin to finding a needle in a large, constantly shifting haystack. In response, leaders are increasingly pursuing outsourcing approaches and analytics and artificial intelligence (AI). In fact, between 2023 and 2027, the percentage of enterprises using AI to automate network operations is expected to grow from 10% to 90% (Source: Gartner: Innovation Insight: AI Networking Has the Potential to Revolutionize Network Operation, ID: G00767496)

Within many organizations, making the move to rely fully on AI for critical network operations will take time. In the near term, AI adoption will be limited, which means teams will be saddled with using a patchwork of scripts and isolated tools. This scenario creates an intensifying administrative burden and leads to lengthy troubleshooting efforts.

When it comes to isolating the root cause of issues in modern networks, AI and advanced analytics undoubtedly hold promise—but this promise will only be realized when advanced capabilities are effectively tailored to the networking domain. To be viable, solutions will need to offer a combination of algorithms, topology-based analytics, and flow analytics. With these capabilities, solutions will deliver the insights needed to achieve accurate and fast identification of network performance issues.

By unifying intelligence across traditional silos, DX NetOps can enable teams to focus on using one console, which streamlines onboarding of new engineers. With the solution's alarm reduction, teams can ensure they're focused on the right alerts, so they can quickly triage network issues that are having an impact on end users.

Fault Suppression

DX NetOps offers a patented, algorithmic approach to fault management. The solution does proactive polling of component status and generates events based on threshold violations. The solution does this while analyzing fault domains, which are collections of alarms that are affected by the same failure.

The solution employs an initiator model in which, if a neighbor indicates it is performing as needed, it can be inferred that the problem lies between the unaffected neighbor and the affected initiator. If connectivity or fault are exceeded, a critical alarm will be generated based on the initiator, which is considered the root cause.

Dynamic baseline thresholds enable NetOps teams to compute baseline averages based on the same hour of a day or day of a week. Users can have alerts based on standard deviations from baseline averages for a sustained period of time. To eliminate false positives, teams can also include a minimum threshold. For instance, "normal" may be 4% utilization, so seeing 12% utilization would be well outside of baseline. However, since it is not significant in absolute terms, DX NetOps would not generate an event or alarm.

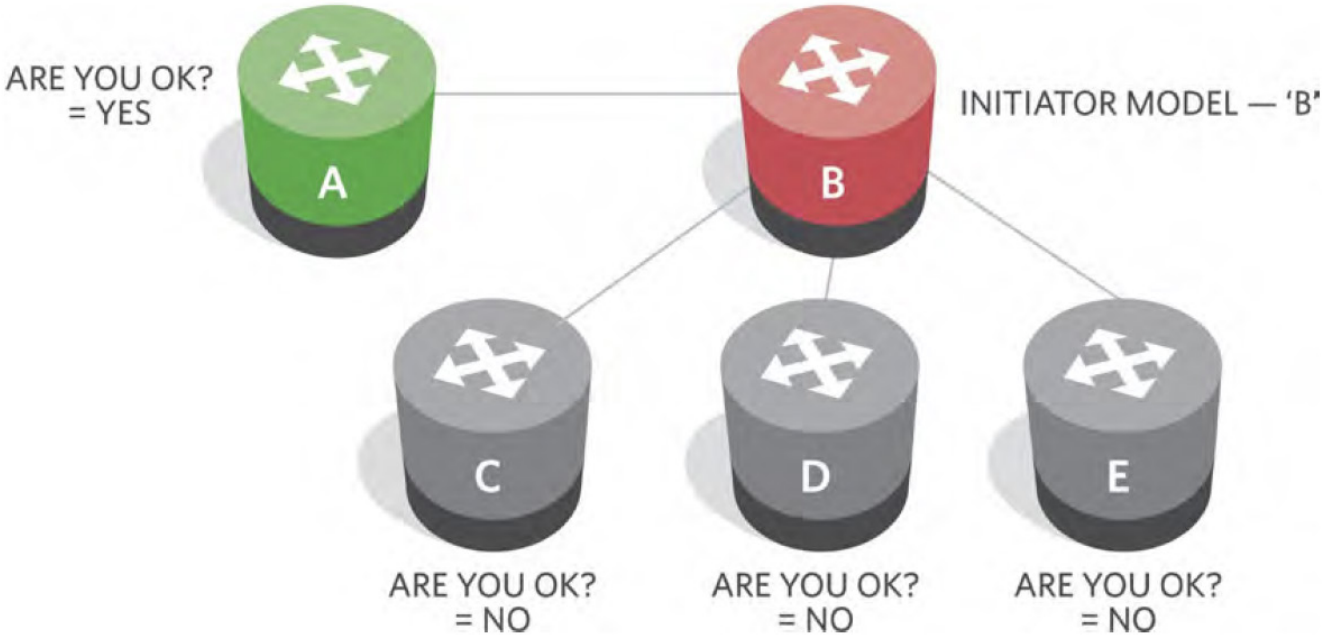

Figure 1: Models that respond with a "Suppressed State" status are put in a suppressed condition to suppress the alarms that are symptomatic of a problem elsewhere in the infrastructure.

The baseline calculation method varies by the registered data source. DX NetOps can feature baseline data that is plotted in many views, while displaying statistical deviations from normal performance for a given statistic.

Metrics are considered to be normal based on the calculated baseline average. The standard deviation is used to gauge the statistical validity of the baseline values. Baseline values are included in charts to help users see places where performance values are changing rapidly.

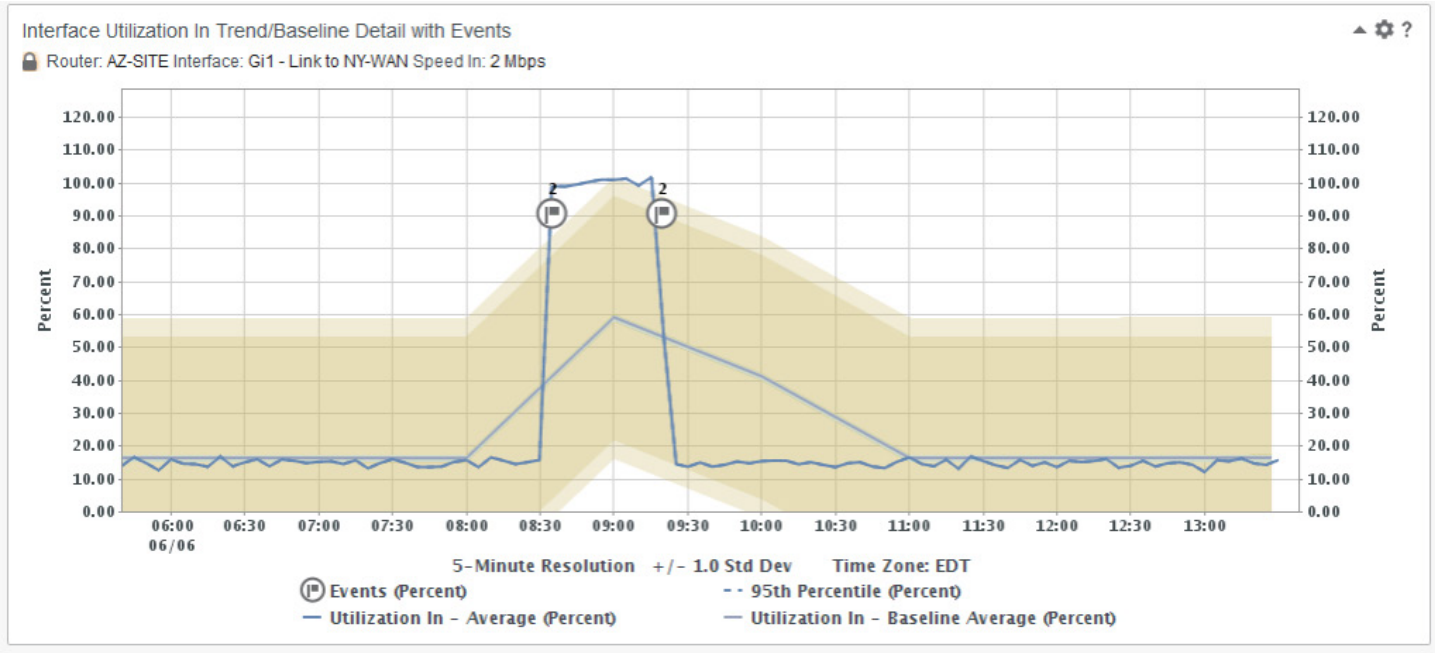

Figure 2: DX NetOps dynamic baseline threshold enables pinpoint visibility into what network operations should care about versus an abnormal blip in network activity.

Baseline data helps to characterize past performance for selected monitored parameters, assess present performance, and estimate future performance. For example, comparing current CPU utilization to a known baseline average level helps to determine whether current utilization is within a typical range. A monitored parameter that exceeds a baseline can indicate additional load on the server from a new application process, an increase in the number of users or sessions, or an increase in the amount of data being processed.

The solution leverages different types of problem solving and planning to comprehensively manage network faults and provide root cause isolation. Some of the key capabilities are outlined below.

Model-Based Inductive Modeling Technology (IMT)

The core of the DX NetOps fault RCA solution is its patented Inductive Modeling Technology (IMT). IMT uses an object-oriented modeling paradigm with model-based reasoning analytics. DX NetOps fault most often uses IMT for physical and logical topology analysis, as the software can automatically map topological relationships through its efficient, automated discovery engine.

The models created are software representations of a real-world physical or logical device. These software models are in direct communication with their real-world counterparts. This enables DX NetOps fault root cause analysis to not only receive, but proactively query for health status or additional diagnostic information. Models are described by their attributes and behaviors, as well as their relationship to other models and algorithmic intelligence.

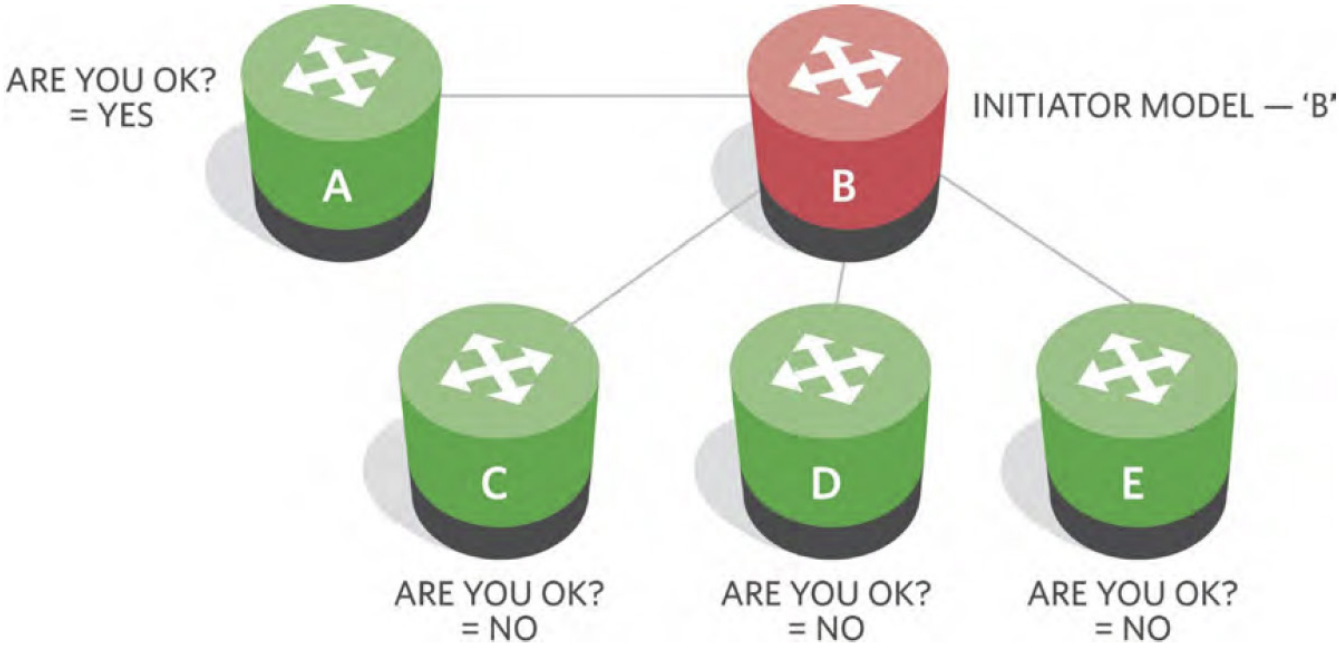

Figure 3: The root cause alarm is established through a sequence of sharing status between models.

Policy-Based Condition Correlation Technology (CCT)

In order to perform more complex user-defined or user-controlled correlations, tools need a broader set of capabilities. DX NetOps offers the full-featured controls required. Here is more information about the terminology the solution employs:

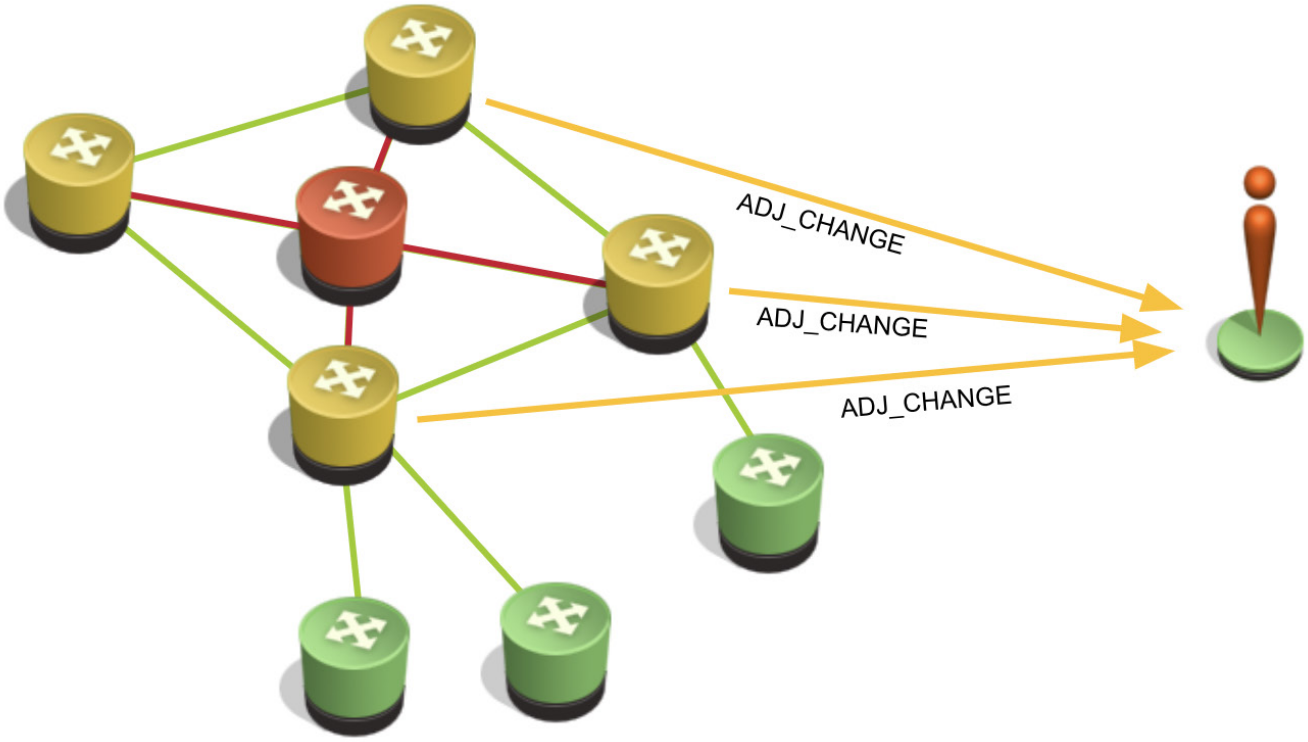

Figure 4: Response time failures due to infrastructure faults are automatically correlated.

Conditions

A condition is similar to state. A condition can be set by an event and cleared by an event. It is also possible to have an event set a condition but require a user-based action to clear the condition. The condition exists from the time it is set until the time it is cleared.

A very simple example of a condition is “port down” condition. The port down condition will exist for a particular interface from the time the LINK DOWN trap or set event (such as a failed status poll) is received until the time the LINK UP trap or clear event (such as a successful status poll) is received. A number of conditions that may be of use for establishing domain-level correlations are defined out-of-the-box and users can add more.

Seemingly Disparate Conditions

Many devices in an IT infrastructure perform a specific function. The device-level function is often without context as it relates to the functions of other devices. Most managed devices can emit event streams, but those event streams are local to each component. A simple example is when a response time test identifies a result exceeding a threshold. At the same time, an event may identify a condition of a router port exceeding a transmit bandwidth threshold. These conditions are seemingly disparate, as they are created independently and without context or knowledge of each other. In reality, the two are quite related.

Rule Patterns

Rule patterns are used to associate conditions in which specific criteria are met. A simple example is a "port down" condition caused by a "board pulled" condition—but only if the port's slot number is equal to the slot number of the board that's been pulled. [Figure # illustrates this rule pattern.] The result of applying a rule pattern can be the creation of an actionable alarm or the suppression of symptomatic alarms.

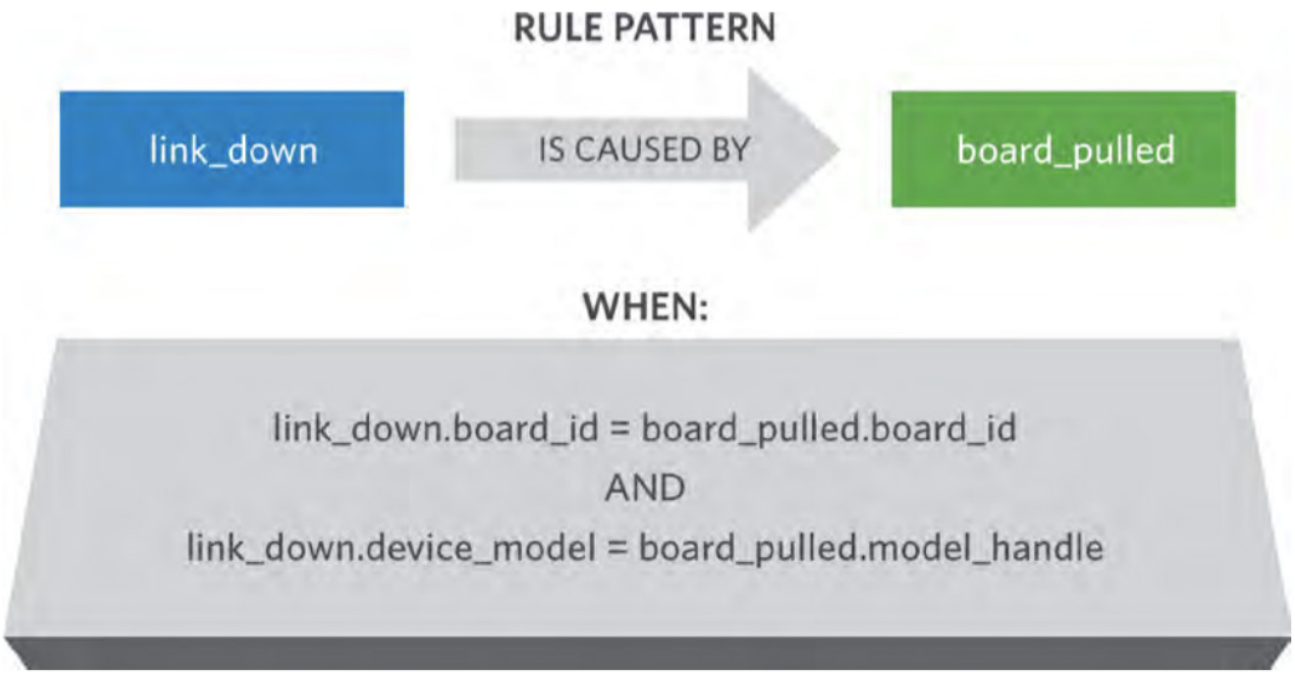

Figure 5: Rule patterns determine the sequence of investigation that will result in either the creation of an alarm or the suppression of symptomatic alarms.

Correlation Policy

Multiple rule patterns can be bundled or grouped into a correlation policy. Correlation policies can then be applied to a correlation domain. For example, a set of rule patterns applicable to correlation of the Open Shortest Path First (OSPF) routing protocol can be created and labeled the "OSPF Correlation Policy." This policy can be applied to each correlation domain as defined by each autonomous OSPF region and the supporting routers in that region.

Correlation Domain

A correlation domain is used to both define and limit the scope of one or more correlation policies. A correlation domain can be applied to a specific service. For example, in the cable broadband environment, a monitoring system may detect a return path failure in a certain geographic area. This "return path failure" condition is causing subscribers' high-speed cable modems to become unreachable and leading to failures in video-on-demand (VoD) streams.

The knowledge that the return path failure, the modem problems, and the failed VoD streams are all in the same correlation domain is essential to correlating the events and ultimately identifying the root cause. However, it is also important to have the ability to distinguish that a "return path failure" condition occurring in one correlation domain (Philadelphia, PA) is not correlated with VoD stream failure conditions occurring in a different correlation domain (Portsmouth, NH).

Condition-based correlations are very powerful and provide a way for teams to develop correlation policies and apply them to correlation domains. When applied to business service management, correlation policies can be likened to metrics of an SLA. Correlation domains can be likened to service, user, or geographical groupings.

There are times when the only way to infer a causal relationship between two or more seemingly disparate conditions is when those conditions occur in a common correlation domain. These mechanisms are necessary when causal relationships cannot be discovered through interrogations of infrastructure components or the receipt of events from those components.

Least Squares Regression (Metric Projections)

DX NetOps can calculate future values based on historical metric data. Metric projection is useful for capacity planning. For example, to verify that the interface bandwidth is sufficient for a specific time in the future, teams can calculate the projected interface utilization.

To see future trends, metric projection supports up to three configurable intervals. For example, operators can project to 20, 60, and 180 days in the future for a given metric. Projection shows an overall trend. Typically, the longer the projection interval, the less accurate the exact value.

Projections are configured for individual metrics and they calculate a linear regression line from the daily percentile values. The calculation uses a linear regression (least squares regression). The calculation uses all the available daily percentile values from the last 90 days as input data. Projection requires at least two days of daily percentile values. Projection accuracy typically increases as more data points become available.

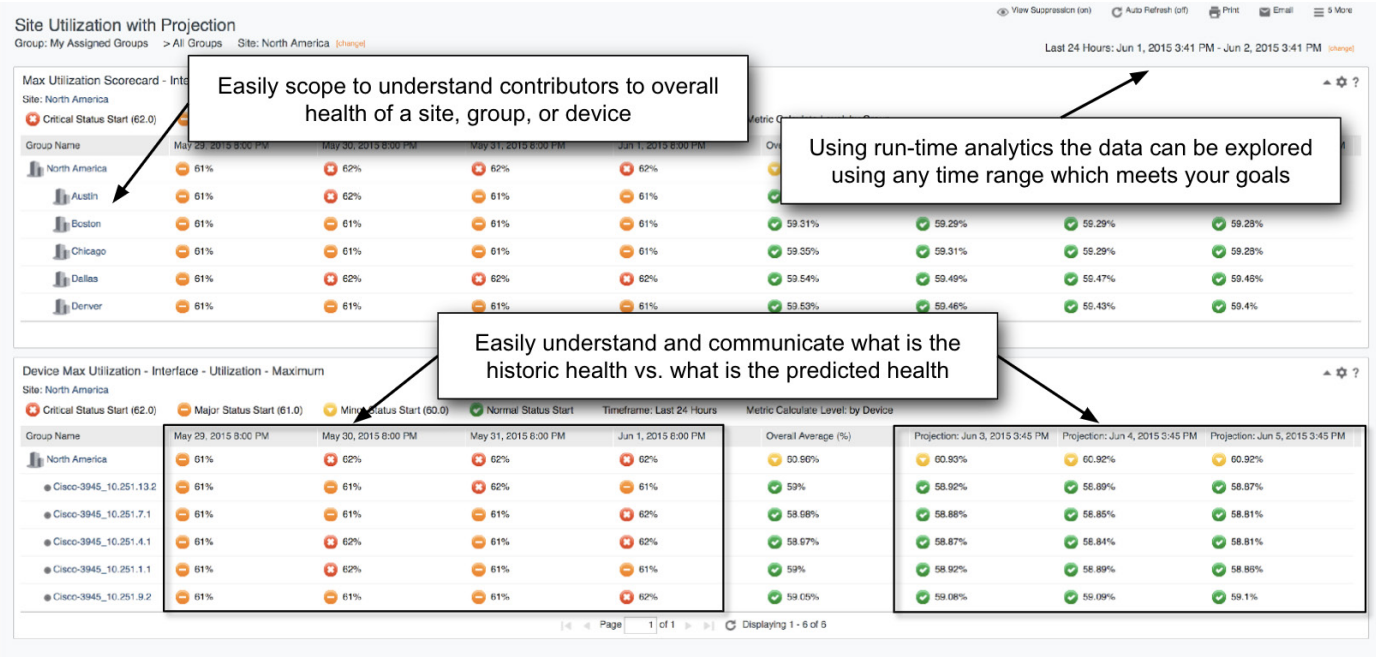

Figure 6: Easy to understand scorecards for intelligent insights into future capacity predictions.

Event Rules and Logic

In order to remove all the noise created from today's complex network architectures, DX NetOps offers policy-based condition correlation. This technology enables users to perform these activities:

- Creation of policies, domains, and disparate event streams or conditions.
- Correlation across sets of managed elements and domains.
- Correlation of component conditions as they map to higher order concepts, such as business services or customer access.

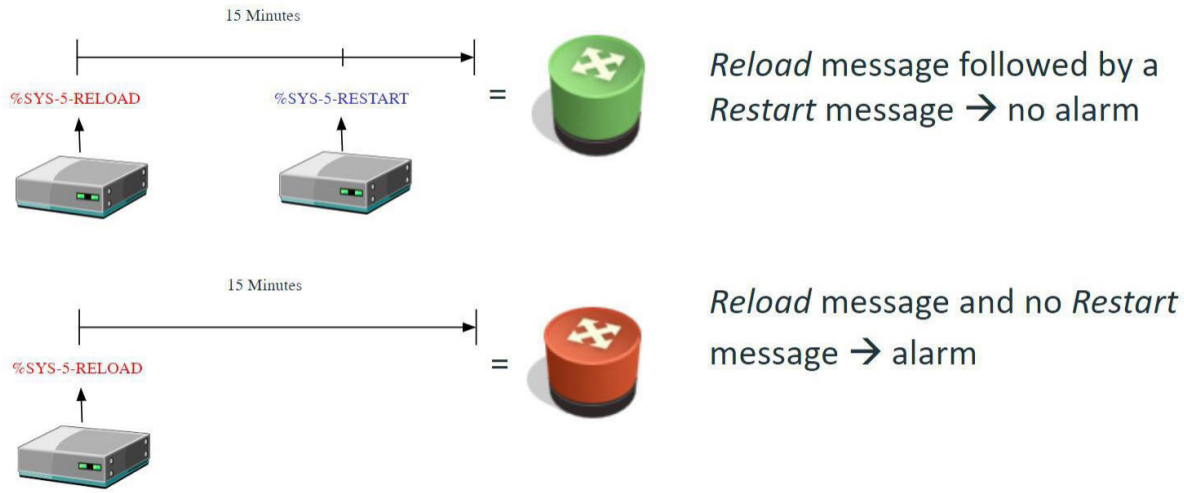

Figure 7: Condition correlations is one way alarm noise reduction is achieved.

These rules and logic provide significant value as teams look to correlate events and determine which actions to perform in response to one or several events. Users can configure the event arrival order, group of events or pattern to generate a different event. This flexibility and correlations are very much needed in today's complex infrastructures, helping to reduce cost and risk and accelerate the move to automation.

For instance, a data center event could be associated with an uninterruptible power supply (UPS) running on battery. This event might indicate a specific issue with that UPS. Something completely different would be to get multiple events about UPS going on battery, this could imply a general power failure. In this case, the user could benefit from condition correlation to get alerted on the major issue (root cause) right away and trigger the right processes.

Topology-Based Fault Isolation

Topology-based fault isolation helps teams pinpoint the devices and infrastructure domains that are responsible for issues, so they can speed resolution.

The solution enables operators to accelerate investigation by automating data comparison efforts. In addition, DX NetOps delivers views within the context of business services and applications, helping operators more quickly spot degradations and affected users, and better target their efforts on those issues that have the most significant business impact.

DX NetOps provides multiple methods for building the physical, virtual, and logical topology model, as well as interdependent connectivity, for any given infrastructure. Following are some of the options available:

- Interactive and scheduled discoveries via GUI
- Event-driven discovery, for example using SNMP traps from a new device
- Integration with software-defined network controllers and orchestrators
- Integration with hypervisors
- Importing inventory and relationship data from external sources
- Using APIs to integrate with external inventory and provisioning systems
- Employing command line and script-based integration

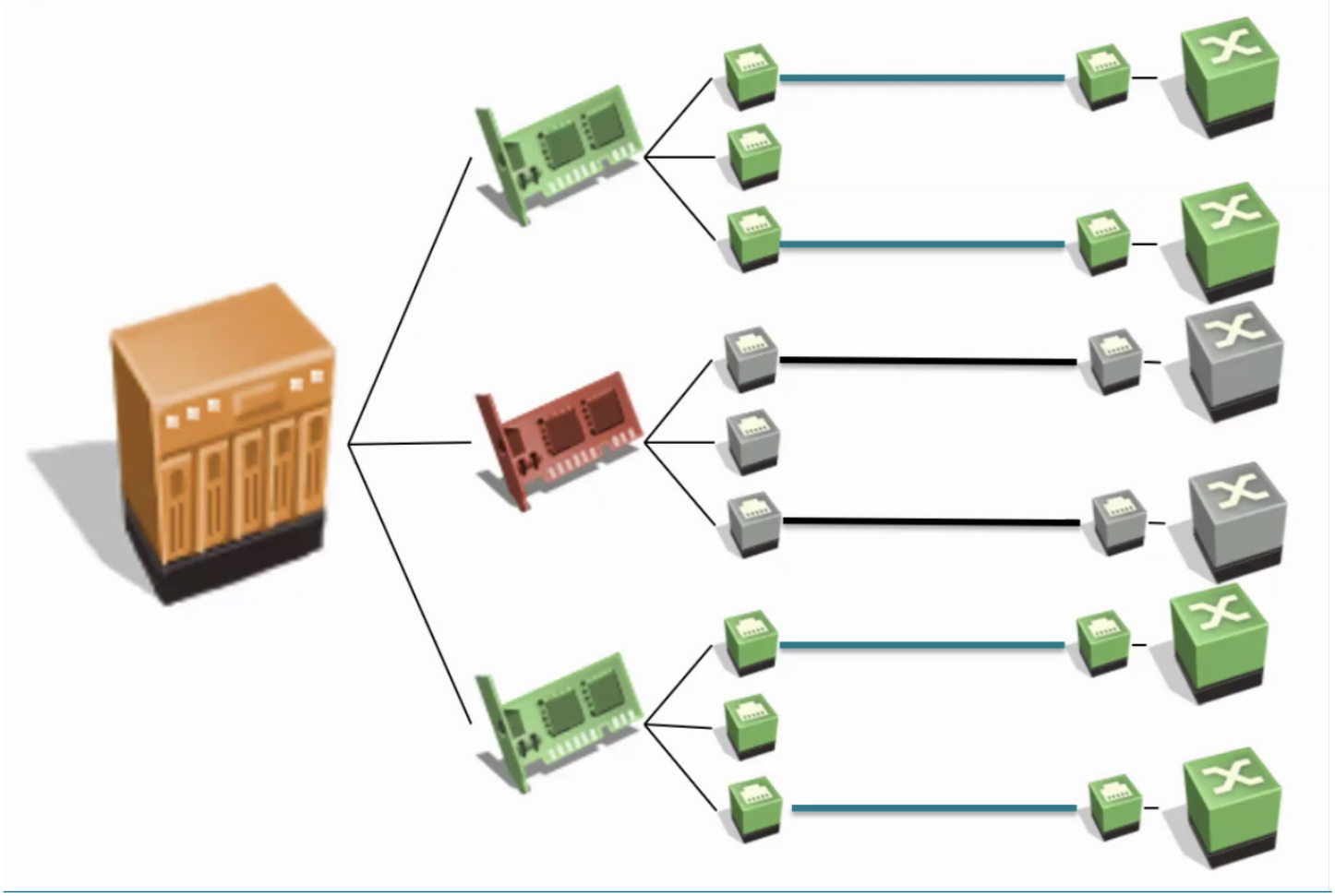

Figure 8: The core of the DX NetOps root cause analysis solution is its patented Inductive Modeling Technology (IMT).

Traffic Analysis and Anomaly Detection

DX NetOps can analyze patterns of network traffic, including source and destination IP, protocols, and port numbers. The solution provides visibility into which apps are in use and where network bottlenecks are occurring.

By unifying intelligence across traditional silos, DX NetOps can enable teams to focus on using one console, which streamlines onboarding of new engineers. With the solution's alarm reduction, teams can ensure they're focused on the right alerts, so they can quickly triage network issues that are having an impact on end users.

With these capabilities, DX NetOps can provide the insights required to speed troubleshooting, optimize network performance, identify security threats, and enhance traffic segregation and routing traffic to ensure adequate bandwidth for critical apps.

DX NetOps provides easy-to-understand charts, such as interfaces over threshold. For each interface listed, the solution can display status, interface name, traffic detection, speed, average utilization, percent time utilization, and whether an interface is at a warning or critical level.

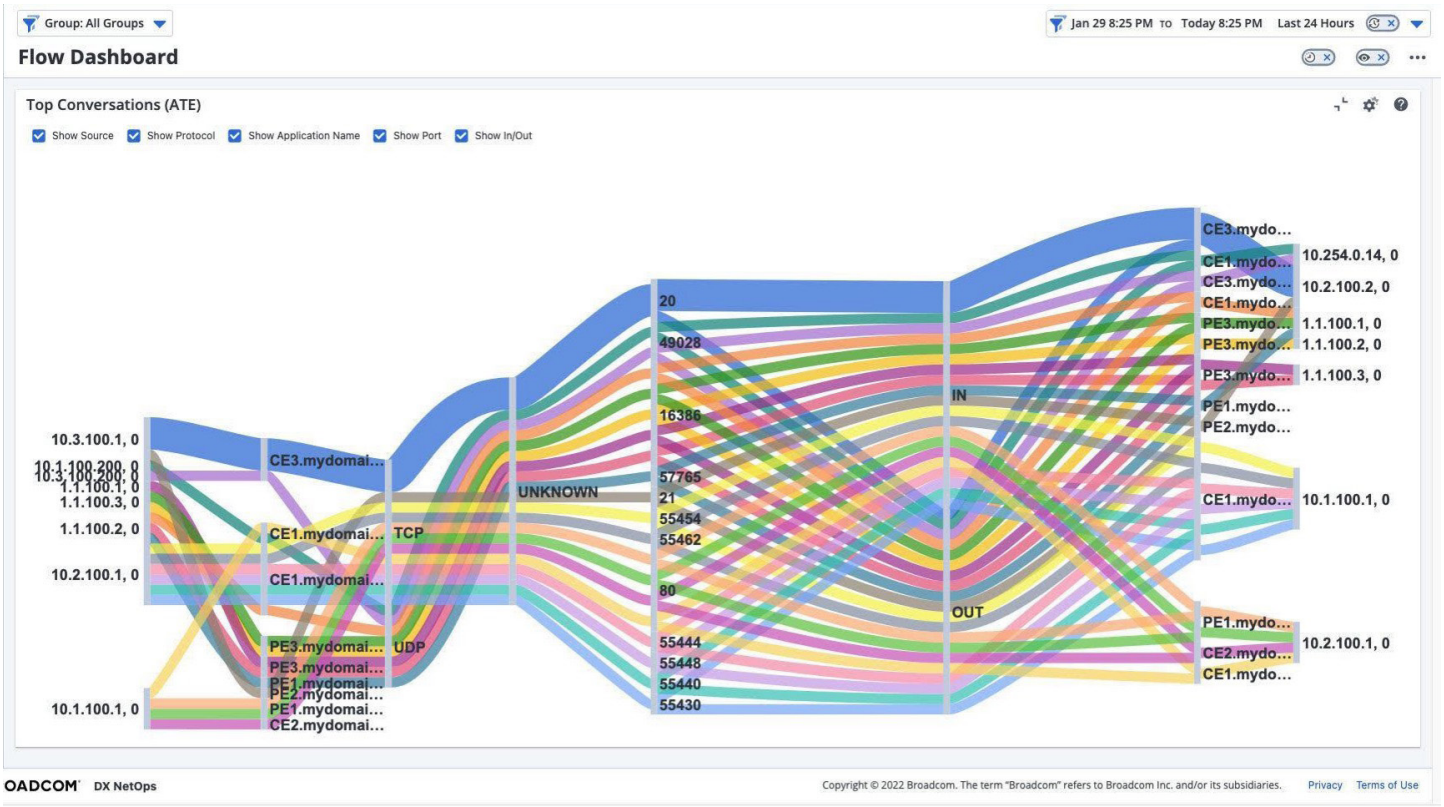

Figure 9: Network flow top conversations easily identifies offender apps and devices and their bandwidth consumption for fast root cause of slow performance issues.

INTELLIGENT TRIAGE WORKFLOWS

Within a significant percentage of NetOps teams, triage workflows are complex, inconsistent, inefficient, and slow. Teams bounce around in multiple tools and reports, they spend hours in lengthy all-hands-on-deck calls, and they're constantly hearing about issues from others, who, whether rightly or wrongly, blame the network for poor responsiveness and outages.

Because they're relying on too many disparate tools, teams fundamentally struggle to build efficient, fast triage workflows. They can't get unified views across their multi-vendor, multi-technology networks. While some teams have started to employ AIOps tools, too often, these tools are built for a level-one help desk, and lack the rich, comprehensive network intelligence that level-two engineers and level-three architects require.

Today, teams need a solution that can tame all this complexity. They need optimized network triage workflows that make intelligence easy to consume and act upon. Teams need correlated intelligence that ultimately presents the targeted insights needed, when they're needed. Further, these workflows need to make it easy for staff members to drill down and get all the details they require, whether that means getting specific data from logs, flow information, packets, or other sources.

The unified alarm portal brings disparate data across multi-vendor, multi-tech, multi-protocol network architectures for a unified view of global network health. With DX NetOps, teams can work with one alarm portal that suppresses hundreds or thousands of collected alerts from across a multi-vendor network landscape. This enables level-one operators to rapidly pinpoint their triage efforts.

With its extensive coverage, DX NetOps can consolidate alarms, events, fault, performance, flows, configurations, logs, network paths, and more. With the solution's standard troubleshooting tools, NetOps teams can work with the same management and monitoring interface for the entire triage process. The solution enables level-one operators to drill down into specific details, helping to facilitate fast, contextual investigation of issues on specific devices. The solution makes it easy for teams to understand how business services are affected by issues, helping guide troubleshooting and prioritization.

DX NetOps centralizes vendor-specific network alarms, while correlating network path health with device-specific performance metrics. In this way, the solution can provide a contextual approach to root cause isolation of network degradation.

In the alarm console, teams can access standard operating procedures and tools for initiating a range of troubleshooting steps, including pinging a device, tracing a route, opening a help-desk ticket, assigning tasks, and comparing device configurations.

The DX NetOps alarm console makes it easy and efficient to leverage the solution's powerful insights. The portal can feature alarms from modern and legacy networks, SNMP, APIs, traps, configuration events, and more. No matter where alarms are sourced, operators can view them in a single location and respond with a single click. The console features an interface based on Mineral UI, technology that enables a high-quality and accessible user interface. The interface makes it easy to accelerate response and offers a seamless way to navigate through the console and filter alarms.

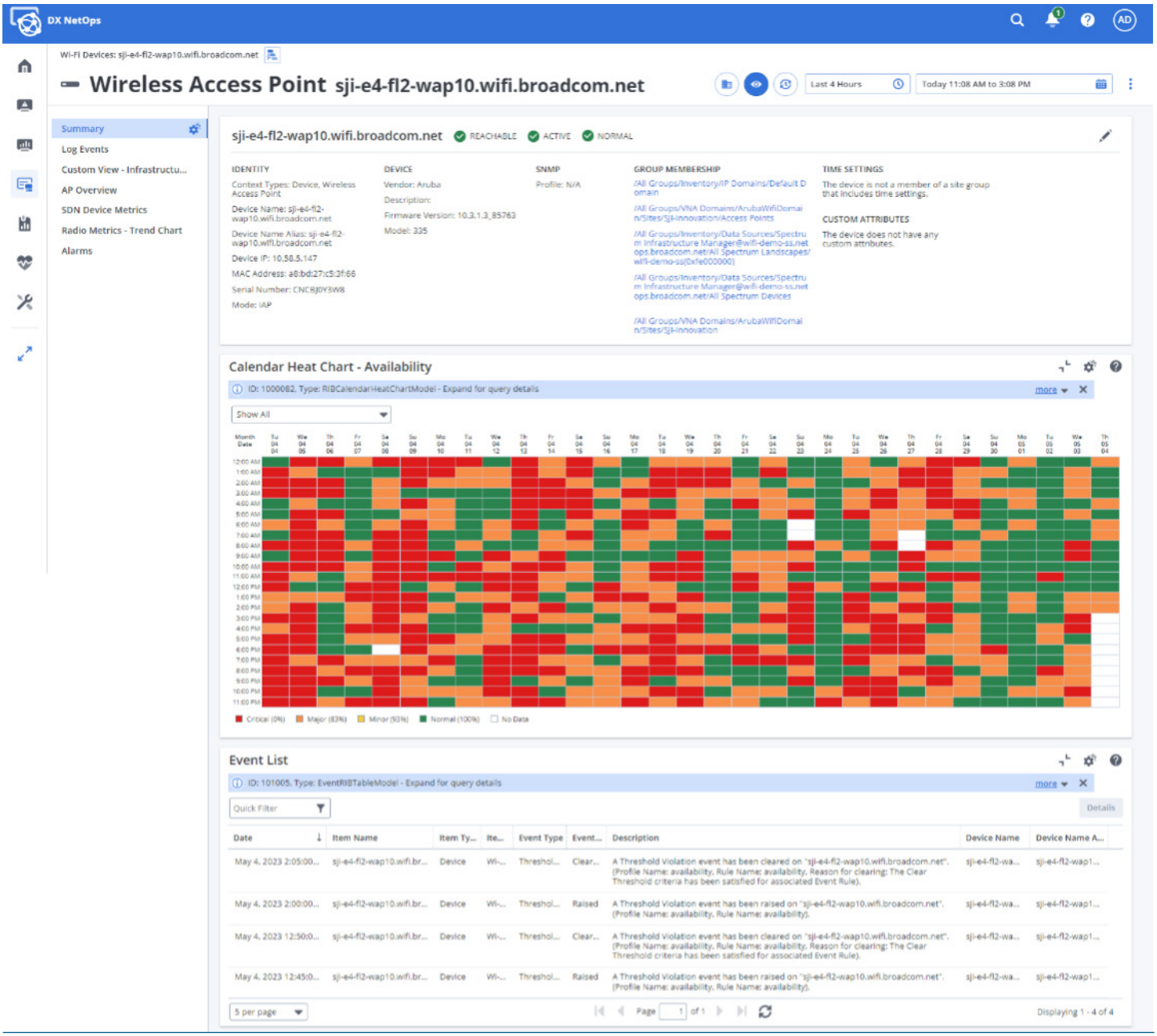

Figure 10: With one click, root cause is easily surfaced through network device context pages that provide every relevant network metric collected from faults, alarms, events, performance, flows configurations, logs, radio interference and more.

Network Configuration Management (NCM) [Network configuration management to understand change and adhere to compliance]

DX NetOps maintains a database of network device configurations and analyzes changes. Once a change is detected, the solution can initiate triage workflows to isolate specific modifications and provide administrators with the option to accept or roll them back.

With the solution, teams can correlate outages to configuration changes, speed the detection and remediation of configuration-related issues and gain detailed configuration audit trails for any network device. Users can create policies to monitor content in configurations and verify that device content is compliant. The solution also enables

operators to reduce policy violations that can introduce security and operational risk. NCM helps teams minimize the business and customer impact of issues, and even preempt issues from occurring in the first place.

Since network device configuration changes are the leading cause of network outages, Broadcom believes that the follow capabilities are required to maintain compliance for any enterprise network:

- **Unsolicited Device Change Notifications** to capture configurations on a scheduled basis, save the updated configuration data and then test against the most recent configuration captures.
- **Global Synchronization of Configurations** enables storing the latest configurations from all network devices for immediate comparisons and notifications.
- **Reference Configurations** should be specified for any network device to determine if the current configuration differs from the reference.
- **NCM Policies** are recommended to monitor content for a device host configuration and compare every time a configuration file is captured. Devices that violate the policy can generate an alarm and receive remediation while preventing any outages and maintaining compliance.

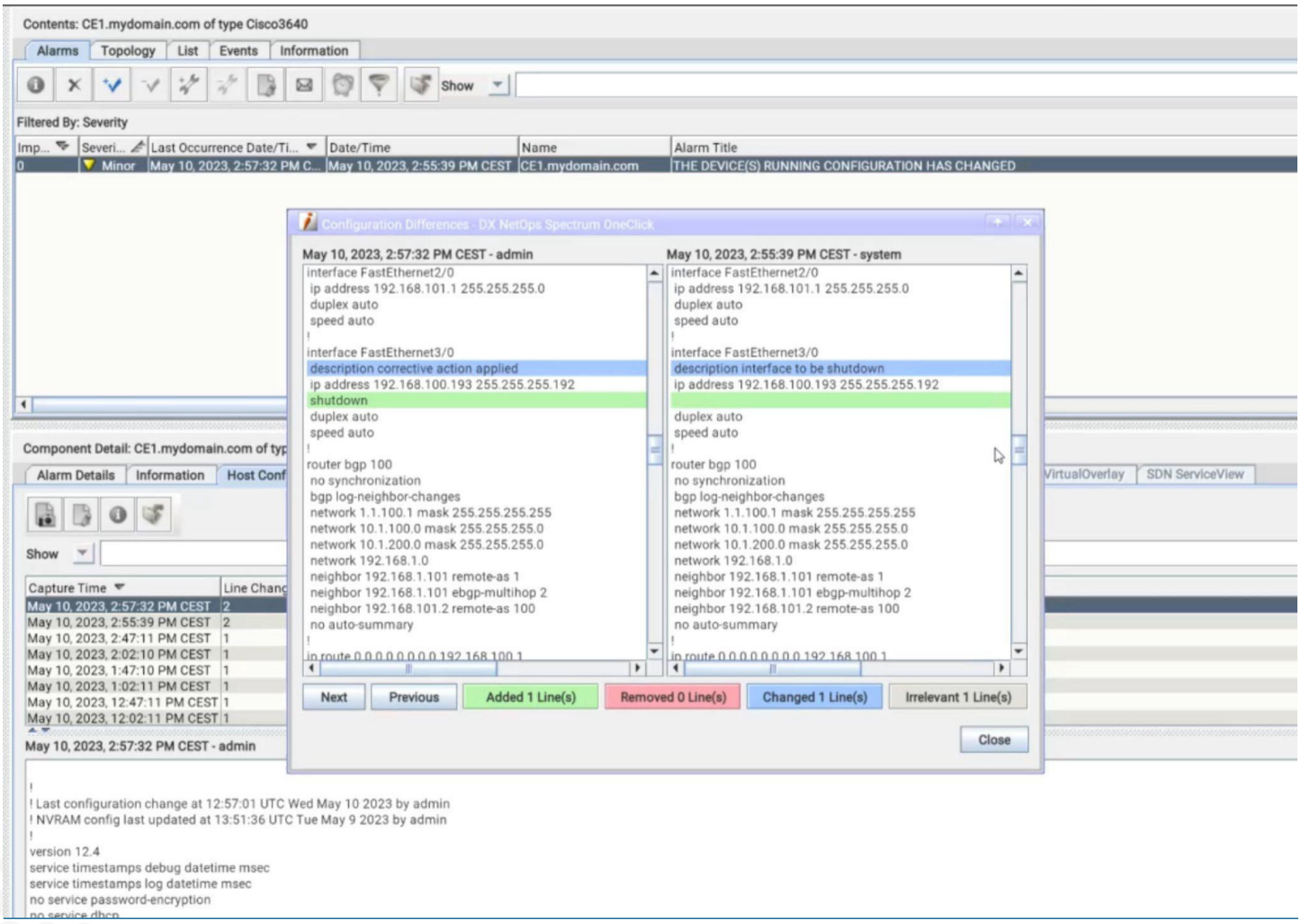

Figure 11: Line-by-line configuration comparisons provide granular operational insights and help adhere to compliance mandates.

CUSTOMER EXAMPLE

Business Background

Altice Portugal is a wholly owned subsidiary of Altice Group, a multinational cable and telecommunications company. They have a presence across Europe, including in Belgium, France, Luxembourg, Portugal, and Switzerland, as well as in the Dominican Republic, the French West Indies, and Israel.

With annual revenues of more than $2.8 billion (2,629 million Euros), Altice Portugal is Portugal's largest telecom company. Altice offers fixed, mobile, and satellite network services to consumers. The company also offers a range of services for business customers, including cybersecurity, cloud and data center services, backup and restore, remote equipment monitoring and management, and more.

Network transformation challenges

As a telecommunications company, Altice has accrued a large, complex IT environment with multiple generations of infrastructure. The IT operations group must continue to pursue digital transformation so the organization can adapt to rapidly changing user, customer, market, and technology demands.

As a result of these transformations, Altice is operating in a new age of networking. Altice continues to expand its remote data center and cloud offerings. Altice customers now rely on cloud services and SaaS offerings in addition to software-defined architectures. Furthermore, work-from-anywhere approaches are now a given for both Altice employees and customers.

Solution: DX NetOps

Over time, Altice continued to expand their usage of various network monitoring solutions, including DX NetOps by Broadcom. Altice leverages DX NetOps to provide coverage of network performance, fault, and flow, in both their traditional and software-defined architectures.

With DX NetOps solutions, the Altice team has been able to adapt seamlessly to new technologies and the demands of new networks. They have used DX NetOps for Simple Network Management Protocol (SNMP) monitoring for years. The team successfully implemented DX NetOps Flow to conduct flow analysis and validate customer connections, consumption, and performance.

Recently, the team started using AppNeta by Broadcom. AppNeta extends Altice's monitoring visibility and control beyond the edge of their networks and into unmanaged networks like home Wi-Fi as well as third-party telecommunication, cloud, and SaaS environments that customers may use daily. With AppNeta, teams can quickly isolate the location of performance issues, including those that arise on networks not owned by Altice. Further, it helps speed mean time to innocence (MTTI), providing objective evidence of the location of outages that arise in home Wi-Fi networks and other ISP and cloud providers' networks.

Altice has uncovered many technical and business benefits by using Experience-Driven NetOps from Broadcom to include:

Optimize service levels of new service offerings. AppNeta's active network testing enables teams to validate every hop in the network path of new service offerings, from client to application. As a result, they can spot and address any issues that would have a negative impact on the user experience, all before rolling new offerings into production.

Improve MTTI. With Broadcom solutions, the team at Altice is able to correlate individual device performance with end-to-end network monitoring, across both internal environments and externally managed networks. As a result, they can quickly pinpoint the location and root cause of issues, speeding MTTI.

Speed MTTR. Broadcom solutions deliver improved visibility into managed and unmanaged networks that customers count upon. With this comprehensive visibility into networks and the user experience, the team can identify and resolve network issues in minutes—not hours.

CONCLUSION

For too long, networks, and the tools teams have used to manage those networks, have kept getting more complex. Consequently, teams spend too much time, effort, and money trying to find the root cause of issues. These trends simply can't continue.

DX NetOps addresses the three fundamental requirements that enable NetOps teams to speed issue detection and resolution:

- **A highly scalable, unified data model.** DX NetOps represents one solution that can collect, normalize, and correlate various disparate data sets from across the organization's multi-vendor, -technology, and -protocol network environments. DX NetOps delivers the "one source of truth" that NetOps teams need today.
- **Advanced analytics.** Once data has been collected, DX NetOps applies advanced and patented analytics. These analytics enable teams to uncover patterns, identify issues faster, and anticipate how changes will affect the user experience or network health.
- **Intelligent triage workflows.** DX NetOps presents operators with the intelligence they need, within intuitive, easy-to-understand troubleshooting workflows. The solution minimizes alarm noise, so NetOps teams can quickly diagnose issues and identify the root cause.

Visit **Network Management by Broadcom** to learn more about how to achieve rapid and accurate isolations.

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

Rapid-Isolation-Tech-WP_BC-NO-2023_CE-3941_v2 November 17, 2023