BROADCOM

WHITE PAPER

Establishing End-to-End Visibility of Internet Performance: 3 Keys to Addressing Monitoring Blind Spots

TABLE OF CONTENTS

OVERVIEW

By 2025, an estimated 51% of spending by IT and network operations teams will have shifted to the public cloud, according to Gartner analysts. When it comes to application software, the number is even higher, with spending in the cloud expected to grow to 65.9%.[1] This continued cloud adoption results in an increasing reliance on internet services, and on a complex mix of external service providers and technologies to deliver those services. For network operations teams, these moves serve to significantly reduce visibility into the performance of the underlying infrastructure that business services depend upon.

The challenge is that, in spite of this diminishing visibility and control, these teams remain responsible for network performance. This represents an increased risk to the overall business, particularly given users are more physically and logically separated from the apps they need to work with. This means outages and performance issues lead to a loss in time and productivity, not to mention lost revenues. Without an ability to remediate quickly, network operations groups also risk losing the confidence of users and business leaders.

Traditional monitoring methods gather passive device-level data, but these approaches are not possible when teams do not own or manage the network. Network operations teams must establish new techniques that help them gain the end-to-end internet visibility they need, so they isolate issues more efficiently and more consistently avoid disruption. In order to accomplish this goal monitoring solutions should provide internet visibility in the following ways:

- **Fully map the route user traffic takes.** When things go wrong, it is critical to identify the problem's domain and who's responsible for solving it—even if the issue arises outside of the team's internal networks.
- **Continuously monitor performance over the route.** On a 24x7 basis, test and consume application and network resources, just like users do. In this way, teams can catch classes of problems that go unnoticed by passive device monitoring, such as protocol and router configuration problems.
- **Understand the full responsibility footprint of applications and networks.** Teams need to monitor as much of the organization's network footprint as possible. Put low-overhead monitoring on every network that users rely on and on important infrastructure. This is essential in determining who is actually affected when problems occur.

The sections below offer a detailed look at each of these capabilities.

1 Gartner, "Gartner Says More Than Half of Enterprise IT Spending in Key Market Segments Will Shift to the Cloud by 2025," February 9, 2022, URL: https://www.gartner.com/en/newsroom/press-releases/2022-02-09-gartner-says-more-than-half-of-enterprise-it-spending

FULLY MAP THE ROUTE USER TRAFFIC TAKES

The increased adoption of technologies like software-defined wide area networks (SD-WAN) and cloud access security brokers (CASB) have added reliability and security to networks. However, these technologies obfuscate the actual route traffic takes between users and applications. Today, user traffic goes through multiple domains with multiple levels of security. Even with trusted applications, user traffic may leave office environments and navigate through proxies and tunnels before being released to the open internet. Each of these hops has an impact on performance. However, organizations need to strike a balance between ensuring security and providing the access and ease that users and the business demand.

With the continued improvements in deep packet inspection (DPI) capabilities, SD-WAN deployments are application-aware, influencing routing decisions. Microsoft specifically recommends that customers of some of its SaaS applications **bypass proxies for their traffic.**[2] Given this, companies are increasingly requiring that traffic take different routes to the internet, depending on the application.

Here's an example of how a large organization may manage internet routing design:

- For trusted Microsoft apps, traffic goes directly to the internet from office sites.
- Internal application traffic is routed through the data center.
- The remaining traffic goes through one of two GRE tunnels, to CASB, and to the public internet.

With the use of CASB services, there is no longer a single dedicated internet break-out for an organization using proxies. Instead, the point of presence (POP) that traffic is being routed through can vary based on internet performance as well as the CASB provider's availability and performance. This means that the internet break-out and subsequent path to SaaS services can vary widely, which requires additional active network testing.

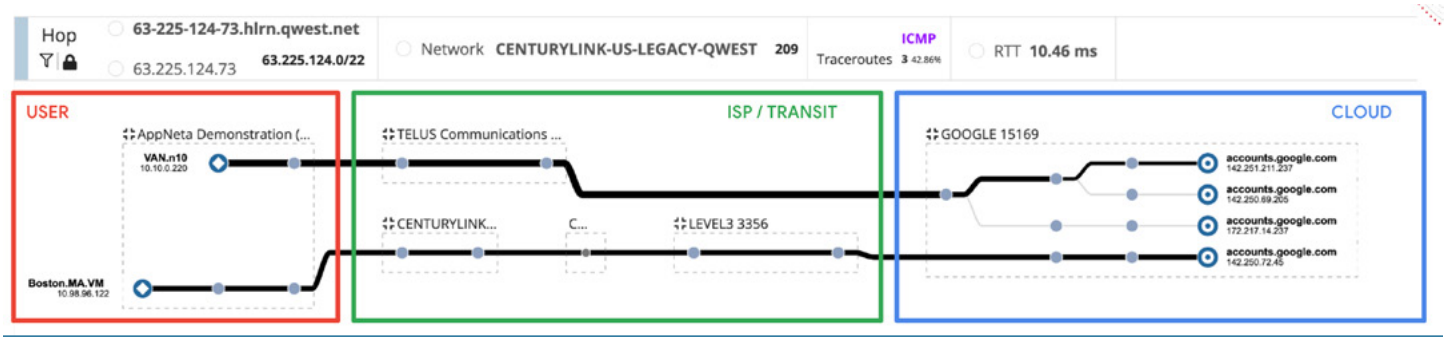
Error Domains

Based on the increased number of technologies available in these modern environments, isolating issues can be difficult. Narrowing the scope is the first step. By segmenting network traffic into specific domains of ownership in which issues can occur, network operations teams can more readily identify who is at fault. Being able to gain visibility into these error domains is essential to reducing the mean time to resolution (MTTR) of issues:

- **End-user domain.** Office or home environments may include wireless or wired connections. In these environments, issues are limited to end-user workstations, wireless access points, and LAN devices.
    - **SD-WAN.** From end-user workstations or from office infrastructure, it is crucial to understand where tunnels can have an impact on the routing or performance of traffic. Additionally, monitoring the underlay is often required for complete visibility and for verification that underlay providers are meeting service-level agreements (SLAs).
- **User's last-mile ISP.** In office or remote locations, user traffic traverses ISPs, either in tunnels or split out for trusted apps, such as Office 365. Centralized network operations teams may have no knowledge of which ISP is in use until tickets are created.

2 Microsoft, "Proxy servers for Teams and Skype for Business Online,"
URL: https://learn.microsoft.com/en-us/microsoftteams/proxy-servers-for-skype-for-business-online

- **Mid-path and transit.** Traffic through ISP peering, cloud transit backbones, and any upstream provider that is obfuscated from the user can be mapped with active testing.
    - **CASB.** When there are separate internet breakouts from proxy environments, blind spots can be introduced for traditional monitoring. Network operations teams must piece together visibility into the full end-to-end path of traffic.
- **Application service provider.** Issues can arise in cloud-based environments or the enterprise infrastructure at the far end of the transaction. Teams must first isolate whether it is an application or network problem. Next, they need to isolate the network environment in front of the application that is the responsibility of the provider.



In order to be able to identify the domain or service provider at fault during times of degradation, teams need to first identify or verify which service providers are in the route at the time of degradation. Additionally, reporting on the exact route, IP addresses involved, and hop-by-hop performance can be used as evidence for working with service providers.

Existing Tooling

Network operations teams have very few existing tools when it comes to understanding internet performance. Basic functions like ping and traceroute are useful, but these are often manual processes that need to be run during periods of degradation. Further, to gain real insight, teams need to be able to have historical comparisons. For users who are outside of the controllable office environment, many operations teams have no visibility and have to rely on asking users to run speed tests. In fact, during the pandemic many organizations required potential new hires to run speed tests and validate they had connectivity that offered sufficient responsiveness. This was vital for cases in which latency could directly affect the critical job functions of remote workers, such as remote call center representatives.

For application-specific issues, online tools like DownDetector can offer general outage information, but can't detail who is affected. Another issue is where the testing is performed. When testing is conducted far away from end users, accuracy is reduced. If the data is coming from general regions across the internet, teams won't have specific enough information for individual troubleshooting tasks. If the data is gathered from the network operations team's location, it won't reflect the exact network path used by affected end users. Additionally, manual testing means no 24x7 monitoring context is established, which is vital in gaining an understanding of the users' experience when they access a network from a remote office or home environment.

To effectively respond to issues, network operations teams need to understand which users are affected and the routes that user traffic takes to access business-critical applications, including connections made from inside and outside of their traditional network. Teams need visibility that provides an end-user perspective. Testing needs to originate from the users' locations, whether they are in offices or homes, and from behind the firewall, out towards application and cloud environments.

How to Gain Visibility From the End-User Perspective

The first requirement of any effective internet performance solution is to enable route determination. By validating what route different application traffic is taking, network operations teams can isolate the error domains in play. ISPs, transit providers, and cloud providers routinely use load balancing to avoid congestion in core locations. They also change peering providers based on automated BGP routing. Continuously building a route map is critical because routing is not a static process. Routes change and adapt to surrounding conditions. Consequently, it can be invaluable to understand the route used during the period of degradation and compare that to historical routes.

One Broadcom customer has applications hosted in AWS, specifically in the cloud provider's US East region. The company has users in Asia, who need to access these applications. Due to BGP weighting in the internet, rather than entering AWS infrastructure in Asia, this traffic is intermittently routed to Australia over the public internet, before entering AWS infrastructure and traversing to the US East region to reach applications. This inefficient routing leads to extremely high latency and poor application performance. With NetOps by Broadcom, this customer was able to match the route with its associated latency and identify the cause of the issue.

It's not just in the office that routes have become more complicated. At home, users are now often connecting over wireless, split tunnel VPN, or no VPN at all, and instead relying on zero-trust network access (ZTNA) and CASB services. For network operations teams, the core question becomes: Are services taking the route expected, and over what infrastructure?

With more users at home, business continuity is now reliant on residential ISPs for last-mile delivery of business-critical apps. Network operations teams now need scalable visibility, so, for a large remote workforce, they can answer a number of key questions:

- What is the mix of ISPs user traffic runs across?
- How do regional ISP outages affect users?
- How do teams know what ISP networks user traffic is traversing?

To ensure that home-based and hybrid-work users have secure, reliable access to critical services, many organizations establish specific access policies. For example, teams may require the use of wired connections, prohibit the use public Wi-Fi, and so on. Enforcing these policies can be difficult without being able to see which SSID or connection type people are using, both currently and over a range of time windows.

CONTINUOUSLY MONITOR PERFORMANCE OVER SPECIFIC ROUTES

As outlined above, a core challenge with using route analysis to gain actionable visibility into internet performance is the fact that the routes between business-critical apps and users are dynamic. At any given time, multiple third-party networks, diverse load balancing systems, and dynamic routing technologies may be in play. Given that, understanding where traffic is flowing is a minute-by-minute endeavor.

While some free methods exist to monitor internet performance, they do not offer any visibility into who is affected by a problem. Another challenge is that, with resilient cloud apps, "slow is the new down." Other solutions specifically monitor BGP updates, which can be useful for teams in large organizations. These solutions can provide insights into peering changes within the internet as well as specific security threats, such as BGP hijacking. However, these solutions fail to provide the context for business-critical applications, and the user experience they're providing.

Traditional passive monitoring based on packet and flow data can be used to understand the capacity needs for an office or to set a minimum baseline for remote employees. Active monitoring is key to understanding the continuous performance of links and to acquiring the insights needed to speed issue resolution.

In order to gain better visibility into internet performance, teams need to understand network performance from the end-user perspective. By gaining this visibility, teams can understand how issues affect users, regions, and specific applications.

In order to troubleshoot issues for users, network operations groups have to combine the device-level data obtained from traditional passive monitoring methods with a new kind of visibility. An active approach is necessary for gaining an understanding of the dynamic networks outside of the internal team's control. Teams need to actively monitor end-to-end performance from the user device, through the last-mile ISP network, and out to third-party application service provider environments. With this visibility, network operations teams can quickly and intelligently isolate where issues are occurring, no matter where they arise. If the issue originates from an ISP's infrastructure, they also have the data to prove it.

Active monitoring also provides the basis for proactive alerting. Active monitoring solutions can be used to gain an understanding of normal operations and they can be employed to alert on deviations from the norm. With these solutions, teams can be alerted to worsening conditions on enterprise networks, so they can proactively work to preempt issues. Given the massive scale of enterprise network usage, teams simply can't know every ISP, every link speed, and even every location users may connect from. However, they can employ a monitoring system that brings that information to them when abnormal conditions arise, which is essential for rapidly isolating issues.

TruPath

The NetOps by Broadcom solution for network observability and management consists of multiple parts. For visibility into external networks, AppNeta by Broadcom features TruPath technology that delivers the active monitoring capabilities that today's network operations teams need. The solution leverages common protocols to continuously monitor network paths. When thresholds are exceeded, the solution provides advanced escalation of monitoring to gather more diagnostic data. The following section describes this methodology in more detail, starting with how the basic concepts work.

TRUPATH SUMMARY

TruPath analyzes network paths in two ways: A functional network model and a dysfunctional network model. Functional implies that the path is performing according to normal network design. In that case, the measurements made represent its capacities and usage. Being dysfunctional implies behaviors that are outside design norms. The simplest example of this is packet loss. Once traffic levels have exceeded capacity, it is possible to have packet loss due to congestion. This means that the network is operating outside of design specifications.

When TruPath detects degradation symptoms, it automatically performs diagnostic analyses against models of network dysfunction. These models isolate and identify characteristics that are specific to a particular source. Each type of degradation affects the testing differently and thus creates a unique "signature" that distinguishes the type of degradation.

PACKET TRAIN DISPERSION TECHNOLOGY

TruPath is based on the monitoring principle of sending and receiving many varied short sequences of packets to defined end hosts, or targets. (A target can be any IP stack that can respond to an Internet Control Message Protocol (ICMP)-based ping or that can send back a Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) packet.) These packet sequences are referred to as packet trains, and are transmitted using commonly available ICMP or UDP mechanisms.

Using this technology, TruPath can build up a complete set of network statistics very quickly—in many cases, in just tens of seconds. However, the Achilles' Heel of past packet train dispersion tools has been that with lots of cross-talk traffic and other performance impairments on the path, the transmitted sequences begin to interfere with each other, which could distort the results.

TruPath automatically avoids this issue by first using special patterns designed to detect if instrumentation packets are interfering with each other. If that happens, it takes more varied samples over a longer time scale to ensure that the resulting statistics are clean.

By sending multiple sets of distinct packet sequences, TruPath can analyze a wide range of different traffic conditions that a user on a network path might experience. By probing the path repeatedly with the packet sequences, TruPath collects a statistically significant collection of responses for each type. TruPath will detect when samples are captured during times of rapidly changing conditions and adjust its measurement patterns accordingly.

Unlike so-called "packet flooder" technologies available on the market, this approach delivers high accuracy without requiring an intrusively high instrumentation load on the network path.

CONTINUOUS PATH ANALYSIS AND DEEP PATH ANALYSIS INSTRUMENTATION

To measure network performance, TruPath uses two instrumentation approaches:

- **Continuous path analysis (CPA).** CPA is designed to monitor a very large quantity of paths with as low amount of overhead as possible. CPA enables teams to see overall path quality and performance. CPA generates a continuous representation of a range of network behaviors over long periods of time, such as bandwidth, loss, jitter, and latency.
- **Deep path analysis (DPA).** DPA can instrument a path to a higher resolution and provide more accuracy. DPA also provides the additional leading indicators needed to feed into diagnostics and troubleshooting workflows.

These techniques help AppNeta to have a very low impact on the network it's measuring. TruPath only needs about 2 Mbps during continuous monitoring. For very slow links or networks with other restrictions, TruPath automatically adjusts its timing, size, and distribution curves. This optimization is done during the startup phase.

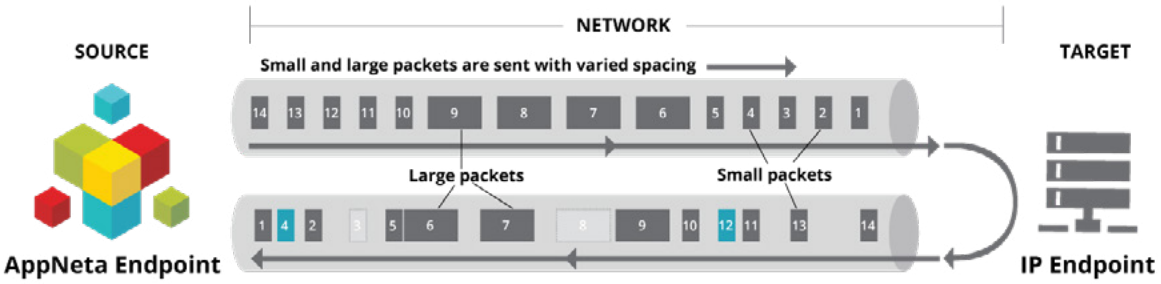
When critical indicators vary from an expected or accepted value, CPA automatically responds by increasing statistical resolution. This escalated mode prevents TruPath from automatically escalating unnecessarily into the more accurate (and slightly more intrusive) DPA mode. DPA is only engaged when a network path is truly dysfunctional.

This automatic escalation, along with variable resolution, lets TruPath monitor tens of thousands of paths and focus on the few paths that deviate from performance norms.

ICMP SUPPORTS TRUPATH'S FLEXIBILITY

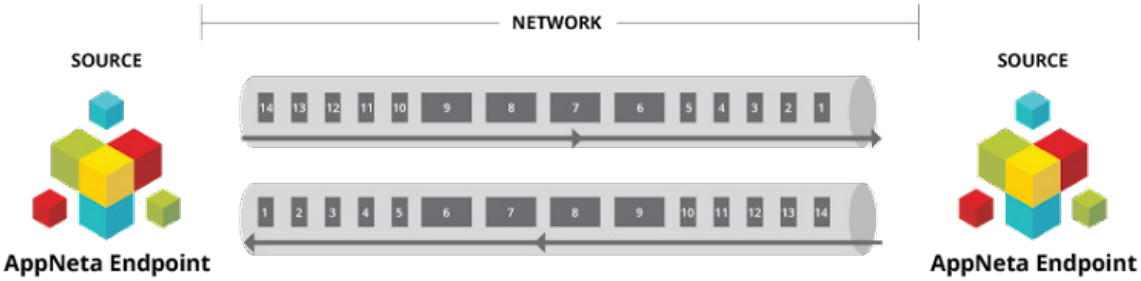
Each of the solution's network paths or group of paths can be instrumented in single-ended or dual-ended configurations, as well as both modes at the same time. Single-ended mode works well for monitoring performance into SaaS provider networks, where dynamic load balancing and software-defined networking are common.

The default single-ended mode requires that TruPath technology only be present at one end of the network path. The solution relies upon ICMP combined with ICMP Echo Mode 8, which is in every modern TCP/IP stack. Because ICMP is a core ISO layer 3 protocol used by routers, the vast majority of IP addresses respond to an ICMP "echo request" with an ICMP "echo reply."



ICMP is predictable and accurate in soliciting responses from any IP-based network host. The TruPath sending device (also known as a sequencer) only has to reside at one end of a given network path in order to measure the complete round-trip performance. TruPath determines what the base IP network (or the layer 3 network) can actually deliver, without the overhead of layer 4 protocols. (AppNeta also offers alternative methods for measuring performance of layer 4 protocols.)

Dual-ended mode requires placing TruPath software at both ends of a path. TruPath measures the asymmetric path to enable users to understand the differences in performance in each direction. In dual-ended mode, more paths are measured using UDP packets in order to measure upstream and downstream performance separately.



It's important to note that the TruPath methodology can take advantage of nearly any network transport mechanism. ICMP and UDP are used because they are both prevalent in every modern IP-enabled device. In addition, measuring some key path metrics, especially bandwidth, at the TCP level often leads to erroneous results, given they can be affected by TCP window size and overall path latency and round-trip time. All three protocols can also be used for route determination. This approach can illuminate network sections in which data routing differs depending on the protocol.

GUARANTEED ACCURACY

TruPath actively probes the specified network path and generates one or more packet timing distributions for that path. These groupings range from single packets to small bursts to short streams, sometimes in varying protocols.

By default, packet sequences are sent at an average of 2 Kbps when monitoring and 30 Kbps when troubleshooting. This approach is designed for network paths that operate at 512 Kbps or higher. If paths are less than 512 Kbps, TruPath controls its own packet rate to ensure proper sampling, without overwhelming the network. TruPath captures packet sequence timings, including loss and various forms of network error, to get critical performance data. The numbers produced exactly reflect the response of the end-to-end path to show how an application will experience the network.

TruPath's lightweight continuous monitoring instrumentation is generally within +/- 5% of results measured on the wire, and the deeper troubleshooting instrumentation will tighten the results to +/- 2%. TruPath's accuracy results are only affected by the quality of the timing distributions generated. For example, TruPath adjusts accordingly for more statistically accurate results.

Most traffic conditions are known to change over time, sometimes as fast as minute-by-minute or hour-by-hour. TruPath's self-feedback loop automatically adjusts for these kinds of conditions. As a result, the solution delivers highly accurate analysis, even in difficult, fast-changing conditions.

AppNeta's TruPath technology enables visibility into internet performance by actively and continuously testing across the exact network delivery paths that transport business-critical apps to users. By escalating only when necessary, the methodology also keeps overhead to a minimum. This means that TruPath can be run continuously in production networks, without affecting users.

UNDERSTANDING THE CURRENT FOOTPRINT

Network operations teams are now responsible for the network architecture. They're also accountable for performance of applications running over the network—even when those apps are owned and run by third parties. With routing visibility and active monitoring, teams are in better shape, but what they still need is the application context. At the core of monitoring internet performance is knowing what apps are critical to the business. Increasingly, this includes apps users run without consulting or involving IT and network operations teams, which is often referred to as "shadow IT."

The increasing frequency of shadow IT has significant security implications, but these won't be covered in this document. Nevertheless, it is vital for teams to know which applications are being used in the organization, and their respective load on the network when it comes to throughput and capacity. This visibility is essential in enabling effective triage processes. To understand when business-critical apps are being affected by other traffic, it is critical to know what apps are taking up network capacity and running on end-user devices. IT and network operations teams also need to verify how performance is affected by new technologies or applications.

"Flooding" refers to the concept of routing an incoming packet to every outgoing link, with the exception of the node that initially received the packet. This is the most common way for network architects to understand the capabilities of their network. Flooding, however, will prevent the network from running for the duration of the test, so it is not suitable for production or business-hour operations. Further, these floods are detected and dumped when they reach ISP networks, which means these approaches are only useful for understanding local networks. Knowing the maximum capacity of the LAN is important, but of limited use when the LAN makes up a small portion of the end-to-end network delivery path.

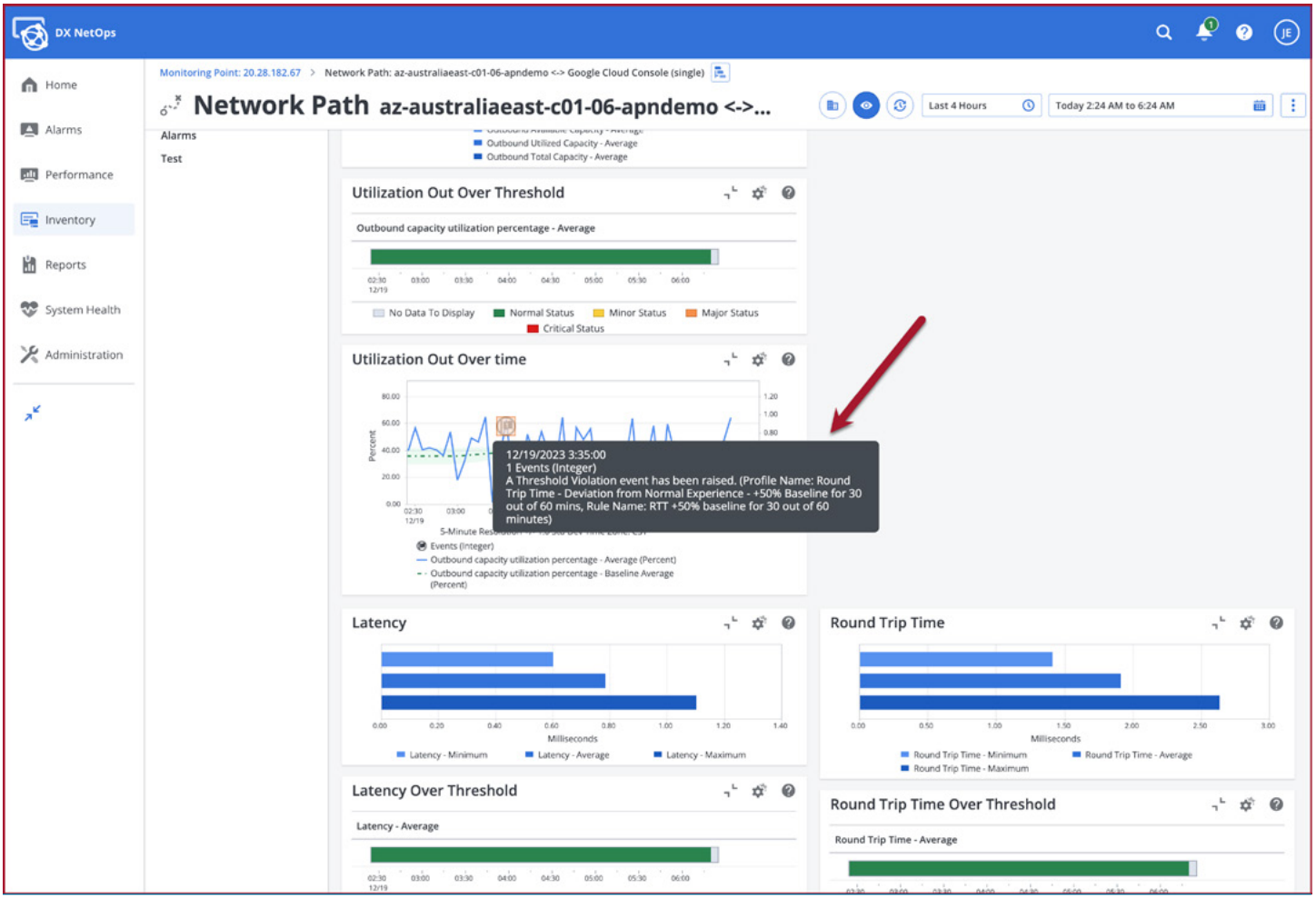
When teams are early in their journey with direct-to-internet approaches and they encounter issues, a common approach is to allocate or purchase more bandwidth from their ISP. While this can help with local congestion issues, it won't help teams get to the root of the problem. Fundamentally, teams need visibility into where issues occur, even if they arise in networks that are managed by external providers. This is especially vital given these externally managed networks continue to play an increasingly vital role in critical business services.

Scale Insights for Networks and Applications

NetOps by Broadcom provides highly scalable monitoring and metrics storage and reporting. The system architecture provides the scalability needed to support some of the largest networks in the world. Metrics gathered across multi-technology, multi-vendor environments and unmanaged networks can be leveraged in a unified fashion, and delivered via reporting, dashboards, and APIs. The Broadcom solution provides intelligent analytics, scalable visualization, and fast processing for instant reporting.

The solution's customizable dashboards and views provide significant flexibility. For example, regional managers can use a dashboard that pins views to each site group in in their region. Systems administrators can use a dashboard for monitoring all the servers they're tasked with supporting. Dashboards can be customized to provide tailored information to a specific group. Context pages can deliver information that is related to a specific item in the system.

The historical data collected is used to establish performance baselines for selected monitored metrics. These baseline averages help teams to visualize past performance and more intelligently assess present performance. The solution features NetOps Portal, which calculates baseline averages and related standard deviations on an hourly basis. The standard deviation provides a statistical indicator of how much variability exists in the population data that factored into the baseline average calculations. Alerting is activated when current performance is over or under normal utilization. Historical data also serves as a source of intelligence for site planning and capacity upgrade planning.



Charts show threshold violations for utilization on a network path.

Advanced Thresholds

One of the core capabilities provided by NetOps is to provide insights into how much network capacity is being used. The solution also provides advanced baseline monitoring and threshold functions, including capabilities for tracking deviation from normal and generating alarms based on time over thresholds.

Thresholds are available on multiple metrics, such as latency, packet loss, and jitter. For example, teams can set up a latency threshold in milliseconds, and percentage thresholds for jitter or packet loss. Teams can also define different alarm values for minor, major, or critical situations. Alarm values can depend on the response time, the transaction time, or the metric type. When latency, jitter, or packet loss metrics exceed the normal threshold value, the appropriate alarm is triggered automatically. This way, operators can keep track of any latency, jitter, or packet loss issues and troubleshoot them quickly.

ISP Validation

Getting an ISP to admit fault for performance disruptions can be difficult. Without an SLA in place, organizations must track performance on their own. Teams can throw more capacity at an issue, but that isn't necessarily the best short- or long-term decision. AppNeta can help with understanding real-time and historical performance of provider links. Teams can use the solution's reporting to prove to ISPs that the capacity delivered is below the level contracted.

By combining active performance data with passive device data and historical comparisons, the solution enables network operations teams to track every app running on enterprise infrastructure and their impact on the overall performance of the network and other applications. By unifying these different types of visibility, teams can accelerate triage. With the solution, teams can readily determine, for example, whether poor performance correlates with high utilization. This combined data enables teams to troubleshoot current issues faster and more effectively strategize for long-term network upgrades.

CONCLUSION

Organizations continue to grow increasingly reliant upon internet connectivity for even the most basic business functions. This means that network operations teams will remain accountable for the performance of networks they don't natively have visibility into. While device-level infrastructure data remains important, it is not enough to tackle modern network issues that involve growing enterprise sites and footprints. Given these realities, it is now incumbent on network operations teams to fully map the route traffic takes, continuously monitor performance over critical routes, and understand the full footprint of networks and applications.

By isolating specific error domains and implementing continuous monitoring of these areas, teams can shift from reactive to proactive triage processes. Further, they can gain the predictive insights that help improve the experiences of internal and external users. Further, because of the low-overhead nature of TruPath, teams can practically run comprehensive network and end-user experience monitoring in production environments. By leveraging the solution's capabilities for isolating what apps are running on the network and what their impact is on business-critical functions, teams can spend less time on troubleshooting, and more time on strategic initiatives.

NetOps by Broadcom delivers visibility into internet performance, tackling the problem of visibility and accountability from multiple angles. By establishing end-to-end coverage of various connectivity technologies and focusing on performance, network operations teams can eliminate finger pointing and shift to a proactive approach for network monitoring.

KYNDRYL BOOSTS MONITORING SCALE WITH END-TO-END COVERAGE

In recent years, Kyndryl has expanded its adoption of cloud services, hybrid work approaches, and software-defined networking technologies, including SD-WAN. Combining DX NetOps with AppNeta, the team is able to get the unified visibility they need to monitor and manage their modern networks. With the Broadcom solution, teams can monitor connections between data centers and cloud services and between hybrid workers and cloud environments.

The Broadcom solution provides visibility into the network underlay and overlay within Kyndryl data centers. By leveraging this visibility, the team is able to get a unified picture of how the environment is performing.

In addition, the solution provides visibility into end-to-end performance that extends beyond the network edge. AppNeta provides hop-by-hop visibility across ISP and cloud environments, enabling the team to get essential visibility into application response, network response, and retransmission time.

WHY BROADCOM

NetOps by Broadcom combines active and passive monitoring technologies to enable end-to-end network management, monitoring, and observability. With the solution, teams can gain a unified view of the internal and external networks that their businesses depend on.

By remaining vendor agnostic and focusing on data analysis, Broadcom can deliver third-party validation to any network and at any scale. Proven in the largest environments, the Broadcom solution eliminates visibility gaps and delivers a comprehensive network observability and management solution designed with tomorrow in mind.

The solution enables network operations teams to benefit from consistent workflows and a unified approach to managing traditional and software-defined environments, while gaining extended visibility into end-to-end network operations. With the solution, network operations teams gain the visibility required to enhance connected experiences for any user, no matter which app they use or where they're based.

BROADCOM
connecting everything®

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

Visibility-into-Internet-Performance-White-Paper_BC-NO_CE-4117_v2 February 1, 2024