AppNeta
by Broadcom Software

WHITE PAPER

FOUR DIMENSIONS OF NETWORK MONITORING

Why "Good Enough" Doesn't Cut It with Performance Monitoring

AppNeta by Broadcom Software

WHITE PAPER

FOUR DIMENSIONS OF NETWORK MONITORING

Why "Good Enough" Doesn't Cut It with Performance Monitoring

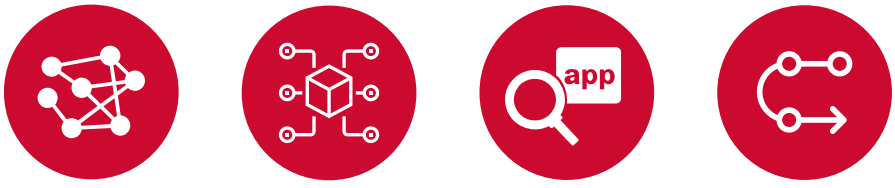
Network performance monitoring solutions run the gamut, from single-purpose tools that simply confirm whether infrastructure is running, to comprehensive platforms that account for all dimensions of the network.

With enterprise networks migrating to the cloud, arming IT with a complete picture they can take action on is essential. While teams used to own and control most areas of their network, the move into network environments supported by the cloud and the decentralization of the enterprise, in general, makes visibility a tall order — that is, without a comprehensive monitoring solution.

When it comes to delivering comprehensive network performance monitoring, no competitor can match the breadth and sheer amount of detail that AppNeta by Broadcom Software delivers. Our platform combines four dimensions of monitoring data—network paths, packets, web/URLs and flow—that give centralized IT a local perspective into end-user experience, regardless of where IT resides. All of this is done without impacting network capacity, and with the ability to scale from 10 to 10,000 endpoints as customers grow.

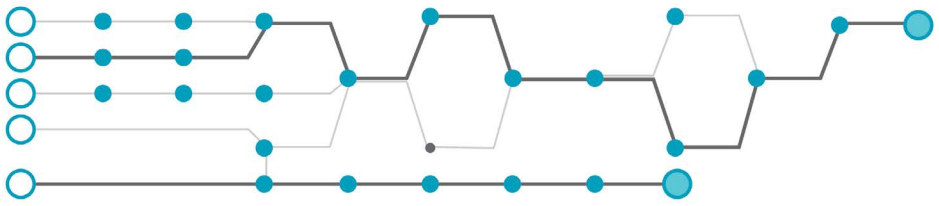
Every dimension of monitoring from AppNeta includes intelligence layered on with either active or passive techniques to ensure the most comprehensive visibility into real network conditions is delivered. Sound too good to be true? **Here's how it's done.**

Four Dimensions of network monitoring



Network Path | Network Packet | Web Applications | Network Flow

NETWORK PATHS



An application delivery path, or network path, is the logical route through layer 3 network devices to reach to a TCP/IP target (whether that's physical or virtual), regardless of device or media type.

A single network path can be as short as a laptop connected to a local file server over the office Ethernet or wireless LAN, or as long as a 35-hop, satellite-enabled WAN connection around the Globe – and everything in between.

Because IP networks are serial mechanisms—that is, made up of a series of consecutive links—only one "bit of data" can really be traveling the network at a given slice of time based on the network's clocking speed. As a result, all modern implementations of IP leverage multiple network queues that are designed to store and forward data frames as they are sent and received by the different clients communicating on the network.

At the highest level, the performance of a given network queue determines the ultimate performance of the network data that travels to, from or through that queue.

AppNeta allows the accurate and efficient reverse engineering of the performance of a given IP stack's queue by varying the data packet sizes, the distribution of sizes amongst a multi-series of packets, the quantity of the packets in a given series, and finally the precise space/timing between the packets (down to the microsecond).

The end result is that TruPath™, a patented core of AppNeta's network technology, is able to quickly exercise any given network path to its maximum possible level, doing so with an absolute minimum of data inserted into the path. Then, it dynamically learns how a given network path will perform from the application's perspective.

Using packet dispersion technology, TruPath can build up a complete set of network statistics very quickly—often in just tens of seconds—using special patterns that detect if instrumentation packets are interfering with each other. If that happens, it takes more varied samples over a longer time scale to ensure accurate data.

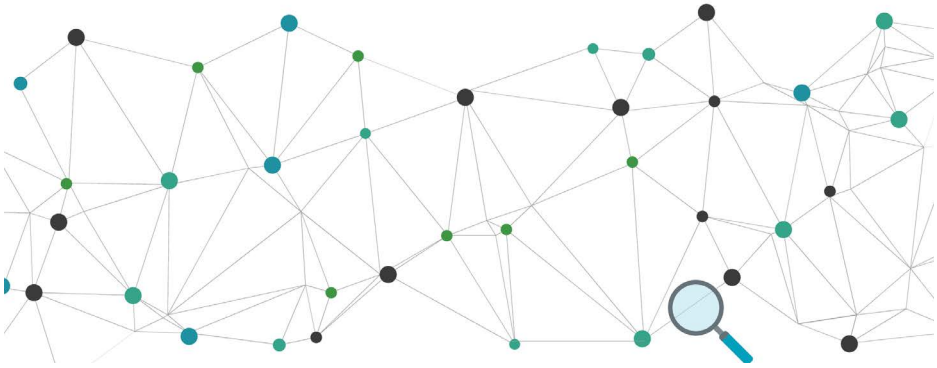
NETWORK PATHS *(CONTINUED)*

By sending multiple sets of precisely controlled packet sequences, TruPath can analyze a wide range of potential traffic conditions. By probing the path repeatedly with the packet sequences, TruPath collects a statistically significant set of responses for each type. It automatically detects rapidly changing conditions and adjusts measurement patterns accordingly.

TruPath was designed to not interfere with active networks by maintaining very low overhead. It actively probes the specified network path and generates one or more packet timing distributions for that path achieving similar accuracy to flooding the network without the impact. These groupings range from single packets to small bursts to short streams, sometimes in varying protocols.

NETWORK PATH SUMMARY An active approach to measuring the health and availability of the network end-to-end, shining a light on "where" network issues are impacting application delivery.

NETWORK PACKETS



AppNeta looks at packet-level data from two perspectives: both active and passive. The active methodology, TruPath, forms, sends, and analyzes packet responses over the network to monitor the delivery path of application data. The passive packet collection and subsequent Deep Packet Inspection (DPI) analysis reveals what apps are currently in use on the network.

TruPath's active approach is based on the monitoring principle of sending and receiving many varied short sequences of packets—called packet trains—that are transmitted using commonly available ICMP or UDP mechanisms to defined end hosts.

NETWORK PACKETS *(CONTINUED)*

We've conducted extensive comparison testing to prove that this approach delivers accuracy without adding a high instrumentation load on the network path — something that packet flooder technology leveraged by competing solutions has become notorious for.

The passive approach involves real-time, 100% packet analysis with an AppNeta monitoring point to identify and discover what apps are currently running on the network. This allows IT to understand the impact that each app is having on the overall end-user experience. AppNeta automatically categorizes and classifies traffic to show IT percentages of their network capacity used up by recreational apps or business-critical ones. AppNeta then lets IT drill down into granular data on the experience of specific office locations, apps, and users. At the lowest level, retransmit rates are displayed alongside the user experience contributions of network and application latency.

NETWORK PACKET SUMMARY The raw data that engineers may need to understand the root cause of issues on the network at a granular level.

WEB APPLICATIONS

Good end-user experience remains the primary "marching order" for enterprise IT, even as enterprise networks undergo significant changes. It's no longer enough to keep networks and applications up and running—now IT has to make sure users aren't dealing with continually slow or poorly performing apps, even (or especially) for apps that IT doesn't control, ie. SaaS or cloud-hosted apps.

Synthetic monitoring is a modern way to see the performance trends of today's SaaS and web applications and networks. It uses scripting to emulate the paths and actions that end users take as they experience an application and runs this test periodically to alert IT when performance degrades. These scripting strategies can take various forms, though, and vary widely in sophistication and complexity.

WEB APPLICATIONS *(CONTINUED)*

Synthetic monitoring is an important part of an overall monitoring strategy or tool as it actively "keeps tabs" on end-user experience, rather than passively investigating after an issue has occurred. Without synthetics, the only way to know an issue has occurred is for that issue to actually impact a user. Synthetics provide the intelligence without the impact. That's essential in the complex infrastructure that many IT teams are managing, where multiple networks, providers, and applications can all consume IT time and resources. Synthetic monitoring is a big help for troubleshooting in these cases, since it shows IT teams what users would experience in a consistent, continuous environment.

Synthetics can also be used to provide a global perspective on performance by monitoring from the outside-in. If you are a multinational corporation, for instance, or a company with offices in remote locations where you care about ensuring a good end-user experience (read: the CEO's home office), then you'll want to set up agents to monitor performance from specific end-user locations, behind their firewall, back to your SaaS apps or data center. The benefit here is that when that CEO calls to complain, you're not relying on a monitor that is at best 30 miles away and likely on a different carrier for the last mile. You'll have actual data from their location over the same ISPs and you'll see it trended over time so you can pinpoint when issues began.

WEB APPLICATIONS SUMMARY A baseline of app performance from the end-user perspective via synthetic scripting, delivered to central IT or networks ops teams without requiring real users to experience and report.

NETWORK FLOWS

In packet switching networks, flow is a sequence of packets from a source to a destination, which may be another host, a multicast group, or a broadcast domain. A flow could consist of all packets in a specific transport connection or a media stream. By analyzing flows, AppNeta can isolate specific conversations between source and destination. Combining flow data with packet data allows AppNeta to identify thousands of applications in use on the network and pinpoint that network usage to specific hosts–and users–on the network.

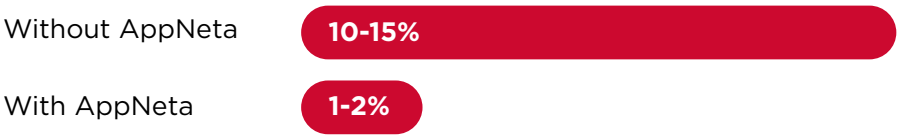
The flow data we deliver is enriched with automatic application discovery and identification to give teams an understanding of the tools that are using the most network capacity. The routers and switches that generate flows don't normally enrich this data on their own application identification without extra licenses options; and even when they do, it's at a material impact to the core performance of this hardware. This leads to the typical 10-15 bytes of flow data for every 100 bytes of raw network data transmitted, which can increase network overhead by 10-15 percent. With AppNeta, that overhead is only 1-2 percent because we compress flow data for the express purpose of saving space over the wire.

NETWORK FLOWS *(CONTINUED)*

On their own, routers do not have enough horsepower to encrypt large amounts of flow data either, which increases a networks security attack surface area, nor do most third-party flow collectors know what do with an encrypted flow. AppNeta tackles both sides of this conversation so that very sensitive data in our flow records is kept private and secure while on the wire.

At the end of the day, delivering four dimensions of network performance data is so much more than a “nice-to-have.” The new reality of the modern enterprise network requires that IT teams have as much data handy to stay ahead of the many potential pitfalls that are so common during digital transformation.

Network Overhead



NETWORK FLOWS SUMMARY A high-level, passive view of all network traffic — users, applications, remote offices — and the impact of performance across the network generally.

To see AppNeta in action, schedule a demo today.

BROADCOM SOFTWARE

About Us

Broadcom Software is one of the world’s leading enterprise software companies, modernizing, optimizing, and protecting the world’s most complex hybrid environments. With its engineering-centered culture, Broadcom Software is building a comprehensive portfolio of industry-leading infrastructure and security software, including AIOps, Cybersecurity, Value Stream Management, DevOps, Mainframe, and Payment Security. Our software portfolio enables innovation, agility, and security for the largest global companies in the world.

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