How AppNeta Monitors the Network

Our TruPath technology powers AppNeta’s modern monitoring.

In the days before cloud computing, a business ran its applications from a physical data center, with a long-established network infrastructure backbone. Now, a majority of companies are moving some or all of their applications to public and private cloud environments.

All this cloud movement means that businesses don’t need infrastructure hardware the way they used to. There are a lot fewer servers, disk arrays and switches than there used to be. All these changes make for a more flexible company, but they’ve also removed the on-site technology that was easy to see and understand. The visibility that went along with that is gone. But when the applications running your business are all off-premises, the network suddenly becomes a lot more important. It’s your company’s lifeline to its infrastructure, apps and employees.

Today, good application performance requires good network performance. The tools traditionally used to monitor systems and networks are almost all device-based. In the new cloud world, IT does not own the devices, and, thus, cannot gain access to the data from them. Devices in today’s distributed modern world include servers, workstations, IP phones, video conference systems, routers, switches, firewalls, load balancers and wireless access points—among others. To monitor apps today, users need to view the application delivery path, which is the logical route through a network device to reach a TCP/IP target, whether physical or virtual. This is increasingly difficult when a single network path could be a laptop connected to a local file server or a multi-hop, satellite-enabled global connection.

AppNeta developed TruPath to provide the visibility that’s disappeared from modern networks. Cloud networks are complex, but understanding their performance doesn’t have to be. TruPath takes into account the complexities of network queuing to monitor any type of path. TruPath varies the packet sizes, the distribution of sizes among a multi-series of packets, the quantity of the packets in a given series and finally the precise space and timing between the packets (down to the microsecond level). This is a reverse engineering of the performance of a given IP stack’s queue. So TruPath is able to quickly exercise any given network path to its maximum possible level with the barest minimum of data inserted into the path. It dynamically learns how a given network path will perform from the application’s perspective.

The Essential Benefits of TruPath

- **Complete visibility.** Unique methodology gives you the application’s view of any network.
- **No device dependency.** See performance across all network hops.
- **Low overhead.** TruPath can be used in production environments without slowing down applications.
- **Scalability.** With low network loads and a SaaS model, TruPath can scale to support any size network without extra hardware or retooling.
- **Flexibility.** Single- or dual-ended deployment is available to measure asymmetric performance.
- **Ubiquity.** TruPath is broadly available on most IP devices.
- **Real-time.** TruPath detects and reports results within minutes.
The Technologies That Power TruPath

1. Packet Train Technology Done Right

TruPath 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, or targets. (A target is any IP stack that can respond to an ICMP-based ping or can send back a TCP or UDP packet.)

Using packet train 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 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.

This approach delivers high accuracy without requiring an intrusively high instrumentation load on the network path, unlike packet flooder technology.

2. Continuous Path Analysis and Deep Path Analysis Instrumentation Work Together

TruPath uses both continuous path analysis (CPA) and deep path analysis (DPA) instrumentation to measure network performance. CPA is designed to monitor a very large quantity of paths with as low amount of overhead as possible 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. DPA can instrument a path to a higher resolution and associated accuracy and also provide the additional leading indicators needed to feed into APEX (more on that later) for diagnostics and trouble-
shooting.

These techniques help AppNeta to have a very low impact on the network it's measuring. TruPath only needs about 2 Mbps per 1,000 unique targets during continuous monitoring. For very slow speed links or networks with other restrictions, TruPath automatically adjusts its timing, size and distribution curves during its optimization startup phase.

When critical indicators vary from an expected or accepted value, CPA automatically responds by increasing statistical resolution. This escalated mode (also called CPA2) prevents TruPath from auto-escalating too quickly into the more accurate (and slightly more intrusive) DPA mode unless a network path dysfunction is truly present.

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

3. ICMP Supports TruPath's Flexibility

Each of TruPath's network path or group of paths can be instrumented in single-ended or dual-ended configuration, 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. It relies upon the Internet Control Message Protocol (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 live at one end of 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 (whose performance can be measured using alternative methods also available from AppNeta).

Dual-ended mode requires placing TruPath software at both ends of a path. TruPath measures the asymmetric path performance 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. And measuring some key path metrics, especially bandwidth, at the TCP level often leads to erroneous results affected by TCP window size and overall path latency and round-trip time. All three protocols can also be used for route determination which can illuminate network sections where routing differs for data sent via each protocol.

The critical requirement for TruPath analytics is to extract packet timings from the end-to-end network—so almost any packet will do.

4. TruPath Measures With 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, designed for network paths that operate at 512 Kbps or higher. If they're 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 the network will be seen by an application.

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 can be affected only 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 and permits the accuracy of the analysis to remain very high even in difficult, fast-changing conditions.

5. APEX Is TruPath’s Analytics Engine

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. So that means that the network is operating outside of design specification.

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 packet trains differently and thus creates a unique “signature” that distinguishes the type of degradation. TruPath’s patented analytics engine, the Application Path Expert system (APEX), performs a form of pattern recognition on the packet timings, loss, and other network errors to assess the type of degradation. APEX uses probabilistic analysis to indicate what problem the current behavior looks most like. APEX contains approximately 88 unique signatures and observations. AppNeta routinely works with customers to identify the cause of any unresolved diagnostics and adds this information to APEX.

![Diagram](image)

*TruPath does diagnostic analysis to figure out network dysfunction*
TruPath describes symptoms of the found network issues

APEX produces the various flags and statements that appear in AppNeta Performance Manager. It also produces the certainty measures that reflect how closely a particular signature has been matched for a built-in confidence scoring mechanism for the end user.

With all these capabilities working together, AppNeta's TruPath sees what's important inside modern networks and applications.