WHITEPAPER

How AppNeta's Technology Works

A majority of companies are moving some or all of their applications to public and private cloud environments. When the applications running your business are all off-premises, the external network your traffic is routed through suddenly becomes a lot more important. It's your company's lifeline to its infrastructure, applications and employees.

The Technologies That Power TruPath

AppNeta developed our patented TruPath technology to provide the visibility that's unavailable from modern enterprise networks. TruPath takes into account the complexities of network routing and queuing to monitor any type of path. Here's how it works, and how it can improve your and your users' daily work.

1. Packet Train Technology for Better Monitoring Data

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. Extensive comparison testing has proven that this delivers accuracy without adding high instrumentation load on the network path like packet flooder technology does. Using packet train technology, TruPath can build up a complete set of network statistics very quickly—often in just tens of seconds. TruPath uses 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.

By sending multiple sets of distinct 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.

2. Continuous Path, Deep Path Analysis for Immediate Troubleshooting

TruPath uses both continuous path analysis (CPA) and deep path analysis (DPA) instrumentation to measure network performance. CPA monitors a very large quantity of paths with as low an amount of overhead as possible (on average just 2 kbps) to see overall path quality and performance. 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 troubleshooting. When critical indicators vary from an expected or accepted value, CPA automatically increases statistical resolution. This escalated mode (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 means TruPath focuses on the few paths that deviate from performance norms. It will start troubleshooting before you do.

3. ICMP and UDP for Flexibility

TruPath's network paths can be instrumented in single-ended or dual-ended fashion, or both together. This flexibility allows you to test various use cases with one tool. The default single-ended mode (shown below) monitors performance into SaaS provider networks. TruPath technology (in the form of a sequencer) only has to be present at one end of the path to measure round-trip performance.

TruPath relies upon the Internet Control Message Protocol (ICMP) combined with ICMP Echo Mode 8, which is in every modern TCP/IP stack. ICMP and UDP are used because they are both prevalent in IP-enabled devices.

ICMP is predictable and accurate in soliciting responses from any IP-based network host. TruPath determines what the base IP network (or the layer 3 network) can actually deliver without the overhead of layer 4 protocols. With dual-ended mode, TruPath measures the asymmetric path performance to understand the differences. More paths are measured using UDP packets in order to measure upstream and downstream performance separately.

4. Lightweight Monitoring for Less Network Interference

TruPath is a low-overhead monitoring technology, designed to not interfere with active networks. 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.

TruPath continuous monitoring uses on average just 2 Kbps and diagnostics use only 10 to 200 Kbps. TruPath captures packet sequence timings, including loss and various forms of network error, to get critical performance data. Those numbers reflect the response of the end-to-end path to show how an app sees the network.

TruPath's 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. TruPath adjusts accordingly for more statistically accurate results.

TruPath's self-feedback loop permits the accuracy of the analysis to remain very high even in difficult, fast-changing conditions.

5. APEX Analytics for Better Root Cause Identification

TruPath analyzes network paths through two network models: functional and dysfunctional. Functional means the path is performing according to normal network design—in that case, the measurements made represent its capacities and usage.

Dysfunctional refers to 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 performs diagnostic analyses against models of network dysfunction. Each type of degradation affects the packet trains differently and thus creates a unique signature. 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 matches the current behavior with known problems using probabilistic analysis. APEX contains approximately 88 unique signatures and observations. AppNeta routinely adds to APEX using customer diagnostics data.

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.

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