

Rescuing routers by eavesdropping

By: Mark Els

Network World Canada (13 Oct 2006)

Network administrators looking for more precise insight into the behaviour of their routers can dig deeper by tapping a relatively new technology called route analytics.

While traditional monitoring tools capture the flow of traffic across the network, helping to ensure devices are up and running, route analytics targets the routing protocols and provides real-time awareness of the router path of IP traffic. The technology is providing tools to discover the exact points of failure in a network by monitoring routing protocols like OSPF (Open Shortest Path First) and then accurately identifying which routers are showing abnormal behaviour. “[Route analytics] looks inside the routing protocol database and gives you a picture of how your routing protocol is behaving,” explains Krzysztof Adamski, network architect for Advanced Knowledge Networks Inc. (AKN), a mid-sized service provider of Internet connectivity and private networks in Toronto.

Adamski uses Nagios open-source software for network monitoring and supplements that with route analytics from a SmartHawk appliance manufactured by Ottawa-based Solana Networks Inc.

He says the tools provided by route analytics allow him to keep tabs on changes in the routing tables of about 50 routers deployed throughout AKN’s core network. “This way, you can see if a router is sending too many updates.” If a router has to reroute traffic to a failover link, for example, that router creates an update of the network topology, which is then flooded to all the other routers so they’ll know where to send the traffic for that route, says Adamski.

Route analytics watches that behaviour to determine when any router is generating too many updates. Every time there’s an update, the routers have to recompute their internal view of the network, which impacts their CPU usage. “When a router malfunctions and starts sending out thousands of updates per second, that can have a severe impact on the stability of your network,” says Adamski.

“Without really having that view into the OSPF database, you have to go from router to router and look at each database to try to find the -inconsistencies.”

The Nagios software could pick up that there was a problem, but couldn’t tell exactly which router was causing the problem, he says. “It doesn’t actually delve into the routing protocols.”

Adamski says SmartHawk’s route analytics identified one router that was generating way too many LSA (link state announcement) updates, and this barrage of changes to the routing tables was driving up CPU usage on all the routers in the network. “Ended up the router had dead memory,” says the architect.



According to systems management analyst Dennis Drogseth, route analytics is still rare in the market. Despite having been around for three years already, only a handful of vendors have twigged on to the technology's benefits.

"And it's actually a mainstream requirement. If you want actual real-time awareness of where a problem is occurring, route analytics is the best place to start," says Drogseth, vice-president at Boulder, Col.-based research firm Enterprise Management Associates Inc.

Since routing paths are changing dynamically based on best route, it's accurate to that specific best route, he says. "The value of that is, when a problem does occur, you know the exact routed path. No other technology can do that." One of the added benefits of route analytics is that unlike other monitoring tools, it doesn't actually add to network traffic. Instead of polling devices with Simple Network Management Protocol (SNMP) commands, route analytics listens to the Layer 3 routing protocols.

"Rather than dispatching riders to various junctions, it's a non-intrusive technology that acts more like a traffic camera to provide snapshots of the network topology," says Glegs Jones, vice-president of business development at Solana Networks.

"The control plane determines how data is shifted around the network, and because the [route analytics] appliance becomes part of that, we know exactly what's going on with the routing health of the network. The device can see any misconfigurations in the network or any congestion issues."

Solana Networks — which last month added BGP (Border Gateway Protocol) support to its OSPF and IS-IS (Inter-mediate System to Inter-mediate System) capabilities — competes with Network Physics, Bluewave Networks, Packet Design and Vancouver-based Apparent Networks.

Hewlett-Packard Co. has also been offering route analytics as part of its OpenView management suite since June 2004, having signed an OEM agreement with Packet Design to use its RouteExplorer software. But the market has yet to fully appreciate route analytics, says Drogseth, adding there have been challenges in terms of awareness of how to use it. "Route analytics is still viewed as a feature of network monitoring," he says, "but this is a major, not a minor, technology."

<http://www.itworldcanada.com//Pages/Docbase/ViewArticle.aspx?ID=idgml-3c0db2e8-ce9c-436f-8bde-c399630047bb>