



Packet Design

Case Study

UC-BERKELEY GETS 'ROUTER'S-EYE VIEW' INTO CAMPUS NETWORK WITH NEW LAYER 3 ROUTE ANALYTICS APPLIANCE

Packet Design's Route Explorer Helps University Detect DNS Server Problems, Locate Unused Bandwidth Assets, Improve Redundancy Design, Minimize Downtime

Hoping to cover as much of the exhibit floor as possible at the CENIC (Corporation for Education Network Initiatives in California) show in May 2002, Cliff Frost and Ken Lindahl split up to scout out new technologies and products. When they met up a couple of hours later, Frost, director of communications and network services for the University of California at Berkeley, and Lindahl, his chief network architect, agreed they had each, independently, seen something impressive: a new tool that, for the first time, could show them not just the physical but the logical infrastructure of an IP network. All routing events would be visible, in real time and historically. This had the potential to deliver a wealth of information indispensable for the operation of a mission-critical IP network, from early detection of routing anomalies to detailed network "forensics" that permit rapid diagnosis and correction of problems.

The UC-Berkeley campus network has some 46,000 end-nodes and 85 routers, with several thousand-fiber connections to off-campus buildings. The network is subdivided into eight OSPF (Open Shortest Path First protocol) areas.

With such a heavily routed IP network, Frost and Lindahl could see immediately the potential usefulness of Route Explorer, the first of a new generation of route analytics appliances made by Packet Design, Inc., of Palo Alto, Calif.

Routing Behavior Knowledge: The Missing Link

"We've always had an array of network tools that could tell us about the status of specific hosts or network devices," Frost said. "But a major missing link was the ability to get direct knowledge of the complex routing events that can lead to serious network operations problems. Here was a product that would let us look at the behavior of routing in our network – both in real time and in the past – and become much more effective at troubleshooting and planning."

Route Explorer, introduced by Packet Design in May 2002, lets network operators look into the IP network "cloud" to gather, display and analyze routing-path information. This enables them to detect and resolve IP layer (layer 3) problems far faster than they could by using conventional methods of analysis, which involved querying each router on an individual basis. Route Explorer works by "listening" to the routing protocols, building an accurate topology map that is updated in real time, revealing all routing changes in the network as they happen. In addition, Route Explorer records all routing events in a local database, which makes them available for later review of routing history, analysis and reports – powerful tools for problem detection and diagnosis.

A single Route Explorer unit supports the largest routed networks, and is incorporated into the network infrastructure as if it were simply another router, though it forwards no traffic and is neither a bottleneck nor a failure point. More important, Route Explorer does not rely on device polling to gather its routing information, and thus places no load on the network.

Frost in particular appreciated the Route Explorer approach "because years ago I'd written software to do the same thing, monitor changes in protocols and reachability, for a much simpler routing protocol, RIP."

Providing Information on Network's End-to-End Flows

Frost's staff has been using Hewlett-Packard's OpenView management platform and other layer 2 (physical layer) tools on their network for years. "The OpenView monitoring station would tell us we couldn't reach a device we were monitoring," he said, "but we wouldn't know why, because we had no information about end-to-end flows. Did the routing tables get corrupted? Did a router interface fail? We just didn't know."

Route Explorer was first installed at UC-Berkeley in June 2002. Within minutes, the appliance began listening to OSPF protocol exchanges and quickly built an accurate map of what the routers themselves were "seeing." Once they had this map, Frost and his routing engineers immediately discovered something they hadn't known before: a T1 line that should have been taken down months before was, through an administrative oversight, still active. This was not only costly – they were being billed for a line that wasn't being used – but, as a backup for a Gigabit Ethernet link, it was useless for failover.

Pinpointing 'Flapping' Routes, Other Intermittent Problems

Beyond problems that showed up immediately, Route Explorer was able to spot some longer-term issues. During the early months of monitoring, Route Explorer found a "flapping" route (a route that goes down and comes back up many times in rapid succession), which had gone undetected by existing logs and tools over a 10-day period. The cause was a newly installed DNS (Domain Name Server) server's network interface that was continually resetting; this disrupted the route intermittently, but not for long enough periods to be detected by SNMP polling. Another, redundant DNS server was helping to mask the problem.

"All our DNS servers have the same IP address," Frost said. "If power goes out in one, the rest of the campus still gets service. Route Explorer confirmed our diagnosis that the problem was a failure of a single machine and not the whole setup."

Planning Future Network Changes Without Experimenting on the Network

Frost said his group has also used Route Explorer for network planning, to test potential routing changes by first simulating them in its topology database. Though off-line planning tools have existed for some time, they often lack accurate knowledge of the working network, so users have had to try out changes on their actual network during off hours.

"Route Explorer has helped us to optimize route metrics before we actually implemented the changes to the routes, avoiding many potential problems," Frost said. "We now have the ability to simulate a downed interface, for example, to verify that sufficient redundancy is built into the network."

Packet Design, Inc.
3400 Hillview Avenue, Bldg. 3
Palo Alto, CA 94304
www.packetdesign.com