

Network Management Time Travel

*Rewinding and Replaying Your
Network for Superior Troubleshooting*



Packet Design

Executive Summary

Enterprise IT and service providers who run large, complex IP networks are under pressure to deliver increased application and service performance across their network infrastructures. Yet engineers know full well that simply locating the part of the network that handled the problem traffic is very difficult, often impossible. Without such basic visibility, troubleshooting the network's part in application and service problems is no more than educated guesswork. More times than not, engineers are reduced to asking end customers to "call back when the problem occurs again", because they have no forensics to understand the network's behavior at the time – an hour, day, or week ago – when the problem occurred.

Today that educated guesswork can be considered a thing of the past. Route analytics technology combined with a small footprint of collected Netflow data can provide application and service traffic visibility not only to every link in the network, but to the network-wide context of each link's traffic, giving network managers a better handle on network issues. Furthermore, route analytics technology has the unique ability to let network managers "rewind" a network-wide recorded model of actual routing and traffic so that engineers can troubleshoot problems as if they were seeing them in real time.

How Engineers Troubleshoot Complex Network Problems Today

Even highly trained network engineers are ill equipped today to troubleshoot large, complex IP networks because they lack both fundamental visibility into network behavior and proper forensic history. As a result, their skills are often wasted on inefficient troubleshooting processes, or worse, sidelined due to a lack of actionable intelligence on the network. Much of network troubleshooting today is a combination of educated guesswork and time-consuming manual data-gathering and correlation.

In a recent survey conducted by analyst firm Kurbernan Inc., two hundred IT professionals were asked how they typically resolve routing and other logical network issues that lead to application degradation and application outages. Of the respondents who were able to give an answer, over 54% responded that they either do a lot of tedious work, typically logging in via CLI to device after device and digging deep into each device's status and statistics; or that they just wait for the problem to happen again and try to capture information in real-time when it does. The irony is that while IT is tasked to automate end-user business processes, network management itself is often highly un-automated, relying on brute-force methodologies. As a result, many application and service problems go unsolved, or are caught in an endless cycle of finger-pointing between application and networking groups, with insufficient information to resolve them. This is clearly unacceptable, not least because it won't address the demands being placed on IT and service provider engineering and operations teams for stricter service-level agreements (SLAs).



Route Analytics—A Game-Changing Technology for Troubleshooting Large, Complex Networks

Route analytics technology, adopted by hundreds of large enterprises, government agencies and service providers, is changing network managers' fundamental assumptions about the level of visibility they can have into network-wide traffic delivery. Route analytics is built on the foundation of a different type of network visibility, afforded by tapping into the routing protocols – the source of intelligence that determines how IP networks deliver traffic.

Route analytics is the technique of acting like a router and peering with select routers across a network, using routing protocols—OSPF, IS-IS, EIGRP and BGP—to record the control messages that routers use to calculate how traffic will be sent across the network. By taking this information and processing it just the way routers do – albeit in a more comprehensive fashion – route analytics knows every Layer 3 routed path in the network, from every host to every other host, and thus can create an analyzable routing topology of the entire network that exactly reflects the way the real network is operating.

Engineers find this sort of routing topology information very useful on its own for troubleshooting and network planning. But its implications for network-wide application and service traffic analysis extend far beyond these tasks, because of the way the vast majority of traffic is disseminated across the network: from a relatively few major ingress points in major data centers, Internet and network and customer peering points - a tiny fraction of the networks' total number of interfaces. By collecting Netflow data from these points and then using knowledge of the precise route that every flow takes at any time through the network, route analytics can create a highly accurate, integrated routing and traffic map that shows the volume of class-of-service (CoS) traffic on every link in the network.

Furthermore, since route analytics understands how every flow gets to every link, it provides the network-wide context for every interface's traffic. For the first time, network engineers can see the big picture – the network as a holistic, dynamic organism – and immediately grasp the impact of routing changes or failures on traffic (even traffic located many hops away from where a change has occurred).

Rewinding the Network with Route Analytics

A major problem in troubleshooting application or service delivery issues is that, when the network is suspect, there is often no history to examine to prove or disprove that suspicion or to localize the problem domain within the network. The limited concept of "history" embodied in most network management tools is the ability to display a tabular view of statistics from a device or interface from a given time range. However, the highly localized nature of this sort of information not only leaves engineers without the big picture, but also forces them to replicate on the network management console what they would otherwise do via CLI: manually dig deep into device after device and correlate suspected symptoms.



Since they don't even know which path the traffic took through network when the problem was occurring, this is a time-consuming and often inaccurate way to troubleshoot a problem.

Route analytics changes the game in favor of network engineers through its fundamentally different approach to understanding networks. While other network management approaches simply collect information on many individual device and interfaces, route analytics utilizes a network model that is network-wide—based on the topology of all the routed links and paths from edge through core to edge again. Routing and traffic are continuously recorded into this model so that it is always up to date and has a complete forensic history of all routing and traffic changes over time. As a result, instead of just looking at one table at a time, network engineers can literally “rewind” the network to look at, and even replay, past event streams (see Figure 1).

This high-fidelity forensic history greatly decreases mean time to repair (MTTR). Engineers can move the route analytics network model to a past point in time when an application or service delivery problem was occurring. Every aspect of the network they look at will be synchronized to the recorded details from that time, providing a holistic context for troubleshooting.

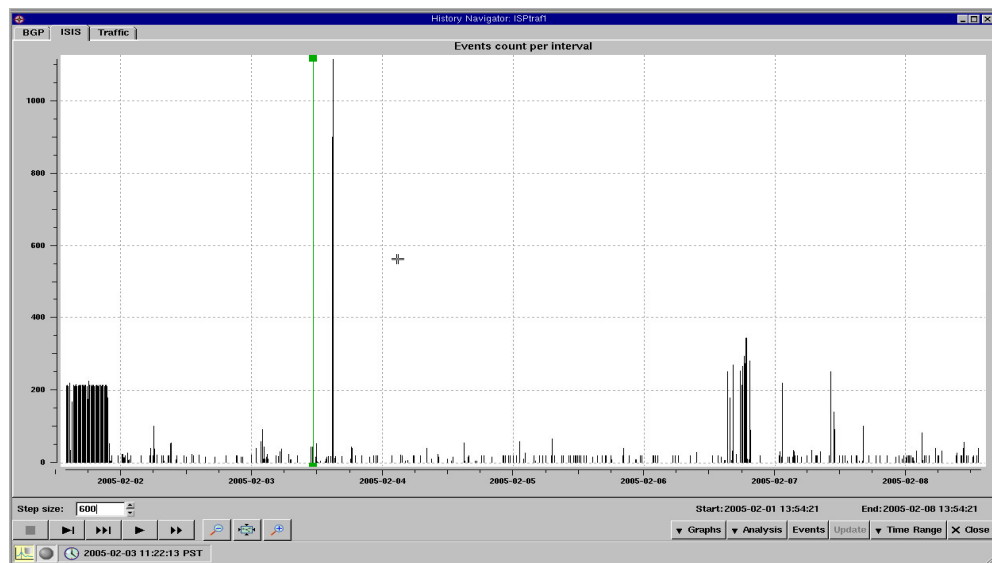


Figure 1: Route analytics' continuously recorded database of all routing and traffic changes can be rewound to look at a particular time when a problem was occurring, providing an unprecedented forensic and troubleshooting history for network engineers.

Once an engineer has selected a timeframe in route analytics, he can see historically accurate information about network behavior. For example, the precise routed path of the application or service traffic in question can be examined for routing instabilities such as

link flapping (where a link is going up or down repeatedly and rapidly) or prefix flapping (where a routed network address is being rapidly advertised and withdrawn over and over by a router) and for out-of-profile CoS traffic conditions, as seen in Figure 2.

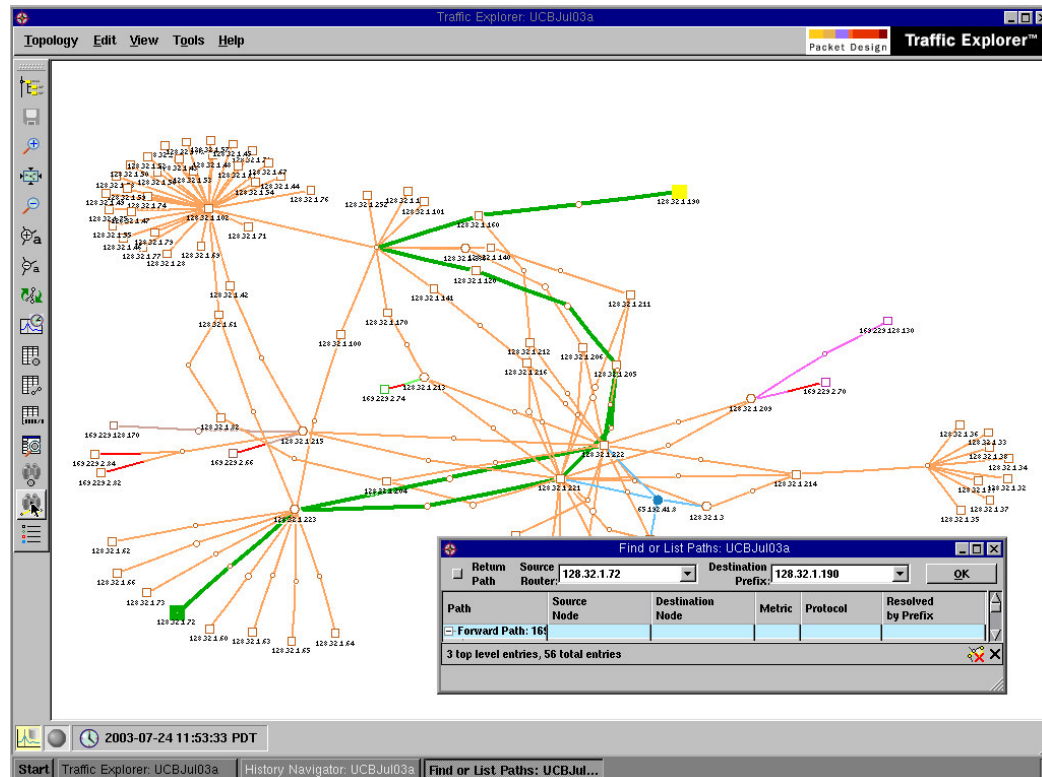


Figure 2: Engineers can select any two endpoint IP addresses and highlight the exact route taken by the application traffic in question at the time a problem was occurring to narrow down the part of the network that needs to be analyzed.

Route analytics provides a wealth of analysis capabilities to help engineers achieve maximum troubleshooting efficiency. Once the path through the network that delivered the application or service traffic is localized, engineers can examine the links in the path to see if there was any aggregate congestion, or congestion for a relevant CoS. If so, the flows traversing the link can then be examined to see if any are out of normal bounds. The path of the flows on the link can also be viewed and any changes in these paths examined to understand if a routing issue caused a flow to change its path and cause temporary congestion on that link, thus affecting the application or service in question. Any changes in the route that supported the application/service's traffic can also be viewed and even replayed, to pinpoint any anomalous routing instabilities affecting the path, since, even without congestion, a routing instability could cause higher latency, jitter or packet loss that

would affect end-to-end performance. Other tools provided by route analytics to aid engineers include:

- Comparisons of routing behavior between two points in time
- Comprehensive routing health audits to find hidden routing issues
- Visibility and drill-downs for traffic on all links in the network by CoS, applications, services, and flows across their entire routed path
- Views of routing changes ranked by their impact on traffic

The Link Between Application Delivery and the Network Infrastructure

Route analytics fills a critical gap in the network management portfolios of organizations with large, complex IP networks. In particular, route analytics provides network-wide visibility into routing and traffic behavior and a holistic, historical context for localizing and analyzing network issues that affect application and service delivery. Complementing other network management solutions, such as application performance management and SNMP device management and fault correlation systems, route analytics provides the Layer 3 network delivery link between end-to-end application performance and the underlying network infrastructure elements.

For more information on route analytics technology and solutions, please:

- Email us at info@packetdesign.com
- Visit Packet Design's web site at <http://www.packetdesign.com>
- Call us at 650.739.1850



Packet Design

Corporate Headquarters

Packet Design Inc.
3400 Hillview Avenue, Building 3
Palo Alto, CA 94304
Phone: 650.739.1850
Fax: 650.739.0590
<http://www.packetdesign.com>