

Enhancing Network Monitoring with Route Analytics



Packet Design

Executive Summary

IP networks are critical infrastructure, transporting application and service traffic that powers productivity and customer revenue. Yet most network operations departments have no way to monitor the IP-layer operation to ensure that the network is able to deliver traffic stably and predictably. The reason is that network monitoring has historically been based on SNMP polling of device and interface status and statistics. While certainly useful, information from individual devices and interfaces can't convey the complex inter-working status of the devices as a whole network. As a result, operations managers are lacking critical monitoring data, particularly in complex IP network topologies that possess high levels of redundancy, and when MPLS VPNs are a major component of the WAN.

Enter route analytics, the network management technology that monitors the network's live routing protocol control plane and uses network-wide routing intelligence to turn sparse amounts of Netflow into network-wide traffic flow visibility. By implementing route analytics, network operations managers responsible for large, complex IP networks can increase the speed and efficiency of network monitoring and reduce operations costs while increasing customer satisfaction.

This white paper reviews the causes and costs of insufficient network monitoring, explains how route analytics works and how it can be used to enhance network monitoring and troubleshooting by adding real-time visibility into routing operations as well as network-wide traffic flows, leading to operations, engineering and business costs savings.

The Cause and Cost of Insufficient Network Monitoring

IP's distributed routing intelligence makes it efficient and at the same time unpredictable. IP routing protocols automatically calculate traffic routes or paths from any point to any other point in the network based on the latest known state of network elements and network routing configuration. Any changes to those elements cause the routing topology to be recalculated dynamically. While this means highly reliable traffic delivery with low administrative overhead, it also creates endless variability in the active routing topology. Not only can a large network be in any one of millions of possible active routing topology states, but application traffic patterns are by nature unpredictable. Network problems – router software bugs, misconfigurations, hardware that fails (often after exhibiting intermittent instability) – can add to that unpredictability.

Unfortunately, traditional SNMP network monitoring tools that operations departments rely on to detect and troubleshoot network problems simply can't perceive the dynamic changes in routing and traffic because they monitor the network on the basis of device and interface status. In a simple network where there is no redundant WAN links, MPLS VPNs or other complex topology, device status does effectively correlate to network status because there is no variation in the way that traffic can possibly transit the network. However, in a redundant or complex network topology, traffic can transit different routers based on the state of Layer 3 routing, which chooses which paths and links traffic uses to get from any point A to any point B. The result from a SNMP monitoring and operations point of view is that when a problem is occurring, it can be very difficult to figure out where exactly in the network to look—which links should be examined to see if they have problems? Furthermore, what if the problem has nothing to do with an interface or device having a hardware problem—what if the routing control plane itself is having a problem such as unstable route advertisement that flaps up and down, causing intermittent reachability

Enhancing Network Monitoring

issues over time? SNMP solutions simply have no visibility into those “software” problems in the network.

The visibility problem gets even worse when the problem is no longer currently occurring, and is handed off to network engineering. Highly trained, expensive network engineers are reduced to playing a glorified guessing game since they have no forensic audit trail of network routing and traffic conditions at the time the problem occurred. One network engineer at a large regional North America bank called this phenomenon “footprints in the sand”—by the time a problem is being looked at by knowledgeable engineers, all evidence has been washed away by the figurative waves of changing network conditions.

All of this fumbling around in the dark and guessing is expensive to network operations and engineering. The time drain itself costs a lot of productivity within the IT department—this isn’t trivial since personnel costs are typically one of, if not the biggest piece of the network operations and engineering budget. More importantly, unsolved problems or delayed resolutions cost end-users the productivity that applications and services are supposed to be delivering. The costs of application downtime are well understood for large organizations—ranging from tens of thousands to millions of dollars per hour, depending on the industry.

Route Analytics—Cost Savings through Greater Visibility

Network management’s purpose is to overcome the complexity inherent in a large network and automate the work of network operations and engineering personnel so that applications can be delivered with high reliability. While traditional network monitoring approaches aren’t sufficient, organizations grappling with the challenges of managing complex network topologies have an answer in route analytics technology.

Route analytics technology works by utilizing the network’s live routing protocols as a new source of network management information and intelligence, complementing traditional SNMP data. A route analytics device – a network appliance running specialized software – acts like a router, listening to routing protocol updates sent by all routers in the network, and computing the network-wide routing state in real-time, just as all the “real” routers do. While the route analytics device itself is passive, never advertising itself as a place to send traffic, it provides real-time visibility, always up-to-date routing-state knowledge, and a completely accurate historical record of all past routing changes. It knows every route or “path” that any traffic takes at any point in time – hence the name “path-based” network management. The network-wide routing topology understanding and the full detail of routing changes provides the basis for many useful analyses of the routing control plane. When combined with Netflow traffic-flow data, the full power of route analytics information emerges. By collecting traffic flows from the ingress points of traffic at the network edge (data centers, Internet peerings, and major WAN links), then mapping them to the precise routes they traverse through the network produces an integrated, always accurate map of all routing and traffic for the entire network core.

Integrated routing and Netflow monitoring enables far more efficient network operations processes, leading to better application delivery. Route analytics can monitor a variety of important network conditions that aren’t visible to any other network management technology, such as:

- Internal IP subnets, for which network reachability is managed by routing protocols such as OSPF, EIGRP, IS-IS: Route analytics can monitor the availability and stability of important individual subnets, such as those hosting server farms in data centers.

Enhancing Network Monitoring

- External Internet networks, managed by the BGP protocol: Route analytics can monitor the availability of subnets on the Internet. For those organizations that maintain multiple Internet peerings to ensure availability of Internet traffic, route analytics can also monitor the level of redundancy of paths to critical Internet networks and servers.
- MPLS VPN-reachable subnets, managed by the BGP protocol: MPLS VPNs typically rob network managers and operators of important visibility, since the routing across the WAN backbone is outsourced to the VPN service provider. Route analytics restores routing and traffic visibility when MPLS VPNs are implemented, monitoring whether all sites can reach each other's networks, traffic levels between sites, and anomalous changes in routing reachability that can occur due to internal or SP errors.
- Layer 3 paths—the specific set of links that traffic must traverse from any point A to any point B in a network. Route analytics can monitor network paths for applications that are sensitive to changes in network latency, or for cases where network paths must stay stable to ensure proper security or other network policies
- “Software”-related link state changes, such as link flapping caused by misconfigurations of routing protocols, network design errors, or router bugs, which can lead to a loss of network or application availability
- Traffic utilization on all links in the network, broken out by CoS or application, without needing to turn on overhead-inducing Netflow export on all the interfaces in the network

Route analytics makes it much easier for network operations to not only detect problematic conditions in the network, but to troubleshoot those problems in real time. For example, when troubleshooting a current application or service outage, operators can examine three key potential causes of the outage: router changes, interface changes, and route changes by using the following steps:

- a. Examine route analytics' real-time topology map to look for any down routers or adjacencies
- b. Examine the network path for the source and destination addresses of the application or service traffic to confirm if the path is functional (figure 1).

Enhancing Network Monitoring

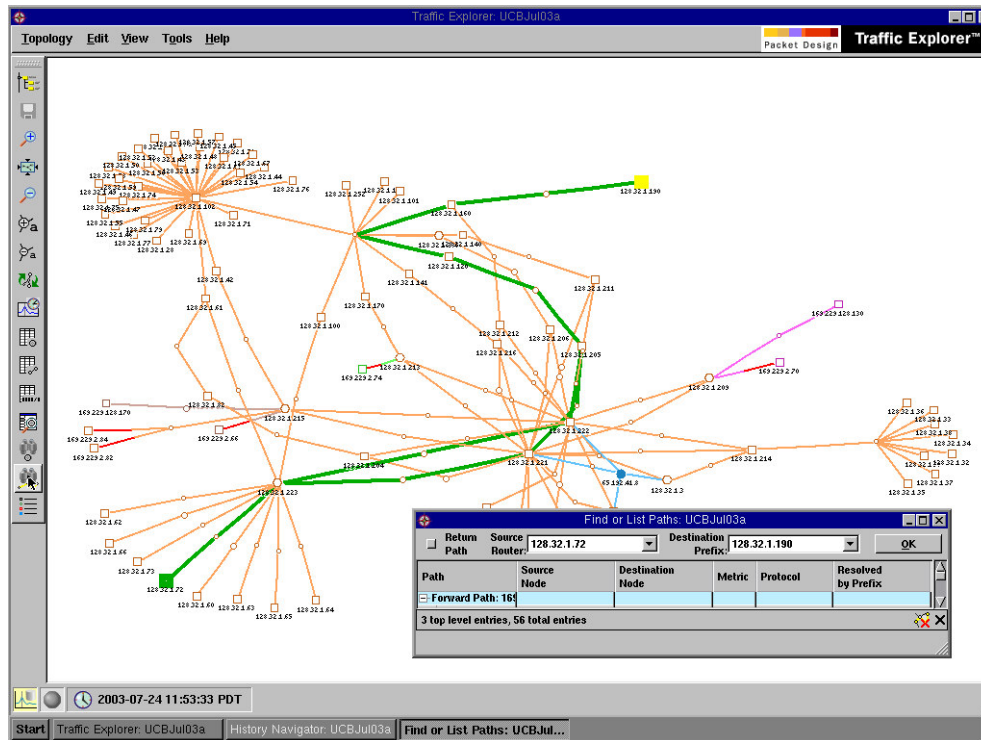


Figure 1: Route analytics allows easy identification and verification of the status of the application or service path through the routed network

- c. Examine the immediately preceding history to the problem for any other possible root causes. Operators can look at routing events, select a time-range leading up to the current time, (figure 2), then examine a list of routing events (figure 3) to see if there were any significant network changes or outages. In figure 3 for example, there are some flapping prefixes—evidenced by the rapid adding and dropping of the same prefixes over and over again. The full event list shows that this occurred for over an hour. While first level support personnel may not be able to analyze and correlate this as a factor in the application or service outage, it is an anomalous and undesirable network event stream that can be escalated to higher level operations or network engineering to analyze in detail

Enhancing Network Monitoring

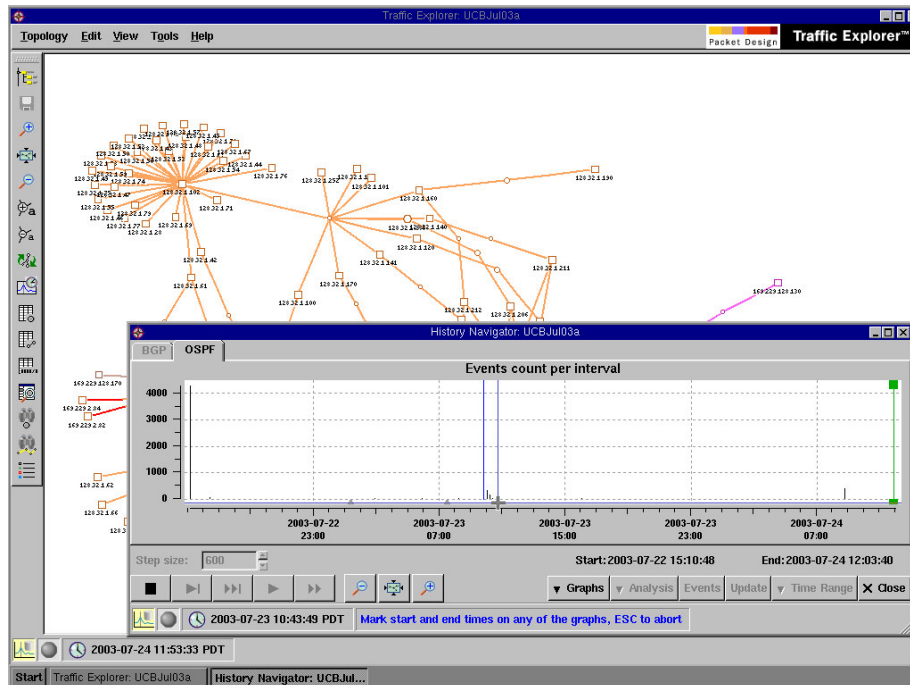


Figure 2: Operators can look at a range of time before the current problem started

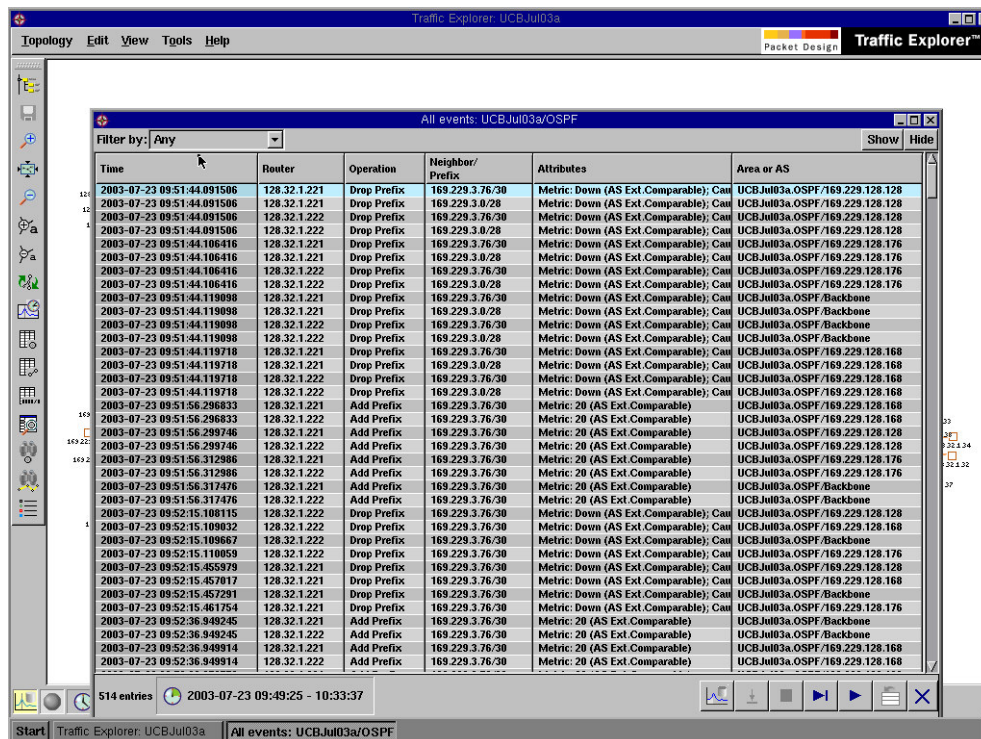


Figure 3: Route analytics displays a list of all routing events in that time range, which can be analyzed for issues that might have an effect on the application or service in question.

Enhancing Network Monitoring

By eliminating a significant blind-spot in network monitoring, helping operators quickly localize the part of the network to troubleshooting, and providing historical forensic information on network behavior, route analytics helps network operations departments save a tremendous amount of personnel time, leading to lower costs in the face of growing demands. In addition, by speeding monitoring and troubleshooting processes, route analytics contributes to higher application and service availability and performance, with tangible top and bottom-line results.

Preventing, Not Just Fixing Problems

Beyond monitoring and operations improvements, there are also many benefits for network engineers. Engineers can now ensure that critical IP networks are adequately engineered to deliver a complex, changing matrix of application and service traffic at various service levels. For example, engineers can perform modeling of a change of Expedited Forwarding (EF) traffic for a group of users based on the projected rollout of a new IP-video distance learning library that is anticipated to cause a spike in traffic. Route analytics can calculate and simulate the network-wide change in routing and traffic where the new traffic is overlaid not on an abstract model, but on the traffic and routing matrix as it actually exists in the network. The new traffic and routing picture will then show whether EF or any other traffic class is affected on any link in the core IP network. If not, then provided usage assumptions are correct, engineers can proceed with confidence in the rollout, knowing that the network will continue to support existing application requirements. This forward looking visibility, in addition to real-time monitoring and forensic troubleshooting helps network managers to ensure that mistakes and design errors are prevented rather than having more operations time tied up with needless troubleshooting.

Conclusion

Network managers are routinely being called upon to deliver more with less. Route analytics' increased monitoring visibility, forensic history and forward-looking modeling capabilities make it a force-multiplier for network operations and engineering teams, helping network managers ensure the reliable delivery of critical applications and services that drive top and bottom line business results, while containing operational costs.

To learn more about Packet Design and its industry-leading route analytics solutions, please:

- Email us at info@packetdesign.com
- Visit Packet Design's web site at <http://www.packetdesign.com>
- Call us at 408.490.1000



Packet Design

Corporate Headquarters

Packet Design Inc.
2455 Augustine Drive
Santa Clara, CA 95054
Phone: 408.490.1000
Fax: 408.562.0080

Enhancing Network Monitoring

<http://www.packetdesign.com>