WHITE PAPER

IP Route Analytics

A New Foundation for Modern Network Operations

Packet Design

Executive Summary

The emergence of IP …

From enterprises to college campuses, throughout government agencies and across the global Internet, the economic advantages of networks based on the Internet Protocol have established IP as today's communication infrastructure of choice. Compared with legacy, connection-oriented networks, IP delivers far greater resiliency and scalability at a significantly lower cost of deployment.

These benefits have resulted in the large-scale migration of mission critical applications onto an IP infrastructure. In turn, these applications have driven the requirement for ever-greater reliability and performance of the network delivering these services.

In addition to the need for higher reliability and performance, the adoption of applications with new demands for guaranteed service levels, such as voice/video communications, data storage and VPNs, requires a degree of predictability from the network that has been difficult to obtain with IP, given the dynamic nature of it's routing.

… and the new management challenges

While the advantages of IP are compelling and undeniable, the distributed architecture behind IP's preeminence also makes managing the network more of a challenge. The growth in size and importance of IP networks has led to increased operational complexity and costs. Bubble-era, brute force solutions of indiscriminately adding bandwidth and IT personnel no longer scale in today's more "normal" economic climate. Network operators and engineers need new solutions for achieving the requisite network visibility, analysis and control capabilities … all essential elements of running a network that have been lost in the transition to IP.

A fundamentally new solution called *IP Route Analytics* offers unprecedented visibility, analysis and diagnosis of complex IP networks, improving service availability and performance, while reducing operating costs and capital expenses. This paper describes a new approach to IP network operations that is based on leveraging IP's inherent intelligence to gain essential knowledge of its dynamic routing functions … a required management foundation for effective service assurance.

IP's Distributed Intelligence – A 'Silver Lining in The Cloud'

IP routing delivers network scale and strength …

The genius of the Internet Protocol lies in its distribution of intelligence throughout the network. Routers exchange reachability information with each other using various routing protocols. Based on this information, each router makes its own decision about how to forward individual packets to their destination. Should any link or node fail, the routers detect and propagate that status throughout the network, automatically redirecting traffic to alternate paths around the failed element. The separation of this dynamic router-to-router coordination, or the *routing control plane*, from the *forwarding path* that actually transports the data, enables IP networks to be highly resilient while efficiently scaling worldwide.

© 2003 Packet Design, Inc.

… but obscures network operation

IP networks are often referred to as “clouds”, and the reference is not unwarranted. The path between any two nodes of a circuit switched network is well known and its characteristics are predictable. With an IP network, however, a packet enters the cloud at one point (say, a user’s desktop) and is delivered from the cloud at another (such as an application server). The individual routers forward the packet from its source to its destination, but the exact path each packet takes is dynamic and unknown at any previous point in time. With each router making its own forwarding decision based on information gleaned from its peers, there is no single repository of routing knowledge in the network. This lack of visibility into the operation of an IP cloud can mask problems that impact both the availability and the performance of network services.

Existing Tools Lack Visibility into IP’s Dynamic Routing

Today’s fault and performance management tools do not address the highly dynamic and operationally opaque nature of an IP network.

Today’s NMS tools monitor device status …

While traditional SNMP-based network management systems can discover and display the individual network elements and their physical, or layer-2 topology, they do not identify the actual routes taken by packets comprising the various applications flowing over the network. Without this knowledge, operators are unable to determine which network services are being affected by individual device failures, a critical requirement in understanding the business impact and in prioritizing IT responses.

More important, the device-centric nature of SNMP-based network management systems often results in service availability or performance problems going undetected, or unresolved for long periods of time due to the difficulty to diagnose and correct the cause. Many network problems cannot be identified directly by the common SNMP objects that are polled by the management system. For example, the problem may be defective memory or software bugs that cause a physical or software component to be reset repeatedly. In such cases, the device may seem perfectly healthy to a management station polling for availability, while the ostensibly operational device could be wreaking unseen havoc on the network.

… while many network problems go undetected

Even more common are situations involving logical instabilities such as route flaps, misconfigurations leading to route loops or black holes, and other layer-3 problems that can have far-reaching effects on network services. Application traffic may follow errant routes masked by IP’s self-healing capabilities, while impacting the performance of unrelated services due to inadvertent traffic congestion. Router misconfigurations can cause critical redundant links to be unavailable just when they are needed most, resulting in catastrophic network outages. Legacy equipment and routes long thought to have been decommissioned may still be active, opening the network to potentially severe security breaches. Unconstrained broadcast domains, inappropriate link metrics relative to capacity, excessive convergence times - the list of common IP layer problems goes on and on. In virtually all cases, these scenarios would go unobserved

© 2003 Packet Design, Inc.

by existing management systems, leading to lost productivity of both users and network operations staff, or worse.

Performance management tools report on the users' experience, but can't pinpoint the source of network related problems

In an effort to better understand and respond to their end users' experience with the quality of the services being delivered by the network, IT managers have more recently turned their focus toward application performance monitoring solutions. Typical performance management tools include host-based agents that monitor server resources, as well as network probes that measure application response times. While both of these techniques are valuable in understanding the quality of service delivery, they offer little visibility into the root cause of any network related problems that are impacting those services. Lacking real-time knowledge of the actual routes being taken by the affected applications, how can the operator know which network devices to investigate?

In a typical network environment, a problem with any single device is virtually guaranteed to produce a myriad of alerts and other event information on the management console. Network operators attempting to isolate the cause of a problem must painstakingly sift through the volumes of traps and alarms - a manual process that is slow and error-prone. Studies have shown that the vast majority of network downtime is spent analyzing information in order to pinpoint the source of the trouble, because only then can service can be restored.

This has led IT organizations to once again look for a better approach to network problem resolution. Root cause analysis solutions (sometimes referred to as Integrated Service Assurance) attempt to span the gap between network fault and application performance management tools, with a goal of correlating network device failures to the services being impacted, while identifying the network devices responsible for any measured service performance problems.

Root cause analysis solutions try to infer the source of a network problem, but are missing critical information

These solutions monitor and gather data from a variety of instruments and systems, utilizing complex rules and analyses to determine the source of a problem. But in the end they are still built on an inference model which attempts to synthesize the root cause based on a dynamic and often incomplete set of information. Despite a variety of techniques developed to automate identification of the root cause, an effective and reliable solution has continued to be elusive.

The lack of visibility into the logical, or layer-3, operation of an IP network highlights the critical gap between the device-level management performed by traditional network management systems, and the application monitoring achieved using performance management solutions. Without the ability to visualize, monitor and analyze the real-time operation of the IP layer, service assurance relies on over-provisioning of the network, along with expert manual intervention, resulting in excessive operational costs, time-consuming problem resolution and lost productivity.

The dynamic and complex nature of today's IP networks requires a fundamentally different approach to service assurance than what has worked in the past.

© 2003 Packet Design, Inc.

Introducing IP Route Analytics – Harnessing IP's Intelligence to "See Inside the Cloud"

The same dynamic routing capabilities that are the basis for IP's scalability, resiliency and economic advantages, also give rise to new management challenges by obscuring the inner-workings of the network. An innovative solution called *IP Route Analytics* represents a fundamentally new approach to IP network operations, improving both service availability and reliability, while reducing total operating costs.

IP Route Analytics provides real-time visibility into IP's dynamic routing

The foundation of IP route analytics is the routing control plane itself – the routing protocols such as OSPF, IS-IS, BGP and EIGRP – that dynamically control the logical operation of the network. Unlike the "bottom-up", device-based approach of conventional management systems, IP route analytics leverages the information in the routing protocols to understand how the network is operating.

An IP route analytics solution works by:

- Listening to and participating in the routing protocol exchanges between routers as they talk to each other
- Computing a real-time, network-wide routing map (similar to the task performed by individual routers to create their forwarding tables, but computed for all routers)
- Monitoring and displaying routing topology changes as they happen
- Detecting and alerting on routing events or failures as routers announce them
- Correlating routing events with other information, such as performance data, to reveal underlying cause and effects
- Recording, analyzing and reporting on historical routing events and trends
- Analyzing the impact of routing changes on the "as-running" network before they happen

Knowledge of IP's dynamic routing is critical for all aspects of network operations including …

The result is the most accurate, up-to-date picture of how the network is operating - a top-down, holistic view of the network's behavior that enables the IT staff to be much more effective at maintenance, troubleshooting and planning.

IP route analytics lets network operators and engineers visualize and understand the dynamic operation of the network as never before. By monitoring the routing control plane, IP route analytics solutions are able to construct the router's view of the network, "hearing" topology changes in real-time as they occur. Loss of IP-layer connectivity is immediately detected, even when device-level status is unchanged or unknown. Routing instabilities or changes that go unnoticed by conventional management systems, but which impact network availability and performance, are visible within seconds, leading to early detection of service outages and reduced time to repair.

… network discovery and documentation …

Large networks tend to be designed, deployed and operated by multiple individuals or groups, and even with rigorous documentation and change management procedures, it is inevitable for reality to diverge from the design. In fact, many network engineers liken the constant activity of "digging up" accurate information about their own network

© 2003 Packet Design, Inc.

to archaeology. This "network archaeology" must be practiced, however, since engineering and operations activities require complete and accurate information about the network, regardless of where it comes from. IP route analytics can automatically perform this vital layer-3 discovery and monitoring task, saving IT time and resources.

… routine maintenance tasks …

IP route analytics can also provide network operators with critical, and previously unavailable information, which aids in performance of their routine maintenance tasks. For example:

- What is the impact of taking down a router or link for service?
- Which network routes or services will be affected?
- How will the rest of the network respond?
- Did the configuration changes implemented have the desired result?

IP route analytics precisely answers these questions based on the network *as it is actually running* – not by relying on a simulation or model of the network. Operators can easily confirm that the network is functioning as planned, both before and after maintenance windows.

… root cause analysis and problem resolution …

IP route analytics is also a logical starting point for trouble resolution. When users complain of service slow-downs or outages, IP route analytics can highlight the relevant routes and network devices involved for a particular application, greatly reducing the time to diagnose, pinpoint and resolve the root cause of a problem.

… early detection and alerting on anomalies to prevent outages …

In many cases, IP route analytics can identify and alert on routing anomalies prior to their becoming problems, enabling corrective action to be taken before users are affected. IP-layer instabilities such as route or interface flaps, potential indicators of impending failure, can be discovered and attended to before resulting in a full blown service outage. IP route analytics can also alert on reductions in path redundancy, averting potentially devastating losses to an organization dependent on a high-availability network.

… diagnosing and resolving historical and intermittent problems …

In addition to providing real-time visibility into IP's dynamic routing, IP route analytics aids network operators in diagnosing intermittent or difficult to detect problems with its ability to record and playback historical routing events. Much like using a VCR, engineers can "rewind" or go back to an outage or significant event and "replay" the routing activity that preceded the problem. An operator may designate a route of interest, such as a customer whose trouble ticket is under investigation, and watch how it was rerouted during the incident. Historical analysis of past or intermittent routing problems is a valuable time- and cost-savings benefit, enabling network operators to resolve and prevent recurring service outages.

… correlating routing activity with other network events for root cause determination …

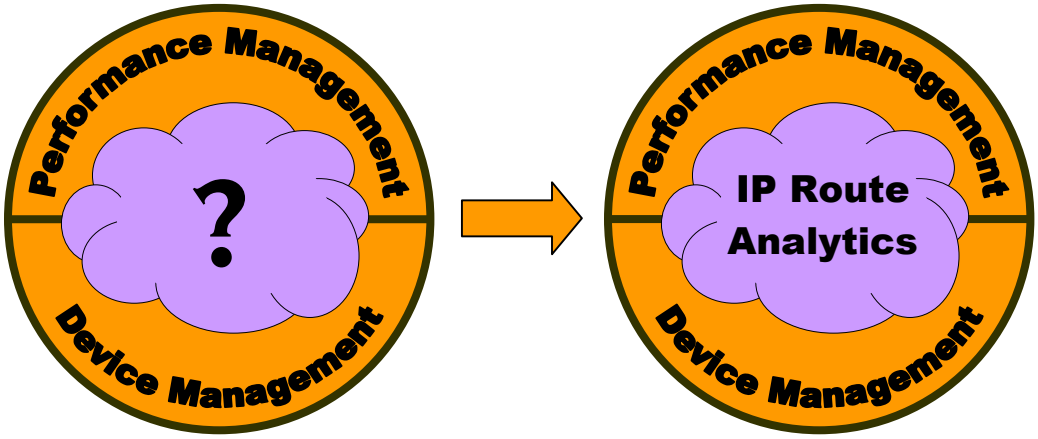
Furthermore, externally collected time series data can be imported and correlated with the routing events history, providing a powerful tool for viewing and analyzing the effects of routing on vital performance parameters such as link utilization, delay or packet loss.

© 2003 Packet Design, Inc.

… network planning and optimization

IP route analytics also aids engineers with some network planning tasks, allowing them to:

- Understand how changing individual route metrics affects the network before making any changes
- Optimize route paths to achieve maximum utilization of existing assets while avoiding unnecessary over-provisioning or other capital expenses
- See the impact of failed routes or routers before something happens; identify and plan for potential points of failure
- Determine and validate the level of redundancy on the as-running network, rather than rely on potentially out-of-date network documentation



Device and performance management tools are unable to see the dynamic routing events inside an IP network, creating a critical operating information gap

IP Route Analytics leverages the inherent intelligence of the IP control plane to provide real-time visibility into the dynamic operation of the network

IP Route Analytics fills a vital information gap in IP network operations

IP Route Analytics complements device and performance management tools, filling a critical information gap for network operations

A network operations model based on dynamic routing information does not preclude the need to gather device-level status or to monitor application performance, but it does provide a foundation and a context by which that data can be collected, correlated, analyzed and applied toward the ultimate goal of assuring highly available and reliable network services. IP route analytics addresses a crucial operating knowledge gap, complementing conventional network and performance management systems to form a comprehensive IP network operations system.

© 2003 Packet Design, Inc.

What Does an IP Route Analytics Solution Look Like?

A router, itself, is a form of IP route analysis device. It participates in the IP control plane and uses the information in the routing protocols to compute a view of the network for the sole purpose of determining how to forward packets. Whereas each router does this for itself, network operators need a complete, network-wide view of the dynamic routing activities. Without this capability, operators are required to log in and query each individual router for its current state - a tedious, expensive and all too common troubleshooting approach today.

Network operators need accurate real-time and historical visibility into IP's dynamic routing

Some management tools can periodically poll each router to collect a "snapshot" of its routing database, then combine the information from each router to present a picture-in-time of the network's layer-3 topology. This technique is inadequate for network monitoring or troubleshooting, since problem detection and diagnosis requires both a real-time, and a complete historical view of the network's routing behavior. Increasing the frequency of polling only serves to increase network load and processing load on the routers, severely impacting the network itself while still leaving the operator with gaps in the routing event history.

What has been missing is a way to understand the combined views of every router in the network, in real-time, without asking the routers to explicitly supply that information.

The solution is an *IP Route Analytics appliance*.

IP Route Analytics lets operators see their network as the network sees itself

An IP route analytics appliance is a device that leverages the IP control plane, participating in the exchange of routing protocols to compute a comprehensive, dynamic view of the logical state of the network. In essence, it lets network operators see the network as the network sees itself.

Unlike a router, an IP route analytics appliance does not forward any traffic, but only participates in the routing protocol conversations. Thus it is neither a bottleneck nor a failure point for network traffic, and requires no upgrading to keep pace with increases in network speed. Additionally, since it does not rely on device polling to gather its routing information, the IP route analytics appliance places no load on the network and easily scales to any network size, automatically detecting routers as they are added or removed.

The key functions and capabilities of an IP route analytics appliance include:

- **Data Collection / Importation**
  - Participation in IP routing protocol exchanges
    - Used to compute real-time, layer-3 topology
    - Supports multiple protocols, multiple areas, etc.
  - Imports external time-series data (e.g. traffic statistics, trouble ticketing)
    - Enables correlation of external data with IP routing events
    - Greatly facilitates determination of root cause and effect

© 2003 Packet Design, Inc.

- **Data Storage**
  - Storage and archiving of all collected / imported data
    - Maintains data for historical and long-term trend analysis
    - Used for report generation / network activity graphs / queries
- **Data Analysis**
  - Real-time, on-the-fly analyses (based on "live" data)
    - Enables real-time updates of topological map
    - Monitors network for alerting on user-defined events / thresholds
  - Historical analyses (based on stored data)
    - Basis for historical topology visualization, reports, activity graphs
    - Ability to "replay" network events for post mortem / root cause analysis
    - Used for correlation of external data with IP routing events
  - What-if analyses (based on combination of "user inputs" and stored data)
    - Allows exploration of hypothetical scenarios on the "as-running" network (e.g., impact of failed links, changed route metrics)
    - Shows how maintenance changes, potential outages would affect the network before they occur
- **Data Presentation / Output**
  - Visualization
    - Real-time updates of the logical network topology map; shows active route(s) between any pair of end points
    - Interactive display of highlighted routes, link status, link costs, etc.
    - Historical views / replays of topology over user-specified time periods
    - Time series graphs / routing event charts highlight activity not easily visualized within the topology view (e.g., protocol activity, flapping links)
    - Visual correlation of external data with time series graphs simplifies root cause analysis
    - Graphically shows the effects of what-if analyses on the topology map
  - Alerting
    - Provides immediate notification of routing changes based on user-defined events / thresholds - sent via SNMP traps or logged to SYSLOG
    - Proactive monitoring of network health aids in early problem detection / prevention and reduced MTTR
    - Enables integration with SNMP-based management system for consolidation of event reporting
  - Reporting
    - Produces on-demand web-based reports over user-defined historical time periods
    - Presents vital network statistics such as flapping routes, changes in link metrics, newly advertised routes/routers, withdrawn prefixes, and more
    - Enables archival documentation of network activity for long-term trending
  - Query API
    - Provides access to routing analysis database by 3rd party applications
    - Standards-based XML RPC

© 2003 Packet Design, Inc.

Implementation of an IP Route Analytics solution is fast and simple

Despite the vital operational role it plays, configuration and implementation of an IP route analytics appliance should be fast and simple, taking no more than an hour to install and be up and running. A single appliance should be able to scale to any size network, regardless of the number of routers, areas or Autonomous Systems. While multiple IP route analytics appliances may sometimes be desired (for example, when parts of a large network are administered by different groups, or when redundancy is desired), there should be no requirement for installation of multiple remote probes or other infrastructure. The IP route analytics appliance should support a wide range of routing protocols, synthesizing all routing information into a comprehensive, network-wide view.

Access to the IP route analytics appliance is via a remote user interface, which should be supported on a wide range of platforms. The learning curve should be minimal, providing immediate benefit without requiring a significant investment in training.

The Benefits of IP Route Analytics

IP route analytics is an essential component for effective network operations and provides substantial benefits to any organization including:

- **Increases Network Availability**
  - Detects common IP layer faults not found by existing network management tools
  - Prevents service outages by discovering IP layer anomalies before they become problems
  - Provides a faster, top-down approach to determination of root cause, rather than deducing the cause based on volumes of alarms
  - Enables diagnosis and correction of historical and intermittent problems
  - Verifies and alerts on changes to routing redundancy, preventing service outages
  - Reduces time to pinpoint and resolve network faults
- **Maximizes Network Performance**
  - Accurately shows whether the network is operating as planned
  - Monitors and alerts on routing changes that could impact performance
  - Identifies routing instabilities that go undetected yet still impact services
  - Enables “what-if” analysis for route path optimization
  - Correlates routing events with performance data for root cause determination
  - Minimizes common configuration errors during maintenance
- **Reduces Total Operating Cost**
  - Reduces lost productivity and customer dissatisfaction due to network outages
  - Improves productivity of network operations staff by reducing time spent in fault isolation and root cause analysis
  - Reduces capital expenditures by maximizing existing network asset utilization
  - Minimizes demands on scarce engineering resources to tackle routing problems
  - Frees IT resources to focus on strategic initiatives, rather than problem resolution
  - Improves service assurance for reduced SLA penalties

© 2003 Packet Design, Inc.

The ROI for implementing an IP route analytics solution is clear and significant when you consider that these benefits can be realized for about the price of a single router.

Conclusion

Without the ability to visualize, monitor and analyze the real-time operation of dynamic IP routing, network availability and performance rely on over-provisioning of the network along with costly manual intervention. This results in excessive operational costs, time consuming problem resolution and lost productivity.

IP Route Analytics harnesses IP's inherent intelligence to deliver indispensable information for the operation of any mission-critical network. From early warning of routing anomalies to detailed forensics after the fact, IP route analytics improves service reliability and performance, while driving down the total cost of network operations.

IP route analytics delivers an extraordinary ROI when considering the valuable benefits it provides with its low cost and ease of implementation. Along with conventional device and performance management systems, IP route analytics is emerging as an essential component for modern network operations.

© 2003 Packet Design, Inc.