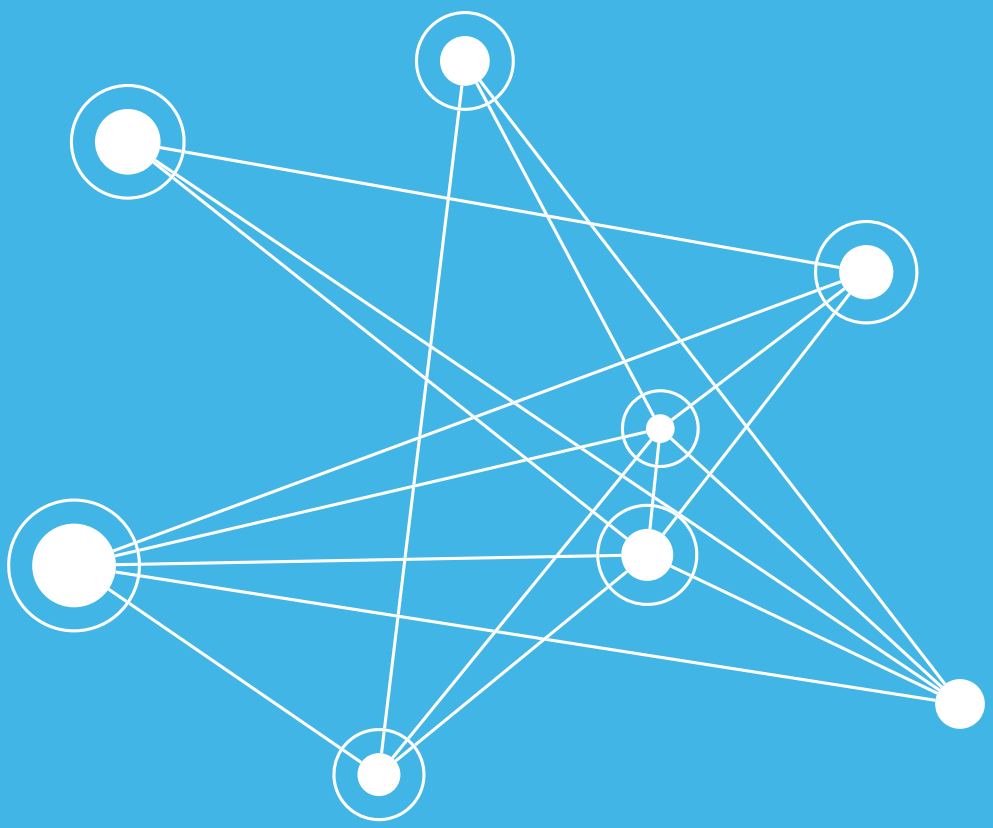
PACKET DESIGN

Route-Flow Fusion℠: *Integrated NetFlow and IP Route Analysis*



WHITE PAPER

Table of Contents

Introduction

IT and network engineering departments are under increasing pressure to deliver more predictable and better performing IP networks. Meeting more stringent Service Level Agreement (SLA) requirements for converged data, voice and multi-media, and coping with the effects of web-enablement and Service Oriented Architecture (SOA) requires increased network management visibility and accuracy.

While new end-to-end application performance management solutions have arisen to complement SNMP device management, the tools utilized by engineers to understand the inner workings of IP networks themselves are still rudimentary. This leaves network managers coping with an opaque network "cloud" of dynamic IP routing and traffic that is the root cause of a large percentage of application problems. The traditional separation between operational monitoring/analysis and engineering planning tools makes things worse, since engineers can't effectively use real-time monitoring data to plan and optimize the network. A new level of networking management best practices and solutions is needed to meet the challenge of evolving network requirements.

Packet Design has pioneered a new technology called Route-Flow Fusion that combines deep visibility into IP routing and flow-based traffic with monitoring, analysis and modeling capabilities. Route-Flow Fusion provides unprecedented visibility into the network "cloud" and enables IT to more rapidly, confidently and accurately optimize IP networks for better application and service delivery. This white paper provides an overview of the increasing demands on today's IP networks, reviews the evolution and current state of network management, then introduces Route-Flow Fusion technology and explores how Route-Flow Fusion can be applied to enhance network management best practices and achieve a rapid return on investment for IT and network engineering departments.

Increasing Demands and Changing Dynamics in IP Networks

Today's IP networks are increasing in volume, complexity and sensitivity of the traffic they are carrying. Web-enabled applications are leading to significant increases in traffic due to the graphical nature of web transactions compared to earlier text-based transactions. In addition, while the vast majority of traffic originates from relatively few Internet peerings and major data centers, converged VoIP, emerging peer to peer applications, and the onset of SOA add a matrix of business-critical and geographically distributed traffic across all parts of the network. As a result, it is becoming more important than ever to understand the correlated state of routing and traffic flows across all links in the network—not just a few WAN links.

Routing issues in particular can cause unexpected congestion that disrupts sensitive applications. For example, studies show that changes and instabilities in Interior Gateway Protocols (IGPs) such as OSPF, EIGRP and IS-IS can cause significant traffic changes in an IP network and disrupt the availability and quality of VoIP deployments, even in carrier-class networks with practically unlimited bandwidth and very low latency.[1,2] For IT and network engineering departments intent on delivering excellent network service, understanding the inner workings of IP routing and traffic is becoming more important than ever before.

1 C. Boutremans, G. Iannaccone, and C. Dict, Impact of link failures on VoIP performance, NOSSDAV, May 2002
2 R. Teixeira, N. Duffield, J. Rexford, M. Toughan, "Traffic Matrix Reloaded: Impact of Routing Changes", Proceedings of the Passive and Active Measurement Workshop, Boston, MA, March 2005

The State of Network Management Practice and Solutions

Traditional network management practices and solutions have largely overlooked the dynamic inner workings of IP networks. Traditional SNMP management solutions are limited to periodic checks on device and interface health and statistics, and don't give real-time intelligence and visibility into routing and traffic. Where traffic and routing issues are concerned, SNMP-based monitoring suffers from a relatively low "signal to noise ratio", because one Layer 3 event can set off so many different individual device, interface (port, circuit) and performance metrics monitored by SNMP events, making it extremely difficult to arrive at an accurate picture of what is happening in the network. While some vendors have attempted to cope with this situation by utilizing sophisticated, pre-set "codebook" algorithms to interpret patterns of SNMP event data, they are still limited by the non real-time and periodic nature of SNMP polling, which misses a significant amount of highly dynamic and sometimes voluminous routing and traffic event occurrences. As a result, codebook approaches only approximately infer root causes from SNMP event streams, and don't provide fundamentally better visibility into the network.

More recently, a number of emerging network management solutions have focused on measuring end to end application performance characteristics from client hosts to servers, while performing network measurements to help fill out the middle of the picture in a rough manner. Yet they can't provide visibility into real-time routing and traffic because like legacy network device management systems, they rely on SNMP polling snapshots that are far too infrequent and lack the detail to give an accurate picture of the network's routing and traffic.

One exceptional development in the network management marketplace is the emergence of high-performance flow collection techniques, and traffic analysis solutions that leverage the data in collected flow records. The most widely used such flow collection techniques are NetFlow and IPFIX. Corresponding to the emergence of practical flow data collection, a new set of network management solutions—Traffic Analysis solutions—organize voluminous flow record data into helpful tabular reports that show the top traffic senders and receivers, and allow for detailed analysis of the flows that comprise the traffic running over particular links, allowing network managers to identify anomalies that may be contributing to congestion on a link. Despite the usefulness of this traffic flow analysis, current solutions suffer from a number of major limitations:

- **Very limited scope of visibility:** Flow records only provide link utilization and flow information on links that are directly attached to the router that is generating the flow records. While theoretically NetFlow or IPFIX can be turned on for every router and switch in an organization's network, it is highly impractical to do so due to the volume and complexity of managing so much data, so most organizations deploy flow collection on a relatively small percentage of their routers. While visibility to perhaps 90% of raw flows on the network is not hard to achieve, standard traffic analysis tools only provide visibility into a small percentage of the links on the network. The result is that network managers end up with islands of visibility in a sea of network management darkness.
- **No understanding of IP networks' routed topology:** Standard traffic analysis tools do not understand network topology, and treat the network topology as a static entity, whereas in reality it is

very dynamic. In fact, traffic analysis solutions generally provide no representation of the network topology at all, but rather only provide aggregated and per-link tabular views of ranked traffic statistics (such as top sending and receiving hosts) and flow details. Since network changes, whether the addition or failure of links, changes in metrics, or other IGP-related events have such a large effect on traffic patterns, this is a major limitation.

- **Poor visibility to emerging issues, limited root cause analysis capability:** Given the above limitations, while standard traffic analysis tools are helpful to understand issues stemming from hosts, or those occurring on the small percentage of directly monitored links, they still offer very little direct intelligence on the network's behavior, and most of the time can't offer an answer to the question of why any particular traffic is flowing over any particular link.

Monitoring vs. Planning—An Unhelpful Divide

Aside from a near total blindness to correlated routing and traffic in IP networks, another significant barrier to sound network management practices today is the unhelpful divide between monitoring and planning solutions. For example, traffic analysis solutions provide real-time monitoring insight into network traffic flows, yet provide absolutely no ability to model how planned or unplanned changes in the network would affect that traffic, making the monitoring data much less useful in practice. Network managers are left to exercise educated guesswork when implementing adds, moves and changes to routers, applications, servers, and users, or when trying to determine if there is sufficient redundancy in place for failure scenarios.

On the other hand, today's network planning tools, while very powerful and able to model a seemingly infinite variety of network details, operate largely on offline, synthetic data rather than any real-time data from the network itself. In addition, the sheer complexity of these tools makes them useful primarily for long-range planning or "greenfield" network build-outs, but not very useful for routine operational or tactical planning purposes. The result of this divide between monitoring and planning is to fundamentally undermine the goal of network engineering and operations best practices, because planning, execution and validation operations lack sufficient data and modeling capabilities to ensure accuracy. As a result, misconfigurations still play an unfortunately regular part in network issues. For example, the previously referenced study on VoIP in a carrier-class network showed that router mis-configurations and resulting routing instabilities after simple link failures caused significant disruptions in VoIP quality and availability. Given the pressures on IT to deliver ever-more predictable network service, it is now unacceptable for organizations to settle for the lack of visibility into network routing and traffic, and for the lack of integrated monitoring and planning solutions.

Route-Flow Fusion: The Fusion of Routing and Traffic Analysis and Planning

Route-Flow Fusion is the first network management technology that delivers complete real-time visibility of correlated, network-wide IP routing and traffic flows, with the integrated monitoring, analysis and

planning capabilities that IT and network engineering departments need to optimize the network "cloud". Route-Flow Fusion creates an integrated and fully analyzable, operationally accurate model of the real network's routing and traffic flow topology, by recording and processing routing protocol updates and traffic flow records. Route-Flow Fusion perfectly complements existing SNMP device management, end to end application performance and long-range planning solutions by giving unprecedented visibility into and modeling for critical IP routing and traffic.

Route-Flow Fusion provides a number of unique capabilities:

- **Real-Time, Network-Wide Traffic Visibility:** Unlike standard traffic analysis tools, route-flow fusion provides visibility into traffic and flows on all links in the network. To do this, Route-flow fusion leverages Packet Design's route analytics technology to "map" recorded flows across their network paths.
- **"Replayable" Routing and Traffic History:** By continuously recording the state of routing and traffic over time, route-flow fusion can accurately portray an analyzable, network-wide map of all links and their traffic flows at any point in its recorded history.
- **IGP and BGP Routing and Traffic Correlation:** Route-flow fusion provides visibility into traffic phenomena from the point of view of both IGPs such as OSPF, IS-IS, and EIGRP, as well as from the point of view of key BGP routing attributes such as AS_Path, Neighbor_AS, Community and Exit Router.
- **Integrated Monitoring and Planning:** Through its highly accurate routing and traffic topology based on recorded routing updates and flow records, route-flow fusion goes beyond monitoring and analysis to provide what-if modeling and planning. Network managers for the first time can model a number of operationally relevant changes, and see the effect on the as-running network based on its real routing and traffic. Planning capabilities include adding, downing, moving or changing any combination of the following items in the network:

    - Routers running any combination of major routing protocols
    - IGP links or BGP peerings
    - Prefixes
    - Routing Metrics
    - BGP community strings, Local Pref, MEDs
    - Individual traffic flows
    - Full or partial traffic matrices

Once a set of changes has been made, route-flow fusion provides detailed before and after analyses to show exactly how routing and traffic has changed in the network. In addition, when in planning mode, the analysis capabilities of route-flow fusion, including reporting, historical analysis, routing and traffic correlation, and routing analysis, reflect any modeling changes made to the routing/traffic topology, providing a closed-loop, what-if analysis of any planned or unplanned change in the network.

Route-Flow Fusion Benefits and Applications

Route-Flow Fusion unveils the inner workings of the network cloud and empowers IT and network engineering departments to be more responsive, accurate and confident in meeting customer needs and emerging service delivery challenges. By integrating routing and traffic, monitoring and planning, Route-Flow Fusion redefines and empowers best practices across a variety of network engineering and operations applications that optimize both the operational cost and the service delivery of IP networks, leading to a rapid Return on Investment for IT and network engineering departments. Following are a number of applications that leverage the unique power of Route-Flow Fusion's integrated traffic and routing analysis and planning capabilities:

- **Peering and Transit Analysis and Planning: Route-Flow Fusion provides network planners with visibility to:**
  - Monitor exit link utilization to ensure customer service levels
  - Monitor traffic by exit routers to ensure adequate load balancing and redundancy
  - Ensure peering vs. transit traffic is within contracted ranges
  - Identify and justify potential peering relationships
- **Capacity Planning:** Network managers can manipulate the full traffic matrix to model traffic growth or changes such as:
  - Moving groups of users to a new location
  - Moving servers to a new data center or co-location Point of Presence (PoP)
  - New application deployments
  - Departmental Chargeback: IT departments can group prefixes associated with a set of servers or users (sites, departments etc.) and record traffic utilization per group for departmental accounting and chargeback purposes
- **Optimized Flow Collection:** Network engineers can gain network-wide, per-link utilization and detailed flow analysis while optimizing the number of flow collection points in the network
- **Routine routing maintenance operations planning and validation:** Network engineers can accurately plan routine maintenance such as upgrading a router, adding a link, changing BGP policies. Route-Flow Fusion provides proactive analysis of the effect on network routing and traffic to ensure that there are no surprises. Real-time monitoring information ensures that no excessive network churn is occurring at the time of the maintenance, and validates that network routing and traffic behavior is as expected after the maintenance is completed
- **Failure analysis and redundancy planning:** Route-Flow Fusion allows for accurate what-if analysis of potential failures on routers and links, using the actual network's routing and traffic as the baseline.
- **Failure response and network remediation modeling:** Route-Flow Fusion's real-time monitoring and planning of routing and traffic allows network managers to respond rapidly to failures with what-if modeling and analyses to quickly decide the best network remediation strategy.
- **Congestion analysis and remediation:** Network managers can view histograms of historical link utilization, perform analysis of congestion patterns and drill down into the specifics of common flows that contribute to congestion on links. What-if planning allows engineers to determine the best remediation strategy. Broader congestion analyses can be performed by manipulating and

analyzing the full traffic matrix.

- **Network planning for cost and service delivery optimization:** Many organizations have a limited number of well-known, critical applications. Route-Flow Fusion provides the broad visibility, detailed analysis and what-if planning capabilities to understand network-wide traffic, see congestion hot spots, and optimize the routers, links and redundancy for optimal cost and service delivery.
- **Tactical network planning:** Complementing long-range planning tools, Route-Flow Fusion allows network managers to accurately plan tactical changes to the network such as adding a new set of routers and links, or enabling a new IGP.

Conclusion

Network managers face SLA pressures that require a truly network-aware complement to traditional SNMP device management, end-to-end application performance management and long-range planning tools. Route-flow fusion fills a critical hole in network management portfolios by providing real-time, network-wide visibility into the network "cloud" of correlated IP routing and traffic, with integrated monitoring, analysis and planning capabilities that speed IT and network engineering responsiveness, accuracy and confidence. Route-flow fusion delivers a powerful and rapid ROI by enabling best practices that lower the cost and optimize the service and application availability and performance of IP networks.

To learn more about Packet Design and Route Explorer, please:

- Email us at info@packetdesign.com
- Visit Packet Design's web site at www.packetdesign.com
- Call us at +1.408.490.1000

Corporate Headquarters

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