

# Ensuring Financial Transaction Delivery with Route Analytics



Packet Design

## Introduction

Timely and predictable transaction processing is the lifeblood of financial services companies. Whether revenue is produced based on transaction fees, by optimizing market timing to extract profit margin or by other means, disruptions and unforeseen variations in the way IP data networks deliver transaction traffic can have a significant financial impact. The challenge for IT managers at these firms is that the complex, redundant IP networks built to ensure traffic delivery can behave in unpredictable ways, leading to costly transaction latency or downtime. Unfortunately, traditional network management technologies, typically based on SNMP device polling, don't provide the insight that network managers need to understand IP networks' dynamic routing and traffic behavior.

Route analytics technology, with its real-time, network-wide understanding of the operational routing topology and the traffic flowing across all network paths and links, provides the missing visibility. With route analytics, network engineers can easily monitor for network topology and traffic problems, strengthen change management processes, proactively uncover network vulnerabilities, and accurately simulate failure scenarios and the resulting network behavior. Effective use of route analytics as part of the network management process can help ensure that complex IP networks will properly support the critical financial transactions that depend on them.

## Why IP Networks Are Inherently Unpredictable

Distributed routing intelligence – the quality that makes IP networks so efficient and resilient – also makes IP network behavior unpredictable and harder to manage. 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. Any change to those elements causes the routing topology to be recalculated dynamically. While this means highly resilient traffic delivery with low administrative overhead, it also creates endless variability in the active routing topology. Large networks with many redundant links can be in any one of millions of possible active routing topology states. This makes it much harder to understand and manage **how** traffic will be delivered.

The lack of IT management visibility into dynamic network behavior is reflected in the time-consuming process of correlating application problems to non device-specific network causes. For example, when a user reports an application performance problem that doesn't stem from an obvious hardware failure, pinpointing the root cause can be quite difficult because in a large, complex network, IT engineers have no way to know the route the traffic took through the network, the relevant links servicing the traffic, whether those links were congested at the time of the problem, or even which devices were servicing the traffic. Change management processes suffer from the same problem, since engineers making planned configuration changes in the network have little or no idea of what the network-wide routing and traffic delivery behavior will look like once the change is effected. This often leads to unforeseen and unwanted consequences during change processes.

For relatively non-critical applications such as email and web browsing, the impact of routing and traffic changes may be slight. But for financial transactions with sensitive latency requirements or other delivery constraints, it can be dire.

## Ensuring Financial Transaction Delivery

### The Need to Transcend Traditional Management Tools

The sheer complexity of the behavioral dynamics in large routed IP network topologies is beyond the ability of even the most educated and intelligent engineers to manage without proper analysis tools. That's why IT departments invest in management tools. However, traditional network management isn't sufficient. The overarching architectural principle of today's network management is to gather information on a vast number of different "points" in the network (e.g., routers, switches, security devices, servers), then correlate various point data to infer service conditions. The key mechanism for doing this is the Simple Network Management Protocol (SNMP). The main data gathered are:

- Device health: uptime, current status, CPU and memory utilization
- Fault indicators: up/down status, uptime, dropped packets, errors
- Traffic information: interface utilization: bytes in/out, packets in/out, configuration
- Service utilization information: utilization per class of service, threshold violations

While having this point data is critical – for example, an interface or device that fails, runs out of memory, or is congested can have a direct impact on application delivery – the sum of all this data reveals much less than the whole picture. Just knowing that an interface is full of traffic doesn't tell you *why* it is full. Where is the traffic coming from and going to? Is the traffic usually on this interface, or did a change in the network or elsewhere cause it to shift to this interface? If so, from where, when and for how long? Without answers to these questions, there can be no real understanding of the logical operation of the network as a whole.

SNMP was never built to understand a network's logical behavior. It is too periodic – polling cycles from 30 seconds to several minutes simply cannot produce an accurate portrait of the network's routing state, with its rapid and high-volume state changes. Even speeding up the polling cycle – say, to every five seconds – would still miss many routing state changes, and anyway would generate so much management traffic overhead as to be impractical.

### Route Analytics—Insight into Dynamic Routing and Traffic Behavior

Route analytics technology addresses the need for better insight into network-wide application delivery dynamics. It leverages the intelligence in routing protocols to automatically build and maintain an always-accurate routing map of any IP network, across AS, areas, and multiple protocols. Route analytics solutions peer with key routers in each AS or area, passively listening to and recording every routing update communicated throughout the network. By implementing the same algorithms that run on routers, they can calculate and deliver as accurate a routing topology map as the network's actual routers see.

Based on this routing map, route analytics then intelligently integrates Netflow data collected from a small subset of network interfaces to create an integrated, dynamically updated routing and traffic map. This is distinct from traditional methods of Netflow analysis, which do no more than present link-by-link flow data in separate tabular reports. Route analytics collects Netflow traffic flow records from routers handling the majority of source traffic flows into a network, such as at data centers, Internet peerings and key WAN links. It then utilizes its always accurate knowledge of routing paths to map each traffic flow across the precise links it traverses in the

## Ensuring Financial Transaction Delivery

actual network. The result is a network-wide map of all links with accurate real-time and historical traffic utilization and flow details. This map can be “rewound” to past moments in time to perform forensic analysis on the exact state of traffic and routing at that time; it can also be used as the basis for simulating routing and traffic changes, showing exactly how the whole network would behave in response. Route analytics delivers this comprehensive intelligence with a minimum of overhead, since it collects Netflow records from only a few exporting routers.

## Route Analytics Applied to Credit Card Clearing Assurance

Banks face a particularly complex challenge in managing extranet peering with their commercial customers to process credit card transactions. The typical extranet architecture has a server in the customer's data center which communicates via a TCP session (used for reliable delivery) with the bank's authorization servers over redundant links; these links are often configured using static routing, with different metrics designating an active primary and a standby secondary route between the customer and bank networks. To ensure security, all extranet connections into the bank network pass their traffic through a stateful firewall.

In most IP networks, when TCP application data travels from one host to another, the path need not be the same in both directions. That is, the TCP/IP packets can follow forward and reverse routes that are “asymmetric” without any problem in communication between endpoints. However, in the financial extranet scenario, when all traffic is routed across the primary link, the primary link's firewall maintains all security state for that session. If the route changes for reasons unrelated to a primary link failure, and packets from the TCP session start to follow the secondary route over the backup link, the second firewall, lacking any history of the session in its stateful cache, will assume the session is illegitimate and drop the packets. As a result of the dropped packets, not only will a particular transaction fail to be approved, but the entire TCP session between customer and bank servers will eventually be torn down, causing the whole authorization process to grind to a halt.

Routing asymmetry can mistakenly occur due to internal bank network or external customer network misconfigurations or other errors. Whatever the source, until the underlying problem is fixed and symmetric routing restored, the authorization transaction process will stay "offline." This means the customer must aggregate credit card authorizations and send them to the credit card provider (e.g., Visa or MasterCard) for “stand-in” authorization, with the bank paying the credit card provider a per-transaction stand-in fee. Such fees add up quickly until the asymmetric routing problem is resolved – which can take several hours when there is no network management insight into the routing behavior of a large, complex extranet.

Route analytics drastically reduces the mean time to repair asymmetric routing issues. Since route analytics has a record of all routing and traffic changes in the network, engineers can first verify that the network is not currently experiencing routing or traffic delivery problems that would impact the customer, then easily “rewind” the network to the time when the problem first appeared, examine traffic routes and all traffic flows corresponding to the customer in question, and find the asymmetry or other routing and traffic problems that would have caused the transactions to fail. If the customer's routing is based on standard protocols such as BGP, route analytics can even send alerts when a route changes, further reducing the impact of a network issue on transaction processing.

## Ensuring Financial Transaction Delivery

### Ensuring Trading Transactions with Route Analytics

Firms that specialize in processing market trades earn transaction fees, and/or utilize micro market timing windows to optimize transactions to garner margin on the trades. The networks built by such firms typically support a number of commercial customer peerings, along with a major web-based retail trading platform. Given the time sensitivity of these transactions, networks must provide absolutely predictable traffic delivery. Engineers must ensure that when they make routine routing changes or upgrades, or add new components to the network, they don't inadvertently introduce routing and traffic behaviors that will compromise transaction latency requirements.

Existing change management tools suffer from a fundamental limitation: while they provide helpful process control for executing device commands correctly and enforcing version controls across multiple devices, they offer no insight as to the network-wide routing and traffic effects of the new configuration. Trading firm networks typically architect their networks with such a high degree of routing redundancy—up to quadruple link redundancy—that understanding the implications of a routing or traffic change can be extremely difficult. If an engineer introduces an asymmetric or sub-optimal route, or causes traffic to shift in a manner that causes even temporary congestion, many transactions could be negatively impacted, causing huge financial losses.

Since route analytics understands all routed paths—not only primary/active ones, but potential/secondary and tertiary routes – it can be used to simulate routing and traffic changes and show their precise impact on the entire network's routing and traffic behavior. Since changes are simulated not on an abstract "model" but on the network's actual recorded routing and traffic, engineers see an extremely accurate projection of the effects of a planned change and know that the network can continue to support its required service levels.

### Ensuring Network Continuity with Route Analytics

Beyond enhancing troubleshooting and change management processes, route analytics can be used in a variety of ways to ensure that critical financial services networks maintain ongoing compliance with integrity and continuity requirements. For example:

- **An always-accurate map:** Route analytics provides an accurate, up-to-the-moment map of the entire routed network topology with which network and security engineers can ensure that all appropriate traffic routes are covered by defensive in-depth security measures.
- **Eliminating routing vulnerabilities:** Using route analytics' insights, engineers can ensure that backdoor routes and improperly filtered peerings with other organizations are detected and shut down.
- **Monitoring overall reachability:** Engineers can set thresholds for overall routed prefixes and be alerted automatically if the volume of prefixes crosses a threshold, indicating either a pervasive loss of communication or the injection of potentially damaging new routes into the network.
- **Monitoring loss of BGP peering, redundancy and reachability:** Internet peerings and often major inter-organizational connections are routed using the BGP protocol. Route analytics can detect the loss of BGP peerings, and can monitor BGP Autonomous Systems for loss of redundancy or reachability to key networks.

## Ensuring Financial Transaction Delivery

- Alerting on changes to critical traffic routes: In any network, certain traffic routes/paths are particularly sensitive. Engineers can monitor and be alerted to changes to these routes in real-time—far faster than SNMP polling periods.
- Simulating disaster recovery scenarios: Route analytics' network modeling capabilities can be used to simulate various failure scenarios to show whether the network as configured will behave as desired. For example, engineers can model failures on critical WAN links and observe how traffic will reroute and whether traffic belonging to various classes of service will exceed their engineered bandwidth prioritization parameters.
- Routing and traffic continuity analyses: Using route analytics' proactive routing audit, traffic trending and capacity planning capabilities, engineers can comprehensively analyze their networks to find vulnerable areas such as single points of failure and failure points that would have an extreme impact on path lengths. They can also obtain an inventory of Equal Cost Multi-Path and asymmetric routes so that engineers can ensure compliance with routing architecture standards. Route analytics also supports easy to use traffic trending based on historical utilization on all links, so that engineers can be alerted to any potential congestion points in the future.

## Conclusion

Financial services transactions demand that the IP networks supporting them be managed to deliver highly predictable, timely traffic delivery. The well-being of financial services business requires that IT organizations ensure these critical networks' integrity and continuity. Route analytics complements traditional network management technologies and provides a strong value as part of the network management portfolio.

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

- Email us at [info@packetdesign.com](mailto: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  
<http://www.packetdesign.com>