SOLANA NETWORKS Visible Intelligence

Routing Health Analysis

A Must Have for Managing Converged Networks

GET PLUGGED IN.

Routing Health Analysis
A Must Have for Managing Converged Networks

Executive Summary

To take advantage of what has been for many years a cost efficient infrastructure enterprises are now deploying mission-critical applications onto their IP Network. The early adopters have seen that mission-critical applications demand more control over the distributed decision making power of the IP network. Once mission-critical applications are deployed the reliability and performance of the network is at risk. With mission-critical applications such as VoIP, transactional data, IP Video, storage and security authentications, running on the network, real-time monitoring and diagnostics are needed in order to guarantee quality of service. Managing a converged IP Network demands more control and the only way to achieve this is to tap into the intelligence of the IP control plane. It is evident that the market is starving for a new technology that will complement Network and Application Management Systems allowing the network manager, for the first time ever, to understand how the network routing functions in real-time. This knowledge and visibility are fundamental to operate a robust network that will guarantee high quality of service to business-critical applications.

Network and Application Management Systems are very well positioned to provide valuable device-level attributes and information on the status and availability of applications and services. But both fail in providing insight into the routing health of the IP network. Network managers need to have real-time knowledge of how the IP network is behaving because mission-critical applications, unlike data, cannot cope with the constant route changes, i.e. the packets must arrive in the same order without loss, otherwise quality is compromised.

Route Analytics technology emerges to fill the gap current Network Management Systems (NMS) fail to address. It provides full visibility into the IP Network. It listens to the control plane information without polling allowing network topology discovery to be accurately available in real-time, making it possible to understand how the network is behaving. Route analytics also provides valuable information that allows network managers to constantly monitor the health of their network.

This paper explains how Route Analytics fills the gap Network and Application Management Systems fails to address in order for you – the network manager – to confidently run your converged IP network. Having insight into the routing health of your IP network allows you to reduce network downtime; improve user satisfaction, lower operating costs, efficiently plan network growth, proactively perform network maintenance, increase productivity and run mission-critical applications.

Network Challenges for Modern Businesses

It is IP Routing protocols that determine how data is shipped around the network. IP based technology does this on a best effort basis which is fine for e-mails, web-browsing or non-critical data. But what about mission-critical data including transactional data, stock trading and VoIP? It is imperative that the routing infrastructure and protocols are set up and functioning correctly to ensure that the network meets the needs of mission critical services. For instance, if there are any routing instabilities in the network this can lead to part of the network being degraded (running slow) or not available at all. This results not only in lost productivity but also in lost revenues.

Infonetics estimates that an average business can lose up to 2% of its annual revenues due to service degradation or network outages. For the average business this can equate to a cost of over $12M per year. For financial institutions such as banks and brokerage firms and businesses critically dependent on their network the cost can be even higher and run into the millions of dollars per hour. Clearly there is a rapid ROI for a solution that can reduce downtime and network degradation.

The migration to converged networks and business critical services has all added to the pressure on IP networks. Unfortunately, traditional NMS tools have not kept pace with the new challenges facing networks and do not have insight into the routing health of the network. New solutions are needed that can keep pace with the dynamic nature of mission-critical networks and provide full real-time network wide visibility. Often to compensate for the lack of network visibility, network managers often have to over provision to maintain networks service quality. Having the ability to look inside the network ‘cloud’ and understanding how the IP routing works is invaluable in helping network operators support the needs of their business.

A report by IDC on layer 3 management stated that routing instabilities and faults accounted for over 50% of all application performance problems. These were not just failures but intermittent routing troubles that are often very difficult and labour intensive to determine the route cause. To avoid such problems, network managers need to have visibility into the cloud.

Visible Intelligence

Why do we refer to IP Network as "The Cloud" and more importantly, how do we get full visibility into it?

The answer to the first question is simple: IP networks do not have one central point of control. IP networks are connectionless requiring its components – IP Routers - to make independent forwarding decisions on a per-hop basis. Up until now, the independent nature of IP routers has enabled IP networks to re-route application data around changes to the network, which has traditionally been considered IP's greatest strength. In fact, IP networks are very dynamic making it very difficult to see changes in real-time thus it is so often referred to as the "cloud".

To successfully run mission-critical application(s) on the network, visible intelligence is needed so that network degradation/outage can be avoided or resolved quickly. Network Managers need to understand how the network routing functions and see changes to the routing in real-time.

The next section will explain how Route Analytics can allow Network Managers to gain visibility into the IP Cloud.

Challenges of Existing Technologies

The routing protocols are the key element for making routing decisions in an IP network. Route Analytics provides new insight into the operation of these networks by unlocking the mystery of the routing protocols. Gaining visibility into the IP layer provides network managers with the ability to examine why certain packets take a particular path, how application data traverses the network, the specific hops along the path, and real-time path changes.

By providing insight into the routing health of the network, Route Analytics bridges the gap between standard network management and application management systems allowing for superior fault diagnostics.

Element management systems are excellent for providing detailed information regarding any network device. This can include things such as the type of router, number of interfaces, the protocol being utilized and the services running on a router. These types of systems are of most value when the scope of the problem has been narrowed down to a particular network element but offer limited assistance in troubleshooting wide ranging network issues involving multiple network elements and routing changes.

Network management systems are typically used to detect, diagnose and correct network and application faults. The most common technology approach used in these NMS systems is Simple Network Management Protocol (SNMP) based polling. This technology is very mature and has worked quite well for non-mission-critical networks but lacks real-time diagnostics capability required for today's converged networks. Since many application problems are due to intermittent issues, polling-based systems would not detect these types of faults as the failure may easily occur between polling cycles.

For example, a interface-flap would be easily missed using a polling-based system. A futile approach to improve the situation would be to increase the polling frequency which would flood the network with unnecessary load and inundate the network manager with unusable data.

Sniffer-based technologies collect application flow information and are typically deployed in key congestion points in the user's network. The captured flow data can offer rich statistics but is limited to detecting network issues which happen to occur in the specific location of the sniffer deployment. In order to utilize this technology most effectively, a large number of sniffers need to be deployed throughout the network which can be an extremely costly approach.

Ping and traceroute are still the most commonly utilized tools for troubleshooting network and application related faults. Test packets are introduced into the network and the behaviour is measured providing the user with information pertaining to the reachability of a destination or the path taken by the test packet. The limitations of this technology are its non-holistic approach and the additional load that is placed on the network. For example, traceroute packets will only specify the path taken by the probe packets, which may not necessarily match the path taken by application data. Similarly, ping packets will not verify if a service from a host to the server is available but only that the ping packet reached the destination. Moreover, it is labour intensive and deciphering the results requires costly expertise.

Finally, application management systems offer visibility into the overall health of IP services such as VoIP and IPTV. By introducing test data into the network, these systems can measure specific metrics including delay and loss which can be correlated to determine if the application is operating properly. The drawback of such technologies is that they treat the network as a single unit by only looking at the "input" and "output" conditions to make a diagnosis. As a result, application layer issues, which may actually be as a result of a network layer problems, will not be readily identified by the application management systems.

Route Analytics offers a new approach to network management and service assurance for today's more complex and ever changing IP networks.

Route Analytics Technology: Bridging the Gap

Route Analytics technology was specifically designed to provide visibility into the routing behaviour within IP networks. Route analytics systems passively listen to the routing protocol (OSPF, IS-IS, EIGRP, BGP), the "conversations" between the routers that determine how data is shipped throughout the network. Because all routers view the route analytics system as another router, all routing related intelligence is, in real-time, sent to the system for easy analysis of the routing health of IP networks. As a result, the route analytics system is instantly made aware of every event that takes place in the network providing for the ability to detect a whole new class of network faults, even intermittent anomalies such as link flaps.

A Route analytics system encompasses the following capabilities:

- Provides real-time visibility into the IP cloud
- Automatically discovers and builds a network topology map
- Monitors, analyzes and visualizes routing related faults and instabilities on network topology in real-time
- Scalable to meet the requirements of large-scale, meshed, multi-domain enterprise networks
- Significantly reduces the mean time to identify and remediate routing faults
- Correlates routing events to performance statistics to uncover application versus network faults

Route analytics will therefore provide the network manager with an advanced system that has the capability to easily troubleshoot and action those hard to find problems on mission critical networks that traditional NMS tools simply cannot find.

Route Analytics technology has three main functionalities accessed through a Single Pane of Glass to determine Routing Health and End-to-End Path Visibility and carry out Network Engineering.

Single Pane of Glass

Most NMS systems are limited in their offerings of a usable IP topology map. The route analytics systems can within seconds automatically discover and visualize an IP network in a dynamic and easy to navigate topology map. Network engineers can visually determine if network devices are available, their interconnection and routing interplay. All vital routing statistics are also available at the user's fingertips from the network wide view right down to the specific router or link. The topology can be quickly determined by listening to the routing protocol exchange between the routers and extracting specific information in a non-intrusive fashion.

In the absence of such a system, the network architect connects to every router, digs out the necessary information and then manually assembles it. This is a very tedious approach that does not take into account the dynamic routing of IP networks.

Route analytics offers a "single pane of glass" from which the user can gain access to a vast array of additional information (QoS and NetFlow) also critical for the smooth functioning of an IP network.

Routing Health

Since the route analytics system listens to routing "conversations" (Link State Advertisements - LSA's) between the routers, it has instant knowledge of all routing events taking place in the network. A network running at steady state exchanges a typical number of routing related messages between all the routers commensurate to its size and the connectivity. Should this number reach an abnormal amount, it is a sign that the network has become unstable and is trying to re-converge. As a result, router resources are unnecessarily used to calculate forwarding decisions rather than actually forwarding business critical data. This would result in dropped packets and service degradation and in extreme cases, network meltdown. Having the ability to correlate router resource limitations and application performance would be extremely difficult without having insight into the control plane information of the routers – a unique capability of the route analytics technology.

End-to-end path visibility

One of the key capabilities of the route analytics technology is the ability to visualize end-to-end application paths, a must for correlating application and network management data. By visualizing the path taken by application data through the network, it is possible to reduce the time for root cause analysis for a potentially degraded service. This is because the application manager can, on the topology map, visualize the specific routers and interfaces in the path which are carrying the application data in question. Moreover, the managers can rapidly verify that all critical paths for a specific application are running and performing as designed.

Network Engineering

Route analytics can assist the network engineer to perform network planning tasks including:

- Determining the effect of routing by modifying link metrics prior to implementation
- Examining the consequence of bringing down a router on traffic patterns using actual network data
- Visually determining the level of path redundancy with live network data
- Understanding the impact of link asymmetry prior to deployment of latency sensitive services such as VoIP

Benefits to Modern Businesses

Having visibility into the cloud together with true real-time information on the routing instabilities that are the cause of the majority of all problems affecting services is invaluable. By implementing route analytics, businesses can improve network performance and realize significant advantages.

Route analytics provides a rapid ROI by improving network support to business operations through high network availability and rapid root cause analysis. It provides real-time network wide visibility and monitoring enabling efficient utilization of IT resources. Its automated approach removes the reliance on tedious manual techniques for finding network problems and troubleshooting. This results in a significantly reduced mean time to diagnose problems leading to higher network availability and performance. Network outages and performance trends can be analyzed through notification of changes to application and service baselines as a result of IP layer instabilities and anomalies.

With Route Analytics you can find out exactly how real application data traverses the network and ensure that the network meets the service requirements of your clients. Furthermore significant capital saving can be made because Route Analytics provides maximum utilization of infrastructure resources.

Network planning is improved because a topology driven interface allows the user to see the impact of any changes on networks using real network data.

Route Analytics Value to Network Team

Network Operators, Network Engineers, Network Architects and Application Managers, all benefit from Route Analytics. Route Analytics provides them with valuable network knowledge that eases their ultimate task of building, deploying and managing a stable network to support business-critical applications and services.

To better achieve their goals, each member of the network team must have full visibility of the operation of the network and understand the impact on their day-to-day tasks.

The table below shows the benefits of route analytics technology to the various functions within the networking groups.

Network User	Route Analytics Benefits
Network Operators: ▪ Day-to-day Network Operation ▪ Monitor Network Health	▪ Real-time view of the IP Layer ▪ Network relevant information at fingertips (routers, links - IP configuration and routing table info) ▪ Fault Alarms notify element status ▪ Determine if network address is reachable ▪ Visualize the routed path between any two points ▪ Determine if routed paths are available ▪ Quickly drill down from network wide, area wide to router specific
Network Engineers: ▪ Building and maintaining the Network ▪ Troubleshooting and resolution of complex network issues ▪ Deploying and configuring new ▪ equipment ▪ Investigate intermittent network ▪ anomalies	▪ Visibility into the routing protocol ▪ Historic replay of network activities ▪ IP Network Health at a glance ▪ Check for routing anomalies ▪ Network relevant information at fingertips (routers, links - IP configuration and routing table info) ▪ Determine if network address is reachable ▪ Verify routed paths through the network ▪ Verify exit points from the network ▪ Track IP topology changes and growth
Network Architects: ▪ Planning and designing the network to meet business objectives	▪ Clear understanding of the production IP network ▪ Plan network changes prior to implementation ▪ Network relevant information at fingertips (routers, links - IP configuration and routing table info) ▪ Determine if network address is reachable ▪ Verify routed paths through the network
Application Managers: ▪ Managing specific applications and services that use the network	▪ Verify exit points from the network ▪ Provides understanding of how the application data is moving through the network ▪ Set, and alarm against, application and service baseline ▪ Determine how application and service data moves through the network ▪ Determine if critical points in the application or service are available ▪ Extract a list of routers and interface along the path

Conclusion

The existing network management tools are ill equipped to deal with the dynamic nature of today's converged networks. SNMP based systems lack real-time diagnostics capability and since many application performance problems are due to intermittent problems, polling-based systems are no longer able to deliver. Sniffer and probe-based systems are similarly plagued with problems making them either too expensive due to upfront capital costs, or require highly skilled personnel to make effective use of the vast amounts of data which is extracted.

Moreover, Application management systems treat the network as a cloud and can only determine application performance by inserting data at the source and measuring the output at the destination. They, however, cannot determine if the application related problem is caused by an application or is a result of the underlying network. Devoid of visibility into the Layer 3 routing protocols, it is extremely difficult to determine if the network is at the root cause of the problem.

Route Analytics fills the gap in existing management tools by providing visibility into the IP cloud. It has the unique ability to analyze routing related issues and can assist in correlating application problems to network management data. Route Analytics technology offers wide-ranging benefits from the ability to detect underlying network faults to its inherently efficient cost structure. IP Route Analytics is becoming a necessary element for dynamic mission critical networks and offers an attractive ROI.