

Managing the “Cloud” in Cloud Computing with Route Analytics



Packet Design

Executive Summary

The latest evolution in enterprise IT outsourcing, cloud computing leverages the ubiquity of the Internet, the flexibility of server virtualization, and the massive scale of today's data centers to provide low-cost IT infrastructure as a network-based service. Though cloud computing is still in the early stages of adoption, enterprises are rightly concerned with how to manage infrastructure that resides on the Internet or shared service provider networks. But while much industry attention has been paid to systems, applications, storage and security issues, relatively little has been directed to the network management challenges of cloud computing. Cloud computing's placement of critical infrastructure components outside traditional network boundaries greatly increases enterprise IT dependence on the complex interactions between enterprise and public IP networks.

To ensure reliable application delivery, network managers need visibility into the routing and traffic dynamics spanning enterprise and Internet domains. But traditional network management tools are incapable of providing this sort of insight. Route analytics, a network management technology adopted and deployed by hundreds of the world's leading enterprises, service providers and government agencies, fills this visibility gap by providing routing and traffic monitoring, analysis and planning for both internal and external IP networks. Routing visibility is critical to ensuring the success of cloud computing deployments, Route analytics can provide this visibility and enhance network management best practices.

The Importance of IP Routing to Cloud Computing Deployments

At the most fundamental level, IP routing is important to cloud computing because cloud computing resources are reached via a complex combination of enterprise and Internet IP routed networks. But IP routing is inherently difficult to understand due to the way it dynamically and unpredictably changes traffic paths. For example, within an enterprise network, redundant links between various nodes create the possibility of many alternate paths between any point A and point B on the network. The role of IP routing protocols such as OSPF, EIGRP and IS-IS is to control which paths traffic flows take between points on the network at any given moment, and dynamically alter them based on the changing states of routers and links due to failures, routine maintenance and planned network changes. Since routing protocols make these decisions with only occasional configuration input from engineers; since the number of possible routing states for a large, redundant network consisting of hundreds of links can be in the thousands or tens of thousands; and since routing can change in milliseconds, it's very challenging to nearly impossible for engineers to tell what's happening.

Internet routing is even more complex, with thousands of service provider and enterprise IP network domains called "Autonomous Systems" (AS) acting as potential hops for hundreds of thousands of network addresses and myriad AS_PATHs. The combination of internal routing and Internet routing adds more wrinkles, since any enterprise that implements critical outsourced applications or infrastructure will have redundant BGP protocol-based links to multiple Internet service providers (ISPs). Selection of a primary or secondary Internet "exit router" (connecting to one of these ISPs) for any given traffic is made by OSPF/EIGRP/IS-IS protocols, but is also influenced by "Local Preference" configuration attribute options in BGP. The AS_PATH from the enterprise is of course influenced by the exit router and neighbor AS that it connects to, but also by dynamic changes in the Internet that affect both the availability of routed networks and the AS_PATH to get to them. For example, the failure of a peering between ISPs can cause many

Managing Cloud Computing

AS_PATHS to shift, while a misconfiguration can withdraw an advertised network from the Internet routing table or mistakenly advertise it in the wrong AS. The combination of redundant enterprise networks, redundant Internet peerings and the Internet's vast routing makes it that much harder to correctly perceive, let alone manage, IP routing behavior.

Why does it matter that IP routing is difficult to understand? Because routing problems can exert an outsized impact on application delivery. Some common routing issues and their impact include:

- A flapping route (a condition when a network address is advertised and withdrawn repeatedly in succession) can cause packet loss and application downtime or slowdowns due to the temporary and intermittent lack of availability of the route to a server farm, user group or cloud computing resource.
- Loss of a path from a data center location to an Internet exit router can cause a service outage, or reduce redundancy so that, even though the primary exit router is still working, the network becomes more vulnerable to a serious outage.
- A change in a path that greatly increases the number of hops can cause increased packet latency and slower application response times.
- Overall instability and high rates of change in the routing plane can cause the network to react slowly or unpredictably to network failures.
- Misconfigured routing can cause an expensive backup link to go unused when a primary link fails.

Because of the complexities of routing, it is quite easy to make configuration errors, causing application traffic to behave in a suboptimal manner which can lead to poor performance or even application downtime. Existing change-management processes and tools are mostly focused on local, device-level issues such as ensuring the right version of OS and correct command syntax. Since one routing change can have a network-wide effect, it's very possible to make the "right" configuration decision locally on a device and end up with the "wrong" behavior in the network as a whole.

The Limitations of Traditional Network Management Tools

Traditional network management tools gather information by "polling" a vast number of different devices in the network, then correlating various point-specific data to infer service conditions. The key mechanism for doing this is the Simple Network Management Protocol (SNMP), which polls information from routers, switches, security devices and servers and their interfaces. The main data gathered include:

- Device health: uptime, current status, CPU, 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 with traffic can have a direct impact on application delivery – SNMP wasn't built to monitor something as dynamic as IP routing. SNMP's key limitation is that it is too

Managing Cloud Computing

periodic: polling cycles from 30 seconds to several minutes long 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—Network-Wide Routing and Traffic Visibility

While traditional network monitoring approaches can't provide visibility into critical routing behavior, organizations grappling with the challenges of managing cloud computing deployments have an answer in route analytics technology.

Route analytics technology works by utilizing the network's live routing protocols as a unique source of network management intelligence that complements traditional SNMP data. The 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. The route analytics device itself is passive, never advertising itself as a place to send traffic, and 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. The network-wide routing topology visualization and complete details of routing changes provide the basis for many useful analyses of network behavior.

When route analytics information is combined with Netflow traffic-flow data, its full power emerges. By collecting traffic flows from the ingress points of traffic at the network edge (data centers, Internet peerings, major WAN links) and mapping them to the precise routes they traverse through the network, route analytics produces an integrated, always accurate map of all routing and traffic from all major traffic sources for the entire network.

New Network Management Best Practices with Route Analytics

Route analytics can be used to establish new monitoring, troubleshooting and planning best practices to help ensure the availability and performance of applications delivered using cloud computing and other resources:

Routing Monitoring Best Practices

- Monitoring critical subnets for routing reachability. Route analytics can monitor the availability and stability of important individual subnets (such as those hosting server farms in internal data centers) or subnets on the Internet (such as those hosting cloud computing resources). Alerts can be sent in real time based on any downtime or flapping of these routes.
- Monitoring critical paths between important application delivery infrastructure components. If paths between important points in the network are monitored for changes, engineers can investigate to ensure that no application or service impact occurs as a result. Some examples of critical paths that are relevant to cloud computing deployments are:

Managing Cloud Computing

- Paths between internal data center routers and Internet exit routers
 - Paths between multiple internal data center routers
 - Monitoring for AS_PATH redundancy levels to the cloud computing network(s)
 - Paths to important user sites, even those reached via outsourced MPLS VPN WANs
- Monitoring for high levels of routing “churn” that can signal potentially harmful instability in the network as a whole
 - Software-related link state changes, such as link flapping caused by routing protocol misconfigurations, 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 turning on overhead-inducing Netflow export on all the interfaces in the network

Enhanced Troubleshooting Best Practices

Route analytics makes it much easier for network operations to not only detect problematic conditions in the network, but to troubleshoot those problems much faster. For example, when troubleshooting a current application problem, operators can examine a variety of potential causes that aren't visible to traditional network management tools. The following steps illustrate an example analysis:

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

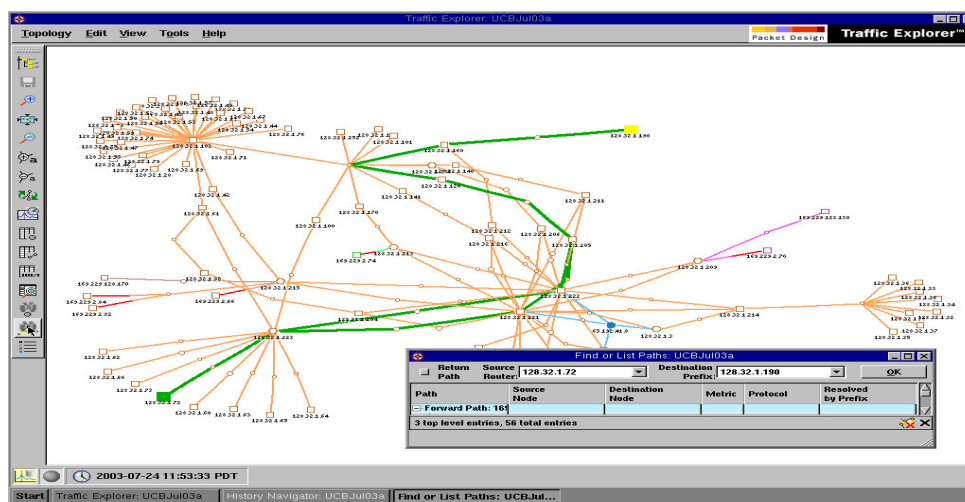


Figure 1: Route analytics allows easy identification and verification of the status of the application or service path through the routed network.

Managing Cloud Computing

- c. Examine the immediately preceding history for the problem (and find other possible root causes) by "rewinding" the route analytics history to the relevant timeframe and seeing the behavior of the entire network at that moment. Operators can look at routing events, select a time-range (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 routes, evidenced by the rapid adding and dropping of the same network addresses over and over. The full event list shows that this occurred for more than an hour.

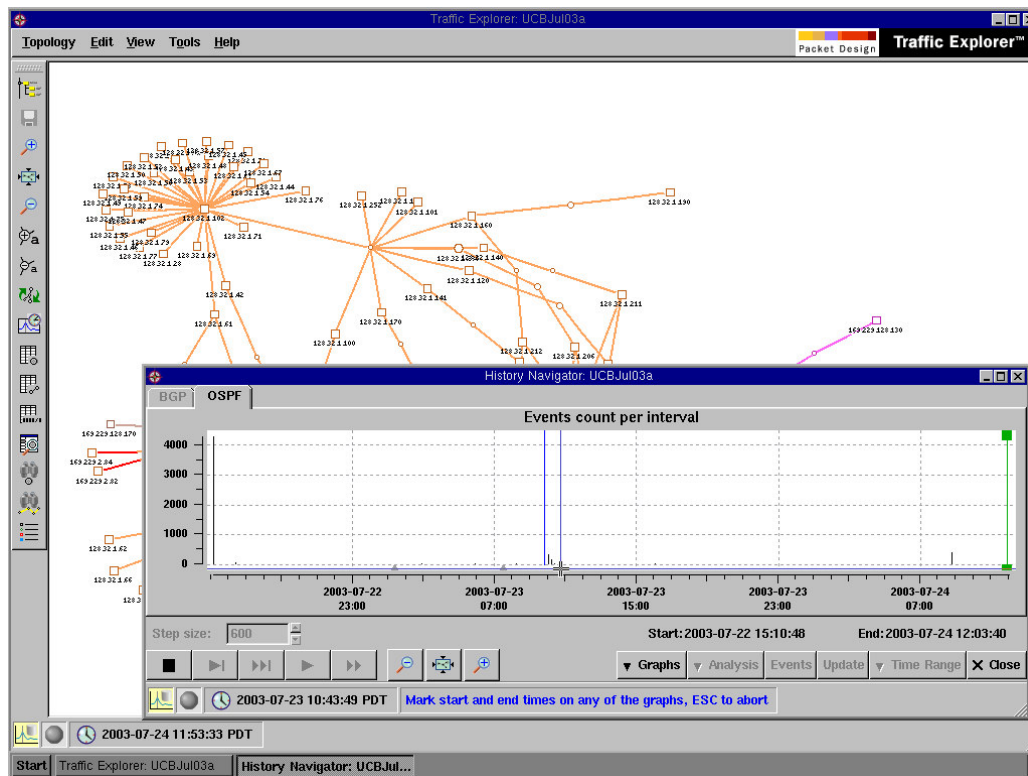
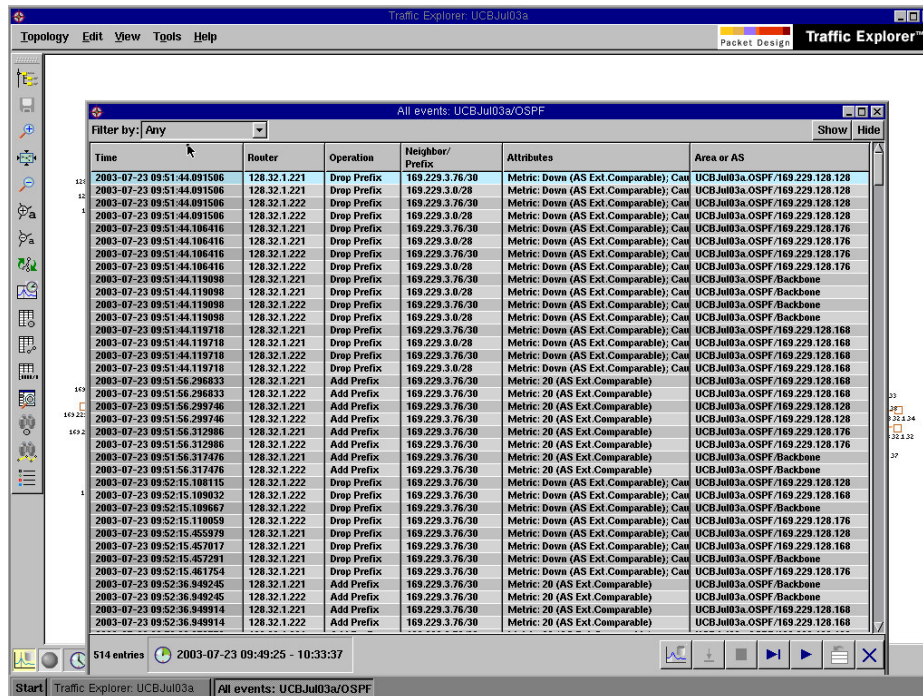


Figure 2: Operators can look at a range of time before the current problem started.

Managing Cloud Computing



The screenshot shows the Traffic Explorer interface with a table of routing events. The table has columns for Time, Router, Operation, Neighbor/Prefix, Attributes, and Area or AS. The events are filtered by 'Any' and show a sequence of 'Drop Prefix' and 'Add Prefix' operations for various IP ranges and metrics.

Time	Router	Operation	Neighbor/Prefix	Attributes	Area or AS
2003-07-23 09:51:44.091506	128.32.1.221	Drop Prefix	169.229.3.76/30	Metric: Down (AS Ext. Comparable); Cau	UCBJul03a.OSPF/169.229.128.128
2003-07-23 09:51:44.091506	128.32.1.221	Drop Prefix	169.229.3.8/28	Metric: Down (AS Ext. Comparable); Cau	UCBJul03a.OSPF/169.229.128.128
2003-07-23 09:51:44.091506	128.32.1.222	Drop Prefix	169.229.3.76/30	Metric: Down (AS Ext. Comparable); Cau	UCBJul03a.OSPF/169.229.128.128
2003-07-23 09:51:44.091506	128.32.1.222	Drop Prefix	169.229.3.8/28	Metric: Down (AS Ext. Comparable); Cau	UCBJul03a.OSPF/169.229.128.128
2003-07-23 09:51:44.106416	128.32.1.221	Drop Prefix	169.229.3.76/30	Metric: Down (AS Ext. Comparable); Cau	UCBJul03a.OSPF/169.229.128.176
2003-07-23 09:51:44.106416	128.32.1.221	Drop Prefix	169.229.3.8/28	Metric: Down (AS Ext. Comparable); Cau	UCBJul03a.OSPF/169.229.128.176
2003-07-23 09:51:44.106416	128.32.1.222	Drop Prefix	169.229.3.76/30	Metric: Down (AS Ext. Comparable); Cau	UCBJul03a.OSPF/169.229.128.176
2003-07-23 09:51:44.106416	128.32.1.222	Drop Prefix	169.229.3.8/28	Metric: Down (AS Ext. Comparable); Cau	UCBJul03a.OSPF/169.229.128.176
2003-07-23 09:51:44.119098	128.32.1.221	Drop Prefix	169.229.3.76/30	Metric: Down (AS Ext. Comparable); Cau	UCBJul03a.OSPF.Backbone
2003-07-23 09:51:44.119098	128.32.1.221	Drop Prefix	169.229.3.8/28	Metric: Down (AS Ext. Comparable); Cau	UCBJul03a.OSPF.Backbone
2003-07-23 09:51:44.119098	128.32.1.222	Drop Prefix	169.229.3.76/30	Metric: Down (AS Ext. Comparable); Cau	UCBJul03a.OSPF.Backbone
2003-07-23 09:51:44.119098	128.32.1.222	Drop Prefix	169.229.3.8/28	Metric: Down (AS Ext. Comparable); Cau	UCBJul03a.OSPF.Backbone
2003-07-23 09:51:44.119718	128.32.1.222	Drop Prefix	169.229.3.76/30	Metric: Down (AS Ext. Comparable); Cau	UCBJul03a.OSPF/169.229.128.168
2003-07-23 09:51:44.119718	128.32.1.222	Drop Prefix	169.229.3.8/28	Metric: Down (AS Ext. Comparable); Cau	UCBJul03a.OSPF/169.229.128.168
2003-07-23 09:51:44.119718	128.32.1.222	Drop Prefix	169.229.3.76/30	Metric: Down (AS Ext. Comparable); Cau	UCBJul03a.OSPF/169.229.128.168
2003-07-23 09:51:44.119718	128.32.1.222	Drop Prefix	169.229.3.8/28	Metric: Down (AS Ext. Comparable); Cau	UCBJul03a.OSPF/169.229.128.168
2003-07-23 09:51:56.298833	128.32.1.221	Add Prefix	169.229.3.76/30	Metric: 20 (AS Ext. Comparable)	UCBJul03a.OSPF/169.229.128.168
2003-07-23 09:51:56.298833	128.32.1.222	Add Prefix	169.229.3.76/30	Metric: 20 (AS Ext. Comparable)	UCBJul03a.OSPF/169.229.128.168
2003-07-23 09:51:56.298746	128.32.1.221	Add Prefix	169.229.3.76/30	Metric: 20 (AS Ext. Comparable)	UCBJul03a.OSPF/169.229.128.128
2003-07-23 09:51:56.298746	128.32.1.222	Add Prefix	169.229.3.76/30	Metric: 20 (AS Ext. Comparable)	UCBJul03a.OSPF/169.229.128.128
2003-07-23 09:51:56.298746	128.32.1.221	Add Prefix	169.229.3.76/30	Metric: 20 (AS Ext. Comparable)	UCBJul03a.OSPF/169.229.128.128
2003-07-23 09:51:56.298746	128.32.1.222	Add Prefix	169.229.3.76/30	Metric: 20 (AS Ext. Comparable)	UCBJul03a.OSPF/169.229.128.128
2003-07-23 09:51:56.312986	128.32.1.221	Add Prefix	169.229.3.76/30	Metric: 20 (AS Ext. Comparable)	UCBJul03a.OSPF/169.229.128.176
2003-07-23 09:51:56.312986	128.32.1.222	Add Prefix	169.229.3.76/30	Metric: 20 (AS Ext. Comparable)	UCBJul03a.OSPF/169.229.128.176
2003-07-23 09:51:56.312986	128.32.1.221	Add Prefix	169.229.3.76/30	Metric: 20 (AS Ext. Comparable)	UCBJul03a.OSPF.Backbone
2003-07-23 09:51:56.312986	128.32.1.222	Add Prefix	169.229.3.76/30	Metric: 20 (AS Ext. Comparable)	UCBJul03a.OSPF.Backbone
2003-07-23 09:52:15.109115	128.32.1.222	Drop Prefix	169.229.3.76/30	Metric: Down (AS Ext. Comparable); Cau	UCBJul03a.OSPF/169.229.128.128
2003-07-23 09:52:15.109115	128.32.1.222	Drop Prefix	169.229.3.76/30	Metric: Down (AS Ext. Comparable); Cau	UCBJul03a.OSPF/169.229.128.168
2003-07-23 09:52:15.109867	128.32.1.222	Drop Prefix	169.229.3.76/30	Metric: Down (AS Ext. Comparable); Cau	UCBJul03a.OSPF.Backbone
2003-07-23 09:52:15.119959	128.32.1.222	Drop Prefix	169.229.3.76/30	Metric: Down (AS Ext. Comparable); Cau	UCBJul03a.OSPF/169.229.128.176
2003-07-23 09:52:15.455879	128.32.1.221	Drop Prefix	169.229.3.76/30	Metric: Down (AS Ext. Comparable); Cau	UCBJul03a.OSPF/169.229.128.128
2003-07-23 09:52:15.457017	128.32.1.221	Drop Prefix	169.229.3.76/30	Metric: Down (AS Ext. Comparable); Cau	UCBJul03a.OSPF/169.229.128.168
2003-07-23 09:52:15.457291	128.32.1.221	Drop Prefix	169.229.3.76/30	Metric: Down (AS Ext. Comparable); Cau	UCBJul03a.OSPF.Backbone
2003-07-23 09:52:15.461754	128.32.1.221	Drop Prefix	169.229.3.76/30	Metric: Down (AS Ext. Comparable); Cau	UCBJul03a.OSPF/169.229.128.176
2003-07-23 09:52:36.949245	128.32.1.221	Add Prefix	169.229.3.76/30	Metric: 20 (AS Ext. Comparable)	UCBJul03a.OSPF.Backbone
2003-07-23 09:52:36.949245	128.32.1.222	Add Prefix	169.229.3.76/30	Metric: 20 (AS Ext. Comparable)	UCBJul03a.OSPF.Backbone
2003-07-23 09:52:36.949914	128.32.1.221	Add Prefix	169.229.3.76/30	Metric: 20 (AS Ext. Comparable)	UCBJul03a.OSPF/169.229.128.168
2003-07-23 09:52:36.949914	128.32.1.222	Add Prefix	169.229.3.76/30	Metric: 20 (AS Ext. Comparable)	UCBJul03a.OSPF/169.229.128.168

Figure 3: Route analytics can analyze and display full details of routing behavior from past time frames, allowing engineers to gain insight into the root causes of application or service problems.

By providing network-wide visualization and analysis of routing and traffic conditions, route analytics helps operators and engineers to quickly localize the part of the network to troubleshoot. Along with its database of network behavior history, this helps network operations departments save a tremendous amount of personnel time, leading to lower costs in the face of growing demands. Ultimately, by speeding monitoring and troubleshooting processes, route analytics contributes to higher application availability and performance, with tangible top- and bottom-line results.

More Accurate Change Management and Planning Processes

Beyond monitoring and operations improvements, there are many benefits for network planners. Engineers can now ensure that critical IP networks are adequately resourced to deliver a complex, changing matrix of application and service traffic at various service levels. For example, engineers can model how deployment of cloud computing resources would affect traffic across the network, including the impact on BGP-based Internet peerings. Route analytics calculates and simulates the network-wide change in routing and traffic not based on an abstract model, but on the traffic and routing matrix as it actually exists in the network. The new traffic and routing picture and accompanying analysis reports show whether any congestion will result. 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, along with real-time monitoring, helps network managers prevent mistakes and design errors and keeps them from spending time on needless troubleshooting.

Managing Cloud Computing

Keeping Service Providers Accountable

Another major benefit of route analytics' visibility for cloud computing deployments is to help keep service providers more accountable for the quality of the connectivity they provide to enterprise customers. With route analytics, operations departments can detect when a secondary ISP cannot route traffic to the cloud computing site, even if the link to that ISP is "up". This empowers network managers to go to their ISPs with specific fault information, and demand that they restore Layer 3 service. Routing instabilities and other anomalous behavior involving cloud computing routes can also be detected and analyzed to monitor service provider network quality over time.

Conclusion

Sound management of cloud computing deployments should include a strategy to contain the risk that increased network complexity poses to application delivery. Route analytics provides the visibility to enhance network management best practices, keep service providers accountable, and reduce risk and operations costs while helping to ensure the success of application delivery across an increasingly distributed IT infrastructure.

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