

Proactive Routing Health Audits with Route Analytics



Packet Design



The Mandate and Challenge of Proactive Network Management

The growing volume, complexity and sensitivity of IP application and service traffic is driving a wedge between what IT organizations know they should be doing and what they seem to have time to do. If asked, any network manager would agree that proactive network management measures are increasingly important. Yet, those same managers would also acknowledge the reality that they live in a world squeezed between dropping staff levels and rising customer demands. At the end of the day, the vast majority of network engineers' time is spent rushing from fire to fire, just trying to keep up. Proactive management seems increasingly difficult to contemplate as a regular part of the network management regimen.

Route Analytics offers a unique way to gain and maintain a proactive network management stance, by leveraging automatically recorded routing and traffic data to provide an always-accurate and historically searchable record of all changes in network routing and traffic, along with easy to run proactive auditing tools that help engineers to discover current and potential network health problems. Equipped with route analytics' network-wide understanding of logical network operations, engineers can anticipate and prevent more fires, as well as respond more rapidly to problems as they emerge in real-time.

Hidden Causes of Network Problems

There are countless real-world examples of application and service problems stemming from ignorance of the way the IP network is actually configured and operating:

- Logical network misconfigurations: A top software manufacturer's two adjacent campuses were exchanging traffic via a low-speed WAN link due to a misconfiguration, resulting in degraded application performance. A leading pharmaceutical company discovered that a manufacturing site's critical control data was being routed through another continent, eating up expensive trans-oceanic bandwidth and threatening manufacturing control visibility.
- Compromised redundancy: A marketing firm paid for an expensive backup WAN link to a site, only to discover when the primary link failed that the backup wasn't correctly architected to carry the traffic.
- Security breaches: A government agency was blind to a backdoor into its network through a contractor's network.
- Loss of application data: A public utility lost critical connectivity to its power grid control data due to a routing misconfiguration that was seen only when a routine maintenance operation caused control data to be lost.
- Degraded services: A service provider failed to detect the root cause - routing instabilities - of weeks of intermittent service outages at a customer site.

The common thread among all these examples is that the problems involved logical network configurations that couldn't be perceived by traditional network management tools because they weren't directly related to the status of individual devices. Traditional device management and end-to-



end application performance management solutions, while necessary, provide no insight into the logical operation of traffic and routing. As a result, the IT department often has no visibility into the causes of application degradations.

Route analytics is a network management technology that meets this critical visibility need by monitoring the routing protocols that control the logical operation of the network. Furthermore, route analytics offers proactive auditing of an entire network's routing operation that can alert network managers of potential problems before they occur.

How Routing Controls the Logical Operation of the Network

If the purpose of an IP network is to deliver traffic from point A to point B, then routing is simply the process of moving traffic from A across a particular path through multiple links and routers to get to B. While that process seems simple, the choice of which path to use for any given set of traffic transiting the network is not so simple, and that's where routing protocols come into play. Routing protocols are best thought of as a combination of software and signals used to calculate and communicate the best network paths for successful traffic delivery. The software runs on all the routers in the network, and the signals are passed between all the routers on the network.

For example, the OSPF routing protocol works by having all the routers signal each other with information on which network addresses they can reach, then having all routers execute the same software program to simultaneously calculate the best paths from any point A to any point B in the network. Once this process is complete, all routers have a uniform understanding of how to route traffic.

Of course, this process doesn't just happen once. Every time things change, which they often do, the process repeats to keep all routers abreast of the best traffic paths and thereby allow the network to fulfill its purpose. Some examples of changes that cause the routing protocol process to update itself across the network are:

- Loss of a network link (such as an Ethernet network), causing all the network addresses accessible via that link to become unreachable
- Loss of a link between routers causing previously valid paths to become invalid, requiring a recalculation of traffic paths
- Addition of new network links or network addresses, requiring a recalculation of best paths
- A soft or hard reset of a router, or the downing of a router for maintenance or due to a failure, affecting multiple network links, network addresses and paths
- Mistakes in configuring the routing protocol software programs or bugs in the routing software, causing misinformation to be passed to other routers, which in turn causes logical breakdowns in routing that affect all aspects of the routing protocol process

Aside from some configuration input from users, the routing protocol process is fully automated, which is great for efficiency but bad for visibility. The vast majority of IT departments have no practical visibility into the logical operation of their networks.



Acute Visibility Need: Large, Complex Networks

While all routed IP networks operate automatically, the lack of network operation visibility is a particularly critical issue for complex, redundant networks built to deliver sensitive traffic with high availability and resiliency. Such networks offer a multitude of potential paths from any point A to point B. This high degree of variability, combined with invisible, automated routing protocol processes, makes understanding the network's behavior and its effect on application performance nearly impossible. Organizations that typically have such networks include:

- Financial services, banking and insurance
- Pharmaceuticals and other information-intensive manufacturers
- Government, public utilities, and military agencies
- Service providers, content providers, cable MSOs and wireless operators

Route Analytics: The Whole Picture of Logical Network Operations

Route analytics is a network management technology that monitors and records the routing protocols' signals and mimics routing software to compute paths, obtaining the exact same understanding of a network's traffic paths that the routers themselves have. Since route analytics receives all the same updates as the network's routers, it maintains complete, real-time fidelity to the true state of the network's traffic routing. In addition, route analytics can collect Netflow data and map all the traffic flows over the actual paths they are traversing. This combination of flows and paths arrives at a highly accurate understanding of the actual state of logical network operations. The continuous recording of all routing path changes and all traffic flows ensures a completely accurate forensic history for precise troubleshooting and faster problem resolution. Given its high fidelity to the actual state of the network, route analytics can also be used to model changes and observe their effects on the network, the links, the applications and the Classes of Service. Route analytics meets the need for visibility into logical network behavior and its role in application performance.

Proactive Routing Health Audits

Route analytics can utilize its recorded model of the network's actual routing to perform proactive, automated analyses of an entire network's routing health at the click of a mouse. A route analytics audit can find a variety of potential problems that may already be affecting application and service delivery, or would in the case of changes in network state. Examples of routing audit information that engineers can gain from a proactive route analytics audit include:

- Comprehensive reports on all paths through the network: The sheer amount of changes over time in a large, complex network can sometimes cause routers to actually lose reachability to some parts of the network. Route analytics audits can list every single routed path through the network, and allow network engineers to identify reachability issues before they become a problem with application delivery. Routing managers also can find links that have been assumed to have been decommissioned, but that due to administrative errors, are still active and possibly costing the organization high WAN fees. Figure 1 shows an example of a list of all paths discovered by route analytics:

Path Reports: ucbJan505/OSPF

All Paths by Source: ucbJan505/OSPF

Filter by: Any

Source Router	Reachable Destinations	Paths	Hops	Metric
169.229.2.66	None	NA	NA	NA
169.229.2.82	None	NA	NA	NA
169.229.2.84	None	NA	NA	NA
128.32.1.1	77	1 - 16	3 - 10	101 - 7786
128.32.1.3	77	1 - 8	3 - 10	100 - 7785
128.32.1.4	77	1 - 8	3 - 10	2 - 7687
128.32.1.11	77	1 - 16	3 - 12	101 - 7796
128.32.1.28	77	1 - 16	3 - 14	1001 - 8796
128.32.1.31	77	1 - 16	3 - 12	2 - 7697
128.32.1.32	77	1 - 16	3 - 12	101 - 7796
128.32.1.33	77	1 - 16	3 - 12	101 - 7796
128.32.1.34	77	1 - 16	3 - 12	2 - 7697
128.32.1.35	77	1 - 16	3 - 12	101 - 7796
128.32.1.36	77	1 - 16	3 - 12	2 - 7697
128.32.1.37	77	1 - 16	3 - 12	101 - 7796
128.32.1.38	77	1 - 16	3 - 12	101 - 7796
128.32.1.42	77	1 - 16	2 - 12	1000 - 8696
128.32.1.43	77	1 - 14	2 - 14	6477 - 13952
128.32.1.45	77	1 - 14	2 - 14	6477 - 13952
128.32.1.47	77	1 - 14	2 - 14	6511 - 13986
128.32.1.50	77	1 - 14	2 - 14	6477 - 13952
128.32.1.51	77	1 - 14	2 - 14	65 - 7540
128.32.1.52	77	1 - 14	2 - 14	6477 - 13952
128.32.1.54	77	1 - 14	2 - 14	6477 - 13952
128.32.1.55	77	1 - 14	2 - 14	6477 - 13952
128.32.1.56	77	1 - 14	2 - 14	6477 - 12972

81 entries

2005-01-04 13:56:17 PST

Start | Traffic Explorer: ucbJan505 | Path Reports: ucbJan505/...

Figure 1: A comprehensive list of routed paths helps engineers identify where there are routing black holes in the network that may affect future application or user deployments, and to audit for paths with excessive hop counts or even paths that should not be in service

- Single points of failure and vulnerable points in the routing topology: To ensure application and service delivery, network managers strive to make design their networks with redundant links where critical volumes of traffic flow. Unbeknownst to network engineers though, design and configuration changes that occur over time can often change the routing operation of the network so that backup routes are no longer functioning. Route analytics network health audits examine all links and report on single points of failure which might cause dropped traffic. Route analytics can also find points in the network where a failure would cause shifts to many other traffic routes, or cause some routes to significantly increase their hop count, leading to increased delays in traffic delivery. Figure 2 shows the results of a failure analysis performed on a campus network using route analytics.

Path Reports: ucbJan505/OSPF

Failure Analysis: ucbJan505/OSPF

Filter by: Any

Source Router	Destination Router	Destination Prefix	Original Paths	Original Hops	Original Metric	Worst Link Failure	Worst Metric Change
128.32.1.60	128.32.1.252	128.32.231.0/25	1	7	211	128.32.1.60 -> 169.229.0.200/29	Path not found
128.32.1.60	128.32.1.130	128.32.1.130/32	2	9	122	128.32.1.60 -> 169.229.0.200/29	Path not found
128.32.1.60	128.32.1.35	128.32.1.35/32	2	9	141	128.32.1.60 -> 169.229.0.200/29	Path not found
128.32.1.60	128.32.1.33	128.32.1.33/32	2	9	122	128.32.1.60 -> 169.229.0.200/29	Path not found
128.32.1.60	128.32.1.208	128.32.1.208/32	2	7	42	128.32.1.60 -> 169.229.0.200/29	Path not found
128.32.1.60	128.32.1.11	128.32.1.11/32	2	9	122	128.32.1.60 -> 169.229.0.200/29	Path not found
128.32.1.60	128.32.1.202	128.32.1.202/32	2	7	21	128.32.1.60 -> 169.229.0.200/29	Path not found
128.32.1.60	128.32.1.201	128.32.1.201/32	2	7	21	128.32.1.60 -> 169.229.0.200/29	Path not found
128.32.1.60	128.32.1.200	128.32.1.200/32	1	7	111	128.32.1.60 -> 169.229.0.200/29	Path not found
128.32.1.60	128.32.1.51	128.32.1.51/32	1	8	6697	128.32.1.60 -> 169.229.0.200/29	Path not found
128.32.1.60	128.32.1.57	128.32.1.57/32	1	8	6697	128.32.1.60 -> 169.229.0.200/29	Path not found
128.32.1.60	128.32.1.68	128.32.1.68/32	1	8	6697	128.32.1.60 -> 169.229.0.200/29	Path not found
128.32.1.60	128.32.1.102	128.32.1.102/32	1	7	202	128.32.1.60 -> 169.229.0.200/29	Path not found
128.32.1.60	128.32.1.101	128.32.1.101/32	2	9	122	128.32.1.60 -> 169.229.0.200/29	Path not found
128.32.1.60	128.32.1.222	128.32.1.222/32	1	5	12	128.32.1.60 -> 169.229.0.200/29	Path not found
128.32.1.60	128.32.1.3	128.32.1.3/32	1	7	111	128.32.1.60 -> 169.229.0.200/29	Path not found
128.32.1.60	128.32.1.1	128.32.1.1/32	2	7	112	128.32.1.60 -> 169.229.0.200/29	Path not found
128.32.1.60	128.32.1.28	128.32.1.28/32	2	11	241	128.32.1.60 -> 169.229.0.200/29	Path not found
128.32.1.60	128.32.1.4	66.28.22.85/32	1	7	22	128.32.1.60 -> 169.229.0.200/29	Path not found
128.32.1.60	128.32.1.221	128.32.1.221/32	1	5	12	128.32.1.60 -> 169.229.0.200/29	Path not found
128.32.1.60	128.32.1.209	128.32.1.209/32	2	7	42	128.32.1.60 -> 169.229.0.200/29	Path not found
128.32.1.60	128.32.1.82	128.32.1.82/32	2	9	32	128.32.1.60 -> 169.229.0.200/29	Path not found
128.32.1.60	169.229.0.122	128.32.1.49/32	1	8	6678	128.32.1.60 -> 169.229.0.200/29	Path not found
128.32.1.60	128.32.1.81	128.32.1.81/32	1	8	6678	128.32.1.60 -> 169.229.0.200/29	Path not found
128.32.1.60	128.32.1.79	128.32.1.79/32	1	8	6678	128.32.1.60 -> 169.229.0.200/29	Path not found

6006 entries

2005-01-04 13:56:17 PST

Start Traffic Explorer: ucbJan505 Path Reports: ucbJan505/...

Figure 2: A routing failure analysis identifies weak points in the routing architecture that usually only become apparent when unexpected failures occur.

- Unused links: Without an accurate and comprehensive understanding of the actual routing operations of the entire network, network managers may be underutilizing assets such as links that through misconfigurations aren't being routed over. Route analytics identifies all links in the network that don't have a routed path over them, as show in Figure 3.

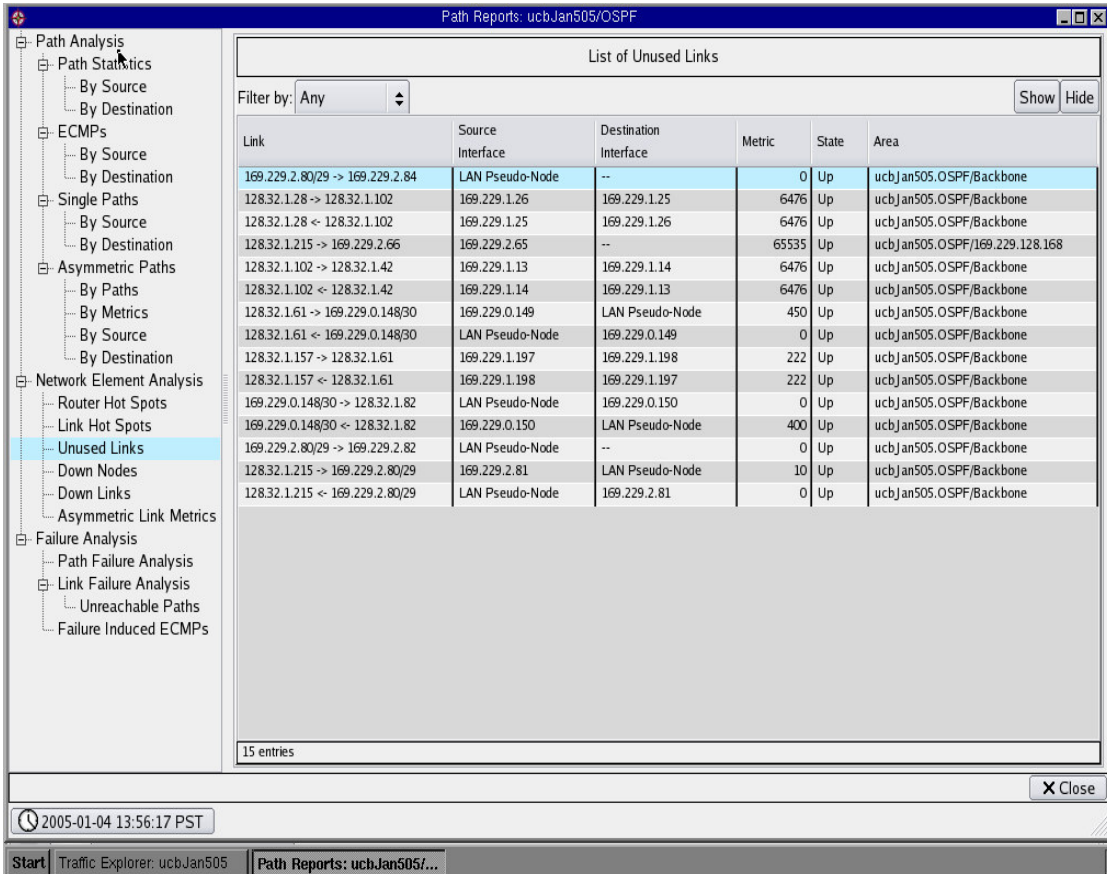


Figure 3: An audit of unused links in this network shows that there links between routers that aren't being utilized actively to route traffic. For some links, this is legitimate since they are only backup links. For others, it may mean that costly resources are being wasted

- Asymmetric routes: Unless there are specific reasons to engineer them, most organizations typically design their networks to use the same routed path through the network in both directions between any source and destination host pair in the network, otherwise as symmetric routes. Asymmetric routes alter this may cause unpredictable application or service behavior. Since large routed networks have so many devices, it is not hard for the network to become misconfigured and permit asymmetric routing operation. With route analytics, engineers can easily find asymmetric routes operating in the network and correct them if they are not compliant with network design policy and established best practices. Figure 4 illustrates an analysis of asymmetric paths.

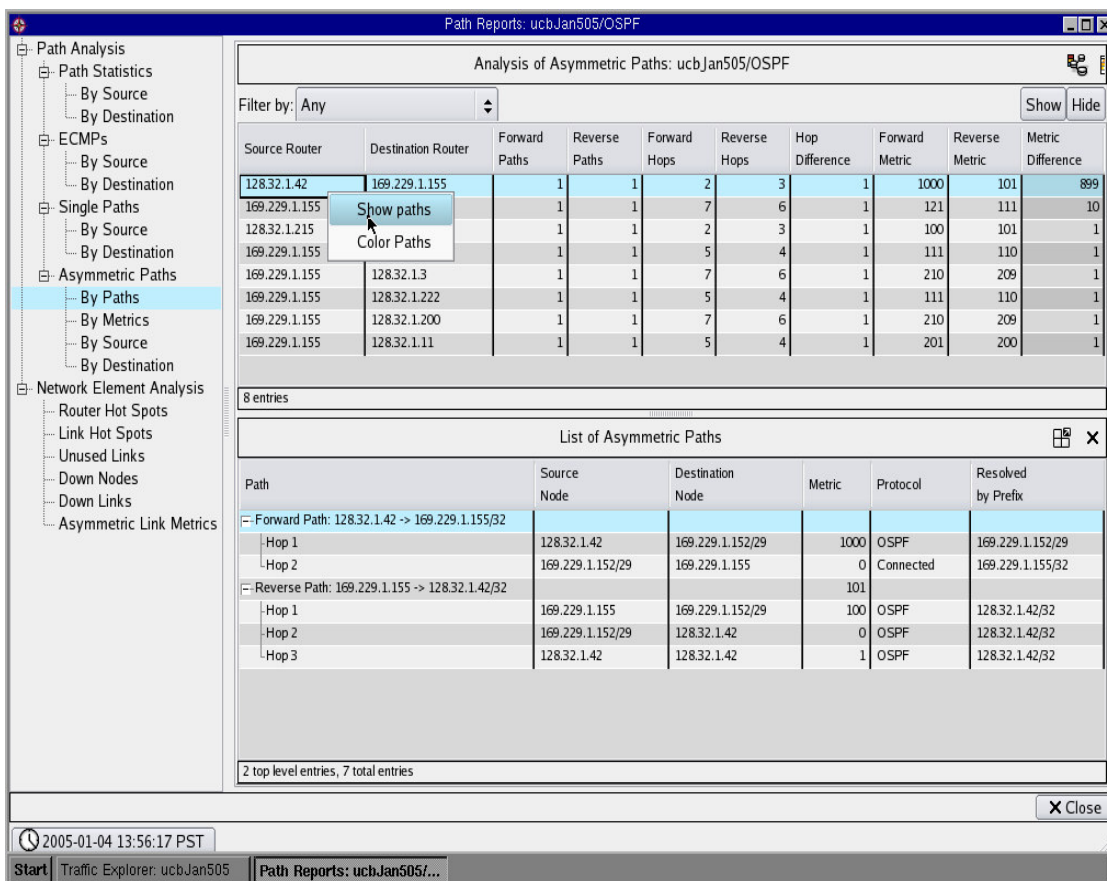


Figure 4: Asymmetric paths can wreak havoc with sensitive applications, such as financial transactions or IP Telephony. Route analytics can identify asymmetric paths so that engineers can either verify their routing architecture or make appropriate corrections

- Equal Cost Multiple Paths (ECMPs): ECMPs are essentially multiple routes between two points in the network, which are often used for the purposes of load balancing in order to ensure that traffic is evenly distributed over multiple backbone links. However, in cases where there are latency-sensitive applications or services such as IP Telephony/VoIP, network managers often prefer to not utilize ECMPs since there may be variabilities in delivery times over different paths in the ECMP which leads to delay-inducing packet reordering when the traffic reaches its destination. Route analytics can identify all ECMPs operating in the network as shown in Figure 5, allowing engineers to make proactive decisions on whether they want to keep them in their active routing topology, or reengineer them.

Source Router	Destination Router	Destination Prefix	Paths	Hops	Metric
128.32.1.215	128.32.1.43	128.32.1.43/32	16	10	6697
128.32.1.215	128.32.1.45	128.32.1.45/32	16	10	6697
128.32.1.215	128.32.1.47	128.32.1.47/32	16	10	6697
128.32.1.215	128.32.1.50	128.32.1.50/32	16	10	6697
128.32.1.215	128.32.1.52	128.32.1.52/32	16	10	6697
128.32.1.215	128.32.1.54	128.32.1.54/32	16	10	6697
128.32.1.215	128.32.1.55	128.32.1.55/32	16	10	6697
128.32.1.215	128.32.1.56	128.32.3.224/27	16	10	7696
128.32.1.215	128.32.1.59	128.32.1.59/32	16	10	6697
128.32.1.215	128.32.1.67	128.32.1.67/32	16	10	6697
128.32.1.215	128.32.1.69	128.32.1.69/32	16	10	6697
128.32.1.215	128.32.1.71	128.32.1.71/32	16	10	6697
128.32.1.215	128.32.1.74	128.32.1.74/32	16	10	6697
128.32.1.215	128.32.1.75	128.32.1.75/32	16	10	6697
128.32.1.215	128.32.1.76	128.32.1.76/32	16	10	6697
128.32.1.215	128.32.1.77	128.32.1.77/32	16	10	6697
128.32.1.215	128.32.1.78	128.32.1.78/32	16	10	6697
128.32.1.215	128.32.1.79	128.32.1.79/32	16	10	6697
128.32.1.215	128.32.1.81	128.32.1.81/32	16	10	6697
128.32.1.215	169.229.0.122	128.32.1.49/32	16	10	6697
128.32.1.215	128.32.1.102	128.32.1.102/32	16	9	221
128.32.1.215	128.32.1.68	128.32.1.68/32	16	10	6716
128.32.1.215	128.32.1.57	128.32.1.57/32	16	10	6716
128.32.1.215	128.32.1.51	128.32.1.51/32	16	10	6716
128.32.1.215	128.32.1.252	128.32.231.0/25	16	9	230
128.32.1.210	128.32.1.43	128.32.1.43/32	16	10	6697
128.32.1.210	128.32.1.45	128.32.1.45/32	16	10	6697

3533 entries

Figure 5: A list of ECMP's in this campus network shows a number of routes with sixteen paths between them.



Conclusion

IT departments are under increasing pressure to help organizations achieve better top- and bottom-line results through applications that automate business processes. To succeed, network managers need to move beyond reactive measures and proactively find potential hot spots in their network before they impact application or service delivery. With route analytics' automated, always-updated understanding of network-wide routing operations, network managers can with a few mouse clicks, move into a proactive stance in their network planning and operations, reducing what would otherwise be unforeseen, time-consuming and service-impacting problems.

Packet Design is the pioneer and industry leader in route analytics. Over 300 global enterprises, government agencies and service providers have deployed Route Explorer and Traffic Explorer routing and traffic analysis solutions. For more information on Packet Design solutions, please visit our website at <http://www.packetdesign.com> or email us at info@packetdesign.com.