

Ensuring SCADA Network Continuity with Route Analytics



Packet Design



The Mandate of Utility Grid Uptime

In the world of "five nines" reliability mandated for electric utilities, network continuity is all-important. In the wake of the disastrous Northeast Blackout of August 2003, when 40 million people in the U.S. lost electric power and outage-related financial losses topped \$6 billion, new reliability standards, driven by the North American Electric Reliability Council (NERC), were put in place that impacted every utility company in America. IT managers responsible for the IP network infrastructure that supports Supervisory Control and Data Acquisition (SCADA) applications, which monitor power grids, are now expected to maintain the highest level of network uptime to meet SCADA availability and performance levels. While power utilities have been under special scrutiny, IT managers responsible for other utility and control grids such as water, waste and even traffic engineering systems are increasingly looking to ensure network and application continuity.

The sheer size and complexity of utility grid IP networks means that traditional network management systems aren't up to the task. SNMP (Simple Network Management Protocol)-based solutions, which focus on device status, can't detect logical network conditions such as routing failures and transient traffic congestion problems that can be just as devastating as hardware failures to application availability and performance.

This white paper provides an overview of the SCADA monitoring and management challenge, explains why large, complex IP networks need insight into their networks' "logical operations", and introduces route analytics technology, an essential part of the network management toolkit for ensuring real-time uptime monitoring and faster troubleshooting, strengthening change management processes, and providing the foresight to prepare for network continuity and disaster recovery challenges.

Matching Information Network Reliability to Utility Grid Reliability

Achieving "five nines" isn't just about keeping a utility grid operational 99.999 percent of the time – it's also about making sure the IP networks that pass along critical information about the state of that grid can meet a comparable level of reliability. According to one electric utility network engineer, "In the northeast blackout, a misconfiguration led to a management systems outage that coincided with an electrical grid issue that couldn't be addressed because of lack of visibility into the system." "Ultimately that cost our economy billions."

SCADA is the life blood of any utility, providing control of generation and distribution of power or other resources, plus insight into any parameters configured into the utility grid itself. Large SCADA systems can gather tens of thousands of measurements per second from asynchronous data control devices known as RTUs (remote terminal units) dispersed throughout a utility's territory. Those measurements – e.g., the voltage level on a given line, the current at a specific location – are passed over communications links such as microwave links, leased phone lines and other channels to an RTU "master" residing on internal SCADA IP networks. The RTU master is a combined computing platform and database that performs a variety of calculations and presents the data in graphical form to grid operators who can do monitoring, analysis and planning.

Of course, the voluminous data from the SCADA RTUs, accurate and up-to-the-minute as they are, are only useful if they're accessible. If there is a failure of any sort in the SCADA IP network itself, the utility may be left with a disastrous loss of management visibility into the grid.

The Challenge of Complex IP Networks

Large, complex IP networks present a network management challenge that is not met by traditional network management solutions and technologies. The widely-used traditional SNMP-based network management tools deployed by most utilities provide only part of the answer: they can show whether a device is up or down or a specific instrumented link was operating, but not whether data is taking the correct path through the network or a particular traffic Class of Service (CoS) is experiencing a spike and becoming congested on a particular link. Achieving the required reliability for the large and complex IP networks that support utility grids means being able to understand logical network operations such as end-to-end IP routing—the paths traversed by network data.

There are countless real-world examples of application and service problems stemming from ignorance of the way large IP network routing and traffic logically operate:

- Logical network misconfigurations: One organization'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 involve the routing logic in the network, rather than 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, IT departments often have no visibility into the root causes of application degradations. For organizations with less critical applications, this lack of visibility may not matter as much, but for utility grids, there is no room for error.

Route Analytics Technology—A Window into IP Networks' Logical Operations

The answer to the need for better insight into the whole network's service delivery lies in a new trend in network management: the combination of router-based traffic-flow measurement and analysis with



route analytics technology. The value of this pairing comes from analyzing the network based not on point devices and interfaces, but on end-to-end traffic flows and the precise paths or routes that those flows travel as they move across the network.

Traffic-flow measurement samples traffic from a particular interface and classifies packet information into “flows” based on source and destination IP address, port number and protocol, and sometimes other, more detailed, criteria. In the past, dedicated hardware probes were required; but since a probe would be needed at every interface, deploying them network-wide would be extremely expensive. Router-based traffic-flow monitoring has existed for years, but became practical only recently when implemented in ASIC-based routers. The most popular traffic-flow monitoring mechanism today is Cisco’s Netflow, while a forthcoming IETF standard called IPFIX will create a vendor-neutral format for traffic-flow collection. In either case, a router samples packets on its interfaces, collects statistics on a per-flow basis, and forwards collected flow data to a server, where it is analyzed. Understanding end-to-end flows provides much greater insight into service delivery than simply collecting generic interface bandwidth statistics via SNMP, because a flow can be correlated to a service. For example, a packet stream from an application server to a user can be correlated to a particular traffic flow based on the source IP address of the server, the destination address of the user, the CoS marking, and possibly TCP or UDP port numbers.

For all its benefits, router-based traffic-flow collection and analysis still generates management traffic overhead, and thus is impractical to turn on at every interface in the network. This leaves IT in the same old visibility bind with regard to network behavior. While network engineers can tell which end devices are exchanging traffic across the network, they still have no idea how specific flows, or all that traffic in aggregate, is traversing the network. As a result, traffic-flow information on its own fails to provide the visibility needed to ensure predictably high performance.

However, when combined with real-time information about network-wide routing state, traffic-flow information becomes extremely powerful. The challenge, unmet until recently, is how to collect all routing-state changes.

Route analytics technology, now in use in many large enterprises, service providers and government agencies, is the answer to understanding the logical operation of IP networks. A route analytics device – typically 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. While the route analytics device itself is passive, never advertising itself as a place to send traffic, it 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 – hence the name “path-based” network management. The network-wide routing topology understanding and the full detail of routing changes provides the basis for many useful analyses of the routing control plane. However, only when this is combined with traffic-flow data does the full power of route analytics information emerge. Collecting all traffic flows and mapping them to the precise routes they traverse over time makes it possible to create an integrated, always accurate topology of all routing and traffic flows for the entire network core. This rich recorded topology combined with analysis tools allows network managers to increase the speed and accuracy of troubleshooting, change management, and network continuity assurance processes.

The Value of Route Analytics for SCADA Assurance

Packet Design's route analytics solutions have been deployed by IT departments responsible for maintaining availability and performance of critical SCADA applications running on large, complex IP networks, including:

- A multi-state electrical power utility
- A county-wide power and water utility serving tens of millions of residents
- A large municipal, IP network-based traffic engineering system

In these examples, the IT departments use Packet Design's IP route analytics and traffic analysis solutions to ensure that the IP network supporting the SCADA application is always available. Route analytics provides value in three major areas for SCADA assurance:

- 1. Stronger Change Management Processes:** Numerous studies have shown that human error and the resulting network misconfigurations are the root cause of many application outages and performance degradations. Many IT organizations have implemented stringent change management processes that seek to ensure that devices are configured with the proper versions of software, and that correct configuration syntax is utilized. However, these approaches are insufficient because engineers implementing changes don't have visibility into whether those changes, even if locally "correct", will have the intended results when applied in large, complex IP network environments. Even organizations that test all changes in small lab environment can't be sure of the effect of the changes when rolled out into the production network environment. Some organizations turn for help to extremely expensive and high-maintenance planning tools, yet since these tools utilize abstract models of the network, they aren't operationally accurate enough to be useful on a day-to-day, week-to-week basis for ongoing network engineering and operations. Route analytics provides a uniquely powerful complement to existing change management processes because it creates a completely accurate model of the network based on actual, recorded routing and traffic data from the live network. Engineers can simulate a variety of changes with high accuracy, see exactly how the entire production network's routing and traffic would behave in the case of such changes, and assess impact on SCADA application data. Examples of changes that route analytics can model include:

- Downing a router for maintenance
- Adding new peerings or network addresses into the network
- Moving servers and their corresponding traffic flows to a new data center
- Building out new parts of the network or populating the network with new flow corresponding to forthcoming application deployments

For example, engineers can model a change of high-priority SCADA data in the network due to the deployment of new RTUs that are anticipated to cause an increase in traffic. The simulated new traffic is overlaid not on an abstract model, but on the traffic and routing matrix as it actually exists in the network at a time (e.g., peak usage period) chosen by IT engineers. The new traffic

and routing picture will then show whether the CoS of the new SCADA traffic or any other traffic class is affected on any link in the core IP network. If not, and provided usage assumptions are correct, engineers can proceed with confidence in the rollout, knowing that the network will continue to support existing as well as new requirements.

2. **Dramatically reduced troubleshooting time and increased network service quality.** Today, due to the lack of visibility into logical network operations and a dearth of forensic troubleshooting data, many application problems—particularly intermittent issues—go unsolved, falling into the “No cause found” bucket. These problems often are indicative of real underlying issues in the network, cropping up over and over again and impacting application delivery. Attempts to solve them can consume inordinate amounts of engineering time. With route analytics, engineers can rewind the recorded routing and traffic state to the time the problem occurred and quickly localize the problem domain by tracing the route/path that a particular service traveled across the network. Then they can easily determine whether there was a routing root cause, and, if not, analyze all links to see if a link, the SCADA application traffic or a relevant CoS were breaching their volume thresholds. If there was congestion, further analysis can show whether a routing issue elsewhere caused traffic to shift, or, if additional, unexpected traffic was present, where it originated, its destination and the route that included the problem link. Even if a routing or traffic problem isn’t the root cause, knowing the precise path provides the most accurate possible starting point for examining devices and interfaces involved in servicing the SCADA traffic. Route analytics visibility allows IT to solve a higher percentage of application and network problems and spend less time on each problem. The result is a higher-quality network that delivers better application availability and performance, and reduced or contained costs in the face of increasing end-user demands.
3. **Network Continuity Assurance:** With route analytics, network engineers can leverage analysis tools to get ahead of the curve by understanding vulnerabilities that exist in their network, before they impact application delivery. Route analytics provides insight into:
 - Routing weaknesses: Engineers can easily audit their entire routing topology to find vulnerabilities such as single points of failure or unwanted routing configurations such as Equal Cost Multi-Path (ECMP) routes, asymmetric routes that may be sub-optimal for converged IP services rollouts.
 - Capacity and utilization hot spots. Route analytics allows engineers to see traffic flow utilization trends for all the links in their network, broken out by CoS or even by application groups if they can be classified using Netflow information. Easy-to-use trending reports and utilization projections can identify links or classes of service that will experience congestion if current trends persist.
 - Disaster recovery: Using a highly accurate and self-maintaining model based on the network’s actual routing and traffic, engineers can simulate failure scenarios, ensure that redundancy will work as anticipated, view exactly how network traffic would reflow across the network, and know in advance about any likely service or application delivery impacts.



With route analytics' operationally accurate visibility into vulnerabilities, network managers can prioritize tasks and justify investments to mitigate risk in the network and ensure SCADA uptime and business continuity.

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 in environments where large, complex IP networks create variability in how application traffic can be delivered, network managers need to move beyond traditional network management solutions and understand their networks' logical operations. With route analytics' automated, always-updated understanding of network-wide routing operations, utility network managers can gain the visibility they need to ensure that their SCADA applications will operate with the greatest network service continuity.

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.