

The Riverbed Cascade Solution: Application-Aware Performance Management for Enterprise Networks

Essentials for Visibility, Troubleshooting, and Proactive Assurance

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMATM) White Paper
Prepared for Riverbed

June 2011



*IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING*

The Riverbed Cascade Solution: Application-Aware Performance Management for Enterprise Networks

Table of Contents

- Executive Summary1
- Network Performance Management 20111
- Priorities for Application-Aware Network Performance Management.....2
 - Getting Started – Seeing the Haystack.....2
 - Monitoring - Keeping an Eye on the Haystack3
 - Troubleshooting – Finding the Needle in the Haystack4
 - Collaboration and Lifecycle: Sharing the Results.....5
- The Riverbed Cascade Solution: Built for Visibility5
 - Platform6
 - Monitoring.....6
 - Troubleshooting7
 - Collaboration7
- EMA Perspective.....7
- About Riverbed.....8



The Riverbed Cascade Solution: Application-Aware Performance Management for Enterprise Networks

Executive Summary

While there are many components and technologies that IT must bring together to deliver value to their host organization, two things are clear – first, IT's core value is in providing applications and services, and second, all of them are delivered to users, customers, and partners over some network. Consequently, any strategy for managing the network infrastructure must include a direct understanding of how well the network is playing its role in application and service delivery. This is the realm of Application-aware Network Performance Management (ANPM), and it is essential to understand the primary requirements for such systems in order to adequately evaluate and select tools and products that will best meet the need. This paper reviews the challenges that ANPM solutions are best fit to address, which qualities and capabilities are of most importance, and how one alternative, Riverbed's Cascade Solution, stacks up.

Network Performance Management 2011

We stand at the dawn of a new renaissance – the return to prominence of networking and network management. The relentless pace of growth in applications and services and new technologies, such as server virtualization and Cloud, are culminating to make networks even more critical than before, and the stakes have never been higher. Complex, multi-tiered, and geographically distributed networks are the circulatory system entrusted to deliver applications' lifeblood to businesses and government agencies. While many technology elements must come together to make it all work smoothly, virtually all applications of any value will be delivered over one or more (usually many) network links.

Applications and IT services are essential in most modern business and government settings, and if there is any disruption, regardless of the reason behind it, business processes and operations can rapidly grind to a standstill. Much focus over the years has been placed on availability of network, systems, and applications, but as fault-tolerant and load-balanced architectures have become commonplace to reduce availability risk, the battlefield has evolved to focus on performance. Recent ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) research (*Network Management and the Responsible, Virtualized Cloud*, Feb 2011) indicates that network and application performance management are the top concerns among those who have deployed server virtualization and Cloud services, both in terms of management/monitoring work activities and management tools readiness.

Network and application performance are top concerns for those deploying server virtualization and Cloud services

The cost of IT service downtime has been often calculated, and ranges from thousands to millions of dollars per hour, based on specific business type and model, but the cost of performance degradation is often not well quantified. And yet, degradations in performance are far more commonplace and, collectively, can be equally as damaging to productivity (and profitability) as the occasional true outage. Best practices indicate that organizations should track degradations and formulate/calculate outage "equivalencies" as a means for understanding frequency and impact on organizational productivity.

So how can IT planning and operations teams prepare themselves to best deal with performance monitoring, management, and optimization? One essential element for success lies in establishing visibility into the ebb and flow of applications and services as they traverse the network. Such visibility must provide detailed insight into all activity, meaning all users/customers and all applications/services, as they come together for delivery across all parts of the delivery infrastructure. Performance

The Riverbed Cascade Solution: Application-Aware Performance Management for Enterprise Networks

monitoring technologies thus need to provide both depth as well as breadth in data collection, coupled with abilities to scale, easily accommodate change, and provide both automated analysis as well as facilitated sharing of actionable operations insights and intelligence. Such enhanced, granular visibility opens the door to the second half of the equation: control and optimization.

Application-aware network performance visibility holds great potential for dealing with the performance battle

Rich, application-aware network performance visibility holds great potential for dealing with the performance battle. Clear understanding of exactly what comprises network usage is essential in accelerating troubleshooting, informing capacity planning, and prioritizing actions to address existing or potential performance issues. These efficiency improvements can translate into direct business benefit, through reduced time to identify, diagnose, and correct performance degradations, known as MTTR (Mean Time to Restore/Repair), as well as longer periods of

sustained high performance between degradations, known as MTBF (Mean Time Between Failures/Degradations). With the cost of downtime and degradation commonly running into six and seven figures per hour, even significant investments in advanced ANPM can quickly show several multiples of returns.

Priorities for Application-Aware Network Performance Management

In a world of many options for ANPM tools, technologies, and solutions, it is incumbent upon IT planning and operations teams to first understand which aspects of the infrastructure, applications, and services they provide to their host organization carry the greatest business priority and business value. With that in hand, it is possible to evaluate the value that various products can offer and compare total cost of product ownership with total value delivered to their organization. The next step is to work through the various solutions in the marketplace and figure out which is best aligned to those cost and feature/capability priorities.

In order to assure that a solution can deliver the insights and intelligence required for today's dynamic environments, there are a number of key requirements categories that should be considered. EMA recommends considering the following as a structure for assembling requirements around ANPM:

Getting Started – Seeing the Haystack

ANPM solutions on a large network can create a huge haystack of performance data. None of the potential values of an ANPM approach can be fully realized without first getting one's arms around the big picture. In this case, that translates into several key capabilities at the platform level that are essential for everything else. In particular, an ANPM solution must support the following:

- **Broad instrumentation and data source options** – There are three primary types of ANPM data sources. First, there are flow records, such as NetFlow, Jflow, sFlow, and IPFIX, which document each application or service “session” including details of who talked to whom, using which applications and protocols, for how long, and in what quantity. Second, there are direct/passive packet inspection monitors that look at all of the bits traversing the network and assemble a fine-grained equivalent to flow records, but also adding network-layer health visibility and response-time metrics. And third, there are synthetic test agents, such as IP SLA, which can continuously check the responsiveness and availability of infrastructure elements as well as essential applications

The Riverbed Cascade Solution: Application-Aware Performance Management for Enterprise Networks

and services, regardless of whether or not they actively being used. All three have something to offer, but the bulk of value is built around types one (flow) and two (packets), so support of those two is very important, and additional support for the third (synthetic test) is an added bonus, although it involves a tradeoff in terms of deployment complexity.

- **Ability to discover what's out there** – No one can get far in understanding application performance across the network without being able to recognize and categorize traffic constituencies. This is important from both an initial deployment perspective as well as on an ongoing basis, and should include not just protocols, but the ability to use combinations of information (such as port groupings, URLs, and IP addresses) to uniquely define and track each traffic contributor. Further, the ability to map and organize applications and source/destination locations in ways that parallel the served organizational or Line-of-Business structure are particularly beneficial.
- **Ability to scale** – Moore's Law has a corollary that goes something like this: If you build a bigger pipe, they will fill it. Scale in ANPM solutions is driven in two ways – first by the need to draw performance data from hundreds or thousands of sources, and second by the fact that some of those sources need to keep up with fast growing network technology data rates. In large enterprises, this means gathering flow records from hundreds of thousands of network interfaces and handling the mainstream shift to 10Gbps Ethernet core networks for packet inspection approaches.
- **Ability to easily navigate the data** – All performance monitoring systems, and ANPM is no exception, can accumulate large stores of raw and processed metrics. Cases in large enterprises are not uncommon where flow records are counted in “billions per week” and forensic packet data stores in the tens or hundreds of terabytes. The key challenge presented here is in organizing all of that data and facilitating navigation through these immense haystacks of data in ways that allow operators to efficiently conduct analysis and demonstrate and share the results of their findings and actions.

If you build a bigger pipe,
they will fit it. ANPM
solutions must scale to
mirror the mainstream
shift to 10Gb

Monitoring - Keeping an Eye on the Haystack

Once coverage and a capable platform for ANPM is in place, the next phase of use will be applying the solution to monitoring performance and activity within the network. Traditionally, this has mostly taken the form of long-term, off-line trending and tracking, but increasingly the emphasis is shifting towards recognizing and alerting on performance issues in or near real-time. Specific needs/practices in this regard include:

- **Dashboards** – With the large volumes of data and metrics to be kept track of in an ANPM solution, a strong yet flexible set of operations dashboards are essential. Ideally, these should provide a means for custom definition of views that can be tuned to individual operators' tasks or responsibilities, or aligned with specific subsets of the managed environment or user/customer population. Finally, an ability to organize performance data according to application or service helps tremendously in aligning awareness, visibility, and actions to business priorities.
- **Performance Alerts and Alarms** – All performance management systems will provide some

The Riverbed Cascade Solution: Application-Aware Performance Management for Enterprise Networks

means of raising alerts or alarms when traffic exceeds expectations, but today's ANPM solutions need to do more than that. There should be support for fully automated thresholds, which recognize normal variations and patterns in traffic over time, as well as recognizing that each flow (application/service type and sometimes consumer/user constituency) can be unique in what would be considered normal or abnormal.

- **Advanced Analytics** – The key to moving from reactive operations towards proactive operations requires that an ANPM system tell you not only what has gone wrong, but also what is soon likely to go wrong. This means intelligent analysis of performance metrics to find abnormal patterns of activity and early signs of problematic trends, and sorting out the true indicators from the noise. Additional automated analysis that points out the likely source of and likely solution to a performance issue is a big bonus here.

Troubleshooting – Finding the Needle in the Haystack

When performance issues do arise, and they inevitably will, it matters less whether the source is an escalation from the help desk or a proactive intelligent early warning alert – operators need a means to quickly assess an incident and get to the root cause as quickly as possible. ANPM systems are in an excellent position to help with this process, and following are specific categories of capabilities they should offer in support:

- **Complete Dataset** – This is where the need for depth, in addition to breadth, becomes especially important. Having layered data with various levels of detail is extremely helpfully in localizing potential sources of issues and then diagnosing them properly. The source of the problem often won't turn out be network itself, but something attached to the network or the way in which an application is behaving as it traverses the network. And sometimes, particularly for those most subtle and thorny of performance degradation issues, the ability to get down to and closely inspect packet-level details is the only way to figure out exactly what is going on.
- **Top-down, Smooth Workflows** – Because of the huge volumes of performance data (particularly with packet-based approaches), the most important attribute of an ANPM system for troubleshooting is the ability to present data in a top-down manner, so analysis can start at a macro level and proceed into successive layers of detailed information, in context, and as needed, but only going as deep as is absolutely necessary. This can easily make the difference between recognizing and isolating an issue within a few minutes versus hours of tedious low-level analysis, hunting and pecking through packet traces.
- **Before and After** – As part of both planning and troubleshooting processes, historical views should evidence trending as well as comparisons of performance before and after attempts have been made at remediation. This provides the conclusive results often needed to close out performance problem investigation tasks, particularly if multiple iterations have occurred to try various fixes.
- **Aids for the Heaviest Lifting** – When troubleshooting does take you down to the packet level, it is incumbent upon the ANPM solution to make this as efficient as possible. In particular, automatic filtering based on the context and specific focal points of a top-down investigation

Efficient top-down workflows
can make the difference
between minutes vs. hours
when troubleshooting

The Riverbed Cascade Solution: Application-Aware Performance Management for Enterprise Networks

must be available to help with narrowing analysis to only those packet traces that are relevant. Further, packet traces can be large – the solution must allow analysis to take place where the captures are located and not require sending big files across the network to be analyzed elsewhere. Finally, access to packets needs to be guided and protected, so sensitive payloads are not exposed to unqualified/uncertified personnel.

Collaboration and Lifecycle: Sharing the Results

While ANPM solutions will bring great value and efficiency to network operators, that value is compounded when those views, insights, and data can be shared with other operations and user/customer constituencies. In particular, ANPM answers need to be able to provide the following capabilities in this regard:

- **Flexible Reporting** – The most common means for sharing ANPM data will be by means of publishing Web-based reports. Two capabilities are important here. First is an ability to configure regular, periodic reports to reveal how well the infrastructure is delivering applications and services on a constituent-by-constituent basis, aligned by business priority as well as organizational group. Second, on-demand, ad-hoc reports that outline and show details around a specific topic or resource of interest (often aligned to or reflecting data assembled in a dashboard view) must be easy to configure and painless to update, so cross-functional teams can best leverage them for collaborative troubleshooting.
- **Integration** – By directly integrating an ANPM solution with other management systems, the operational intelligence can be truly maximized. First and foremost, performance-based events/alerts/alarms must be shared with event management platforms entrusted with correlation across multiple technology domains. Second, integration with service desk and service management systems can facilitate escalation and problem tracing processes. And lastly, data integration with inventory and configuration management systems, such as CMDB and CMS solutions, allows the ANPM system to pick up and use the same naming conventions as the rest of the management stack, further improving communications across teams.

The Riverbed Cascade Solution: Built for Visibility

In addition to its well-known WAN optimization solutions, Riverbed offers Cascade, which comprises an enterprise-class ANPM solution. The initial basis of the Cascade solution was the fielded, proven architecture of the Cascade Profiler and Cascade Gateway products for flow record collection and analysis, based on technology assets that Riverbed acquired from Mazu Networks. In 2010, the solution was significantly expanded by addition of the Cascade Pilot and Shark products, which add packet-based ANPM data sources and investigative analysis features, and which joined the product family following Riverbed's acquisition of CACE Technologies. These products have been tightly integrated from both a workflow and data perspective, and the solution thus offers the ability to bring together the two most important forms of ANPM source data, flow records and packet inspection, into a contiguous solution. Functional capabilities are delivered in a scalable, distributed manner that supports a majority of optimal priorities for ANPM solutions as outlined above. Following is an assessment of how it stacks up against each category:

The integration of CACE Technologies into Riverbed's Cascade solution significantly expanded ANPM capabilities and completeness

The Riverbed Cascade Solution: Application-Aware Performance Management for Enterprise Networks

Platform

Recognizing the important complementary nature of the flow and packet data sets, the Cascade solution organizes ANPM data that is collected and analyzed within the system into four categories:

1. Packet – full, sub-second granularity, captured in large volumes, stored on the Shark appliance for relatively short periods of time
2. Microflow – second-by-second metadata derived from packet inspection, used for detailed analysis and as a contextual guide into packet data, also stored on the Shark appliance
3. Flow – minute-by-minute resolution, used to drive dashboards and real-time snapshot reports, kept in the Profiler database
4. Macroflow – 15-minute summarized performance data, used to drive behavioral analysis as well as long-range trending, calculated and used by Cascade Profiler and stored in the database over long periods of time

The Cascade solution is designed for high scale across both ANPM data source types, supporting collection of millions of flows/minute via distributed flow collectors plus 10Gbps speeds for packet-based monitoring. Discovery capabilities include rapid recognition of flows and guided, operator-enabled definition of newly recognized applications and services. The four-tier data architecture and contextual UI navigation facilitates easy traversal through the resulting large performance data stores.

Monitoring

The Cascade solution offers multiple levels of monitoring, with intelligent proactive alerting at the Macroflow level, where Cascade Profiler is deployed, as well as true real-time “Watch” alerts at the Microflow level, where Shark appliances are deployed. Cascade Profiler includes a primary monitoring dashboard interface (see Figure 1), with the ability to track overall performance health on a service-by-service or application-by-application basis, coupled with myriad configurable charts, tables, and graphs to display deeper layers of details regarding flow compositions and locations, accessible directly or via context-sensitive drill-down.

Service Health by Location										
Service Tree ↓	Overall	SAS	Twiki	ERP	Exchange	Oracle	Exchange-ef	Sharepoint	MarcoTest	
Seattle	🚨	🟢	🟢	🚨	🟢	🟢	🟢	🟢	🟢	🟢
San Francisco	🟢	🟢	⚪	🟢	🟡	🟢	🟢	⚪	🟢	🟢
Phoenix	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Philadelphia	🚨	🟢	🟢	🚨	🟢	🟢	🟢	🟢	🟢	🟢
Los Angeles	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Hartford	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Data Center	🟡	🟡	⚪	🟡	🟡	⚪	🟡	⚪	🟡	🟡
Columbus	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Cambridge	🟡	🟡	⚪	🟡	🟡	⚪	🟡	⚪	🟡	🟡
Austin	🟢	🟢	🟢	🟢	🟢	🟢	🟢	⚪	🟢	🟢

Figure 1: Cascade Profiler Service Health Dashboard

The Riverbed Cascade Solution: Application-Aware Performance Management for Enterprise Networks

Troubleshooting

The Cascade solution offers a uniquely powerful, guided workflow paradigm for isolation and troubleshooting of performance issues, made possible via its combination of performance data sources. The four-tier data is used in reverse order to provide top-down, efficient investigative workflows for triaging, isolating, and diagnosing performance issues and problems. Tight integration offers the opportunity to start from service-oriented dashboards, move down through successive layers of differentiated performance information in context, and if necessary launch packet-level analysis on microflow using Cascade Pilot and view packet-level information in Wireshark, the hugely popular network protocol analyzer. The consistent use of context in navigation brings in details directly focused on the element, address, or application of interest.

Deep packet analysis is applied against microflow data, enabling Cascade Pilot to expose details regarding how application transactions are structured and working (see Figure 2). This means difficult and subtle application design and protocol issues can be quickly recognized and investigated during troubleshooting.

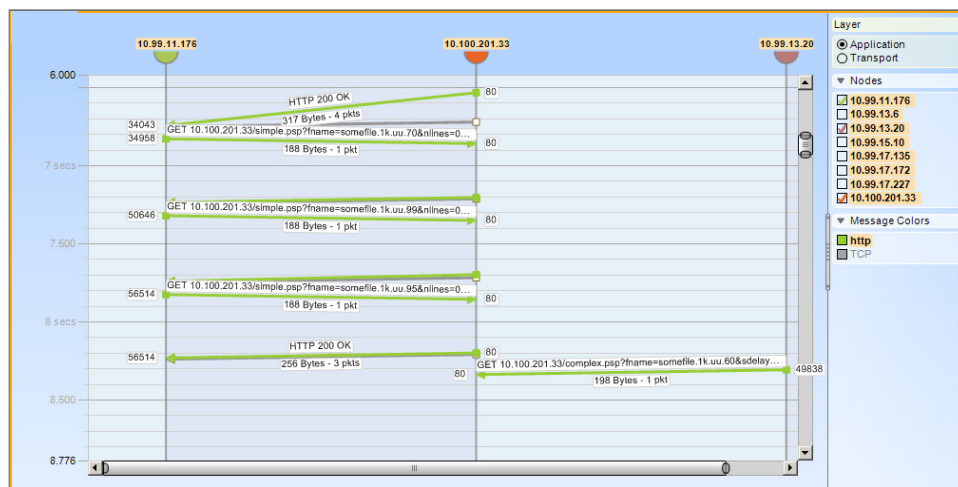


Figure 2: Cascade Pilot Sequence Diagram

Collaboration

The Cascade solution provides flexible, operator-customizable Web reporting, both on a scheduled and ad hoc basis. Integrations have been certified with leading event management systems, trouble ticketing systems, and CMDB/CMS products.

EMA Perspective

At a time when operations teams, and particularly those focused on the network, are facing such a tremendously renewed level of importance to the organizations they serve, careful review and rationalization of management tools, technologies and practices are in order. EMA believes that the single most important transition that network operations can make is to embrace application awareness, particularly in terms of performance monitoring and management, so that they can better understand, respond, and plan in ways that are consistent with the top and bottom line priorities of

The Riverbed Cascade Solution: Application-Aware Performance Management for Enterprise Networks

the organizations they serve. If review indicates a need for new management tools, then requirements should be gathered and should, at a minimum, include considerations of scale, richness/completeness, workflow efficiency, and support for cross-team collaboration.

Riverbed has made significant investments in assembling an answer to these challenges. Initially built and field proven as a flow-based approach, the recent acquisition and integration of packet-based monitoring and analysis technologies from CACE Technologies has vastly expanded the scope and completeness of the Riverbed Cascade solution. Riverbed's commitment to maintain sponsorship of the Wireshark open-source project, which was originally created by members of the CACE team, gives Riverbed further street credibility in packet capture and analysis. As a result, the Cascade solution can now support the full scope of requirements most enterprises will share for performance monitoring, troubleshooting, and reporting, with particular strengths in proactive behavior analytics, top-down visibility, and discovery/dependency mapping to support service-oriented operations. Consequently, EMA considers the Cascade solution worthy of consideration for any organization seeking enterprise-class, application-aware network performance management.

The Cascade solution can now support the full scope of ANPM requirements for most enterprises

About Riverbed

Riverbed delivers performance for the globally connected enterprise. With Riverbed, enterprises can successfully and intelligently implement strategic initiatives such as virtualization, consolidation, Cloud computing, and disaster recovery without fear of compromising performance. By giving enterprises the platform they need to understand, optimize and consolidate their IT, Riverbed helps enterprises to build a fast, fluid and dynamic IT architecture that aligns with the business needs of the organization. Additional information about Riverbed is available at www.riverbed.com.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise IT professionals, lines of business users, and IT vendors at www.enterprisemanagement.com or follow [EMA on Twitter](#).

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. "EMA" and "Enterprise Management Associates" are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2011 Enterprise Management Associates, Inc. All Rights Reserved. EMATM, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common-law trademarks of Enterprise Management Associates, Inc.

Corporate Headquarters:

5777 Central Avenue, Suite 105
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com
2282.060811