Network Visibility in the Data Center: Best Practices for Staying Ahead

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for Cisco Systems

April 2014

EMA™ IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

Network Visibility in the Data Center: Best Practices for Staying Ahead

Table of Contents

Network Visibility in the Data Center: Best Practices for Staying Ahead

Executive Summary

As data center architectures make the transition to highly virtualized, highly dynamic, internal cloud forms, traditional methods for monitoring and troubleshooting infrastructure health and performance have struggled to make the transition. Monitoring activity from the network perspective is an essential source of operational intelligence, but monitoring tools must provide sufficient capacity and flexibility to handle rapidly growing traffic volumes and a dynamic, ever-changing resource landscape. This ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) whitepaper examines the specific challenges of network-based monitoring in modern data centers and reviews the most recent evolution of the Cisco Systems Network Analysis Module solution in light of its ability to meet the new and emerging requirements.

Evolving Needs of Monitoring in the Data Center

If there is a constant within the realm of today's data center infrastructures, that constant is change. Change is becoming more frequent all the time, along many dimensions, all at the same time. Compute is increasingly virtualized, allowing servers to be turned up, moved, and decommissioned on a moment's notice. Storage virtualization is evolving towards programmability, allowing automated allocation and distribution of capacity. And networks are fundamentally changing, moving away from dedicated physical infrastructures and towards a mix of physical, virtual, and programmable services. All of this is happening in order to keep up with ever-accelerating rates of application development, change, and deployment.

The arrival of cloud services adds another interesting wrinkle. The use of external cloud services aggravates the change equation, as the normal checks and balances associated with infrastructure/equipment procurements are cast to the wind. Further, cloud services are often engaged by line of business as a means to avoid perceived lack of responsiveness and support from traditional IT. Political and control issues aside, the bottom line is that external cloud, whether private or public in nature, adds additional change variables together with even less visibility for monitoring and operations assurance than is possible with private, wholly–owned data center infrastructure.

The response to these pressures is in some ways revolutionary, and in other ways evolutionary. Some will consider software-defined, programmable approaches to infrastructure to be a true revolution, especially when contrasted with fixed legacy predecessors. But this path really began with the many incremental steps taken in virtualizing networks, storage, and finally compute, and thus is in many ways more of an evolution, in reality. Of equal or perhaps greater impact are the changes in best practices, workflow, and organizations that are accompanying the next generation data center technology changes. EMA has been following the steadily growing percentage of operations teams that are organizing around application-aware monitoring and troubleshooting practices based on cross-domain, service-centric management paradigms. Again, for some organizations, this is a radical departure from prior, silo-centric approaches to operations. But other organizations, particularly those who had embraced some form of integrated service management, such as ITIL, COBIT, or ITSM, will see this shift as an inevitable evolutionary step.

So what can networking engineers, managers, and operators do to prepare for this service-centric, application aware approach? The key lies in finding and leveraging as much data as possible about exactly how the data center infrastructure is performing, in context with the applications in use and the functions/purposes behind the activity. While EMA recommends that a mix of monitoring approaches be used, one of the most consistently reliable and valuable viewpoints is that of application-aware performance

gathered from the network perspective. In fact, despite all the layers of virtualization and change, there are still a few essential truths upon which networking pros can rely. In particular, application traffic and activity will, at some point, travel across a physical network link and through physical or virtual network components. While an executable may live within one hypervisor now and another in the next hour, and an external cloud the day thereafter, the sessions and transactions associated with that application must still travel across a network, either virtual or physical. This means that strategically placed, application-aware monitoring technologies can continue to provide essential visibility and valuable insights for characterizing and troubleshooting performance. That said, network-based monitoring technologies that were developed for more static, lower-speed infrastructures cannot necessarily be directly adapted and deployed successfully in the dynamic data centers of today and tomorrow.

Best Practices: Network Monitoring in the Data Center

In order to keep pace and fulfill the value required, network monitoring tools, technologies, and practices must advance and evolve alongside the changes that are occurring within the managed environment. In particular, network and application activity monitoring must contend with new demands for scalability, new visibility barriers represented by virtualization and cloud services, the rising focus upon application and service awareness, and the need for facilitated collaboration and communications. Following are more detailed assessments of each of these areas of new and evolving requirements.

1. ***Planning for growth***: Scalability represents a key challenge to network monitoring tools, as physical network speeds continue to rise at a torrid pace. Recent EMA research indicates rapid adoption of 40G Ethernet and fast-rising interest in 100G. While network monitoring tools that rely purely on SNMP, log files, or NetFlow as data sources are only indirectly affected by such escalation, those that provide packet analysis insights must directly accommodate this shift. As of early 2014, most packet-based network monitoring solutions have been upgraded to accommodate 10G Ethernet speeds, but only a very few have begun to address 40G and higher speeds. Creative approaches exist to extend the effective use of lower-speed packet inspection technologies, but a clear path towards reliable, lossless monitoring is ideal.
2. ***Accommodating constant change***: The rate of change occurring in today's dynamic data center impacts network monitoring in a couple of important ways. First, new services and applications are being deployed on a regular basis, and application-aware network management and monitoring systems must be updated to properly recognize and track them. Second, with the advent of programmability and a greatly expanded virtual networking tier, network monitoring systems must be able to accommodate rapid rates of change as well as increasingly short life spans of virtual connectivity, such as VLANs. Finally, the advent of cloud services requires network monitoring tools and practices to adapt to operate across a hybrid mix of internal and external resources.
3. ***Optimizing visibility/response***: As operations teams converge and coalesce around solidifying a better and more complete understanding of the performance of hosted/delivered applications and services, coupled with the end user/customer experience, network monitoring must be aligned to support this shift. Key to success is having enabling features for organizing and prioritizing monitoring based on the most important and most sensitive applications and services, including the identification and subsequent tracking of key performance indicator metrics, such as connections, volume, and response times. Also of tremendous value here is an ability of the network monitoring system to provide related context, revealing potential negative influences

upon application or service performance arising from other workloads and activity occurring within or being delivered across shared resources, whether within the data center, cloud, or distribution and access network layers.

4. ***Communicating and collaborating***: In the old days, it was just fine if networks were monitored and managed in a completely insulated and independent fashion, and monitoring data was kept within the confines and control of the network operations group. But the organizational shift towards service centric operations as well as the astounding rise in complexity of application and infrastructure architectures is making cross-team collaboration and communications an absolute necessity. As part of this, integrating network monitoring with a broader suite of management practices, tools and technologies is becoming a related mandate, so that critical insights can be brought to the fore and investigative/mitigating workflows can be truly optimized.

Collectively, network management and operations teams that embrace and successfully address these four key best practice areas will be in position to fully support and assure a high performing, highly reliable data center network. But even more importantly, they will be able to do so in a manner that aligns with the most important and mission-critical applications and services that the network helps to enable and deliver.

Cisco Network Analysis Module – Advanced Monitoring for the Modern Data Center

As a globally recognized leader in data center infrastructure equipment and solutions, Cisco Systems is in an excellent position to understand the scope of needs for monitoring and management of both the network as well as the broader data center environment. In parallel with its infrastructure equipment solutions, Cisco has developed a wide and growing range of management tools and technologies to help practitioners deploy, provision, tune, optimize, and assure data centers successfully. One key component within the management suite is the Cisco Network Analysis Module (NAM), which provides direct, application-aware monitoring insights and visibility from the network perspective. Deployed either as a blade in Cisco switches or routers, a physical appliance, or a virtual appliance, the Cisco NAM has become a commonplace tool for network managers and operators.

The Cisco NAM solution was originally designed to function primarily as a troubleshooting tool for the networking team, but has evolved to play a larger role in supporting data center operations. Recent additions and enhancements to the Cisco NAM portfolio reflect this evolutionary path, and are designed specifically to help networking and cross-domain teams keep pace and stay ahead of the challenges, despite the changes that are happening in the data center.

Staying Ahead of Scale

The new Cisco NAM Integrated Services Module for Nexus 7000 (NAM-NX1) is the highest capacity Cisco NAM solution ever, and is able to handle sustained traffic monitoring at over 30 Gbps. Internal storage capacity of 900 GB supports substantial packet caching, and advanced hardware and software filtering, much of which are implemented within ASICs for high performance, further expand effective capacity.

Staying Ahead of Virtualized/Cloud Infrastructure

The new Cisco vNAM is a purely software-based version of the NAM solution, offering full NAM features that can be deployed directly within a hypervisor. Initial support for KVM and ESX hypervisors will be followed by support for Hyper–V at a later date. The Cisco vNAM can gather and analyze packets via SPAN and ERSPAN, from a Cisco switch, as well as harvest NetFlow from any source. This allows organizations to restore visibility inside of virtual compute environments and even to establish direct visibility inside some external cloud settings (depending on cloud provider networking control options). For example, by installing an instance of vNAM inside select hypervisors around the data center, traffic flowing between VMs within those hypervisors (which never crosses a physical wire) can be seen/monitored/analyzed. Further, deployment of NAMs for specific monitoring or troubleshooting activities becomes much quicker and more flexible, since there are no physical appliances to deploy or cabling to install for the vNAM.

The Cisco NAM has also been substantially enhanced to help recognize and maintain visibility into and through various types of virtual network overlay encapsulations. For instance, existing support has been expanded to add OTV, VXLAN, FabricPath, GRE, LISP, and others (see example in Figure 1). The enhanced NAM automatically recognizes encapsulation protocols and applies de-encapsulation, even in nested encapsulation situations such as VXLAN over OTV. With the use of network overlays expanding rapidly, these capabilities are essential for revealing the true identity and nature of encapsulated traffic, so that activity can be rightfully recognized and actions prioritized during both monitoring and troubleshooting activities.

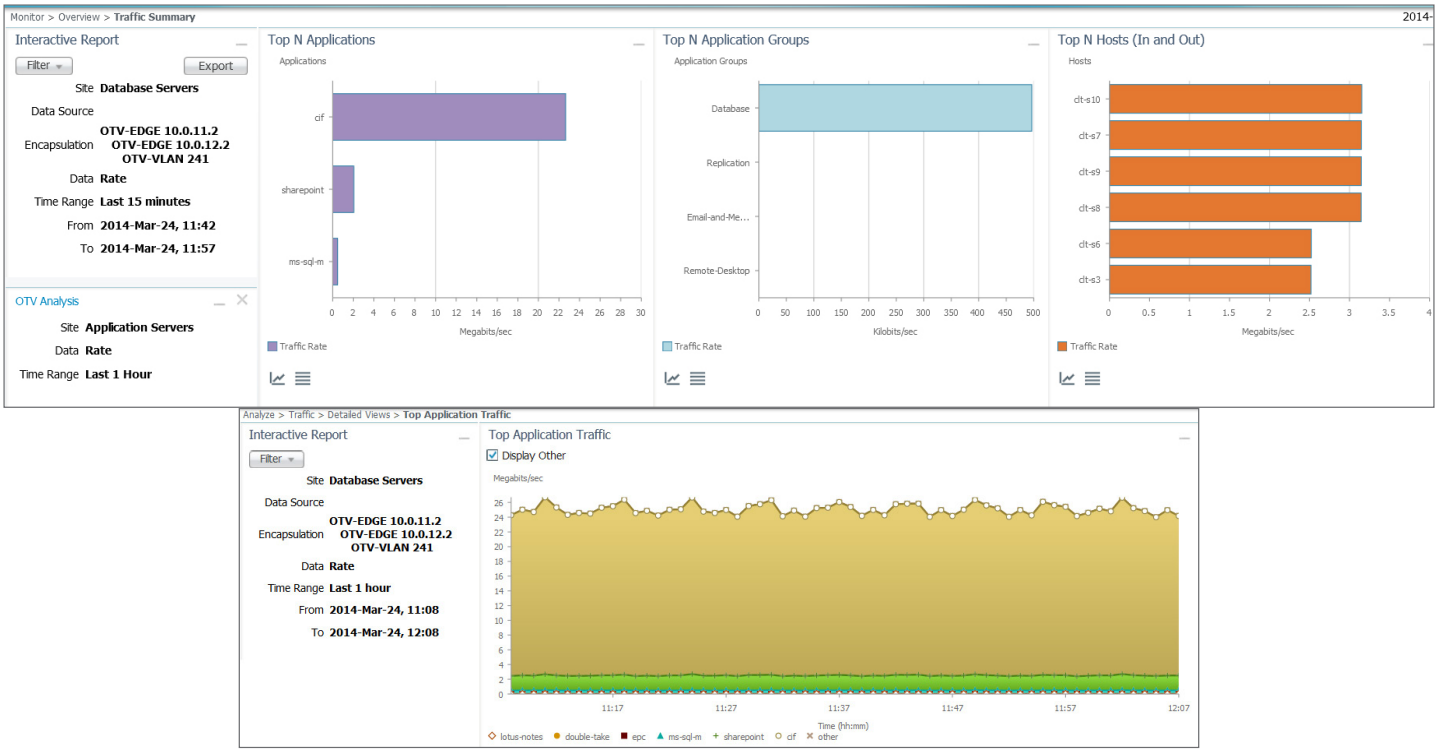

Figure 1: Visibility into OTV:Profiling the traffic across DCI link; identifying the Top Talkers and Applications consuming the most bandwidth

Staying Ahead of Complexity

The primary focus of the NAM solution is to provide direct application visibility, via deep network visibility, sustained monitoring, and performance analytics. This viewpoint and capability allows network and operations pros to understand how each application is performing over time, for each end user, in context of everything else that is going on across the shared infrastructure. For instance, a complex application may involve multiple executable components distributed across the data center, together with networked database and storage tiers, all ultimately accessed via a virtual desktop platform by mobile end users. The Cisco NAM can gather performance data from multiple source locations spanning such complex environments, so that the full context of each individual application ecosystem can be understood, while also recognizing that certain parts of the delivery infrastructure are being shared with other applications and used for other purposes.

Such context is essential when investigating performance issues, and for times when it is necessary, a number of major enhancements have been made to the Cisco NAM to facilitate faster troubleshooting and more efficient workflows. For instance, the technique for capturing packet sequences has been completely reworked, evolving from a condition-based trigger approach to instant snapshots via a constantly rolling buffer. Additionally, captures can be scheduled based on time or volume triggers, and the capture process can also raise an alarm automatically if conditions of concern are recognized and met.

A long list of console view and operator interface enhancements provide further efficiency improvements for accelerating incident recognition and analysis. For instance:

- The overall design of views presented in the operator console is structured around client/server/application/site data, rather than the traditional network monitoring approach of organizing around monitored network links (see Figure 2). This reflects application/service-orientation, speeding workflows that would otherwise have to start from an infrastructure-centric perspective.
- Site-to-site traffic views expose specific activity and traffic traveling between locations, NetFlow sources, subnets, VLANs, etc., exposing top applications, top talkers, and traffic trends.
- Hovering a mouse pointer over response time data reveals server, network, and data-related contributions so problem sources can be easily assessed.
- When drilling into details around a specific server for further information, all applications associated with that address are shown, so the full context of related/shared resource influences on performance become immediately apparent.

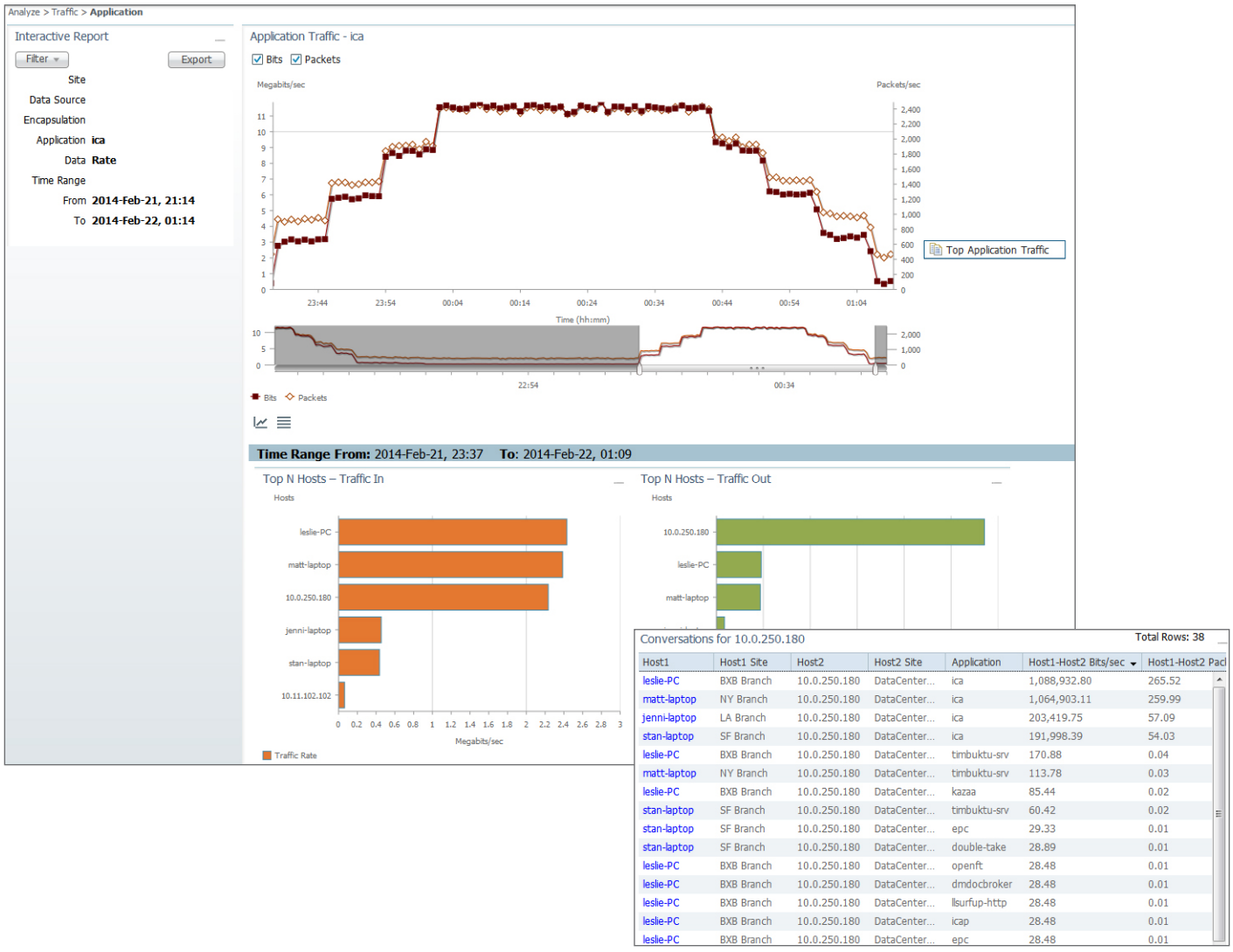

Figure 2: Analyzing Traffic Behavior; Investigating the cause of traffic increase, isolating the host and conversation

- Application Response Time (ART) distribution views highlight important trends in end user experience (see Figure 3). Also visible in the same figure are the sliding-window controls provided within the operator console to set and adjust the interval of interest. In this case, both the Application Response Time Distribution chart and the Other Metrics chart have been automatically updated to reflect only data points occurring within the interval chosen in the upper Transaction Time graph.
- One-click capture allows an operator to instantly assemble a trace of activity from any IP address.
- The packet capture analyzer supports Google-like type-ahead search for quickly finding and applying available filters. Further, a unique aspect of the NAM approach to packet analysis is the preliminary error scan feature, which is used against capture files to highlight problematic patterns, and from which network managers can drill directly to the packets associated with any listed error.

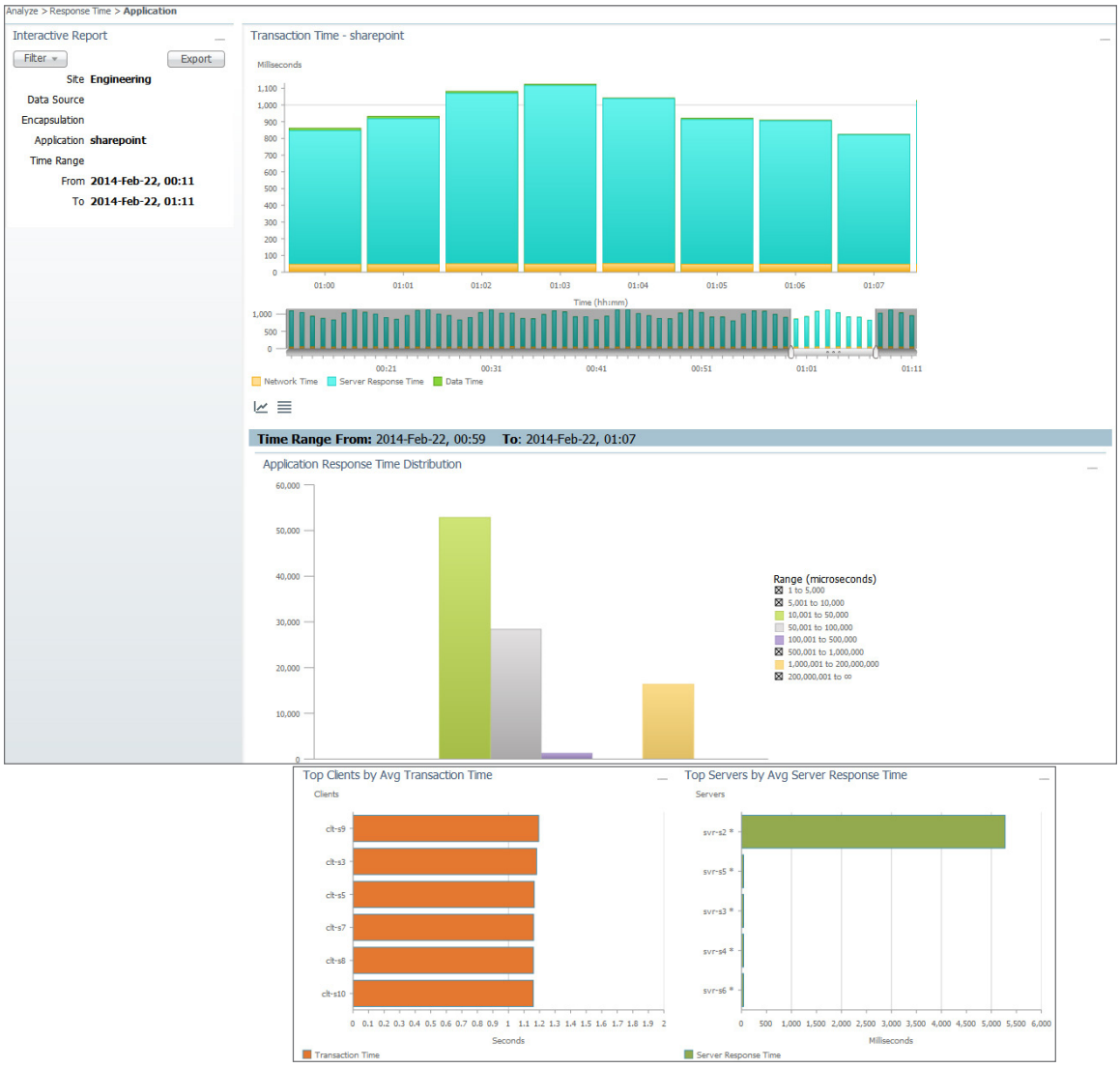

Figure 3: Monitoring Application Workloads with vNAM; Isolating the server as the cause of application performance degradation

The result is a flexible network monitoring solution that can help operators understand and analyze performance across a wide range of important use cases, including mixed physical/virtual and hybrid infrastructures, multi-tier applications, mixed wired/wireless networks, critical data center interconnect links, and more.

Staying Ahead via Collaboration

The Cisco NAM's ability to support cross-team communications and collaboration has been substantially enhanced via a number of new scheduled report features. First, the existing web-based console views can be shared directly with others, by simply forwarding the URL of the view of interest to authorized recipients – no independent NAM licenses or logins are required. Also, reports can now be generated to directly reflect the interactive console views that an operator has set up to investigate a particular incident or problem. Results can be exported to CSV or PDF, and distributed automatically via email. Further, reports can be run across multiple NAM instances, either for specific days or on a custom interval basis.

Additional new features help with a broader range of management and monitoring objectives adjacent to and beyond the data center, such as awareness of Trustsec Secure Group Tags (for confirming tag matches between user and server) and CAPWAP decode and analytics for monitoring and troubleshooting mixed wired/wireless access. Further, RESTful XML APIs are a standard feature of all NAM products, allowing integration with broader management suites/architectures and direct participation in programmable networking and infrastructure initiatives such as SDN.

EMA Perspective

Today's data centers are changing in deep, fundamental ways. In the face of the dynamic nature of application and virtual component layers, one of the few steady and reliable viewpoints into health, activity, and performance will come from using the network perspective. But while network monitoring continues to offer strong/growing value, it must adapt to the new order and change to reflect evolving technologies and operational organization demands.

Based on ongoing research with practitioners as well as dialogue with industry solution providers, EMA recommends that networking professionals focus on four key areas to ensure that their network monitoring tools can keep pace and continue to add value. Network monitoring solutions must be scalable to accommodate increasing volumes of activity. They must be flexible and adaptable to provide visibility into a constantly changing mix of applications and services across physical, virtual, and cloud environments. They must directly facilitate rapid problem recognition/diagnosis/resolution. And finally they must participate in a broader management ecosystem that empowers collaborative communications across the operations organization.

Cisco's NAM products, long a mainstay element in network managers' kitbag of troubleshooting tools, have evolved/progressed significantly beyond their heritage. Newly added features and capabilities, including a 30G-rated data center switch blade and virtual form factors, have moved the NAM solution into position to meet best practice needs for network monitoring in today's dynamic data centers. And while many of the most recent enhancements are specifically intended to increase the utility of the NAM solution within the data center, the full line of NAM products, including the many already deployed both inside and outside of the data center, will benefit from the new features and capabilities. This means that both existing NAM shops as well as those looking at NAM for the first time will reap the rewards of the solution improvements.

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 line of business users, IT professionals and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

2869.040214