Cisco Systems Network Analysis Module Software 5.0

Enterprise-Class Performance Monitoring and Analysis for Modern IP Networks

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

January 2011

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

Cisco Systems Network Analysis Module Software 5.0

Table of Contents

Cisco Systems Network Analysis Module Software 5.0

Executive Summary

Effective network performance monitoring and analysis tools are a must have for today's dynamic, distributed IT environments. They provide the visibility required to assure smooth and predictable delivery of applications and services across the network and fast troubleshooting when things go wrong. One player in this category, the Cisco Systems Network Analysis Module (NAM) has recently undergone significant enhancement via the release of NAM 5.0 Software, bringing it forward as an enterprise-class alternative. Cisco's NAM now offers powerful features for fast access to performance data, efficient troubleshooting, rich information for managing network optimization, and open interfaces for integration into broader management architectures, all delivered via self-contained, flexible options for cost-efficient deployment in the data center, campus, or branch. This ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) paper examines current top requirements for network performance monitoring and analysis solutions and reviews how the Cisco NAM meets those requirements.

Introduction

Network managers today are facing an unprecedented level of new demands. The growth of voice, video, server virtualization, and Cloud services, combined with the relentless pace of organic traffic expansion, is stretching networks and operators alike on a daily basis. In fact, network capacity and resilience are receiving renewed attention from IT management at all levels, given the critical role it plays in more and more organizations for delivering applications and IT services to users, partners, and customers.

In order to establish control in network operations, the first requirement is establishing clear visibility across the stack.

In order to get the edge and establish sufficient levels of control of today's dynamic network operations, the first requirement is establishing clear visibility across all parts of the stack – from the lowest connectivity layers all they way up and into the application layer. Within the application layer, it is essential to be able to recognize all of the applications and services that are in use, so that individual user issues can be easily isolated for analysis and troubleshooting. Further, such visibility delivers the details necessary for best practices in business-aware capacity planning and delivery optimization.

There are several network management technologies that can provide this type of visibility. Most well known are packet and protocol analyzers – traditional utilities kept close at hand by every seasoned network manager. But individual analyzers only work where they happen to be connected, and so remote-accessible packet inspection probes have also become a popular option. During the past several years, infrastructure devices have started delivering another alternative – flow records such as NetFlow – that document application traffic on a per-flow basis as they pass through switches and routers. Finally, test agents can make discrete measurements of specific types of traffic and traffic metrics on a synthetic basis. Ultimately, to gain sufficient visibility, most networking operations teams will deploy a combination of these technologies.

Selecting such technologies and tools can be difficult due to the number of offerings in the marketplace; however, there are three overriding concerns that should guide evaluation of the alternatives. First, the solution must address the need for speed, enabling quick recognition and diagnosis of performance problem sources so that corrective actions can be taken as rapidly as possible. Second, the solution

must address the need to optimize, supplying clear evidence for determining whether or not network traffic prioritization and optimization techniques are delivering the value intended. And third, the solution must address the need to play nice, integrating smoothly with other management tools by sharing data and easily fitting into complex workflows. Ultimately, there is a fourth consideration as well which cannot be forgotten – a solution must also address the need for doing all of the above at an effective, affordable total cost of ownership.

One of the options available for delivering visibility is Cisco System's Network Analysis Module (NAM). This management tool has been around for over a decade, and represents an increasingly popular option for network instrumentation due in no small part to its tight integration into Cisco's broader solutions for network architecture. With the most recent release of Cisco NAM software, version 5.0, its capabilities have been substantially enhanced and now represent an enterprise-class, application-aware network performance monitoring and analysis solution.

Essentials for Monitoring, Analyzing, and Optimizing Performance in Today's IP Networks

Before looking more closely at how the Cisco NAM aligns with high priority requirements for network performance visibility, we should first take a closer look at those three core areas of need. Each of these is multifaceted, and thus each should be put in context of the specific operating priorities of any IT organization; however, they should in large part represent common themes that will be present in more settings than not. And each general area can be translated into a number of specific feature/function capabilities that will be important to look for when considering product choices.

1. Fast-tracking Problem Resolution

Ask any network manager or operator to name their first priority for performance monitoring and analysis technologies, particularly those that focus on packets, protocols, and applications, and their answer will be "troubleshooting." There's little debate on this point – these products must do one thing first and foremost – provide the data and analysis to rapidly understand the context of a performance problem and find the most likely root cause as quickly as possible.

As much as the other areas of functionality can deliver directly measurable business value, fast problem resolution is commonly the most visible from a broad organizational perspective because when applications are not responding or available, everyone hears about it – the traditional "fire drill." While no one has attempted to quantify the cost of performance degradations, many studies have looked into the impact of downtime on enterprise or service provider environments. While the impact is highly dependent on the type of business or customer being supported, EMA research has indicated a range from $25k to over $1 million per hour. Performance degradations will be a pro-rated lesser amount than these worst-case costs, but regardless, the quicker network managers are able to get to the root of an issue, the faster normal operations can be resumed, and the less impact on the customer or organization. In business value models, the term used for tracking this is Mean Time To Repair/Restore, or MTTR.

> The first functional priority for network performance monitoring and analysis is effective troubleshooting support.

In order to deliver fast problem resolution, network performance monitoring and analysis tools need to provide a number of key features. First, they will need to have the capability to present

performance data in detail by source/destination, protocol, and application – across the entire stack – because the root issue may be just about anywhere, and job one is characterization/isolation. Next, that information must be available in real-time (to diagnose problems that are in progress) as well as historically (to diagnose problems that happened in the recent past). Along the way, intuitive and graphical presentations of data are highly valuable because human operators are quicker at recognizing patterns visually than numerically. Smooth, context-sensitive navigation of data with drill-downs and roll-ups can also greatly accelerate the investigation. Integrated intelligent data filtering and pre-processing/analysis play a positive role here as well. And finally, while performance monitoring and analysis at any individual location can certainly be helpful, most environments will require many points of instrumentation, and so consistent data collection and presentation is essential for scaling up and solving issues in distributed settings.

2. Optimizing the Optimizers

No discussion of performance management can be complete without evaluating both sides of the coin. On one side is visibility, and on the other is control. Performance control primarily takes the form of optimization techniques and technologies applied at various levels of the stack. One primary goal is to improve the likelihood that a particular application or service will be delivered with sufficient levels of quality so that workers and customers will not be inhibited from efficient use – commonly delivered via Quality of Service (QoS) policies and tagging. Another top goal is to better manage the total flow of traffic between geographically disparate sites across a Wide Area Network (WAN) link to keep the total cost of connectivity under control – commonly referred to as WAN Optimization. The Cisco Systems Wide Area Application Services (WAAS) products are examples of this latter type.

As an organization embraces QoS and WAN Optimization, there comes with that a need to monitor how those optimization approaches are working, or not working, to keep them tuned for delivering peak efficiency and maximum value. A common example of QoS usage is setting up priority traffic handling for latency-sensitive traffic, such as VoIP and videoconferencing, to ensure that jitter and packet delay are kept to an acceptable minimum. If any such traffic is not properly tagged as high priority, or non-critical traffic leaks into high priority queues, quality will likely suffer. In the case of WAN Optimization, most such products require ongoing tuning in order to ensure that all of the traffic regularly seen on the network has been classified and optimized – an ongoing challenge in most organizations, where new or enhanced applications and services are being introduced on a regular, sustained basis.

Network optimizations require constant monitoring and tuning to ensure maximum effectiveness.

While network infrastructure elements will actually be delivering the QoS and WAN Optimization functions, network performance monitoring tools are an important adjunct for making sure the optimizations themselves are operating in optimal fashion. To meet this area of need, there are several key features and functions required. First, there must be an ability to analyze traffic activity on a site-by-site and application-by-application basis, with baselining and trending. This will provide the basis for planning and configuring optimizations, as well as the standards against which the optimizations will be evaluated when in place. Next, a means of before-and-after comparison is needed, including reports by site, policy, and class, so that operators can easily recognize how much improvement is being achieved. Finally, optimization impact should be available as one of the metrics used for real-time alerting, so optimization problems and issues can be recognized early and dealt with effectively.

3. Supporting the Management Technology Team

The old maxim "No man is an island" could be applied to management tools as well. With the broad range of technologies that must fit and operate smoothly together to comprise today's IT infrastructure and application environments comes a plethora of management tools that should also work together as best possible. Most organizations will have management tools focused on systems, storage, and applications, as well as the network. There are configuration tools, security tools, fault/alert tools, performance tools, and even usage/billing tools within each of the technology domains, as well as broad platforms that pull all of this data together centrally for aggregated visibility and control. As a result, network performance monitoring and analysis solutions must participate in and support an entire ecosystem of management products to play an optimal role in the total context of engineering and operations.

Network performance monitoring products in particular offer important – often crucial – operational insights that help in isolating problems to their most likely source, whether network or not, as well as contributing diagnostic insights that are essential for remediation. EMA research indicates that well over 60% of user/customer-reported problems end up in the hands of the network team for initial diagnosis and triage, and yet the root cause is found to be within the network only about 20% of the time. As a result, EMA advocates that network managers proactively assume the role of problem isolator as a means for helping reduce MTTR across the organization. And while raising one's hand in the tiger team meetings is one means for taking the lead, a better and more manageable/predictable approach is to integrate management tools so that information transfer can be as efficient and automated as possible.

Network performance monitors offer important – often unique – operational insights that should be shared easily and openly.

In order for network performance visibility solutions to integrate with other management tools, there are several feature/function priorities. First, there must be open interfaces that can be used both for importing data (such as common device names, access controls, and raw performance measurements) and exporting data (such as alerts and calculated performance metrics). Next, the interfaces must be easy to use and easy to maintain, with backward compatibility assured by the solution provider for preventing unexpected breakage during maintenance upgrades. And finally, any means for integrating into operational workflows, such as contextual programmatic launch and automated data transfer, is of additional value.

NAM Software Version 5.0: Next Generation Solution for Optimizing Network Operations

Cisco Systems offers a network performance monitoring and analysis solution in the form of its Network Analysis Module (NAM). The NAM is designed to take many forms for flexible deployment in a wide variety of operational settings – as physical appliances, router/switch blades, and more recently as a virtual blade/appliance for deployment within virtual switches such as the Nexus 1000V or WAN Optimization Controllers such as the WAAS 574/674. This provides multiple options for deploying NAMs in data center, campus, and branch settings.

With the NAM 5.0 software release, significant enhancements have been made which advance the solution towards covering a significant majority of network performance management requirements

for supporting today's enterprise and service provider operations environments. A few of the new feature highlights include:

- Completely new GUI for faster performance data access/presentation and efficient workflows
- On-board historical data store for retrospective analysis
- Support of Cisco's Network-based Application Recognition (NBAR) for consistent representation of services and applications (imported via NetFlow v9)
- NetFlow v9 data export for extended network reporting
- Packet Capture Error Scan for intelligent "expert" analysis

In order to fully appreciate these new features in combination with existing capabilities of the NAM solution (such as advanced analytics for Voice, TCP application responsiveness, QoS, and WAAS) it is helpful to view them as they contribute to major feature categories, which can be tied back to the three requirements areas presented earlier in this paper.

Interactive Reporting

The first point of daily access for any user of network performance monitoring and analysis tools is the summary report or dashboard. This is where status is assessed and investigative tasks begin. It is also where data presentation and workflow can be optimized so that operators can access and navigate the extensive array of data such products collect in a way that helps them work quickly and efficiently.

The new GUI that comes as part of NAM 5.0 software has been completely redesigned with interactive efficiency in mind. The newly added internal data store now means that historical metrics are available in the same views as real-time data, and no longer require discrete report configuration. Quick and powerful graphing and charting has been added which include leading-edge navigation techniques such as panning, zooming, and easy filtering. Automatic synchronization of all data charts based on selected time range filters also accelerates the analysis process. Performance data from multiple sources – packets as well as NetFlow – can be presented side-by-side in common views. Contextual drill-downs are available throughout for facilitated investigations, and fast data export is offered for sharing results with other team members. An innovative example of the new capabilities, multi-metric comparative charts, can be seen in Figure 1 below, along with other elements of the new primary dashboard.

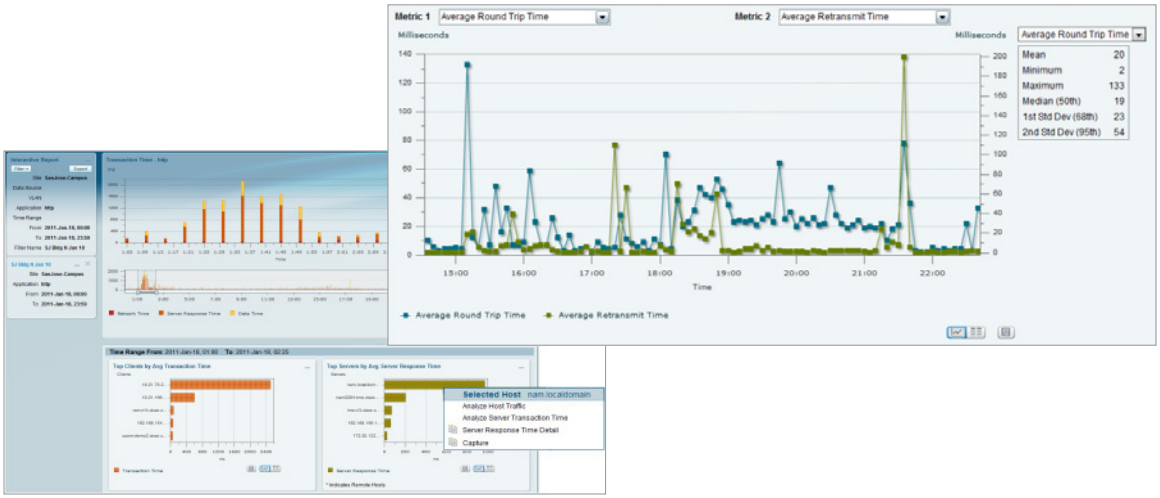

Figure 1. NAM 5.0 Software multi-metric view/report and new GUI dashboard

These new features are relevant to two of the three major requirements areas. First, they represent the primary interface through which fast problem access and diagnosis (#1) is delivered. And with the mix of historical metrics, it will also be the method by which the optimizers will be monitored (#2) so that they themselves can be optimized.

Historical Analysis

Anyone who isn't fortunate enough to be sitting at their console when a problem happens realizes that the ability to study what happened an hour ago, or last night, or yesterday may be essential to understanding and characterizing a network performance issue. And even when one is fortunate enough to be there at the keyboard, diagnosis often requires a study of factors that led up to the occurrence – not just starting now and watching going forward, but immediately accessible data representing the recent past.

A major enabling capability that comes with NAM 5.0 Software is the internal database, which captures and maintains historical performance metrics and data. With this new feature, the NAM enters a new realm of solutions, expanding from being primarily a real-time analysis and troubleshooting solution into providing network performance monitoring solution capabilities. The historical data allows contextual inquiries during troubleshooting as well as baselining and trending for any metric. A great example of this is the new capabilities for presenting before/after results of WAN Optimization, as shown when tracking WAAS solution impact in Figure 2 below.

Figure 2. Historical views of WAN Optimization impact

These capabilities are also relevant to two of the major requirements for network performance monitoring and analysis. First, the historical view directly supports fast access for troubleshooting (#1) by allowing operators to recognize issues that have occurred in the lead-up to a problem under study. Since these metrics are on-board in a database, access is very quick and contextually efficient. Second, with the inherent capability for trending and baselining, this provides an essential underpinning for monitoring and optimizing the optimizers (#2), whether keeping an eye on QoS class policy compliance, or determining how well WAN Optimization is functioning.

Site-based Monitoring

One of the most important questions asked when planning network changes or investigating an issue is, "which site or group is affected?" The need for grouping monitoring information is essential for sorting this out, and for prioritizing management tasks and activities towards those issues that have the most critical impact. It also forms the basis for best practices in engineering and planning, by enabling recognition of trends and changes in the context of where they have significant effects.

In the NAM 5.0 Software release, new grouping functions have been added so performance data can be presented and organized by a wide range of criteria, including data source/site, VLAN, IP address range, and more. The ability to group by VLAN is especially valuable for service providers seeking to understand discrete representations of performance on a customer-by-customer basis – an essential element in Service Level Agreement/Objective (SLA/SLO) optimization and policy enforcement.

The ability to group performance data by VLAN will be of special interest to MSPs, who need to view information on a customer-by-customer basis.

This new site-based monitoring capability is also relevant to two of the three performance monitoring and analysis requirements areas. First, it supports rapid problem analysis (#1) by helping operators understand which sites, groups, customers, or applications/services are affected and which are not. Second, site-by-site and application-by-application analyses are important techniques for recognizing the impact and success of optimization tools (#2).

Intuitive Workflows

The most successful, impactful network performance visibility products achieve favor because they are easy to use and easy to understand. Also important is a task-based organization of features, so typical steps followed in executing network performance analysis work processes can be made easy and efficient. This has other side benefits in reducing training time and improving total feature usage.

The NAM 5.0 Software release implements a number of such intuitive feature approaches. Time-based filtering allows fast adjustment of views. Visual correlation of multiple metrics makes comparison of events and trends simple. Contextual drilldown enables fast navigation of performance data from high-level summaries down to the lowest level needed – even directly to the packets. The NAM GUI has also implemented using the new UI structure employed within Cisco's LAN Management System (LMS) 4.0, which was released in 2010, so operators will enjoy common navigation paradigms, simplifying workflows where the two products must be used together. An example of this new approach, which includes an innovative task-based organization of features, is shown in Figure 3.

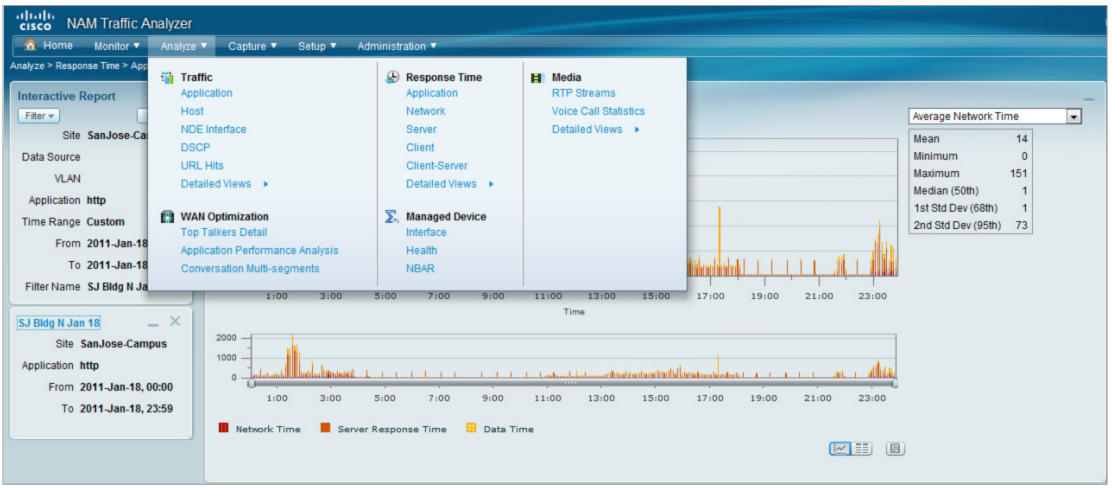

Figure 3. NAM Task-oriented Analysis Feature Grouping

The workflow features are relevant to two of the network performance monitoring and analysis requirements areas. Firstly, intuitive presentation and navigation of data is hugely beneficial for accelerating the problem identification and troubleshooting process (#1). And secondly, the task-oriented conformance with Cisco's LMS product, together with the ability to share/export data quickly and easily as part of a workflow process, helps the NAM fit into the broader tools ecosystem (#3) efficiently and effectively.

Standards-based APIs

When it comes to putting any management product side-by-side with others and making the sum greater than the parts, the best approach is through direct integration. By sharing information, significant advantages can be enjoyed in facilitating and accelerating cross-functional and cross-domain collaborative tasks. Integration also represents an opportunity for adding important operational data into consolidated monitoring and reporting systems for functions such as service quality management and reporting.

The NAM 5.0 Software release brings a number of advancements in this area. First, data exports can now include not only measured data points, but also calculated metrics. The NAM can also format and issue NetFlow v9 records for consumption and analysis by other management tools. On the inbound side, the support for gathering NetFlow data means that any compliant information stream can be directed at a NAM and included in presentations, reports, and analysis. Finally, the new REST XML API eases consistent configuration for simplified, common representations of managed elements and constructs.

The NAM 5.0 Software integration features are helpful in supporting all of the network performance monitoring and analysis requirements, including sharing data beyond those using NAM directly in the service of fast problem analysis (#1) and optimization analysis (#2). But these features are most important in the third area – supporting the broader management systems "team" (#3).

EMA Perspective

Without question, the role that networks play in today's dynamic, distributed IT infrastructures is becoming increasingly critical, and thus highly effective, proactive performance monitoring and management is becoming equally critical. EMA dialogues with network operators indicate common acknowledgement of this need, but also that one of the key challenges is in figuring out which product options will be the most cost effective and the most operationally impactful. Also of great concern is ubiquity – many performance monitoring and analysis solutions provide great insights, but their total effectiveness is heavily dependent on how broadly monitoring coverage can be pragmatically achieved.

With the NAM 5.0 Software release, Cisco's solution is taking big strides in both sophistication and maturity, adding substantial monitoring and troubleshooting features to its existing strengths in application-aware network performance analysis

With the 5.0 release of NAM Software, Cisco's solution is taking big strides in both sophistication and maturity for addressing these dilemmas. With over 30,000 units shipped, the NAM is already one of the industry's most broadly deployed solutions, offering a range of options (appliance, blade, or virtual) that puts it on par with the best of the network performance monitoring and analysis category. The self-contained, integrated nature of the NAM solution also sets it apart form others, making deployment and administration simple and straightforward. The latest feature set also moves NAM from ad hoc troubleshooting/analysis to true performance monitoring, with historical data, an advanced and intuitive GUI, direct support for optimization analysis as well as expanded APIs.

Some longstanding industry questions about the role of the NAM are being answered clearly within Cisco Systems itself. Now part of Cisco's core strategies for long-term network evolution and the move towards integrated solutions, the NAM will find increasing usage beyond it's historically tactical role. Cisco's NAM fits neatly into the Borderless Network strategy, and is a specifically named component of the Application Velocity initiative. The NAM also plays a specific role in Cisco's Unified Network Services solutions for datacenter architectures (for Analysis and Monitoring), and further is included in Cisco's Unified Communications solution (for Voice Quality monitoring).

In the end analysis, network managers and operators must establish visibility if they aspire to maintain control – both for rapid response to issues as well as sustained, proactive monitoring and planning. There are many options for gaining visibility, and now the Cisco NAM should be considered highly among them. This should particularly be the case for those who have existing Cisco network infrastructure, into which the NAM can be easily deployed, and especially for those who have already deployed prior NAM versions and are eligible for free upgrades to NAM 5.0 Software under Cisco's SMARTnet programs.

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.

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

2216.012511