

SPECIAL BRIEFING

A Guide to Stabilizing Your Network

by Jeffrey Nudler
Enterprise Management Associates

Sponsored exclusively by:



Produced by:

NETWORKWORLD[®]
CUSTOM MEDIA SOLUTIONS
www.networkworld.com

Networks operate in a state of flux. There are, in fact, an infinite number of behavior modes for network operations including persistent “brownouts” and catastrophic failures. The effects of network instability can be seen daily, coping with troublesome, persistent and hard-to-diagnose problems. So how do you go about improving what can seem to be a futile and often reactive lot in life? Stabilizing your network requires you to find a way to limit your network’s operational modes in order to produce more consistent performance. You can begin to do this through a few thoughtful steps that will help you to view your network’s performance from a life-cycle perspective — combined with good diagnostic and monitoring tools.

So what really is network stability?

Most people in the business community have accepted the idea that IT is a corporate asset. This means that business executives want to understand network performance in business rather than technology terms. A network slowdown for 30 seconds, on average, results in a \$100,000 loss in business productivity, while degraded network performance can cost your company new business, and in some cases thousands of customers, when the cost to replace dissatisfied customer is more than \$200. And this isn’t just in large enterprises. As the integrated IT-business ecosystem expands through business federations - small, mid-tier and large, the services that IT can deliver over a network are equally vital to business competitiveness. After all, the Internet is only a leveling ground for smaller businesses as long as every business in the food chain is equally efficient.

But your networks operate in a state of constant flux. The growing number of users, the increasing mix of traffic types, the increasing number of hops and the addition of new components into the IT infrastructure, as well as constant patches and updates, incompatible device firmware, and even aging can all contribute to you having a very bad week.

To achieve network stability, IT operations and management must ensure that network performance remains within defined confines such that business losses do not occur. But to do this you have to begin with – as the saying goes – “knowing who you are” from a network perspective. For instance, the network stability required for movie streaming will

likely be different than that for an anthropology online magazine. In other words — your “network identity” is really defined by the critical business services that your network must support. So that’s where you should begin your planning.

Network life cycle

Expectation creep, service diversity, and infrastructure complexity and growth are continually raising the bar on network performance. Expectation creep, for one, is so real and so visible that ironically it’s all too easy to ignore it, or at least take it for granted. For example, just several years ago a dial-up Internet connection was a luxury while today’s users, with high-speed wireless broadband access, look up friend’s telephone numbers online, while, at the same time, using instant messaging with others, and wondering “how did we live before the Internet?” Given this exponential growth in user expectations surrounding both service diversity and service performance — the need to assess your network future requirements becomes even more difficult but all the more critical. In other words, you have to be able to plan for network stability in the middle of a hurricane of change. This means more frequent assessments for one. It will also necessitate more automated management technologies, and management solutions that are more responsive to shifting business demands.

Setting a baseline for your network

The most obvious approach to baselining your network is to identify its total capacity for network traffic with projections for possible overload condi-



tions. However, the problem is that this is a moving target. EMA research has statistically shown that the average network grows at the rate of about 48% per year. So you have two choices. You can be happy, deluded and wrong – by assuming a linear growth curve for your network. Or, you can factor realistic growth expectations for your network from the start. Factoring in such growth figures leads to better decisions for everything from load balancing, to planning redundancy levels, to threshold setting. Do this in context with the appropriate metrics and technical descriptors such as traffic mix, latency/jitter tolerance, inbound vs. outbound link utilization profiles, packet retransmission and loss patterns, traffic congestion incidents, as examples.

And don't be lulled into false security simply by building in redundancy. The use of redundancy to ensure network performance is reaching negligible returns. For instance, in a federated network environment redundancy in one segment may actually cause congestion or even catastrophic failure in another. For example, in a multi-server farm, a server with high connection redundancy gradually became the de facto focal point for maintaining network connectivity for all the servers in the farm. This fact was neither visualized nor understood until the catastrophic failure of the entire farm occurred when the server in question went down. Recovering from this particular failure required several hours of rebooting each server in the cluster and reestablishing a proper balance in network connectivity. More effective monitoring tools – including insight into network connectivity and load balancing drift — could have prevented serious losses for the enterprise in productivity and regulatory compliance.

Finally, in setting your baselines and planning for your network's future, you should also factor in business policies and regulatory requirements that may impact your network's performance. For example, at many universities WAN traffic is deliberately reduced because of restrictions designed to keep student calls and Internet usage in line. By contrast, a similar network in a real-estate firm would permit unlimited access. Being aware of these factors and

including them in your baseline planning is probably the first step to proactive self-empowerment.

Looking at toolsets – some primary network management issues

The IT staff must have reliable, deployable and usable tools to monitor, troubleshoot and remediate a wide variety of potential issues. Here are just a few things to look for in selecting tools to help free you from those ungovernable weeks of reactive slavery.

Plan for a more cohesive approach to gathering management data:

Despite the popular perception to the contrary, collecting voluminous amounts of data does not necessarily lead to a cohesive view of the network for easy troubleshooting and remediation. The challenges of synchronizing management data from different network segments serve to reduce the quality and usability of management-related data, often making it redundant but incomplete and categorically unreconciled. Random duplicate data collected by numerous independent management sources creates a Catch-22 situation in which no cohesive troubleshooting can be achieved: either significant amounts of potentially valuable data is ignored, or else unwieldy and inconsistent data will force you and your peers to sort through enormous amounts of information just to assess routine faults.

As a reference point, the growing popularity of Configuration Management Database (CMDB) deployments as a system for management is driven precisely by the recognition that this siloed, random approach to data gathering can no longer continue. CMDB systems don't mean dumping everything in a single repository and hoping for the best. For the most part, effective CMDB systems are architected around metadata – pointers to trusted monitoring tools, for instance, that everyone understands are the "trusted sources" for particular performance problems impacting particular components of the infrastructure.

In CMDB systems, trusted sources of network management information are identified and shared across the full IT organization – including both the data center and the network operations center. This enables a more comprehensive pinpointing where the problem may be. For example, analysis of CMDB data may identify the fact that a specific router is contributing to traffic congestion associated with a particular application service. You can then respond to a business problem directly, rather than negotiating your way through a sea of infrastructure issues, many of them not particularly relevant to business performance. In this and many other ways, CMDB systems actually streamline the way network managers can do their job, by eliminating non-policy compliant sources of management information and enabling IT professionals to collaborate rather than go to war with each other armed with siloed tools.

To ensure integrity of network management information – you should invest in software solutions that provide consistent insights into time and service impact. This means, for instance, standardizing on consistent approaches for auto-discovery and configuration management as resources for network troubleshooting and problem detection. It also means ensuring that you have an effective “trusted source” for capturing application traffic flows across the network in terms of usage, impact and segment-specific resource vulnerabilities.

Get prepared for more automated network management tools:

To maintain network stability, EMA anticipates a gradual but steady shift toward tools with analytical capabilities coupled with automated actions in order to provide increased control in support of network stability. Flow-based tools are natural candidates for becoming the initial representatives of such tools. These tools deal with relationships between various devices in the IT infrastructure by focusing on where, what and how application traffic volumes are traversing the network. Identifying

top talkers, prevailing network connectivity and resource consumption for specific types of talker/resources can help to define policies for specific environments in a manner that's cohesive enough to support automated or semi-automated actions.

Although, the number of users who deploy automated actions is increasing, a vast majority of IT skeptics still express major reservations about allowing any automation beyond notification and trouble ticket generation. Be prepared to wean yourself and your team from such traditional caution as vendor solutions mature. New technology trends such as virtualization and Web services and service-oriented architectures (SOA) will require that IT professionals overcome their inhibitions in trusting automated management capabilities.

Invest in tools that help you recognize the applications that traverse the network are not all the same:

Many applications, as they traverse the network, present conflicting management requirements. Perhaps, the most dramatic instance of this is recent experience with VoIP introductions into the environment where VoIP was treated as “just another application” with often disastrous resulting consequences. VoIP sensitivity to latency, jitter and other parameters has

**SOLARWINDS**Free eBook

The Shortcut Guide to Network Management for the Mid-Market




Chapter 1: FCAPS, Network Management Fundamentals and Fault Management

Chapter 2: Performance Management

Chapter 3: Configuration Management and Security

Chapter 4: Network Troubleshooting and Diagnostics

DOWNLOAD NOW



www.solarwinds.com

proven to be uniquely detrimental. This was aggravated by the use of management tools that did not encompass functionality specific to VoIP requirements. For example, the inability to determine the specific paths of inbound and outbound packet transmissions often resulted in poor MOS scores, as well as dropped conversations that were difficult to troubleshoot and therefore remediate. As another example, client server and Web-based applications have distinctive requirements for monitoring quality of experience (QoE), with client-server tending to be more agent-driven and Web-based applications more pervasively monitored by observed and synthetic response times. And Web services and SOA-based applications will further challenge network managers by placing an absolute requirement on real-time awareness and control.

As the mix of applications in the environment increases, the need for tools that can focus on specific application requirements in real time will become more essential. The growing usage of flow-based tools — be it NetFlow, sFlow, or a number of others in use — addresses network behavior in support of the changing application mix. These flow-based tools focus on relationships between IT infrastructure components and provide information about real-time and historical information on network behavior, and bandwidth usage by network traffic such as HTTP or VoIP. In addition, flow-based tools can address security and compliance issues, what users are the “top talkers”, profile networked application usage, and expedite troubleshooting networked application performance issues. Flow-based data are also used to help generate usage-based insights relevant to capacity planning and even financial planning based on service consumption and real user demand.

Summary

Businesses of all sizes face a number of challenges in addressing network service stability. The dynamic nature of network service behavior and shortage of technical staff in many IT shops necessitates multi-

phase lifecycle process supported by reliable and flexible tools to achieve network stability. As change in requirements on network service increases, network operations needs to execute a broad range of tasks to stabilize the network services over accelerating frequency of life cycle. These include:

- Setting a viable definition of network stability based on current conditions and requirements.
- Establishing baseline to help plan for the lifecycle management of the network.
- Investing in a more cohesive approach to data gathering for more efficient operations and management activities.
- Preparing to leverage analytics and automation to alleviate increasing number of transitory issues and shortage of IT staff to troubleshoot them.
- Appreciating and documenting the unique requirements of increasing the number and type of applications as they traverse your network.
- Deploying a cohesive set of tools that supplement rather than duplicate management information.

Stabilizing your network will require you to convert information obtained from monitoring along with determining the behavioral patterns, and converting this knowledge into long-term strategies and quickly executable tactical procedures. But self-empowerment isn't magic, simple or fast. Being effectively proactive also means accepting the fact that there are no “silver bullets” just life-cycle adjustments to accommodate the dynamic nature of network services.

© 2007 Network World, Inc. All rights reserved.

[To request reprints of this special briefing contact networkworld@reprintbuyer.com](mailto:networkworld@reprintbuyer.com)