Managing Networks in the Age of Cloud, SDN, and Big Data: Network Management Megatrends 2014

Research Summary

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) Research Report
Written by Jim Frey, Tracy Corbo

April 2014

Sponsored by:

Silver Peak

IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Table of Contents

Executive Summary

Networks have never been more critical to the success of IT and the business. New virtualization and Cloud technologies and services are remaking the face of IT and the way in which infrastructure is architected. But the common thread throughout is the network, which must be both highly available and high performing. The tools, technologies, and practices of network monitoring and management address these needs, and are thus essential to the success of every enterprise and governmental organization.

This Enterprise Management Associates® (EMA™) research report takes a detailed look at the current state of networks and network management, and examines five major areas of change and evolution affecting network management, including Cloud and virtualization, Software Defined Networking (SDN), big data, the rise of log data and APIs as management data sources, and the ongoing convergence of network operations teams and tools. The report also examines the context and influence that broader IT and organizational priorities and projects are having on network management priorities, as well as resulting requirements for network management products and solutions. The findings within this report reveal the experiences and objectives that a broad range of organizations have had regarding network management, and thus should serve as a source of requirements and input for strategic network engineering and operations planning.

Introduction

Enterprise Management Associates® (EMA™) analysts closely follow the evolutions and revolutions of managed enterprise network environments and how that is impacting best practices for monitoring, troubleshooting, and designing modern networks. One key item that separates today's networks from networks of old is that modern networks are expected to be more than just highly available – they must also be high performing, because the business relies on them. Network availability and performance are, more than ever before, a critical part of the way in which IT supports the enterprise. As new initiatives such as cloud, virtualization, and big data are gaining popularity; it is up to the network engineering and operations teams to ensure that network services can adapt to those changes and fulfill the roles of connection and delivery.

Over the past several years EMA has conducted a series of research studies, which EMA calls "megatrends" reviews, that are designed to cast a broad net around both macro and micro factors affecting network management tools, technologies, and practices. This study represents the third such megatrends study. For this latest version, we have carried forward a number of ongoing questions and threads that are designed to track how the network management landscape is changing over time. We've also included many new questions and queries intended to help us characterize and quantify the very latest new technology trends, be they evolutionary or revolutionary. In particular, new questions were added in this report to begin assessing the influence and impact of Software Defined Networking (SDN) and big data phenomena, while checking in on the ongoing impact that cloud and server virtualization is having on networks and network management.

What we found were a number of interesting variations in both priorities and practices across the enterprise community as a whole and also in the contrast between responses provided between various subgroups within the respondent base. In particular, cloud and virtualization continue to be a problem for networking professionals, SDN is still an emerging phenomenon with as many questions unanswered as answered, and big data appears to be having a recognizable impact on networks and network management practices.

Setting the Stage, Part One – The Managed and Management Environments

Snapshot of Existing Managed Environment

While the number of employees may be a relatively good measure of the size of an organization, and hence the challenges with managing its IT infrastructure, a more direct measure can come from understanding precisely the number of devices under management. And for the purposes of the study, those devices are most relevant when they are network devices, such as switches, routers, load balancers, access points, optimizers, and other in-line network devices that perform specific network functions. When we asked about the size of the managed network environment in this way, we received responses as shown in figure 1.

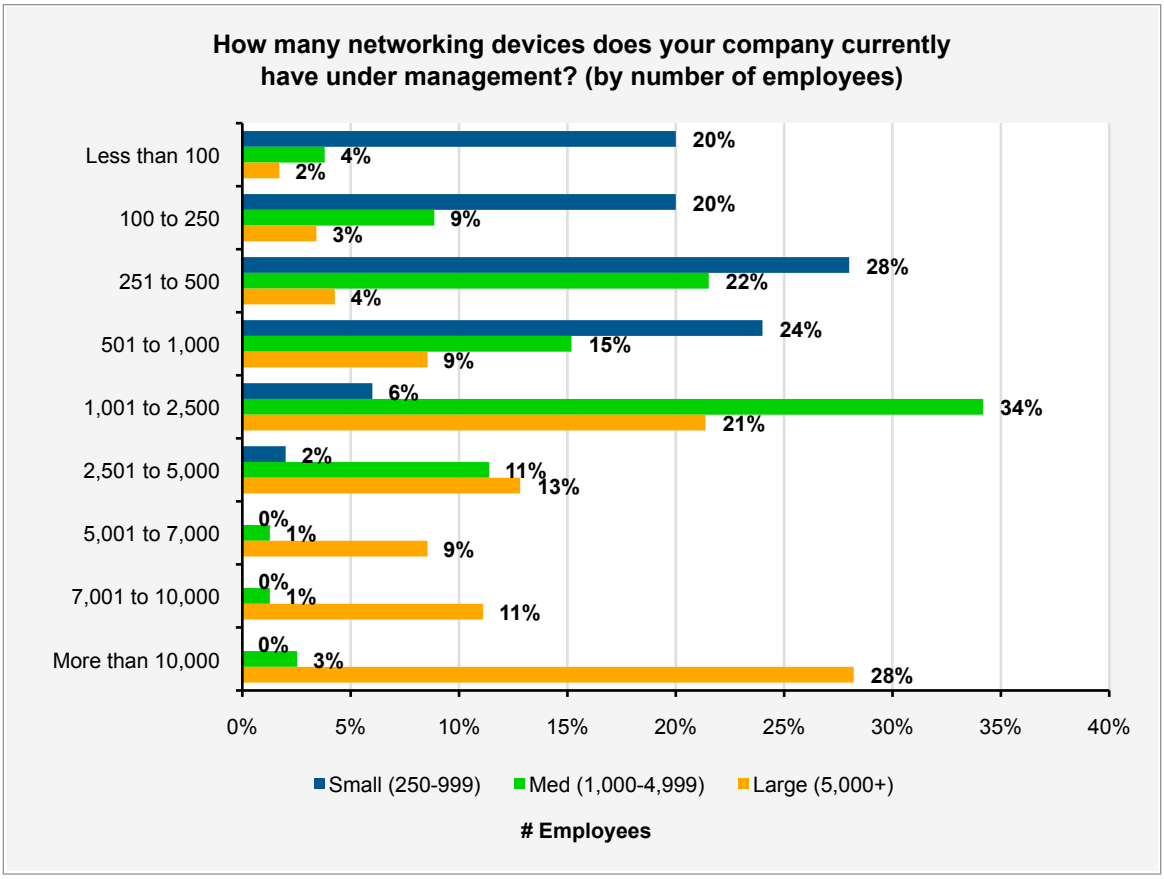

Figure 1: Number of networking devices currently under management, by organization size.

These results show that by and large, the number of devices under management tracks fairly closely to the size of the organization in terms of number of employees. However, there are a few clear outliers – small organizations with very large networks and large organizations with relatively small networks. As EMA continued its analysis, EMA found that the number of managed devices was a good way to differentiate responses to certain questions – particular those that had to do with technical requirements and feature values within network management tools and technology.

A Look at Root Causes (a.k.a. It's Not Always the Network)

Whether being reactive or proactive, a lot of time is spent by networking pros trying to figure out what is at the root of reported or growing problems. A considerable amount of network management technology is also aimed at answering this question, even though the answers very often lie beyond the realm of the network itself. We took the opportunity to ask the participants what their experiences have been in terms of what lies behind the issues and problems that they have managed to resolve.

The interconnected nature of today's highly virtualized and distributed IT infrastructures, combined with increasingly sophisticated and complex application architectures, makes performance degradation troubleshooting far more challenging than full failures and outages. Understanding the root causes of degradations is more difficult to quantify because of the wide variety of potential failure modes and a wide range of independent and specific environmental qualities and conditions. EMA's approach to gathering some insight was to seek empirical data regarding the participants' most recent experiences. Shown in figure 2 are recent primary root causes of difficult performance/degradation issues – those that required collaboration across technology teams to solve.

Figure 2. Recent root causes of difficult performance/degradation issues.

In these results, we found some notable discord. First off, our study is largely focused on the networking function, and participants tend to point the finger at others when asked who is to blame. Despite this, the top two issues were networking related – performance/congestion and problems related to configuration changes. The other notable result is that with some small variations, many other root cause sources can and do exist. Storage comes out relatively innocent, though it is mentioned by one in four. In the middle are four root causes that each got roughly 1/3 of respondents' mentions – server

systems including VMs, security systems, application design, and end client system/user. While there is no one place to lay all the blame, it does indeed appear that the network may be the most legitimate starting point when seeking the root cause of performance issues.

An Avalanche of Tools

There is no one tool to rule them all in the NOC. After many years of dialogue with enterprise networking pros the same theme seems to persist – network operation teams use a mix of tools to do their job. As part of this research, EMA took the opportunity to ask the participants just how many tools they indeed were using for network monitoring and troubleshooting, and responses are shown in figure 3.

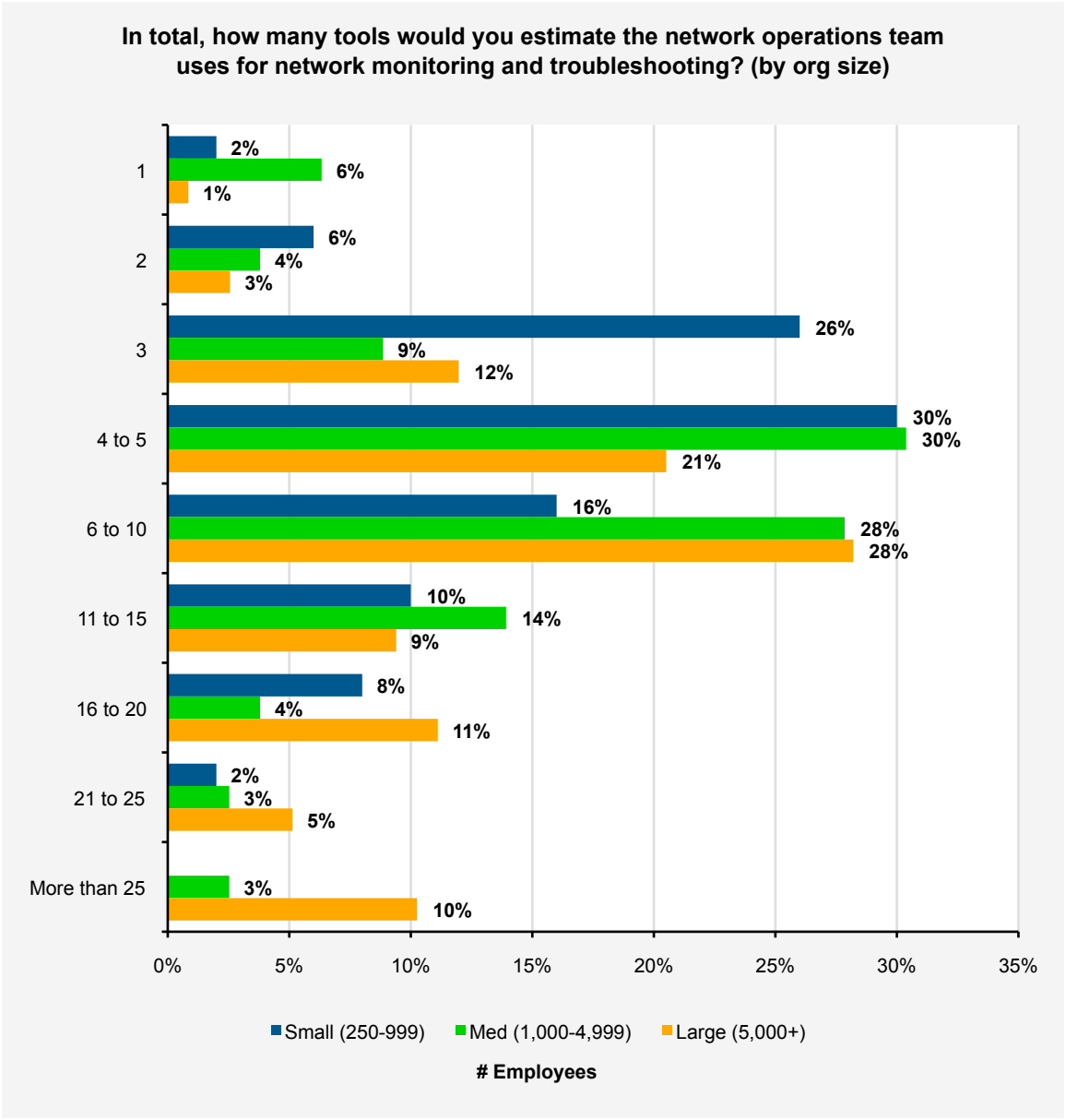

Figure 3. Estimated number of tools in use by network operations for network monitoring and troubleshooting (by organization size).

EMA was quite simply amazed by the answers received to this question. While a few shops have only a handful of tools (less than 5), the vast majority of organizations are still dealing with far too many. There is a direct correlation between organization size and the number of tools in place. Small organizations report 3 or 4–5 tools in use while medium-size organizations claim anywhere from 4–5 to upwards of 10. Large organizations indicated 6–10 tools as the norm, but other large organizations claimed upwards of 25 or more tools in use. And surprisingly there were even some small organizations (20%) with 10 or more tools in use.

The bottom line is this – there are many tools in use, because no one solution provides the level of visibility and cross platform support most enterprise network operations teams need to do their job. The problem with this approach is that it is fragmented and it is difficult to maintain and keep all the disparate components in sync with one another. Each tool must be individually installed, configured and maintained. Integration between tools is often a manual process. Not only can this negatively affect work efficiency, but also ultimately will lead to less total cost efficiency.

Setting the Stage, Part Two – Networking and Broad IT Initiatives

Key Networking Initiatives Affecting Network Management Priorities

One of the key objectives of this study was to understand which specific technology initiatives are impacting network management priorities. Because we know initiatives both inside and outside the domain of networking can influence project prioritization, we asked about both networking and non-networking initiatives. First, respondents were asked which networking-related initiatives within their organizations were affecting their priorities around monitoring and managing networks and networked application performance. The responses to this initial question are shown in figure 4.

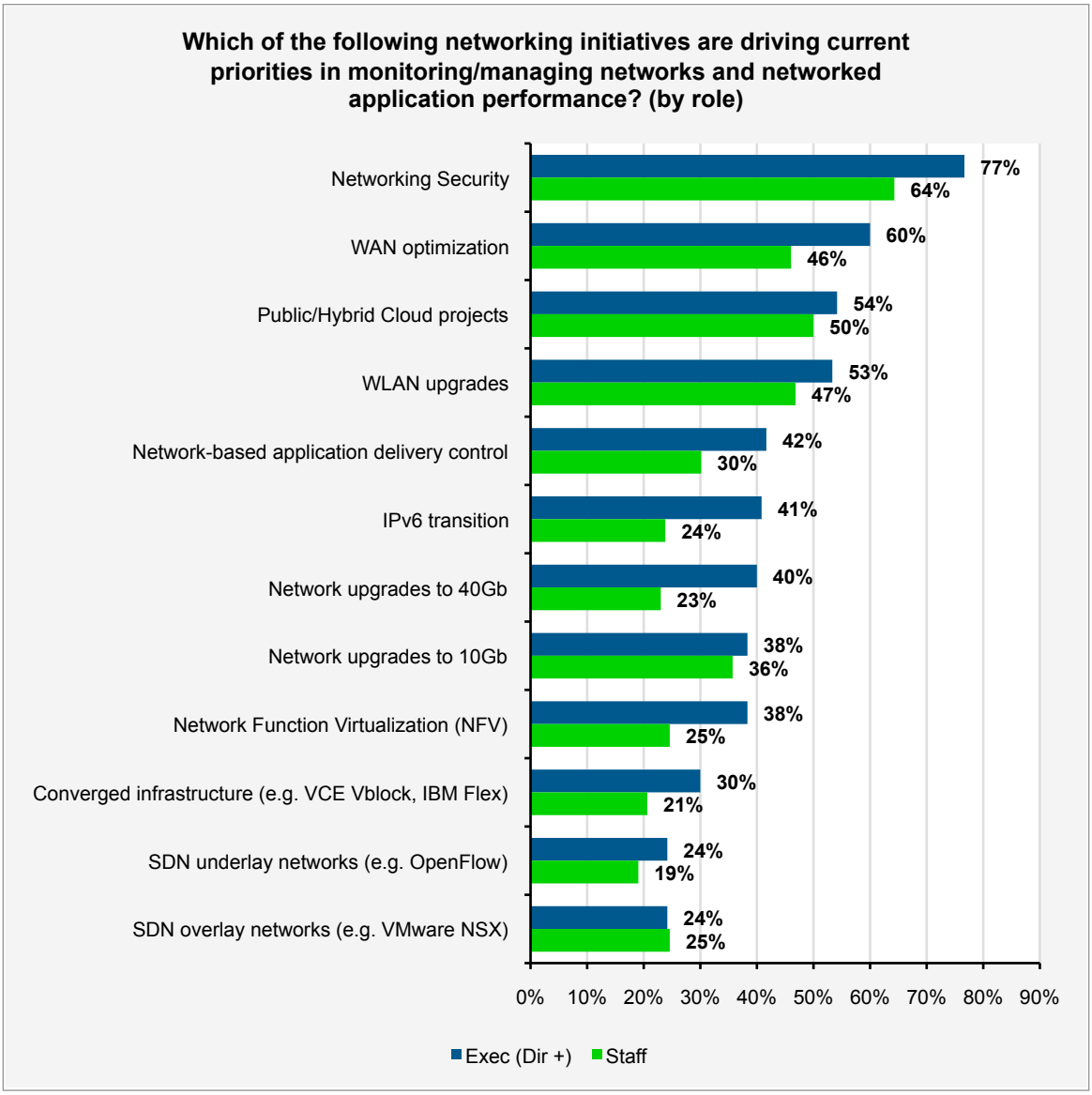

Figure 4: Networking initiatives driving current priorities in monitoring/managing networks and networked application performance.

It is no surprise that when security appears on any priority list, it almost always receives the most attention. This was indeed true for this study and it was true in the prior version of this study in 2012. This was also true no matter who was asked. While we received the strongest response (82%) among small organizations, it was the top response from organizations of all sizes, and no matter how you sliced the data, such as by industry vertical, security remained the biggest impact initiative.

Despite rumors to the contrary, WAN optimization is not dead. This study indicated a huge resurgence of focus and interest in WAN optimization – from 37% in 2012 to 53% in 2014. While the WAN optimization market may not be growing at the same rate it once was, these results indicate that it continues to be a top priority of IT shops regardless of size of the business. Obviously, the level of importance is higher in businesses that have more branch and remote locations, such as healthcare and finance verticals, that not only have many remote locations, but also require high levels or performance. But the takeaway was clear – WAN optimization projects are still being funded and are a high priority for networking and network management.

One of the big movers from 2012 to 2014 was public/hybrid cloud projects. The growing number of cloud solution providers and general acceptance of cloud from concept to reality has helped accelerate market growth. Since 2012, cloud projects have moved from early adopter status to mainstream business initiatives, and their impact on network management grew from 36% in 2012 to over 50% in 2014.

Despite all the press that SDN enjoys, the hard-core reality is that SDN is not ready for the enterprise. While bleeding-edge service providers and greenfield build-outs might fully embrace SDN as the next-gen network design infrastructure, established, mature enterprise IT department are going to "wait and see" which way the wind blows. As indicated here, SDN is not a major impact factor at this time, and remains primarily an interesting test case, still in the research and evaluation stage (see more details in Megatrend #2).

Broader IT Initiatives Affecting Network Management

Beyond specific networking initiatives impacting network management, EMA sought to understand the impact of broader IT initiatives. Almost every IT initiative will have some impact on networking and network management, some direct and some indirect. We asked our respondents about the relative impact of initiatives ranging from server virtualization to VoIP and cloud to ITIL, and many others, and their responses are shown in figure 5.

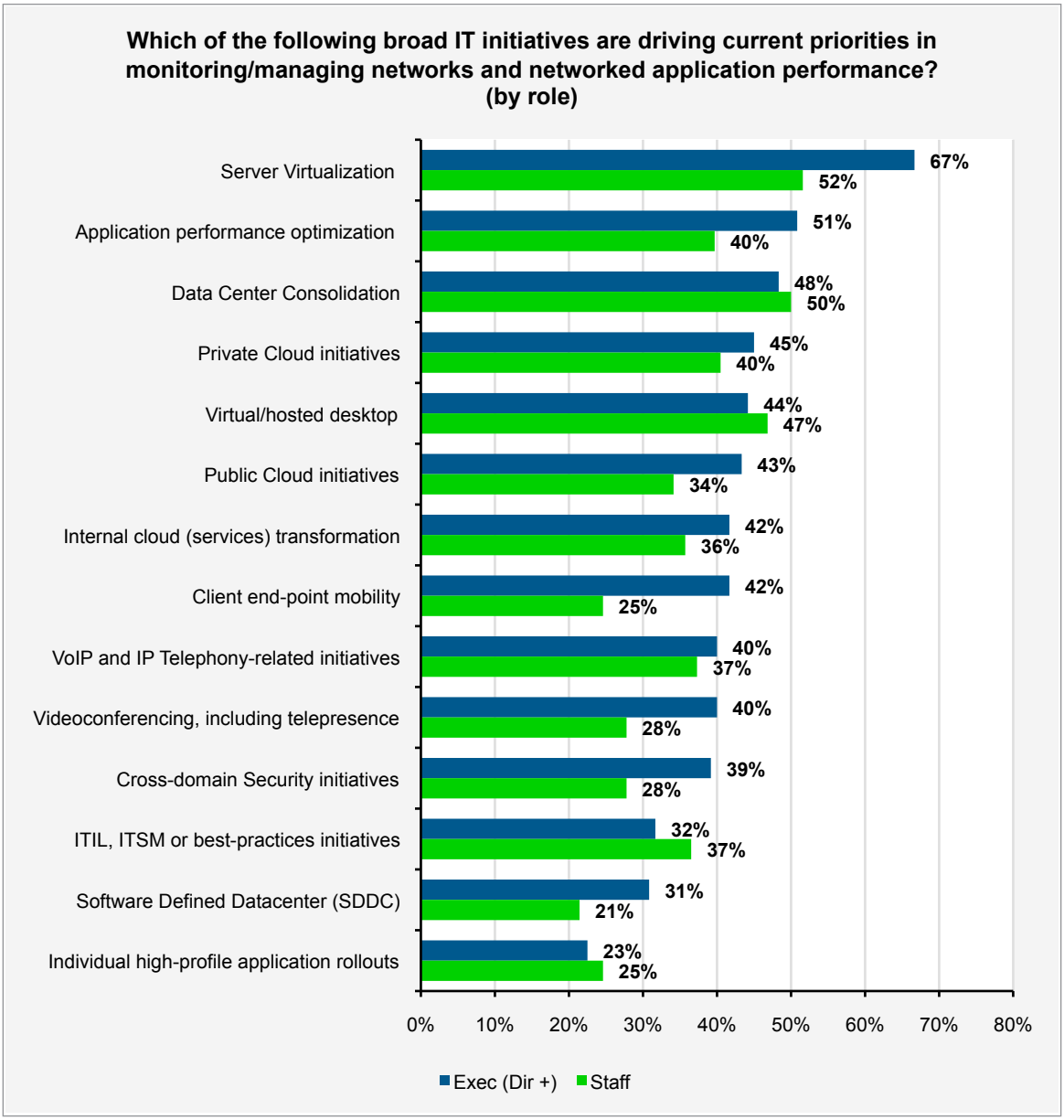

Figure 5. Broad IT initiatives impacting priorities for network management.

While this is a very long list, some important trends can be identified. For the last six years, server virtualization has had the greatest impact regardless of organization size. This was the case in 2008 in the first Megatrends report, and again in 2012. Server virtualization has the largest impact across all verticals, both role groups (though execs indicated this influence at a higher rate than staff – 67% vs. 52%) and all organization sizes. In fact, it was the only technology initiative that garnered a majority response across every subgroup within this study.

Data center consolidation, virtual/hosted desktop, and application performance optimization rounded out the top four in 2012 and did so again in this 2014 refresh, though in slightly different order. Data center consolidation is a higher priority within the largest organizations (56%) and among the manufacturing vertical (65%). Virtual/hosted desktop was favored most heavily by healthcare (59%). Application performance optimization was considered as having a greater impact by execs (51%) versus staff (40%) and in the manufacturing vertical (55%).

In the 2012 survey EMA asked about public/hybrid cloud initiatives as a combined choice and this year EMA split up the choices to see if any specific cloud initiatives were more significant than others. Interestingly, among this group of respondents, private cloud initiatives (43%) were slightly ahead of public cloud (39%) and both have grown from the original private/public cloud initiatives of 36% in the 2012 survey. Digging a bit deeper, EMA found that the manufacturing sector was the strongest proponent of private cloud (55%) and public cloud (45%) with other verticals averaging 43% for private and 39% for public cloud initiatives. It should be noted that EMA was surprised to see that cloud was not a relatively higher priority in small organizations.

Similar to observations regarding SDN, Software Defined Data Center (SDDC) was definitely of interest but showed relatively low impact in contrast to other initiatives. This is not really surprising, since it is more of a data center-centric initiative at this point in time and has focused first and foremost on server resources. That said, SDDC will require further monitoring as the impact of virtual overlay networking solutions such as VMware NSX continue to grow in the data center.

WAN Connectivity Persists, Grows, Adapts

Traditional WAN connectivity typically involves expensive, bandwidth-constrained links. Such links can be a significant source of latency, and are thus often one of the most common points of congestion and packet loss. The widespread availability of broadband Internet connectivity has given rise to alternative WAN connectivity choices in the form of managed Internet services and multiplexing multiple unmanaged Internet links. EMA has been monitoring the growing interest in these alternative WAN solutions and as part of this study wanted to test the waters to see if there is any data to support a move away from traditional WAN connectivity.

First, EMA asked the respondents about their plans in the coming year for expanding or reducing their WAN/remote connectivity. EMA qualified WAN/remote connectivity as one of three types:

- "Managed services" refers to dedicated links such as MPLS, Frame Relay, and metro Ethernet offered by communications service providers.
- "General Internet" refers to unmanaged connectivity, via traditional ISP and local broadband connections.
- "Managed Internet" refers to optimized business internet access via local broadband connections (e.g. Akamai, Aryaka).

In figure 6 we see that very few respondents (less than 10%) indicated plans to reduce their WAN connectivity. What is most interesting is that more respondents will be maintaining the same type of WAN connectivity, neither adding nor reducing services. In terms of new WAN connectivity planned the edge goes to *managed services* being the most likely category to see expanded use in the next year, showing particular favor among mid-sized and financial services subgroups. The lack of strong differentiation along connectivity type is interesting.

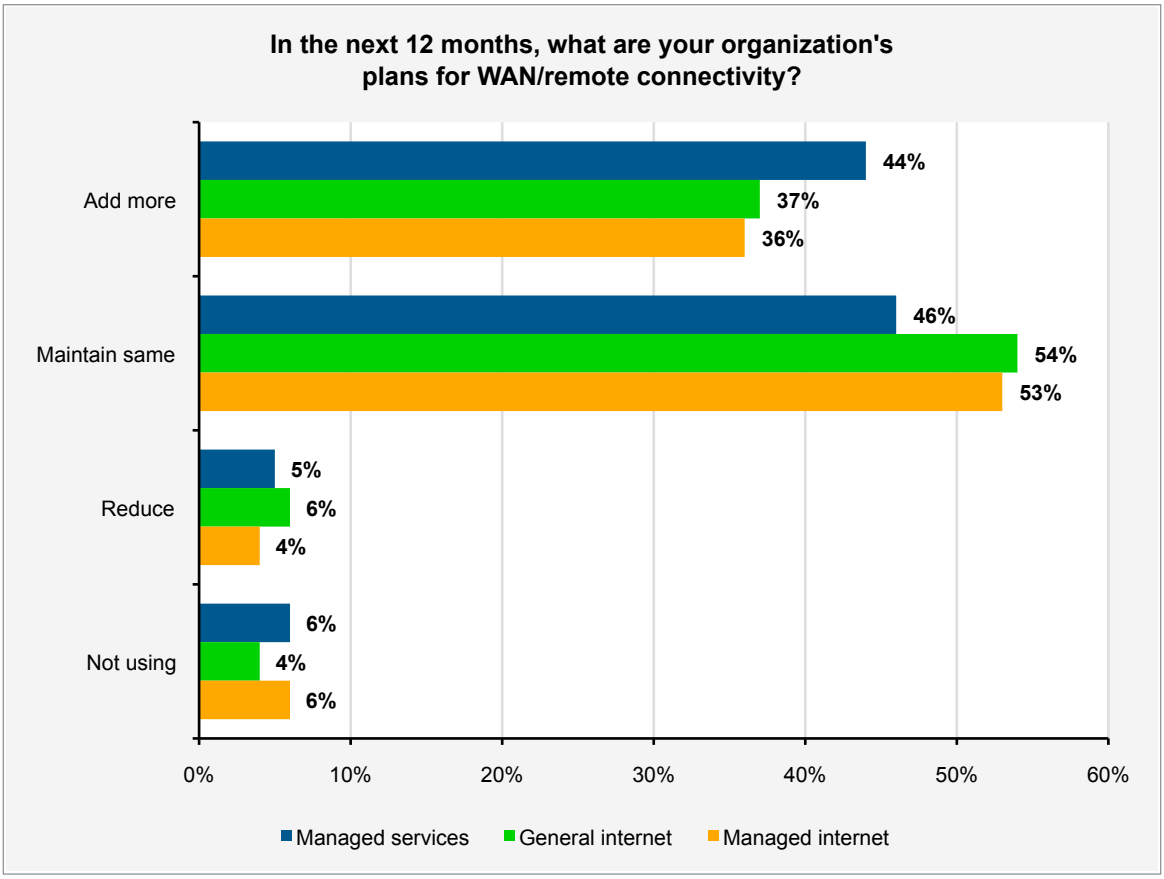

Figure 6. Plans for WAN/remote connectivity in the next year.

Second, we asked respondents whether or not the mix of WAN connectivity choices is changing and if they were planning to replace traditional managed services WAN connectivity with alternatives such as general Internet access or managed Internet. Originally, traditional managed services were the only game in town for remote site connectivity, but the public Internet and broadband have given rise to new ways to connect remote sites. Public Internet and VPNs create their own unique performance, reliability and security challenges, but the increased mobility of today's workforce means companies are already dealing with those issues. What matters is that there is now a choice that did not previously exist, and mobility is teaching organizations what does and does not work over public Internet connections. So respondents were asked if they had any plans to replace their managed services with one of the other options, and their responses are shown in figure 7.

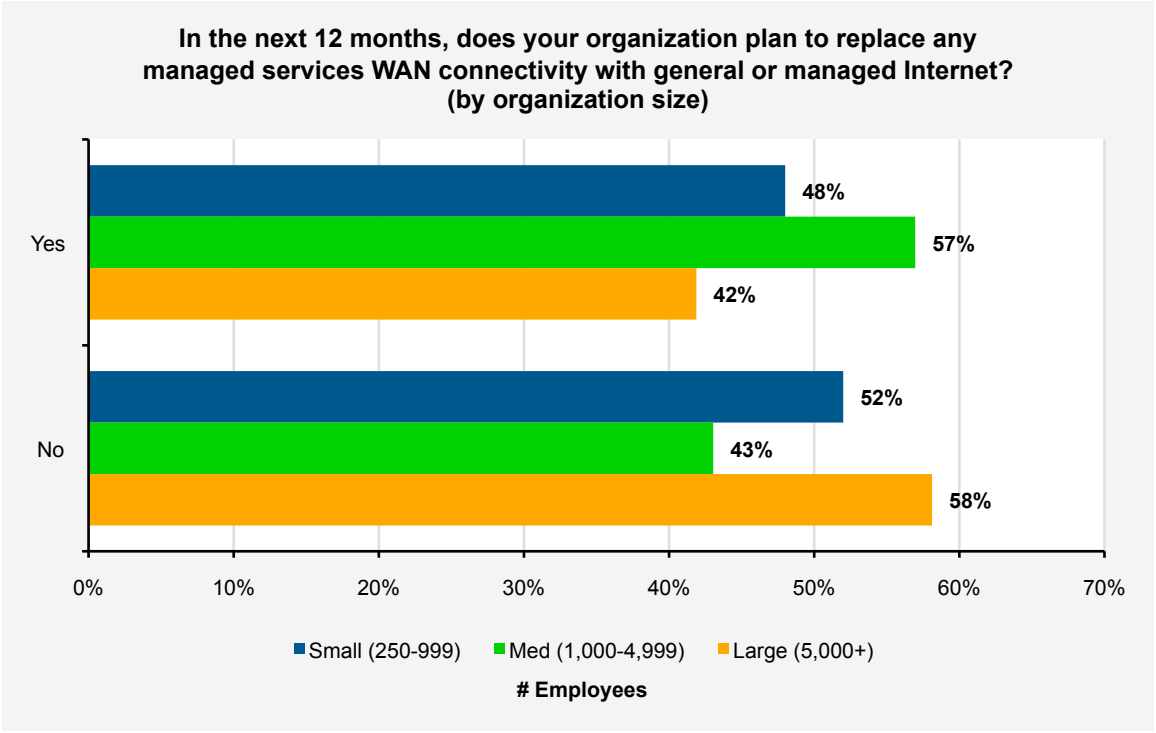

Figure 7. Organizations planning to replace managed services WAN connectivity with general or managed Internet in the next year .

Clearly, this seems to indicate that a significant number of organizations are indeed reevaluating their mix of traditional versus nontraditional remote connectivity. But as with the growth plans above, there were clear differences in responses based on the organization size. Medium-size organizations seem most interested in making this change, while small and large organizations are less so. This is likely due to the fact that small organizations are already less likely to be using expensive managed services, and large organizations are likely able to leverage purchasing power to reduce the cost of managed services in a more successful manner than medium-sized businesses.

Megatrend #1: Cloud and Virtualization Still a Work in Progress

For the past several years, EMA has been tracking the impact that virtualization technologies have had upon the tools, technologies, and practices of network management. In particular, server virtualization brings with it new infrastructure in the form of virtual network components and topology that require both visibility and control measures. Networking pros are held responsible for performance and availability of networks end to end, including virtual links; however, they often are given neither the control nor the visibility they need to be fully successful and efficient.

Cloud services are built upon virtualization technologies, spanning server, networking, and storage domains. With no access to physical infrastructure, those subscribing to external Cloud services will only have access to virtual elements for visibility and control purposes.

Cloud services are slowly and steadily achieving mainstream status within most organizations, and EMA wanted to understand how the respondents were feeling about their ability to do their jobs in these complex environments.

EMA wanted to gauge how good of a job current sets of tools were doing in providing visibility and control into the various cloud environments, contrasted against the internal data center. Results are shown in figure 8. Of these environment choices, internal data center is the piece of the puzzle into and over which IT organizations should ideally have the greatest visibility and control. As expected, the internal data center received the most positive results, especially from respondents that were in large enterprises. But the results also show that as cloud deployments become more mainstream, the tools for providing adequate control and visibility in the cloud need to catch up. It should be noted that respondents who replied "none of the above" do not feel that they have adequate visibility or control in any of the listed environments.

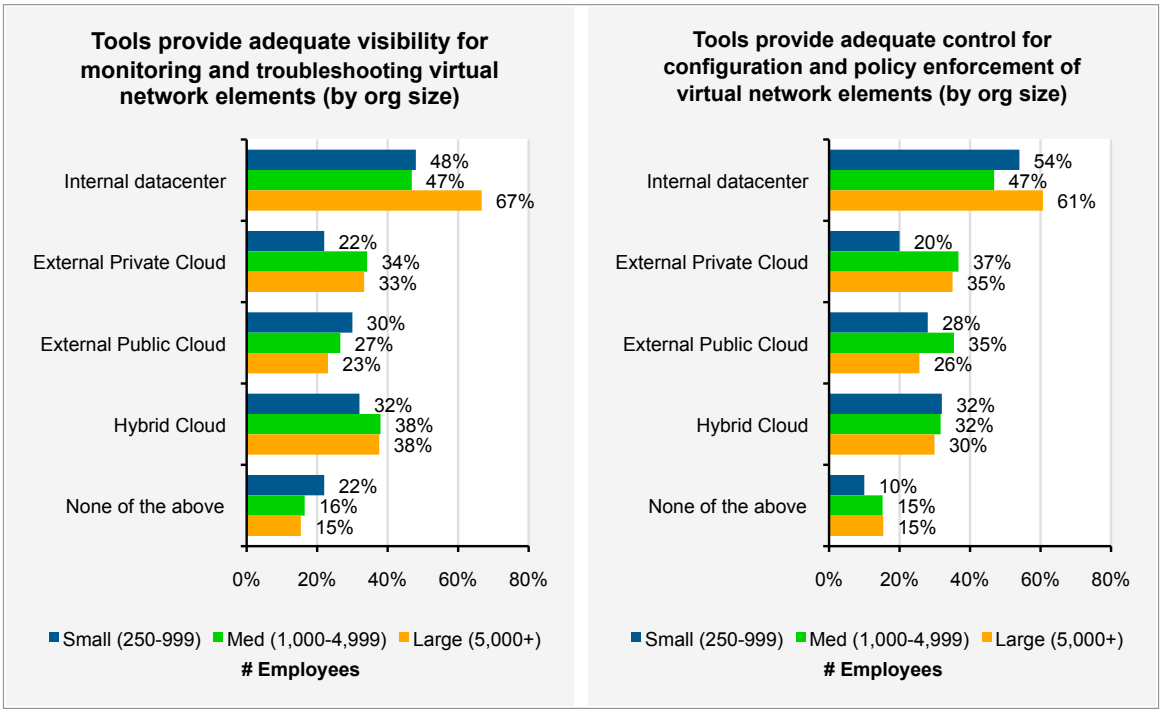

Figure 8. Network visibility and control adequacy in various Cloud environments.

Megatrend #2: Early Days for SDN and SDN Management

Software Defined Networking (SDN) technologies are slowly solidifying into tangible solutions, but far too many unknowns still exist with respect to how these new, software-centric, programmable networking techniques will affect management tools, technologies, and practices. SDN promises to be as disruptive, if not more so, than server virtualization. Given the ongoing management headache that server virtualization continues to be, it is fair to expect SDN will cause an even greater and longer lasting one.

SDN is a term that can encompass a wide set of approaches to network virtualization. For the purpose of this survey we focused on just two flavors of SDN. One form of SDN involves the use of technologies that change the behavior of physical network devices by splitting the control plane from the delivery plane and introducing new network controller elements. OpenFlow is the most often-cited protocol that would be used between controllers and switches in this type of deployment. EMA refers to this as an SDN "underlay" network. Another form of SDN technology is the virtual network "overlay" which creates a virtual network infrastructure that is independent of and rides over the existing physical network. Product examples of SDN "overlay" networks include VMware NSX, Alcatel Nuage, and Midokura MidoNet.

For the purposes of this research, EMA first asked our respondents to tell us what stage their organizations were at with respect to deploying underlay and overlay SDN technology (as defined above) and the results are shown in figure 9.

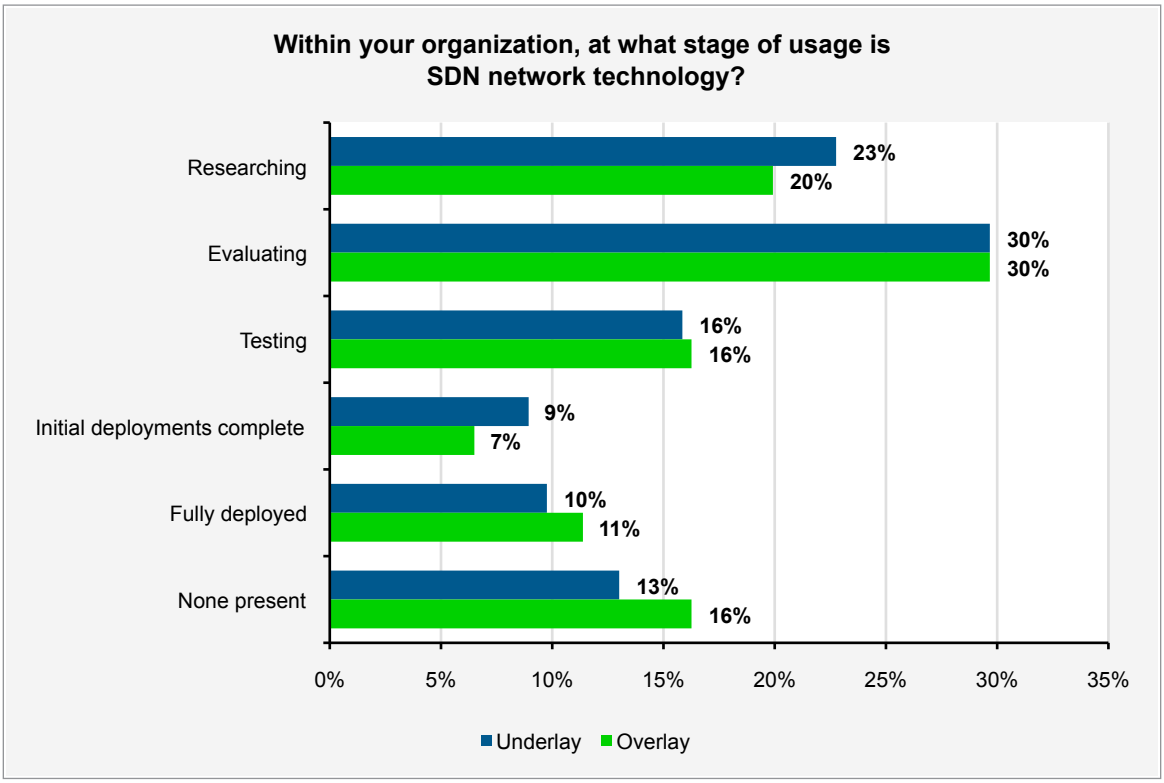

Figure 9. Stage of usage of SDN "overlay" and "underlay" network technology.

These results reinforce the fact that SDN technologies are still quite early in terms of market adoption and usage. Less than 20% of respondents have deployed, either initially or fully, underlay or overlay SDNs. But interestingly, the vast majority of respondents indicated that they were somewhere in the research and evaluation phase. This means that while only a few have gotten the point of actually deploying SDN technology, it is clear that enterprise shops are taking it seriously and are looking to determine how to best leverage the technology in their organization.

Finally, we checked with our respondents regarding their overall concerns with deploying and adopting SDN technologies, from a management and operations perspective. Their responses are shown below in figure 10. Within this view, we've identified how everyone responded (even those who indicated that they had not engaged in any SDN analysis or deployment) and have also shown responses from those who indicated either initial or full deployment of SDN overlay or underlay technologies.

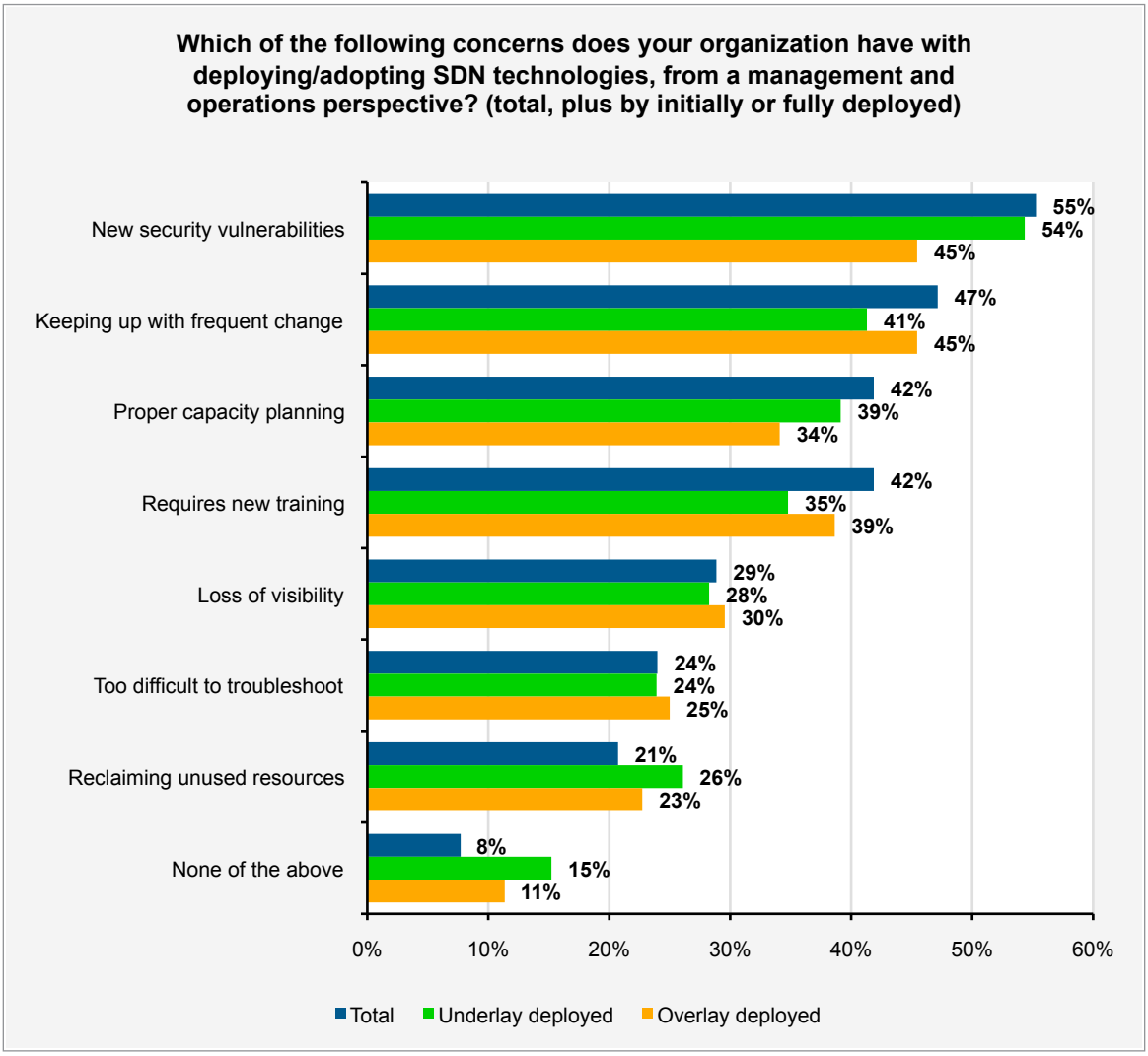

Figure 10. Management and operations concerns with deploying/adopting SDN.

The interesting thing about these results is that overall concerns tend to mirror actual experiences, with only small variations. For instance, those who have deployed overlays are somewhat less concerned than everyone else regarding new security vulnerabilities; however, that is still the number one overall response for that group. In general, those who have undergone deployments are a little less concerned with most of these topical areas, or at least the top four most common responses. The only case where those who have actually deployed SDN had concerns that exceeded the respondent group as a whole was with respect to reclaiming unused resources, and even that variance is quite small.

Megatrend #3: Big Data Shows Signs of Big Impact

The phenomenon of big data is vast and far-reaching, and as with many new, overly-hyped technology trends, represents far fewer truly new technologies than the many vendors and marketers out there would have you believe. EMA's definition of big data includes the concept of large volumes of structured or unstructured data housed in one of the new big data constructs such as Hadoop or Cassandra. Big data analytics, therefore, is a field concerned with guided/automated mining and analysis of data contained within such big data stores. Vendors of technologies all across the board, including many in the network management sector, are trying to hitch their wagons to the big data train. Some vendors in the network management sector are merely reinterpreting the term to describe large volumes of data that may be a common occurrence within their tools or approach. And some are using the term big data analytics to describe their automated data processing and analysis techniques. While EMA does not hope to resolve all of the conflicting messaging and claims out there in the marketplace, we decided to try and start capturing some of the perceptions among enterprise practitioners, specifically regarding how big data might intersect with network management.

To start with, we asked our respondent base whether or not they were using big data analytics to support any of their network management practice areas. Results are shown below in figure 11.

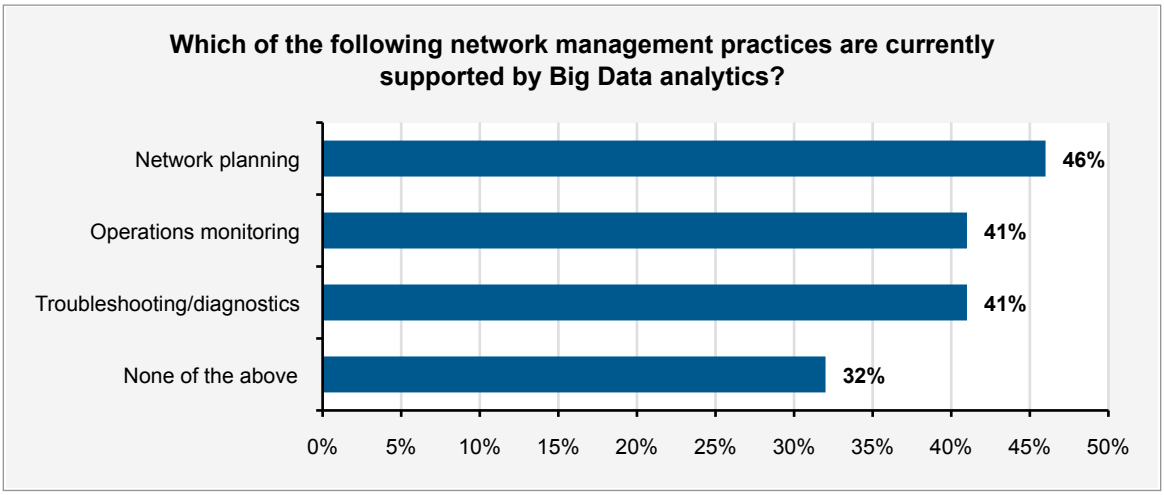

Figure 11. Network management practices currently supported by big data analytics.

What was surprising about these results are two things. First, a near-majority indicated regular use of big data analytics in each of the three practice areas – network planning, operations monitoring, and troubleshooting/diagnostics. Even more surprising was that only 32% indicated that none of these areas were being supported by big data analytics. This means that a large majority of our participants – 68% – are using big data analytics to support at least one of these use cases, and many are using them for more than one.

Another related use case that EMA wished to investigate was whether or not data normally collected within network management and monitoring systems was being exported for use in big data initiatives that stretched beyond network management. Results of this query are shown in figure 12.

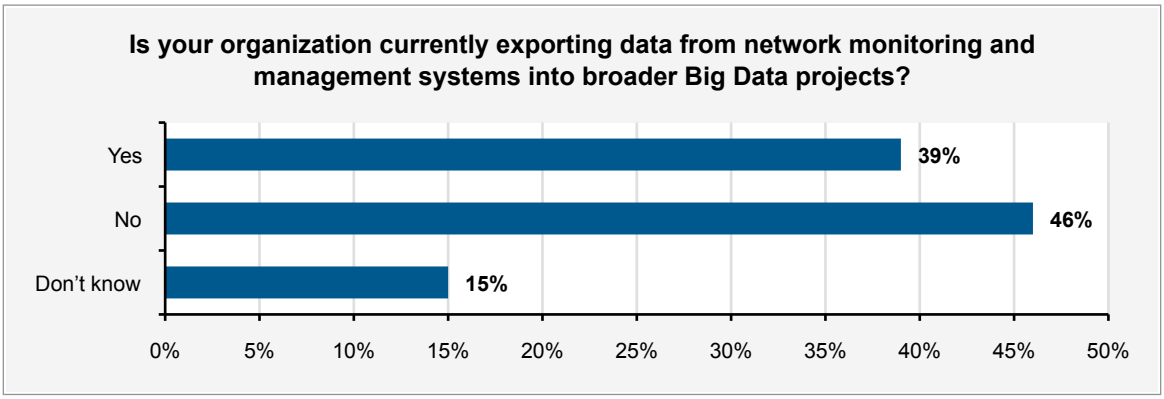

Figure 12. Organizations currently exporting network monitoring and management data into broader big data projects.

While a few of the respondents were undecided on this question ("don't know") a surprising number (39%) indicated that yes, indeed, data is being forwarded from network management systems into broader big data projects. Unfortunately the scope of this survey did not dig deeper into the details of these projects and how the network management data has been selected and used, but it does provide a point of inquiry for future analysis.

There was another theory we wanted to test having to do with the growing market hype we hear around big data's impact on the network itself. Our hypothesis was focused on two possibilities – higher traffic loads due to the collection of big data and higher traffic loads due to storage and backup related to the big data stores themselves. Responses are shown below in figure 13.

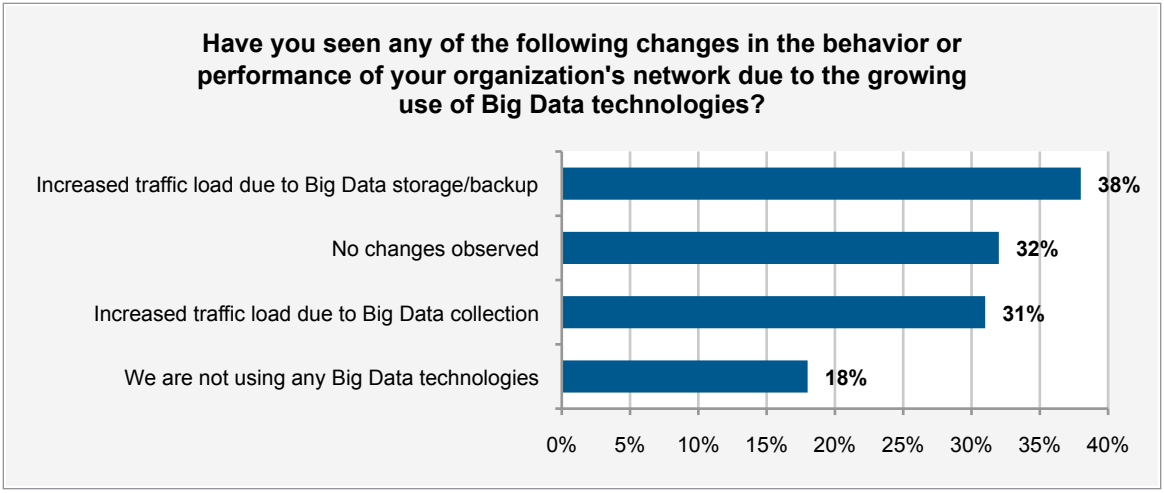

Figure 13. Changes in network behavior or performance due to growing use of big data technologies.

Fully half of our respondents indicated that they either had observed no changes or were not using big data technologies; however, the balance of our respondents have indeed recognized impacts, and some of them have recognized more than one type of impact. This points to a possible opportunity for network management solutions providers to ensure that big data traffic can be appropriately classified to ensure better capacity planning, monitoring and troubleshooting.

The clear takeaway is that big data technologies are impacting networking in a way that makes it relevant to network monitoring and management. Further in-depth study will be required to develop a detailed understanding of best practices to accommodate big data traffic and minimize its ability to negatively impact the network.

Megatrend #4: Changing Landscape of Data Sources: The Emergence of Log Data and APIs

EMA's *Network Management Megatrends 2012* study revealed a growing interest in log file analysis as a key set of features related to network management, particularly among staff members (versus executives). This has led to a number of follow-on points of study for EMA and was worth following up within this refresh to see if interest in log data had changed in any way. The 2014 survey results shown in figure 14 found a continued strong and growing interest in log file data for the purposes of multiple network management practices. The chart also shows the breakdown in responses between executive and staff.

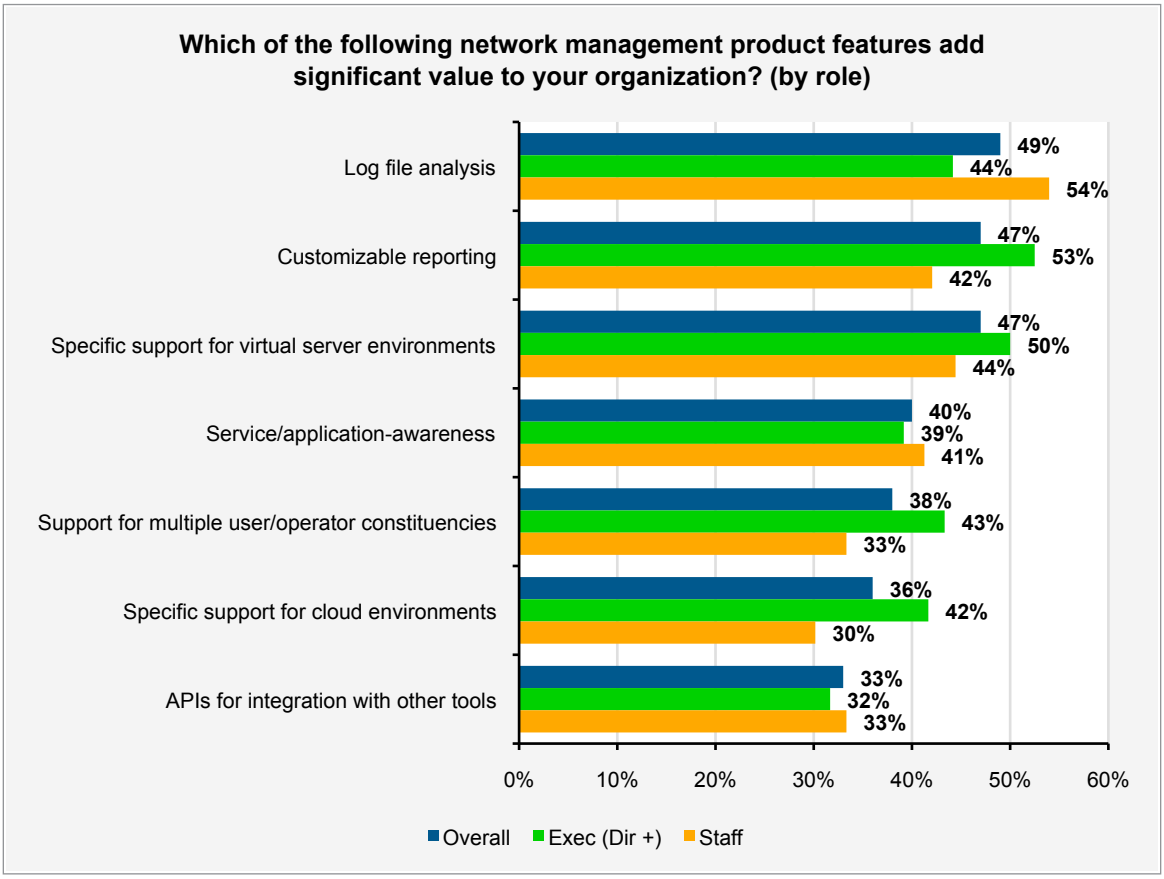

Figure 14. Network management product features adding most value.

The data in figure 14 is presented in order based on overall/aggregate response rates. But it is clear that there is a fair bit of contrast between executives and staff in terms of which is most and next most important. In 2012, executives called out reporting and virtual server environment support as their top two, while staff emphasized scalability and log file analysis. When averaged across roles, the top two were support for virtual server environments and flexible reporting, followed closely by log file analysis. These results in 2014 indicate the same priorities exist; however, in slightly different order. Further, average priority rates in 2012 were in the low 30% range, but now the top features are all well over 40% – a rise in focus on key priority areas.

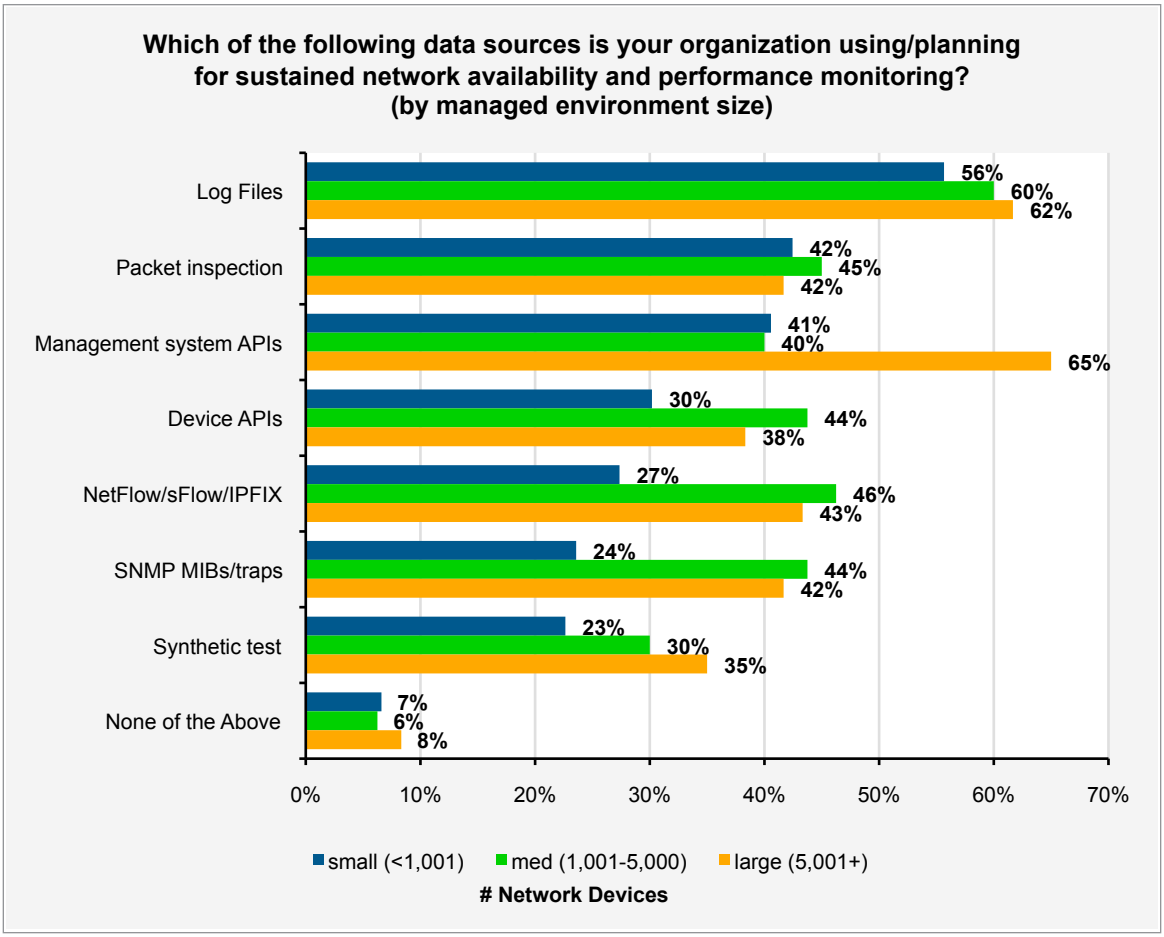

Figure 15. Data sources for sustained network availability and performance monitoring (by managed environment size).

We next asked about data sources used for network availability and performance monitoring, and results are shown in figure 15. Here, you can see that while log files continue to have strong significance across all three groups, in companies with large managed environments, management system APIs become the most important data source for sustained monitoring. Further, an interesting trend is present in terms of the relative rank of other data sources. For instance, while the use of packet inspection is similar amongst all three groups on a percentage basis, it's relative popularity drops from number two to number three to number five when moving from small, to medium, to large managed environments. As another example, NetFlow/sFlow/IPFIX is fifth-most popular among small environments, but second-most popular in medium environments and third in the largest environments. And finally, SNMP is seeing relatively low usage (less than 25%) in small managed environments but consistently higher use (greater than 40%) in medium and large managed environments.

It's also worth noting that in general, small managed environments are using fewer data sources as a whole as part of sustained monitoring. With relatively minor exceptions, those respondents who had small managed environments chose all of the data source options at a lower rate than those respondents who had medium or large managed environments. The clear conclusion here is that as your managed environment grows larger, sustained monitoring is more important and more data is needed in order to do so effectively.

EMA asked a similar question regarding data sources used or planned for network capacity planning and engineering purposes, the results of which are shown in figure 16. As with the monitoring findings, log files came out on top as the most prevalent data source, followed again by management system APIs.

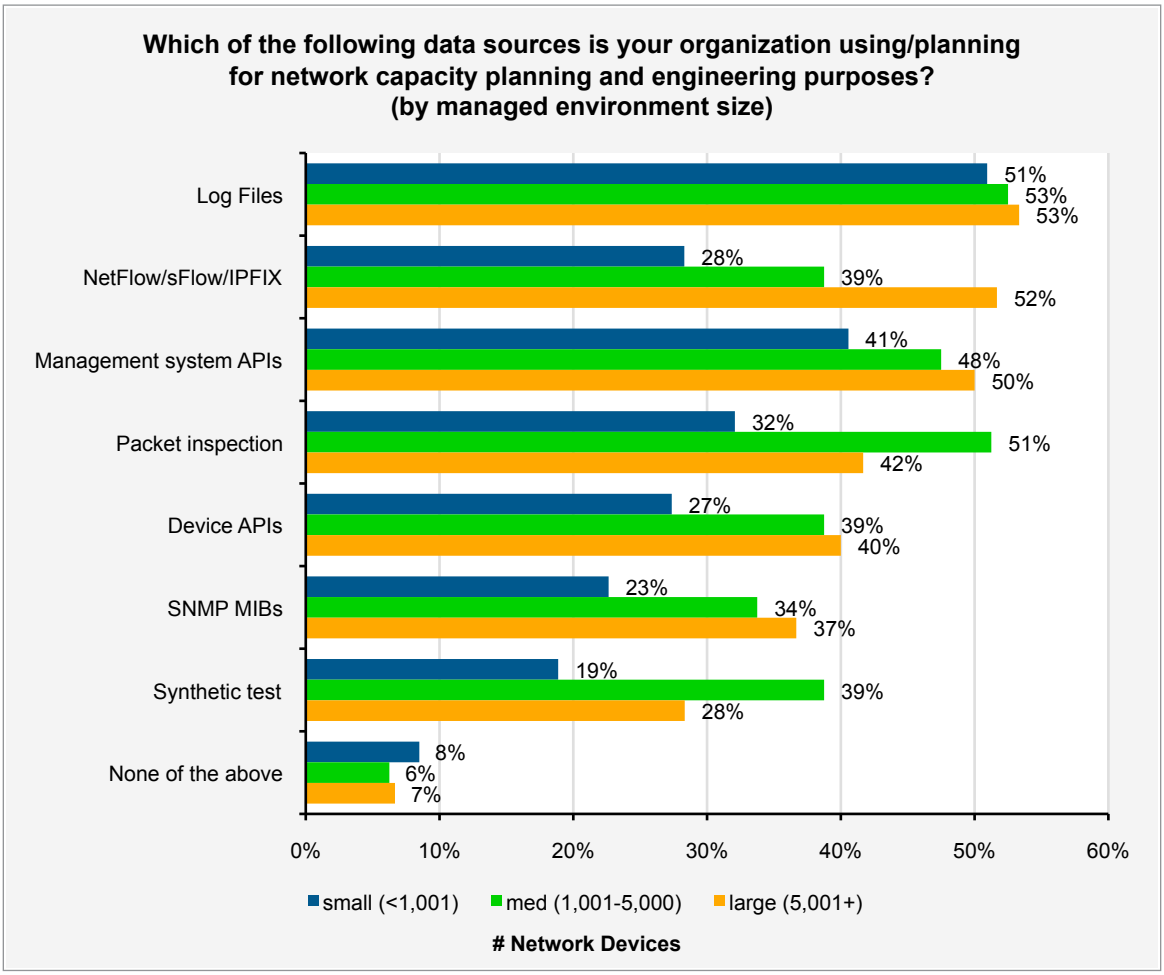

Figure 16. Data sources for network capacity planning and engineering (by managed environment size).

As observed in responses regarding monitoring, the smallest managed environments tend to use the fewest number of data sources for capacity planning and engineering. Log files, again, was the most popular answer regardless of managed environment size. But that is where the similarity ends. Medium-sized environments are leveraging packet inspection at nearly the same levels as log files and are using NetFlow/sFlow/IPFIX at a much higher rate than smaller environments. Large managed environments are using a fairly even mix of log files, management system APIs, and NetFlow/sFlow/IPFIX as their most important data types.

As the size of the management environment grows, the types of flow data in use also changes. For instance, packet inspection is used at a much higher rate within medium and large sized environments than by those in small managed environments, although the highest level of usage is in the medium-sized environments at 51%. There is also a direct linear correlation between the size of the managed environment and usage of NetFlow/sFlow/IPFIX data types. EMA believes this is a logical correlation,

because exhaustive packet inspection techniques become cost prohibitive in ultra-large, distributed environments. NetFlow/sFlow/IPFIX-based application awareness is a viable and more cost effective alternative for gathering consistent data in these instances, although rarely to the complete exclusion of packet inspection technologies.

The final data source question looked at those used for network troubleshooting. Figure 17 shows that once again, log files rose to the top as a dominant data source for network troubleshooting, outpacing even the long-trusted ping function and packet capture/analysis. Interestingly, Command Line Interface (CLI) was a source for network troubleshooting but did not fair as strongly as other sources, but at least for now any rumors of its imminent demise appear to be premature.

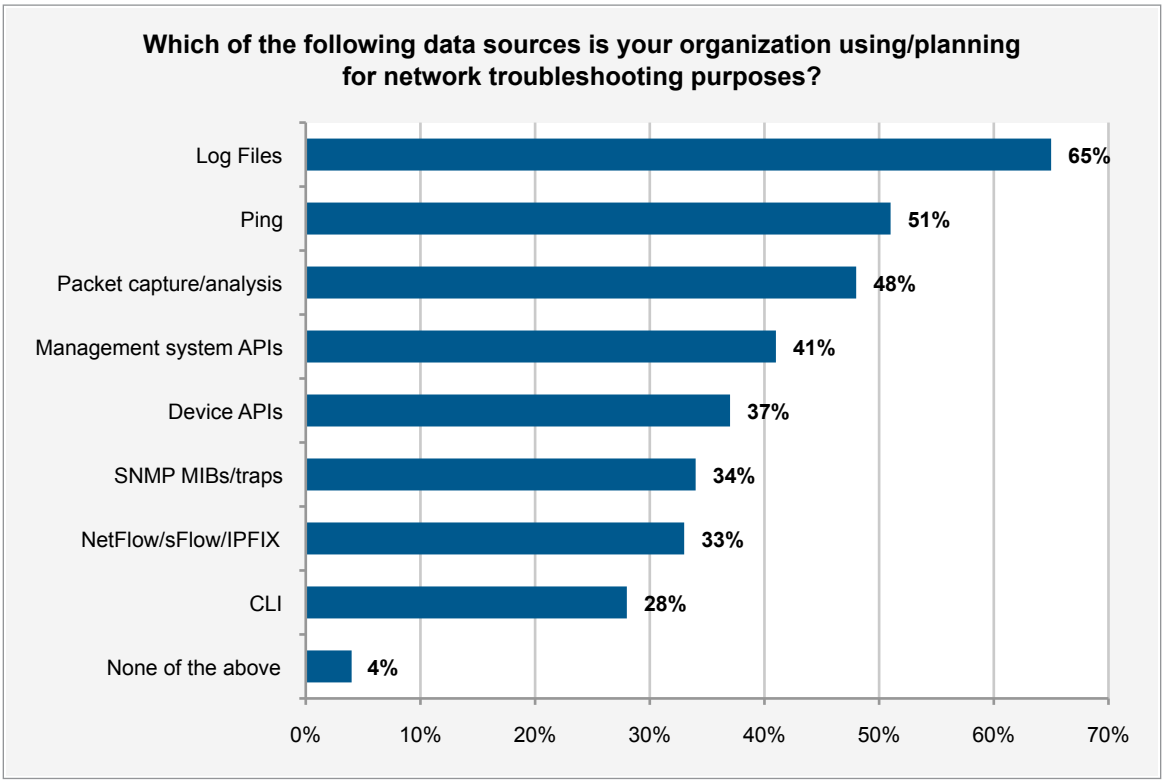

Figure 17. Data sources used or planned for network troubleshooting.

In this case, variations between the managed environment sizes were far less pronounced. The only notable difference was that larger and medium-sized environment respondents continue to use more data sources than those in small managed environments. Also, there was a slight uptick in use of CLI, ping, and device APIs in medium and large managed environments, and a slight decrease in use of management system APIs within large environments.

The biggest takeaway from this series of data points was that regardless of which network practice EMA looked at, log files are proving to be the most common and popular data source. EMA believes these results demonstrate that traditional network monitoring and management techniques are leaving out critical information regarding what is happening over the network. Also, EMA suspects that use of management system APIs, as well as device APIs, will continue to rise going forward due to the increased use of APIs as a primary management interface – particularly among the growing number of software-based networking technologies such as SDN, NFV, etc.

Megatrend #5: Convergence in Network Operations Teams and Tools

The way in which a network operations team is organized has a direct impact on both the practices of network management as well as the tools that are chosen and deployed. In parallel with the technologies within network management and the managed environment, EMA has been tracking the organizational aspects of those who use network management tools. Over the years, EMA has observed what seems to be a trend away from formally independent network operation teams/centers, long known as "the NOC," and towards more collaborative, cross-domain operations teams. This is consistent with parallel trends related to increased focus on service management and use of cloud services. But to date, EMA had not reached out to enterprise practitioners and asked them specifically whether or not they were moving into a formalized cross-domain operations model.

There have been a number of ways that the formal NOC has changed over the years. Some organizations have disbanded the formal network operation center and instead had operators work from wherever they were via shared on-line tools. Other organizations have outsourced network monitoring to third-party service providers. But the long arc of IT evolution towards an internal service provider model is causing some organizations to embrace a single, integrated operations team approach. Such teams typically bring together specialists from each of the major infrastructure technology domains (network, server, storage) with application operations and even security operations. We asked respondents about which direction their NOC was going and the responses are shown in figure 18.

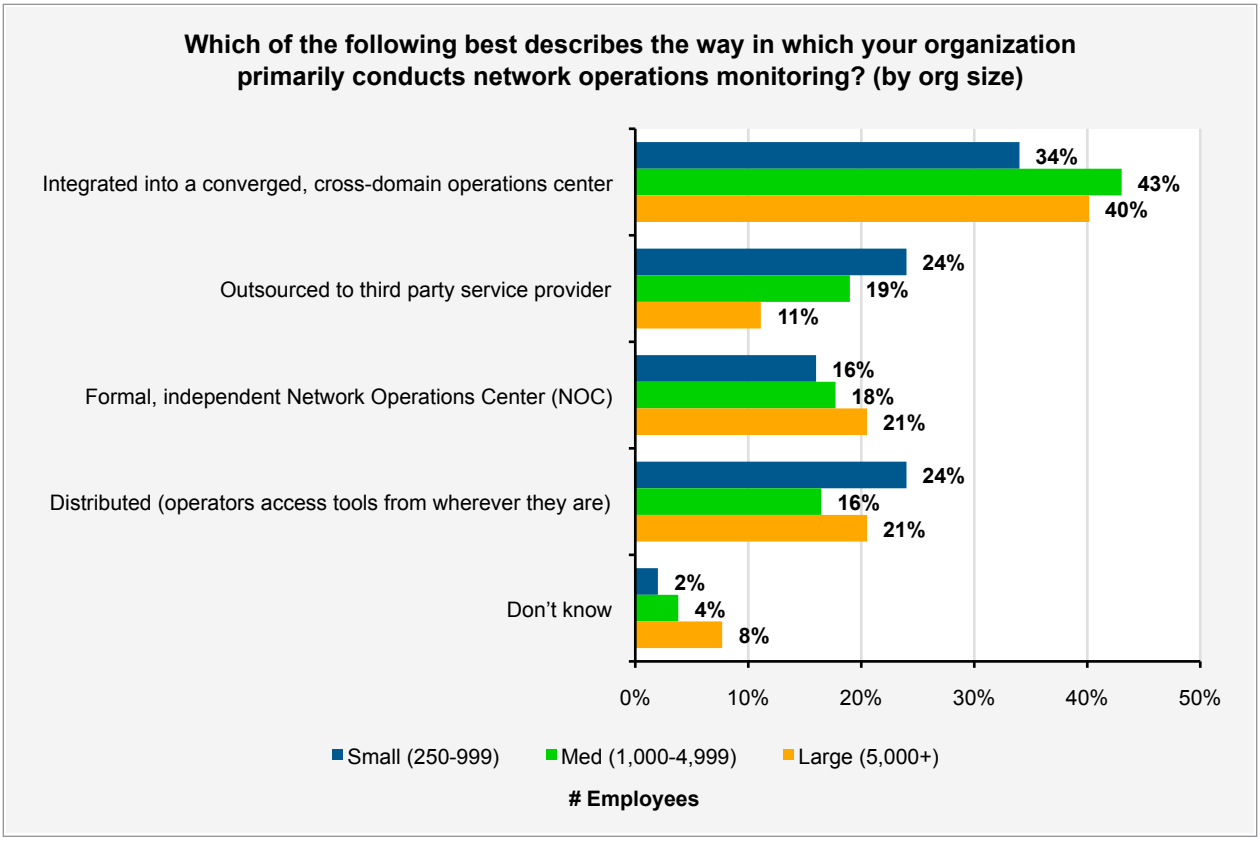

Figure 18. Ways in which organizations are primarily conducting network operations monitoring.

These results represent the strongest evidence to date that organizations are increasingly moving towards an integrated, cross-domain model. This group is still in the minority, but barely so, and has been steadily rising over the past several years. Informal assessments and related research by EMA produced estimates in 2008 – 2009 that roughly 18 to 20% organizations had made this transition. In parallel with the arrival of and initial engagements with cloud services, that number had risen to around 30% in the 2011–2012 timeframe. This latest result indicates that the transition continues for a growing number of organizations. It should be noted, as demonstrated in figure 28, that medium-sized organizations are most likely to embrace this new model, nearly reaching 50%. Smaller organizations have less need, and large organizations are still able to and willing to support silo teams and perform cross-domain integration in another way. Not surprisingly, the smallest organizations are also the most likely to have outsourced this function, typically due to a lack of qualified resources and coverage internally.

Whether or not organizational realignments are afoot, a growing number of network management teams are beginning to focus on higher-level objectives beyond simply network availability and network-layer performance. EMA asked whether some of these objectives were important and the results are shown in figure 19.

Figure 19. Higher-level objectives for the network management team.

Of all the choices here, the most comprehensive is probably service quality. True definitions of service quality can include almost all of the other items offered – end-user experience measures, application performance, problem avoidance, and internal SLAs. To be fair, service quality is a very broad term and could also include a number of other measures, such as project completion time, repair accuracy (i.e. number of times that problems are fixed the first time and do not recur), Mean Time To Repair/ Restore (MTTR), Mean Time Between Failures (MTBF), and even call return times for escalated issues. Despite this, a focus on service is clearly becoming a standard part of the networking pro's world.

It's also not surprising that those who selected and indicated that service quality was important to their network management team were the most likely to have indicated that network operations have been folded into an integrated, cross-domain group (44% versus overall average of 40%). Also, only 4% of our participants indicated that none of these higher-level objectives were important to the network management team, and in fact most participants selected two or more of the choices presented here.

For organizations that are looking at integrating their operations teams, one related initiative involves integrating network management products. Using such approaches takes advantage of sharing data to reduce manual data correlation across tools, tasks and viewpoints within network management functions. It also greatly simplifies efforts to identify and track application/service quality objectives. We asked two questions related to integration, and the first is shown in figure 20, regarding how respondents would most prefer to acquire and deploy network management products.

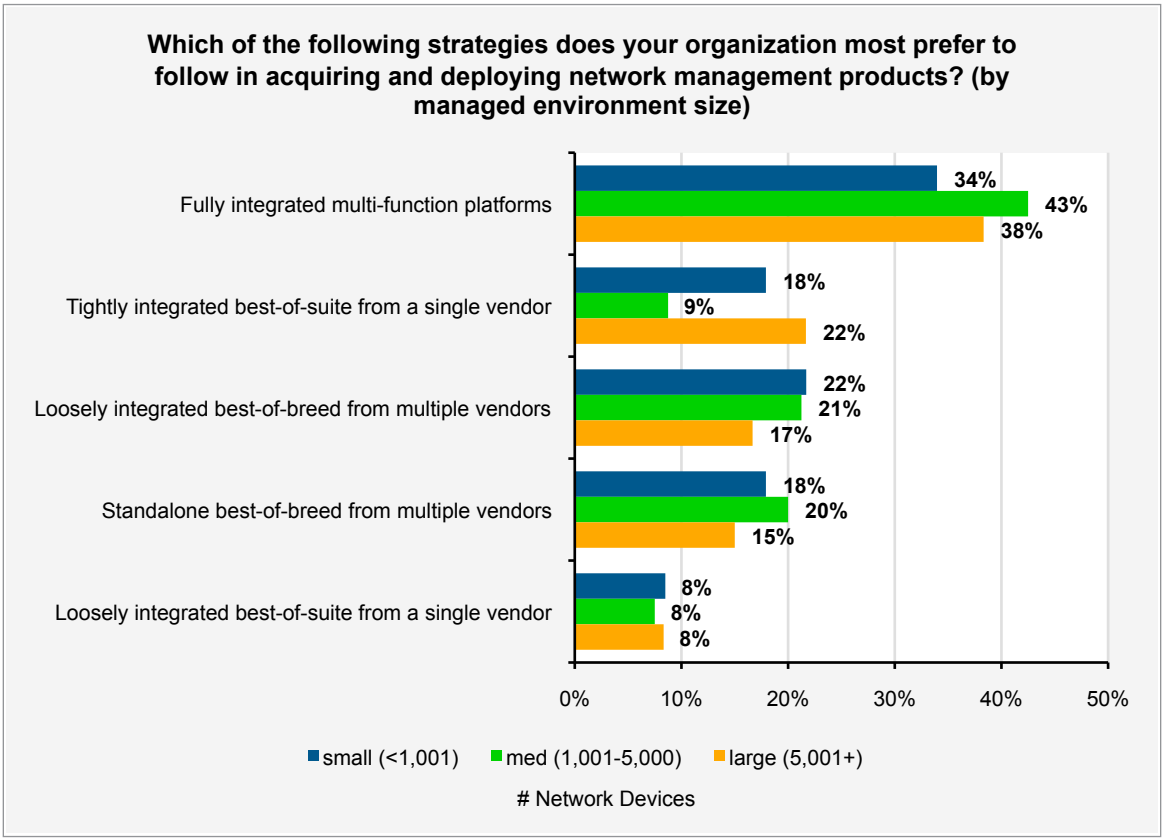

Figure 20. Strategies most preferred for acquiring and deploying network management products.

There are a number of interesting findings to be drawn from these results. First of all, there is no overwhelming majority favorite in terms of approaches. With that said, fully integrated, multi-function platforms were clearly the most popular choice. Such products support multiple network management functions across the primary use cases of planning, monitoring, and troubleshooting. The next-most closely aligned type of approach is the tightly integrated best-of-suite from a single vendor, which in general did not garner nearly the same level of interest as the other models. At the far end of the integration spectrum are standalone or loosely integrated best-of-breed from multiple vendors, where a lot of the heavy lifting for recognizing and correlating viewpoints and data is left to networking pros.

EMA Perspective

This study covered a broad range of topics related to network management, and there are many, many conclusions and inferences that can be drawn. As with previous editions of this study, here are a few of the major takeaways that EMA believes are of most importance:

- The number of management tools in use to support network operations is still far too high. Strategies focused on more proactive, service-oriented management objectives are not well served in such fragmented settings.
- Cloud and virtual networking persist as a source of significant stress for network engineering and support, both in terms of visibility and control. Much room for improvement still exists.
- SDN is still very early in its lifecycle as a broadly adopted enterprise technology. Initial indications, however, are that existing management tools may be adequate for covering the needs, with the possible exception of capacity planning for overlay SDNs.
- Big data is already having a noticeable impact on networks and network management, and big data analytics should be considered a potentially important technique for supporting network management activities and for further leveraging the data collected by network management systems.
- Log files and APIs are rising in importance across all network management use cases, and are driving networking pros to seek new skills in programming and scripting.
- The steady forces of convergence continue to push network operations teams towards an integrated, cross-domain teaming alternative and network management tools towards tighter integration.

More study will be appropriate in a number areas identified in this study. EMA plans to conduct deep research into the use cases and specific ways in which log data is being collected and analyzed in support of network and datacenter operations. Additional research is ongoing to follow the ways in which big data is changing both the technology and practices of network management. And of course, EMA plans to maintain a steady watch over the evolution of both SDN and cloud technologies, assessing their impact on network management tools, technologies, and practices along the way.

Case Study: Regional Business Bank

Setting: This enterprise supports business and professional banking needs, including deposits, loans, treasury, leasing, and investment management. We spoke with a network security engineer who indicated that the organization has over 250 network devices under management in a mixed physical and virtual environment, across one primary and one backup datacenter and 40+ remote branch locations.

Network Management Tools in Use: The company primarily uses the SolarWinds product suite to span fault, performance, and configuration management needs, including Network Performance Monitor (NPM), Server and Application Monitor (SAM), Network Configuration Manager (NCM), and Web Performance Monitor (WPM). For packet analysis they use free tools such as tcpdump and wireshark. For NetFlow collection and analysis, the team chose Plixer Scrutinizer. For log analysis the team has two tools – TNT Software's ELM for Windows event logs and SolarWinds Kiwi Syslog Server for everything else, including VMware, switches, Linux servers, and firewalls.

For WAN optimization the company is using Silver Peak products, in two use cases. The first is for replication of 500 servers between primary and recovery datacenter sites. Even with a 100Mbps DC-to-DC link, there was not sufficient capacity to carry all of the replication traffic, but the Silver

Peak solution's de-dup and compression capabilities delivered 80% reduction in traffic, converting the link to an effective 500Mbps. The second use case is for improving WAN performance to remote branch sites, 90% of which are connected via T1 links. Here, the caching and de-dup features are making it possible to reduce one common file transfer from 30 seconds to 2 seconds, and has made regular patch and antivirus updates far less taxing.

The most significant technology challenge for the networking team is workforce mobility and cloud services. The last three most difficult performance issues were related to network change and configuration errors, application design/health, and client system/user errors. The biggest challenge from an operations standpoint is a lack of a formal process for including IT when new projects are launched. New projects are often started within individual LoBs without including IT, and by the time IT is brought into the process there is insufficient time to meet project deadlines.

Megatrends Experiences:

In terms of our study's first three megatrends – Cloud, SDN, and Big Data, there was not much of a story to be told. No Big Data or Cloud services are currently being used, and while there has been some experimentation with underlay and overlay SDN products and technology, the team has decided to wait until standards emerge and mature before they proceed further. Regarding megatrend four, this organization uses log file and both management system and device APIs in all three network management areas – monitoring, troubleshooting and planning. And finally, in terms of megatrend five, the organization has definitely moved to a converged, cross-domain operations team of about 20 individuals, three or four of which are primarily focused on network monitoring.

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

2892-Silverpeak-Summary.060314