The Essential Guide to Modern Network Monitoring

ca technologies

TechTarget | Custom Media

Suddenly, the network is cool again. Tech trends such as the Internet of Things, software-defined networking and growing end-user expectations all add up to a demand for "dial-tone" network performance and reliability. But with the data deluge continuing to accelerate, and organizations relying on multiple clouds to achieve business goals, how can the network keep up, much less meet tomorrow's demands? This e-book looks at the trends that are impacting enterprise networks, what issues they create for network management and insight, and what organizations should be doing today to plan for the future demands of tomorrow.

In today's "I want it now" world, the user experience, powered by an application's performance, has become a competitive differentiator for enterprises of all shapes and sizes. Now that the consumerization of IT has led to the deployment of apps for virtually every business function, enterprise user expectations take a similar cue. Subsecond response times are now deemed the norm.

Performance demands are exacerbated by the mobile workforce. Not only do users demand access from any device—from laptop to wristwatch, whether provisioned from the business or brought from home—organizations are also expected to provide round-the-clock application availability every day of the year for employees, customers and partners, securely and simply, from anywhere in the world.

And everything is connected. At the heart of the business is the enterprise network—connecting users, applications and data across the globe—and all these demands are putting network performance back in the spotlight.

TABLE OF CONTENTS

CHAPTER 1

The Hidden Danger: Growing Network Complexity

Market forces and technology both have a significant impact on overall network performance. More than a half century after Moore's Law was first observed, it still holds true, yielding a data deluge unlike anything in human history. Billions of emails are sent every week, but the very nature of Internet traffic is changing, with a pronounced shift to rich media. Visit a business website and it is likely to start playing a video, either in a window or as a background. What is the impact on network traffic? Just two sites, Netflix and YouTube, now account for more than half of all broadband network traffic during peak viewing hours.

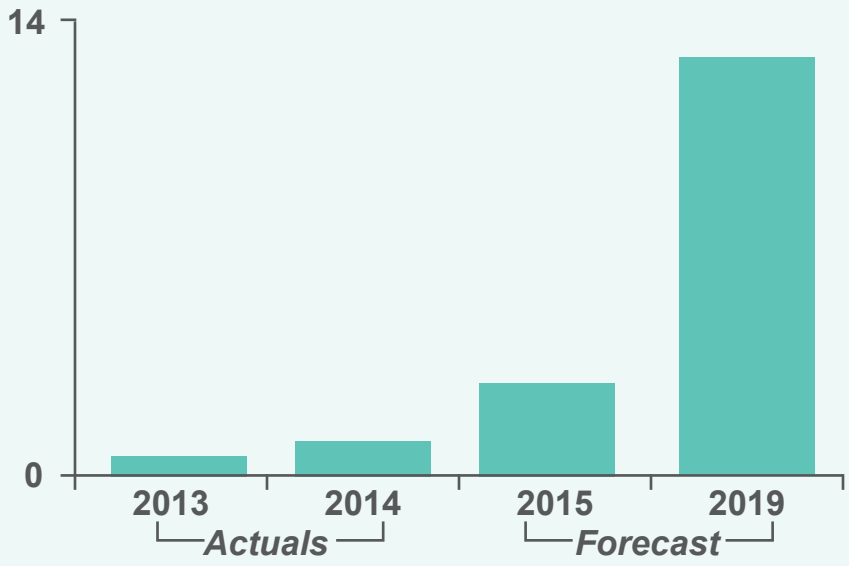
The number of applications businesses use has increased by orders of magnitude, and it is not uncommon to have thousands of applications in use throughout an organization. This application economy has led to not just more applications, but more data, structured and unstructured, and more endpoints—all demanding network connections and access. As complex as networks are today, consider the coming onslaught of traffic brought by the Internet of Things (IoT). From self-serve kiosks to smart watches, IoT is expected to bring as many as 50 billion new network nodes by 2020,[1] with trillions of yet to be imagined transactions in their wake. Network operations (NetOps) is already feeling the pain: A recent study found that over half of all IoT projects create network "blind spots."[2]

Most organizations have adopted some form of cloud computing, from simple software-as-a-service (SaaS) subscriptions like Salesforce.com to platform or infrastructure as a service (PaaS or IaaS) to accelerate development or offload server and storage deployment headaches to a cloud provider. As the cloud matures, many businesses now find themselves relying on a multi-cloud approach, to match workloads to specific cloud provider attributes or ensure availability should an outage occur either on premises or at a cloud provider.

However, moving workloads between clouds or to and from on-premises infrastructure can create network visibility gaps. Workloads can be spun up, moved or spun down so rapidly that traditional network monitoring software, which runs discovery services only periodically, never sees them at all.

1 "Special Report: Network Performance Management (NPM) in the Cloud Era," SDxCentral, 2016
2 "Report: EMA Names CA Technologies as 2017 Networking Innovator for Predictive Network Behavior," EMA, Q3 2017

Network functions virtualization (NFV) hardware, software and services revenue to top $11B by 2019.



© IHS, *IHS Infonetics NFV Hardware, Software, and Services*; July 2015

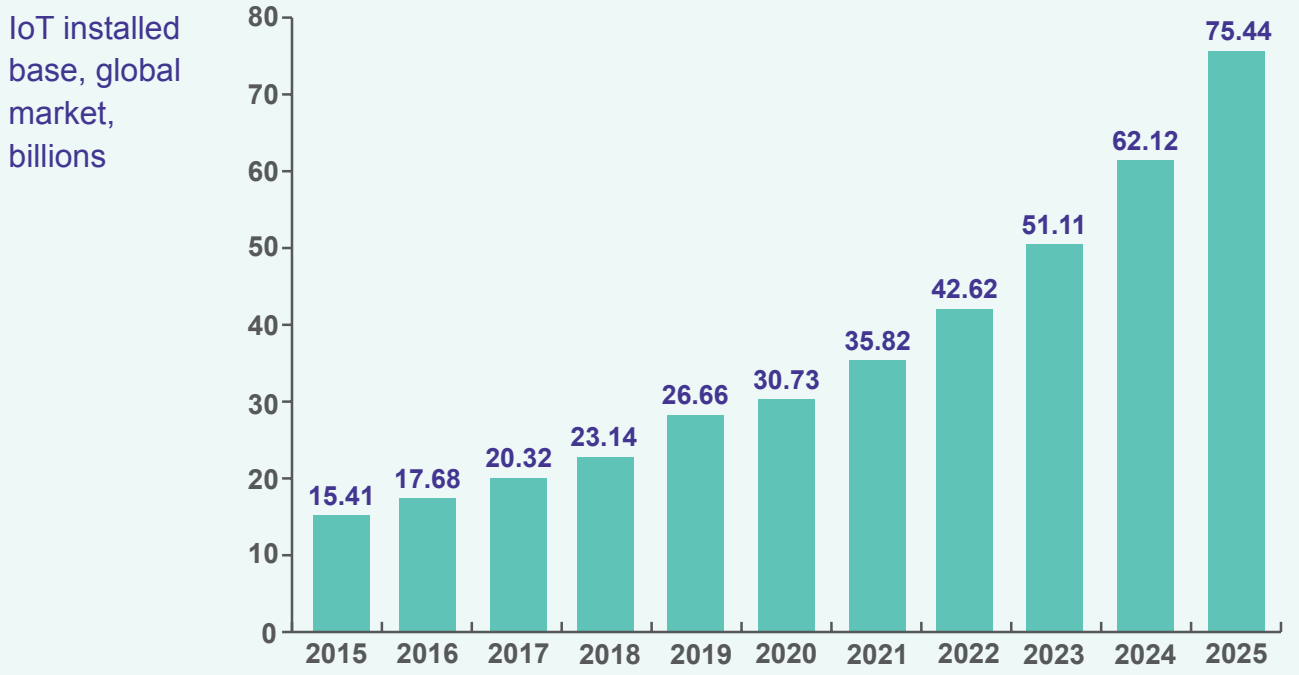
The days of "set it and forget it" network administration and monitoring are gone...

Integrating legacy and cloud workloads over Internet connections brings performance challenges into sharp focus. The Internet wasn't designed to deliver enterprise applications the way local-area networks do. Chatty protocols and latency can bring an application that performs perfectly when all the pieces are in the same place to its knees when delivered over the Internet. There is no doubt we will continue relying on cloud for many functions and applications, but all the benefits of cloud computing come with the increased challenge of ensuring network reliability in an environment where entire applications may be in transit.

Finally, there is the growing impact of network function virtualization (NFV) and software-defined networking (SDN). Although relatively new in comparison to server and storage virtualization, NFV is rapidly gaining in popularity, as it promises the agility and flexibility of decoupling network functionality from the underlying hardware. As organizations move to converged or hyper-converged infrastructure, networks will be able to grow and shrink on demand, as virtual network devices come and go, move between hypervisors and chew up resources in a heartbeat.

The days of "set it and forget it" network administration and monitoring are gone, and the management tools currently deployed can't handle our increasingly dynamic, virtualized and complex network environment.

The IoT market will be massive



Source: IHS

CHAPTER 2

Convergence for New Visibility

Because of rapid advances in networking technology coupled with user demands, network managers often find themselves with a multiplicity of tools, each designed to manage or monitor a single aspect of the enterprise network and application performance. Today, half of enterprises already find themselves using 11 or more network tools, and for many, this may be just the beginning. For example, as organizations continue the adoption of software-defined WAN (SD-WAN), with the goal of replacing older MPLS connections with modern broadband Internet, they find the existing monitoring tools aren't efficient, and over two-thirds of SD-WAN adopters have added yet another tool or thrown up their hands and outsourced management to their network service providers.[3]

3 "Network Management Megatrends 2016: Managing Networks in the Era of the Internet of Things, Hybrid Cloud, and Advanced Network Analytics," EMA, April 14, 2016

The problems created by relying on swivel-chair management—where data is entered into one system and then entered manually into another system—are many. First, there is the duplication of effort involved in managing multiple tools and interfaces. Then there is the uncertainty brought on by having to rely on a variety of tools for various infrastructure components. Just keeping track of which tool is used for which network element can induce stress.

As a result, network managers now spend over 70% of a typical workday troubleshooting, according to a recent EMA report.[4] Split almost evenly between problem prevention and reactive firefighting, harried network managers are able to devote only 29% of their time at work on anything even resembling productive tasks.

As a result, network managers now spend over 70% of a typical workday troubleshooting, according to a recent EMA report.

Perhaps the biggest problem created by this fragmentation is a lack of end-to-end network visibility, cited as the No. 1 challenge to successful network operations in the same EMA report. Right behind is lack of resources, cited as the second greatest challenge. It's not surprising the EMA report concluded that as network teams add more tools, they become *less effective* at network problem detection and their networks become *less stable*.

Network teams need a convergence of operations. This begins with a comprehensive monitoring and analytics platform that includes:

- **One NetOps portal** with full-stack monitoring and management for both traditional and modern architectures that spans the greatest number of protocols and vendor landscapes. Enterprises are increasingly virtualizing every part of the network. However, that does not mean traditional network infrastructure is going away anytime soon.
- **One Open API** enabling customization of the NetOps experience. Just as today's consumers want their experience their way, NetOps should demand the ability to customize methods of ingesting and presenting any network data for a truly intuitive, personalized experience that enables faster triage and better executive consumption.
- **One data collector** that spans multiple protocols and doesn't rely on old-school polling mechanisms but instead utilizes modern, real-time streaming functionality that can keep up with the speed and dynamism of current and future network architectures.

4 Ibid. footnote 2

- **One context** for troubleshooting application experience issues related to network impact, with only the relevant protocols and endpoints (physical, virtual or logical) surfaced. This enables network operations staff to remove any "noise," simplifying root cause analysis by minimizing the number of clicks to resolution even in highly virtualized environments.

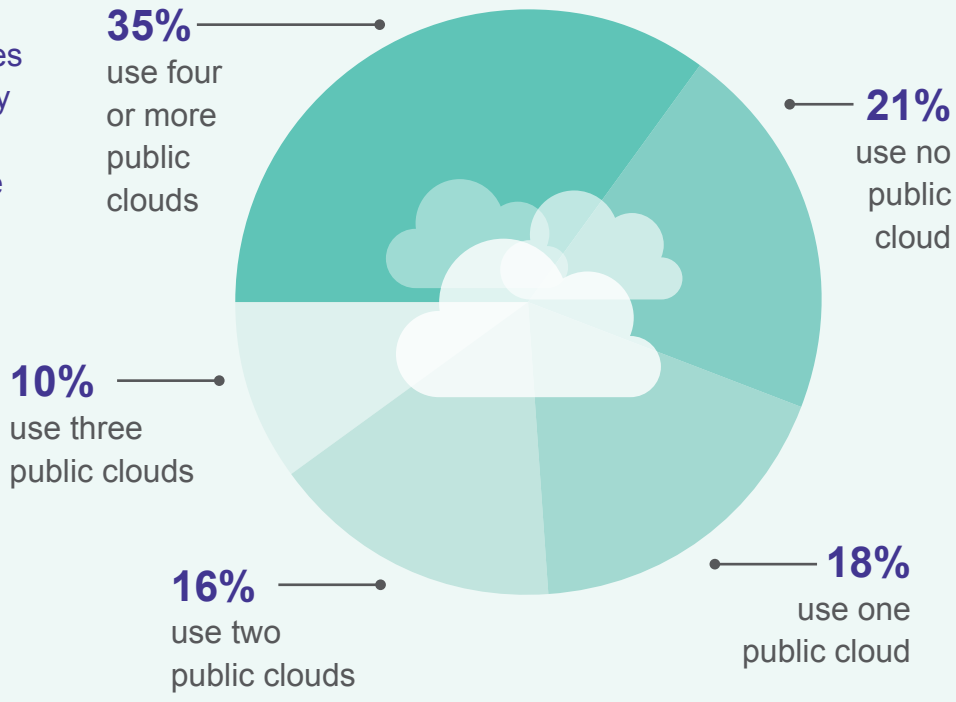
In an increasingly data-driven world, it is no surprise that analysts predict that wire data—created by reassembling network data into full streams to provide payload analysis and full context in real time—will play a significant role in availability and performance analysis.[5]

To that end, CA Technologies has coined an acronym to help enterprises remember the essentials to consider when sourcing a network management tool: FITPAL, which stands for Fault, Inventory, Topology, Performance, Application, and Logs. A good network monitoring and management tool for traditional and software-defined networking for hybrid environments should incorporate all those data streams. Let's consider why each metric is important.

5 Ibid. footnote 1

Multicloud Mania

Amoung the 260 enterprises EMA surveyed, the majority of respondents—61%—reported using two or more public cloud providers



Source: Ten priorities for Hybrid Cloud, Containers, and Delvops in 2017; Enterterprise Management Associates

CHAPTER 3

FITPAL for Healthy Networks

FITPAL represents a baseline for the types of information that a modern network monitoring and management platform requires for full visibility. Here's why each type of data is critical to the enterprise.

Fault: Capturing fault data becomes more valuable when it can be correlated to performance issues in a "single pane of glass." For example, if a fault occurs but has negligible impact on application performance, remediation can take a back seat to more pressing issues.

Inventory: In hybrid or multi-cloud environments, it is imperative to have a good handle on physical, virtual and logical network elements. With infrastructure inventory data coming from multiple data sources, it is easy to lose track of what's where. Ultimately, you can't manage what you don't know about.

Topology: Using topology mapping, network managers can determine if neighboring infrastructure is causing a performance impact on a given application, providing insight into if or how routing should be adjusted, surfacing a hidden problem.

...why each type of data is critical to the enterprise.

Performance: There are many aspects to performance data in heterogeneous environments. Modern multiprotocol networks demand that NetOps track SNMP, API, packet and flow data, often from multiple vendors—in real time.

Application: Since the user experience is the most important metric, having the ability to triage application experience issues back to network infrastructure is a critical requirement for networks today and in the future.

Logs: Having the ability to perform log analytics against the other five FITPAL elements provides predictive capabilities for fault, performance and capacity planning.

CA Technologies is offering a complimentary FITPAL network health assessment to readers of this e-book. You can see how your current tool set stacks up by visiting the assessment at http://cainc.to/gotfitpal.

Case Study: Small Business Computer Software Company

If you think choosing the right networking tools is only important for large companies, consider this small business software company. When their current monitoring solutions couldn't scale to meet their needs, they turned to CA for a solution that fit their budget and could monitor, store, and analyze performance data across a complex, multi-vendor network infrastructure. By adopting the CA tools, they improved scalability by 75%, leading to a similar improvement in user experience, reduced complexity, and a significant improvement in the ability to monitor virtual networks throughout their business.

Source: TechValidate Nov. 10, 2016 TVID: E79-5E3-BD3

"CA Performance Management provides a better overview of the performance of all network components and ports."

- Global 500 Telecom Services Company Source: TechValidate May. 18, 2017 TVID: 988-475-92C

CHAPTER 4

NetOps, Big Data, and Analytics

Collecting metrics, even all the FITPAL elements, is just the beginning. The challenge is turning that data into actionable intelligence for the network operations team. Visibility is good. But visibility in context to the user experience, while enabling you to troubleshoot physical, virtual or logical devices or components in relation to the rest of the network, can reduce the number of clicks and speed triage.

The lack of actionable data is the primary reason the first indication of most networking problems is user impact and not fault reporting.[6] To solve this issue, enterprises must use a tool set that combines both traditional and software-defined network elements into a single analytics platform, capable of handling all the FITPAL data elements in real time while presenting relevant data back into a converged NetOps solution.

6 Ibid. footnote 2

Enterprises must use a tool set that combines both traditional and software-defined network elements into a single analytics platform.

With networks incorporating traditional, SDx, NFV, IoT and SD-WAN elements, network tools must be in a continual state of discovery, constantly looking for new elements being created, or transitions between hypervisors of network element and workload alike. A centralized analytics engine that brings together data gathered from monitoring and topology can provide predictive capabilities to the enterprise, and should support network self-healing and application-to-infrastructure correlation, and predict customer impact based on any network event.

Ultimately, tying network monitoring data back into an analytics engine can reveal insights that provide operational intelligence while anticipating possible impact on the user experience itself.

What should enterprises demand when considering a modern network monitoring platform?

- A future-proof platform that offers scalability and real-time performance
- An API that allows integration with business intelligence dashboards and reporting
- FITPAL data streams offering “in-context” and comprehensive diagnostics to speed triage
- Support for legacy, software-defined and virtual networking in one dashboard and context
- Elimination of network blind spots introduced by cloud
- Modern analytics that consistently looks for optimization opportunities

“CA Performance Management has provided stability, scalability, and usability to our network monitoring environment.”

- Large Enterprise Financial Services Company Source: TechValidate Nov. 10, 2016 TVID: 704-F8C-221

CHAPTER 5

Making it Real: NetOps and Analytics in Practice

What real-world impact does selecting the right network tools have? For one company, the results were dramatic. Challenged by scalability issues with its existing monitoring solution, a global telecommunications services provider opted for CA Technologies' network management platform.

After adopting the CA Technologies solution, it improved the overall end-user experience by more than 75%, along with a similar increase in scalability.[7] The company also gained significantly more predictive network analytics capabilities.

On the other end of the spectrum, a global banking company adopted the CA Technologies solution and not only reduced its network complexity and improved its ability to monitor virtual networks by more than 50%, but was also able to deliver an improved user experience and speed mean time to resolution.[8]

7 "Case Study: Global 500 Telecommunications Services Company Improves Network Insight by Switching from HP to CA Performance Management," TechValidate, May 18, 2017

8 "Case Study: Global 500 Banking Company," TechValidate, Dec. 8, 2016

"CA Performance Management helps our organization speed and simplify the triage of infrastructure network performance issues."

– Fortune 500 Insurance Company

Source: TechValidate May. 23, 2017 TVID: CEF-8EA-3C0

How can one platform serve the needs of both large enterprises and smaller companies? The Network Operations and Analytics platform from CA Technologies delivers an out-of-the-box, single-pane dashboard that's ready to go, as well as an Open API portal that lets network teams design their own dashboard and reports as desired.

CA closes the gaps and delivers a comprehensive network monitoring and management solution designed with tomorrow in mind. The ability to gain deep visibility into network issues in context reduces the time to resolution, helping to ensure the kind of user experience that keeps customers happy.

If your enterprise isn't ready for the double whammy of software-defined networking and IoT in today's application economy, how can you guarantee the user experience your business units demand? **To find out how CA can help future-proof your network transformation initiatives, visit http://www.ca.com/netops.**

Case Study: Global 500 Telecommunications Services Company

Network performance is the most critical factor for any telecommunications company. So when a Global 500 telecom behemoth was looking to solve two major problems, namely scalability issues with their existing monitoring software that led to an and an overly reactive NetOps team, they came to CA to see how their solutions could help. Their analysis led to a switch to the new CA offering.

By switching to CA, they were able to proactively address network performance issues, thus speeding triage time. And the results were impressive, as the benefits they realized included improving the user experience and scalability by more than 75%, while greatly reducing network technology complexity at the same time.

Source: TechValidate survey May 18, 2017 TVID: 988-475-92C