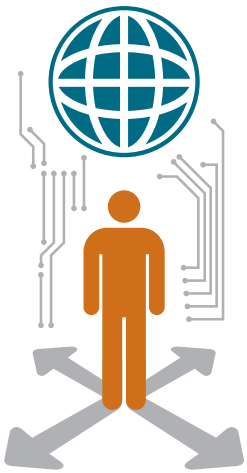
21ST CENTURY NETWORK MANAGEMENT

With more complex networks and the ubiquity of mobile devices, network management strategies and technologies must change.

The network of today is nothing like the network of five years ago — and nothing like the network will be five years from now. Today's typical network is no longer simply an interconnected set of technology that gets data from Point A to Point B. Instead, it is pressed into service in ways that network managers couldn't imagine.

Organizations today have adopted many technologies and services that make operations more efficient and effective — but put tremendous pressure on network performance, bandwidth, capacity and security. What's more, it's happening at a time when IT budgets and resources are stagnant. (No significant increases are forecasted in capital budgets or headcount in 2013 per the research firm Computer Electronics.)



The use of cloud computing has also complicated the issue. For example, servers and storage used to sit side by side, but today, many organizations can have parts of applications sitting in different physical locations.

To add to the complexity, some of the infrastructure isn't even owned or managed by the organization that is delivering the app to users. That can increase network latency and make WAN-related connectivity — things like response time monitoring — more critical than ever before.

Fortunately, there is a range of tools and strategies designed to keep entities ahead of the seemingly increasing plethora of network changes and demands. In addition to being technology enablers, they can also serve as catalysts to improve service quality, reduce cost and enhance security.

Network Complexity — All-time High

The fundamental nature of networking is shifting. Today, bandwidth is stretched by the impact of unified communications (UC) and multimedia-enabled applications (including bandwidth-hungry video), while mobility adds security and compliance complexities.

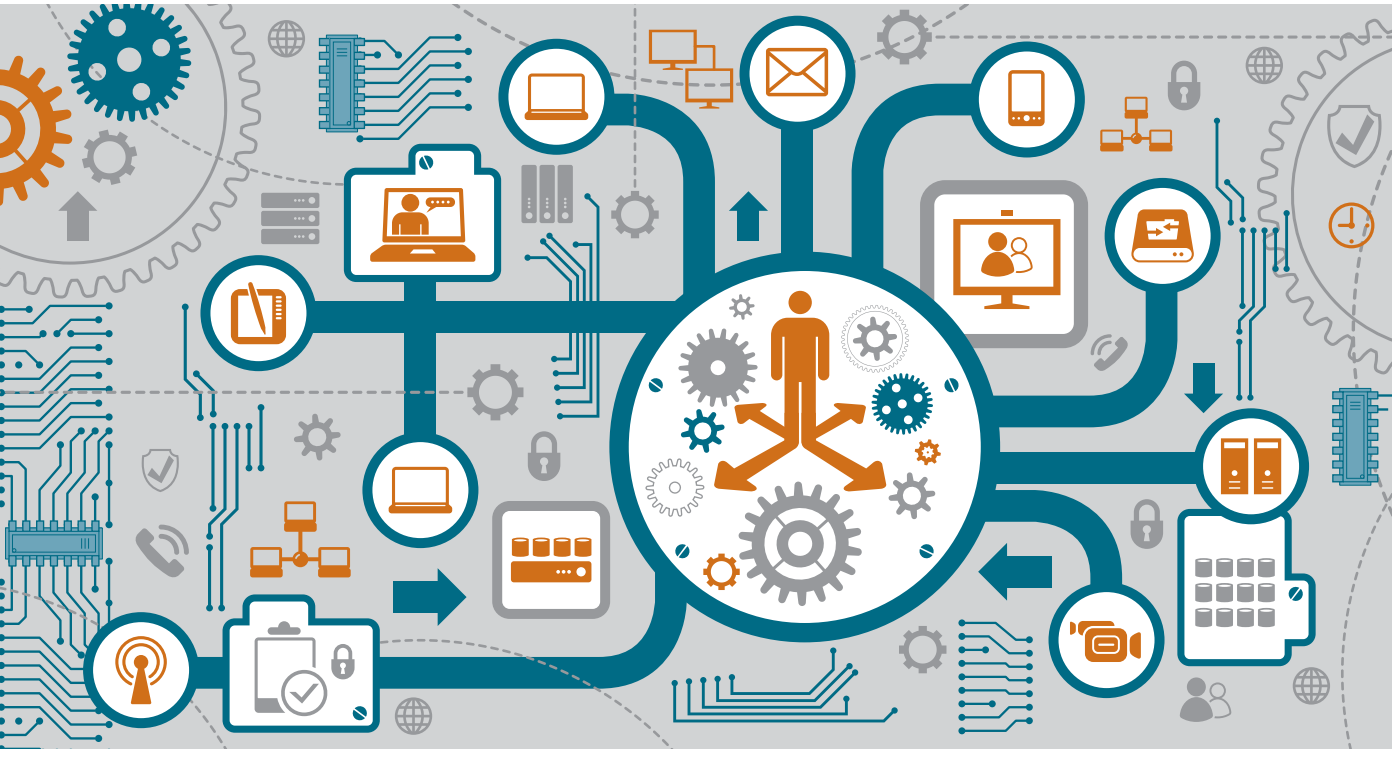
The increase of virtualization, while extremely beneficial in many ways, puts a great burden on the network by increasing the bandwidth input/output needed for each physical server. The growth of e-commerce requires always-on, no latency networks. And the network may even be asked to handle physical security.

"You can test an application you have developed by putting it on a server and connecting that server to a 10G switch in a lab. Put a PC on the other side of that 10G switch and sure enough it works perfectly," says Doug Roberts, director of product strategy at Visual Network Systems (a part of Fluke Networks). "But if you take that same application and deploy it across an eclectic mix of never-before-thought-of types and kinds of bottlenecks and forms of interconnectivity and distances, all of a sudden the app doesn't work."

The crux of the issue, he says, is how to deal with new interdependencies of the network, applications and servers. "How those pieces work together is what dictates the data sources you need to leverage, where you need to collect data from, how you need to collect data and most importantly, how you need to present data to key stakeholders so they can resolve problems quickly."

At the same time, network traffic is increasing — in a big way. According to the *Cisco Visual Networking Index: Forecast and Methodology, 2011–2016,* annual global IP traffic will reach 1.3 zetabytes (one zetabyte equals one sextillion bytes) by 2016.

The forecast also predicts the following:



- By 2016, 1.2 million video minutes (equal to 833 days) will travel the Internet every second.
- Average global IP traffic will reach 150 petabytes per hour.
- IP video conferencing will grow more than twice as fast as overall IP traffic.

"Each of us increasingly connects to the network via multiple devices in our always-on connected lifestyles," says Suraj Shetty, vice president of products and solutions marketing at Cisco. "The sum of our actions not only increase demand for zetabytes of bandwidth, but also dramatically change the network requirements needed to deliver on the expectations of this 'new normal'."

It's critical to provide the bandwidth for the growing amount of network traffic to travel, but it is equally important to monitor and prioritize that traffic. Without the right tools and processes in place, organizations will experience higher costs, lower productivity and reduced security.

"As capacity requirements increase, service levels will often degrade if demand is not monitored and managed," says Bob Tarzey, an analyst and director at Quocirca Ltd., in a May, 2012 report. "Standing still will, in effect, mean going backward."

To manage these issues, most organizations are using some networking management and monitoring tools. Around-the-clock monitoring saves time, supports administrators in planning resources, and helps optimize the network.

"To maximize the user experience, constant network monitoring is needed to ensure that all network ports are used to the full extent and that every last drop of available bandwidth is consumed before more capacity is purchased," Tarzey says. "Furthermore, when network traffic increases, upgrades can be planned rather than implemented in a hurry while fire-fighting."

For today's organizations, the message is clear: the network must be managed as a mission-critical asset. As Tarzey succinctly puts it, "A well-managed, high-availability, high-performance and secure network can be a distinct competitive advantage, a poorly managed one is a fundamental risk."

Network Management Tools

Network management today means being able to diagnose and resolve bandwidth, latency and performance problems before they impact productivity; gain visibility into load-balanced environments; and identify security threats such as zero-day threats, malware, insider breaches and policy violations.

All have the basic ability to monitor connections, CPUs, memory utilization, bandwidth, latency and server uptimes and downtimes. All have analysis and reporting capabilities, and most include a dashboard-like user interface allowing for remote management via the web, a desktop client or mobile device.

Beyond that, different types of network management tools have different levels of capabilities, from the basic (device discovery) to the complex (real-time monitoring and tracking; root cause analysis and event correlation; real-time behavior analysis; >

rule-based threat classification; location tracking and visualization; and the ability to see application traffic as it is traversing the network).

The option an entity chooses can rest on many factors. Budget is one factor — there are big-budget and small-budget options, while specific points of pain are another.

Network management at its basic level mainly means knowing which devices are connected to the network at any point in time. One example is Cisco's FindIT Network Discovery Utility, which allows organizations to discover most Cisco products and display information on status, serial number, IP address and version. HP's Peregrine Enterprise Discovery goes a step further, discovering and taking inventory of all devices and software on a network, up to 50,000 devices per server and 500,000 devices through multiple distributed servers.

The Peregrine application suite displays where each device and software is located, and provides metrics on utilization. Microsoft takes yet another approach with its Network Discovery tool, which searches the network for IP-enabled resources by querying Microsoft Dynamic Host Configuration Protocol (DHCP) servers, Address Resolution Protocol (ARP) caches on routers and Simple Network Management Protocol or SNMP-enabled devices. It can also search Active Directory domains and IP subnets.

Using these types of tools is often a good first step for organizations that need more information on what is accessing the network, along with information on when and how. That information is critical to moving to the next step; knowing how traffic flows and where the biggest demand is focused. This can help organizations determine the biggest problems and how to address them.

That's where point solutions can make sense. If you have specific bottlenecks or network pain points, it can make sense to add a tool that monitors a specific aspect of the network. If the network is experiencing a lot of faults and availability issues, for example, a network node manager might be a good choice.

If some network thresholds are routinely exceeding capacity, a network traffic analysis and management tool is a good bet. The same is true for application performance problems. For load-balancing issues, consider a load-balancing tool or link load-balancing tool, depending on the issue. Other types of valuable point solutions include sniffer analysis, packet flow visibility and event managers, which can detect network performance issues and send important information to the service desk for resolution.

Network Pain Points

1. More users
2. More traffic
3. More data
4. More components
5. More complexity

Going to the Next Level

When the entity is ready to take network monitoring and management to the next level, it often opts for more full-functioning enterprise network management software. There are two basic ways to achieve this type of integrated network management — either by using all parts of an integrated network monitoring suite, or by assembling specific products that together make up a full solution.

"A comprehensive tool allows users to gain visibility, control and automation over their network from the time a problem comes into the help desk, or realizing that it could be a problem, to putting a new rule in place," says Paul Kraeger, worldwide marketing leader for IBM Network Management. "It's about drilling down, fixing the problem and putting an action in place so it doesn't happen again."

A full-fledged, soup-to-nuts approach to network management should:

- Be able to discover devices and applications
- Collect data on the health of the network
- See all devices and subsets of the network
- Perform root cause analysis to discover problems
- Use predictive analysis to discover problems likely to occur
- See application traffic as it is traversing the network
- Handle IPv6
- Send alerts about potential problems via several methods, including email, pager and text
- Scale to handle millions of events
- Escalate problems
- Correct some problems using

automated processes (such as port resets or restarts)
- Integrate with other software the organization may be using, such as help-desk software
- Produce timely and customizable reports, such as a report on a specific part of the network for a specific time period

Many vendors offer a series of tools that address part of the network management puzzle, allowing the organization to combine the tools that make sense into one plug-and-play network management solution. One example is IBM. Together, its Tivoli Netcool/OMNIbus and Network Manager make a comprehensive solution.

Netcool/OMNIbus uses data about physical and logical network connections gathered and stored by Tivoli Network Manager as a basis for its processes, which provides real-time event management, network discovery, network monitoring and network configuration and compliance. Many other vendors use the integrated product approach to network management, including HP, LANDesk, Microsoft Systems Center, Novell ZENworks and Symantec Altiris.

An example of a vendor that prefers the all-in-one approach is Cisco. The company's Prime Infrastructure product suite combines wired, wireless and remote network management spanning lifecycle, assurance and compliance. In the last year, the product has matured significantly, adding end-to-end network visibility, application traffic analysis and reporting, packet-level debugging, LAN optimization and deep application analysis.

Another is Enterasys. The company's NetSight Suite includes policy management, identity and access, automated security management, network access control (NAC) management, asset management and mobile device management for both wired and wireless networks. It uses a web-based graphical user interface (GUI) to manage and fix problems.

One of the most important features in a comprehensive network management solution today is the ability to see application traffic traversing the network.

"We were working with a major organization, where the network operations team was frustrated with network performance, which was subpar despite the fact that their network monitoring system showed green across the board," says Dan Klimke, networking product manager for Fluke Networks. "What they really needed was the ability to drill down and see the actual application traffic in detail, so they could determine where the performance problem was occurring. Most of the time, it's the only way to identify root cause and fix an issue."

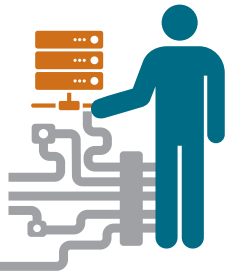
Don't Forget the Mobile Devices

The sheer number of smartphones and tablets used today — often on the network — is staggering. What's more, many of them are worker-owned devices that can present security issues if not handled properly. While many entities have implemented some type of mobile device management (MDM) policy and technology, forward-thinking organizations are looking for ways to incorporate mobile device management with their network management strategy.

"The idea is to be able to know as much as possible about what devices are on the network and how they are being used," Kraeger explains. "We would be able to know, for example, that on the third floor of the facility in the second room, wireless productivity is low. That information is critical to optimizing the network."

The most common way today to handle managing the network access of mobile devices is by employing a specific >

NETWORK MANAGEMENT TOOLS: RANGE OF OPTIONS



Depending on goals and pain points, an organization might choose one of the tools noted below:

AirWatch enterprise-grade network management tools
Brocade Network Advisor
CA eHealth
Cisco Prime Infrastructure
Enterasys NetSight
Extreme Networks' Ridgeline Network and Service Management
F5 BIG-IP product suite
HP Network Management Center
IBM Tivoli Netcool/OMNIbus + Tivoli Network Manager
MaaS360
Microsoft System Center
NETGEAR ProSafe Network Management System (NMS200)
NetScout nGenius Service Assurance Solution
Novell ZENworks
Numara Cloud
Symantec Altiris IT Management Suite
Visual Network Systems' Visual Performance Manager

Solutions to address specific issues:

Network traffic analysis:
CA NetQoS ReporterAnalyzer

Network traffic manager:
F5 BIG-IP Local Traffic Manager

Application performance monitoring:
Fluke ClearSight Analyzer

Network availability monitoring and management:
Juniper CTPView Network Management System

Link load balancing:
F5 BIG-IP Link Controller

Packet sniffer visibility and analysis:
NetScout nGenius
Sniffer Analysis module

Network performance detection and resolution:
LANDesk Event Manager

Stagnant IT Spending

Many North American organizations are not expected to make significant increases in IT capital budgets or headcounts in 2013.

Things holding back growth:

- ➔ Domestic budget deficit negotiations
- ➔ Ongoing recession in Europe
- ➔ Uncertainty about Chinese economy

Source: Computer Economics, *Outlook for IT Spending and Staffing in 2013*, January 2013

solution geared to managing mobile network traffic. Over time, network management systems will begin integrating mobile device management into their systems.

Vendors that are doing well with their stand-alone mobile network management systems are AirWatch, Aruba, Cisco, Enterasys, IBM, MaaS360, Microsoft and Symantec.

As an integrated cloud platform, MaaS360 simplifies MDM with rapid deployment, comprehensive visibility and control spanning across mobile devices, apps and documents. The AirWatch MDM solution facilitates quick device enrollment, configuration and update over the air, security and compliance, access to enterprise resources and remote lock and wipe.

Aruba's AirWave Network Management offers full monitoring and troubleshooting capabilities. The Enterasys Mobile Identity Access Manager provides everything from granular policy management and real-time tracking to full threat response and security information and event management (SEIM). While Microsoft offers its Intune and System Center solutions, IBM its Endpoint Manager and Symantec its Mobile Management solution.

Cisco has also made progress in combining wired and wireless network management with its Prime Infrastructure product. During the past year, it has merged formerly stand-alone MDM functionality into its Prime Infrastructure product.

"Organizations tend to have different mobile use policies for different types of users and situations, which complicates network management," says Mahesh Bommareddy, director of product management for Cisco's Wireless Networking group. "You need to be able to not only manage those policies, but also troubleshoot and manage in a way that combines assurance and compliance for both the wired and wireless network."

Moving Forward

For many organizations, the future may be a hybrid of the traditional network infrastructure and software-defined networking (SDN), often regarded as the next-generation network. SDN is a more flexible, software-oriented network environment with many network management benefits, including improved visibility, programmability and provisioning of network resources.

While today's network management tends to be reactive, SDN is more proactive, explains Lee Doyle, principal analyst at Doyle Research Associates. Doyle expects early adopters to be organizations whose networks are critical parts of their IT infrastructure.

Vendors are already jumping on board. HP is one of the first out of the gate. The HP Virtual Application Networks SDN Controller, expected to be released this year, offers a dynamic control plane with the intelligence to automate and program the network to enable network agility. ■

NETWORK MONITORING IN THE CLOUD

Becoming comfortable with the technology, more organizations are considering network management in the cloud.

The benefits are obvious: It provides real-time monitoring and access to performance data and can scale up or down depending on usage. You pay for only the capacity you use and can provision resources in a way that meets service management goals. What's more, management is completely centralized and disaster recovery isn't an issue.

However, moving network management to the cloud isn't a slam-dunk. Many cloud-based network management services provide only part of the services needed, so the organization itself has to do the rest. In many cases, some monitoring must be done locally, and most entities need two to three layers of monitoring, down to the data center.

The key is to choose carefully. The more robust the cloud-based offering, the better. Cisco's recent acquisition of cloud-managed networking vendor Meraki has allowed it to offer a cloud-based network management offering that was built from the ground up for the cloud.

Another good solution is IBM's Netcool Network Management, which provides end-to-end visualization of the network infrastructure. It provides discovery WAN and LAN of network elements and topology, and also supports root cause analysis when technical issues emerge. The cloud-based solution also discovers both virtual and physical network elements.