Network management is a complex topic. In today’s diverse networking infrastructure, the network has to handle more instances of unified communications, video, and virtualization. The role of the network manager encompasses not only monitoring for performance and security, but also anticipating future network problems and transcending technology silos to ensure everything runs well together, whether it’s the network, the server, or the application.
Network Management Fundamentals

Table of Contents:

- Networked application performance management—Where to start
- Network management frameworks: FCAPS and ITIL
- Understanding the network application environment
- Related Resources from CA
Networked application performance management—Where to start

Networked applications are nothing new. What is new is the shift in the management focus from availability and event management to application performance management. Network availability/reliability is no longer the pre-eminent problem it once was. The topics of interest now are the service levels experienced with the increasing number of networked applications (VoIP, MPLS, etc.) appearing in the enterprise. In general, short of a physical break from whatever cause, the network is pretty much available and accessible, 24/7, x365.

The problem with all these networked applications, however, is maintaining—in the face of escalating demand—acceptable levels of performance, whatever the service level metric (such as the performance of an individual service application or overall access for a class of critical end users). IT is spending more and more of its time analyzing and tracking what is happening across the network, at endpoints and in-between, to keep service performance at acceptable levels. What can be done?

A strategy for application performance management

The solution is to work from a coherent strategy to understand what needs to be done, assess what you have today that can help, and then determine what you need to add or change to accomplish the task. Only rarely is such decision making and planning done from a completely clean slate without existing tools or with a blank check to rip and replace existing tools with a totally new solution set. Therefore, the next best starting point is to plan on using as many of the existing monitoring and management tools as possible.

1. What needs to be monitored?

First, you need to define the scope of what needs to be monitored and managed when dealing with networked applications. To provide satisfactory performance levels, you must first be able to identify an array of problems that can have their source in the applications themselves, in the servers on which the applications run, or in the network. In the network, devices, connections and configuration can all have an impact on the end-user service experience. Next, you must determine how to resolve these problems.

For now, we'll concentrate on assessing monitoring and management needs. At a minimum, you must plan to monitor:

- End-user experience: You need to know whether there are response time problems before end users call the help desk or service desk to complain. You need to know whether a business application or service could fail or slow dramatically, threatening business revenues.

- Servers at both ends and the devices in the network: You need to know whether everything is configured correctly. Are servers performing correctly? Do performance level trends indicate an emerging problem? Is anything near a saturation point?
Traffic through the network: You need to know which applications are consuming the most resources. Is the routing appropriate? Are some links over- or underutilized?

### 2. Which monitoring tools do you have now?

Once you understand what you need to monitor, you can move to inventory and assess which tools and application resources you have available to do that task today. Then, determine what data and information is currently collected. This information can provide insight into what is happening in the operational environment and how it will affect business service delivery and performance commitments. Knowing which tools and data you already have available will allow you to determine the additional resources you need in order to perform the overall management task.

Remember, you need to be able to understand not only the performance of the infrastructure but also the interactions and—this is important—what the impact is on the service delivery as experienced by the business or business customer. Your requests for additional resources will be more effective if you can report to the business managers that—unless a router is updated or bandwidth added or the workload reduced—their biggest customer won’t be able to enter orders to meet end-of-quarter goals.

### About the author:

Richard Ptak is founder and partner at Ptak, Noel & Associates. He has more than 30 years of experience in systems product management. He was VP at Hurwitz Group and D.H. Brown Associates and worked at Western Electric’s Electronic Switch Manufacturing Division and Digital Equipment Corporation. He is frequently quoted in the trade press and is author of Manager’s Guide to Distributed Environments.
Looking for a more rounded view of your IT infrastructure?

Get a 360 degree view with CA Network & Voice Management

Delivering a unified view of your IT infrastructure is a daunting task. Until, that is, CA introduced the industry-leading Network & Voice Management (NVM) solution. Find out how CA’s solution enables you to detect problems before users complain, solve problems faster, maximize your IT investments, and manage and report against service level commitments.

Get the full picture with a 360 degree view of your IT infrastructure today.

For a more rounded view visit
ca.com/converged
Network management frameworks: FCAPS and ITIL

Network management is a complex topic. In today’s diverse networking infrastructure, the network has to handle more instances of unified communications, video, and virtualization. The role of the network manager encompasses not only monitoring for performance and security, but also anticipating future network problems and transcending technology silos to ensure everything runs well together, whether it's the network, the server, or the application.

While not a complete answer, two frameworks exist that can be of some use for understanding and taming network management: FCAPS and ITIL. Learn more about what these FCAPS and ITIL are and how they can help you evaluate management tools and define network management tasks in this crash course.

**FCAPS**

FCAPS (fault-management, configuration, accounting, performance, and security) is an acronym for a categorical model of the working objectives of network management. There are five levels:

**F—Fault management:** At the F level, network problems are found and corrected. Potential future problems are identified, and steps are taken to prevent them from occurring or recurring. In this way, the network is kept operational, and downtime is minimized.

**C—Configuration:** At the C level, network operation is monitored and controlled. Hardware and programming changes, including the addition of new equipment and programs, modification of existing systems, and removal of obsolete systems and programs, are coordinated. An inventory of equipment and programs is kept and updated regularly.

**A—Accounting:** The A level, which might also be called the allocation level, is devoted to distributing resources optimally and fairly among network subscribers. This makes the most effective use of the systems available, minimizing the cost of operation. This level is also responsible for ensuring that users are billed appropriately.

**P—Performance:** The P level is involved with managing the overall performance of the network. throughput is maximized, bottlenecks are avoided, and potential problems are identified. A major part of the effort is to identify which improvements will yield the greatest overall performance enhancement.

**S—Security:** At the S level, the network is protected against hackers, unauthorized users, and physical or electronic sabotage. Confidentiality of user information is maintained where necessary or warranted. The security systems also allow network administrators to control what each individual authorized user can (and cannot) do with the system.

(Source: Whatis.com’s definition of FCAPS)
ITIL

While the FCAPS framework is a great model for defining the objectives of network management, another best practices approach for service delivery was designed to align itself with current IT organizational structures and expand upon the FCAPS model.

The Information Technology Infrastructure Library, or ITIL, was designed to provide a better framework to deliver high-quality, consistent application delivery over a network infrastructure. Many organizations are adopting the ITIL framework within their environments to provide quality assurances toward providing better network management practices. These practices include a framework for application, service, and security management. For each area, I have included a general description and the questions it addresses for network management teams:

Service support: This is typically a network operations center (NOC) in most organizations. The service support discipline is focused on ensuring that the end users have access to the applications that they require. This area focuses on aspects of troubleshooting, help desk, and supporting new applications over the network. Underlying disciplines for service support include problem management, configuration management, and change management. Problem management would track the number of incidents and facilitate troubleshooting of faults or performance problems that occur in the environment. To troubleshoot a network environment, a good understanding of what devices are on the network and their configuration is handled by the configuration management (often referred to as configuration management database (CMDB)). Change management also involves both aspects of problem management and configuration management as the change board would approve planned changes for the infrastructure, update the CMDB, and record any problems encountered during the change. Efficient service support would include the ability to create a process for troubleshooting and escalation to higher level engineers, PC and client PC installations, and access to other aspects of the organization that are responsible for implementation and design of the network among other duties.

Service delivery: For many organizations, the key management functions of a service are delivered in this area. Service delivery consists of ensuring that as applications are flowing across the network, they are being delivered consistently. This discipline includes capacity management and application modeling. Service level objectives and agreements are the key metrics used to distinguish how well an application is being delivered to end users.

Security management: Security has been a prevalent network management focus for several years with its key characteristics in ensuring that external threats are mitigated with firewalls and access prevention. Security management also includes proper configuration management of rights and permissions of users to ensure that unauthorized access is not granted to end users. Security management is an area of focus to ensure that unauthorized or unintended access of sensitive application data is not obtained.

Infrastructure management: In larger organizations, the teams that design and troubleshoot the systems are separate entities than the team that installs the equipment. This is why accurate configuration management is essential to the success of IT organizations. Infrastructure management is responsible for
the installation and physical configuration of all network devices in the organization. When changes are approved by the change teams, infrastructure teams are the army that enforces these changes and does all of the heavy lifting based on the designs by other architects and engineers.

**Application management:** Application management is designed with the sole purpose of ensuring that an application has the right configuration and design to be implemented in the environment. This discipline can cover many various aspects of network management, from number of application dependencies to delay timers for satellite links. Application management is designed to ensure that the application, end-to-end, is fully enabled to provide the service and delivery to the end users.

**Software asset management:** Software asset management is often considered a vital aspect of managing an organization. Software licenses and products are expensive commodities. Software asset management is designed to be partially configuration management as it provides essential information about the software installed on each device, its revision or platform level, and how many instances are required. Accounting for proper licensing and software maintenance is a big business with many larger IT organizations.

It's also important to note that even in smaller IT operations, these key functions are essential to proper IT management initiatives. Many of these functions can be collapsed together like help desk and service delivery to provide the same services as larger organizations.
Understanding the network application environment

Understanding the network application environment is one of the foundations of application performance management, as I discussed in the tip entitled Application performance management: Developing a strategy. In this tip, I go into detail about how you can better understand the application environment for your network.

Three areas are essential to understanding the application environment:

1. **The network environment:** This includes the network geography in terms of end users and application locations (data centers/servers) and the design of the network to support application delivery.

2. **The application mix:** This includes understanding both the number and types of applications as well as the resources consumed.

3. **The business environment:** This includes current and future initiatives that will have an impact on the number of applications delivered.

All of these are primarily discovery tasks. The objective is to gain a complete, enterprise-wide understanding of the application environment, then assess the technologies and tools required to control and monitor the application services.

It can be very hard to determine which applications are running on the network and even harder to maintain their performance proactively. The first order of business is to discover the applications. There are several techniques that can address this, including interviews with the network and server staff, as well as the business units, to ask what applications they are aware of. This is generally step 1 and can be a good way to determine important applications, as well as problematic applications. Try to develop a classification of applications prior to beginning the interviews so that you can ask questions relevant to the categorization. A general rule of thumb is to categorize as follows:

1. **Real-time, delay-sensitive applications:** These require strict controls on the network to ensure performance. SAP, Citrix, VoIP and signaling protocols are common examples.

2. **Mission-critical applications:** These can be both office applications and applications that drive business production (such as credit card transactions over the network).

3. **Best-effort applications:** Commonly used but not necessarily critical to the operation of the business. Internet traffic is a good example of this.

Once you have categorized the applications, you can move on to discovery and allocation to a category.

Interviews take you only so far during application discovery. In order to fully understand the application environment, you have to gather actual application information from the network. Many products provide application discovery, and choosing among them can be daunting. Multiple vendors provide products that sit on the wire and capture application statistics, as well as report on the performance of those
applications. Some form of tool is critical, as you must collect application information, then monitor on an ongoing basis, to provide true application performance management.

In addition to application discovery and classification, the network plays a huge role in application performance management. Traffic is traversing different parts of the network in different quantities. Depending upon server locations and network geography, the traffic patterns can be significantly different for different areas of the network. This requires a wide view of the network in terms of capturing application flows.

Today, technologies for server virtualization and consolidation, along with application acceleration techniques, make data center centralization a key to application performance monitoring strategies. Centralizing applications can also provide a centralized capture point for application traffic flows. Understanding and controlling that traffic is critical, and centralizing computing facilities for servers can provide greater visibility without the need to decentralize application traffic capturing capabilities. Having probes or application data collection engines at data centers and key sites is much more cost-effective than distributing appliances to all sites.

Intelligence in the network via QoS allows the real-time and mission-critical applications to get bandwidth when they need it and pushes the less critical traffic down the priority stack for delivery over the network. Understanding the network capabilities and designing the network appropriately should be priorities. A discovery and assessment of QoS capabilities embedded in the network technology should be addressed immediately. QoS is well understood and is supported in all major vendor products, and it is a critical component for gaining control of the applications and application delivery.

Finally, the business drivers must be understood. This will provide the justification for enhancing the tools and the network, but the business units must also understand that new application deployment cannot be done just at the business level. There must be open lines of communication between IT and the business units.

These are the key tasks that can be initiated right now in any environment. The choice of tools and network design lies in the hands of IT, and the interface process between the business units is the responsibility of both parties. A good plan is to start with discovery of the applications, looking at the appropriate tools and looking at the network.

**About the author:**

Robbie Harrell (CCIE#3873) is the National Practice Lead for Advanced Infrastructure Solutions for SBC Communications. He has more than 10 years of experience providing strategic, business and technical consulting services. Robbie lives in Atlanta and is a graduate of Clemson University. His background includes positions as a principal architect at International Network Services, Lucent, Frontway and Callisma.
Related Resources from CA

Infrastructure Optimization Drives Efficient Service Delivery

Technology Audit: CA Unicenter Network and Systems Management

Redefining Network Fault Management

Managing VPNs with CA SPECTRUM

Simplifying Performance Management

About CA

CA is one of the world's largest IT management software providers. Our software and expertise unify and simplify complex IT environments in a secure way across the enterprise for greater business results. More than 3000 developers worldwide create and deliver IT management software that keeps our vision real. CA is a global company with headquarters in the US and 150 offices in more than 45 countries. We serve more than 98% of Fortune 1000® companies, as well as government entities, educational institutions and thousands of other companies in diverse industries worldwide. Driving our next level of growth is a our four-part strategy of product development, leveraging partners, global expansion and strategic acquisitions—all with the goal of helping our customers realize the full power of IT to drive their business.

www.ca.com