Brought to you by:

GFI Software™

Aurea SMB Solutions

# Network & Application Management

for dummies®

A Wiley Brand

Meet network bandwidth challenges

Optimize application performance

Deliver top service levels

GFI Software Special Edition

Allen G. Taylor

# About GFI Software

GFI Software, part of Aurea SMB Solutions, develops right-sized, smartly engineered IT solutions for businesses of all sizes. The company helps IT administrators and business people easily and efficiently discover, manage, and secure their business networks, systems, applications, and communications. Thousands of organizations worldwide choose GFI Software. For more information about GFI Software, its products, and success stories of customers from more than 120 countries, please visit www.gfi.com.

# Network & Application Management

GFI Software Special Edition

**by Allen G. Taylor**

for dummies®
A Wiley Brand

# Network & Application Management For Dummies®, GFI Software Special Edition

Published by
**John Wiley & Sons, Inc.**
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com



ISBN 978-1-119-62410-3 (pbk); ISBN 978-1-119-62411-0 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

## Publisher's Acknowledgments

We're proud of this book and of the people who worked on it. Some of the people who helped bring this book to market include the following:

**Project Editor:** Martin V. Minner

**Editorial Manager:** Rev Mengle

**Acquisitions Editor:** Ashley Coffey

**Business Development Representative:** Molly Daugherty

**Production Editor:** Tamilmani Varadharaj

# Table of Contents

# Introduction

Managing a network and the applications that run on it is a demanding job. To keep things running smoothly and provide the level of service that users and the organization expect, network managers need tools that can help them meet those expectations.

## About This Book

*Network Application & Management For Dummies,* GFI Software Special Edition, looks at the challenges that network managers face, some of the tactics that managers use to meet those challenges, and some of the reasons why those tactics often don't produce the desired result. This book also describes a solution that can help you deliver the level of service your users need, at a reasonable cost.

Dummies books don't require you to begin with Chapter 1 and read straight through to the end. You're welcome to choose the chapters that interest you. Of course, you're free to read the chapters sequentially if that's what you prefer.

## Foolish Assumptions

In this book, I assume that you, the reader, fall into one of three categories:

- You're responsible for a data center, and you are running up against capacity limits.
- You're a C-level executive and your data center is of strategic and fiscal importance to your organization.
- You're curious about how the operation of an organization's network might be optimized.

# Icons Used in This Book

The little pictures in the margins of this book indicate information that deserves your special attention. Watch for these icons:

REMEMBER

The Remember icon identifies important information that is worth committing to memory.

TIP

The Tip icon indicates helpful insights and bits of knowledge that may make your job easier.

IN THIS CHAPTER

- Exploring networks
- Understanding what an application is
- Recognizing that the app is king

# Chapter 1
# Understanding Networks and Applications

A major breakthrough in information technology took place in 1981 with the advent of the IBM PC. Where previously an enterprise might have used one room-filling, expensive mainframe computer, inexpensive personal computers proliferated and took over many of the jobs done by mainframes. Whereas a mainframe could be connected directly to resources such as storage and printers, multiple PCs now needed access to those resources. Networks developed to connect multiple PCs to shared resources. This was the origin of the local area network (LAN).

## Exploring Networks

The word *network* is used in a variety of ways in a variety of contexts. In computing, a network is a system containing a combination of computers, peripheral devices, and telecommunication equipment or cables that tie these things together. Networking computers enables them to share resources and perform their tasks more efficiently than would be possible if each computer stood alone.

## Small networks

Networks come in all sizes, from a server and a few workstations operated by a mom-and-pop business to an enterprise-wide network that supports hundreds of thousands of workers. Any organization with a small network likely doesn't need to worry about supporting hundreds of thousands of users, but efficient management of even a small network is important. As the organization grows, the ability to grow the scale of the network to match the growth in workload is equally important.

REMEMBER

Network management relies on the ability to monitor, on a real-time basis, what is going on with the hardware, the applications, and the users. Performance issues must be identified and addressed before they start to affect productivity. Visibility of performance issues is a necessary first step in network optimization. After a problem has been identified, the next step is to configure a traffic policy that will assure that the most important tasks always have the bandwidth that they need.

A small office network may have on the order of a hundred objects or users. Available bandwidth must be such that those users can do their work without delays caused by bandwidth limitations, low-priority resource-hogging apps, or users who are using resources inefficiently.

## Medium networks

A medium-sized office network may need to support thousands or tens of thousands of users. This requires considerably more throughput capability than the small office network case. It also needs to be scalable because networks that have reached this size may grow even larger, becoming even more demanding of system resources.

## Large networks

Large networks are those with hundreds of thousands of elements and users, potentially spread all around the world. For such a system, the productivity impacts of network inefficiencies are greatly amplified. With large networks, the need to monitor the network on a fine-grained level, to diagnose the causes of problems, and to allocate resources to users, applications, and groups, based on their value to the organization, are all critically important. Equally important is the ability to maintain consistency across the network in traffic policy.

# Understanding What an Application Is

The purpose of having a network is so that applications can share and be shared: communicating with each other, accessing common data, as well as distributing and aggregating actions. *Applications* are software programs that perform tasks intended to accomplish useful work for the organization. Some applications are more important than others, and thus deserve a larger share of network resources. Applications may also have different requirements for network resources and quality of service. Voice over IP may not consume a lot of bandwidth but it demands low-to-no latency in order to be effective.

## Critical apps

*Critical apps* are those that your organization depends upon for its normal operation. These apps must run smoothly and predictably whenever they are needed. Whatever resources they require must always be available to them. What qualifies as a critical app varies from one organization to another, but whatever it is, organizational efficiency depends heavily on its timely execution. If, for any reason, execution of a critical app is slowed to the point where it interferes with the timely completion of important tasks, something must be done to correct the situation.

Some examples of common critical applications on networks are Office 365 or anything that has voice communications — for example, video/audio conferencing such as Zoom or Skype for business, or Voice over IP.

These are common critical apps requiring stringent SLAs (service-level agreements) to manage. Other examples are business backbone enterprise resource planning (ERP) systems such as finance or human resources applications. Educational institutions may rely on e-learning systems that record student actions and engagement, or administer timed examinations.

## Other useful apps

Many applications and software tools, although not considered to be critical apps, are valuable contributors to the success of the organization. If they run a little slower than usual, organizational operations are not significantly handicapped. Valuable as these apps are, if they contend with critical apps for bandwidth or other system resources, the critical apps should get more of those

resources and the useful but lower-priority apps should receive less — perhaps *much* less, depending on the useful app's value to the organization.


TIP

The network manager should be able to allocate bandwidth resources to applications depending on their value to the organization, as well as change allocations and network resource attributes to match organizational priorities.

### Unsanctioned apps

In addition to the critical apps and the other useful apps that are supported by the IT department, users often install apps that the IT department has no control over. Some of these apps are innocuous and have a minor effect on system resources. Others can be major bandwidth hogs. Even worse, some such apps may represent a security risk, providing an entryway for malware into the network. These are the apps that keep network administrators up at night.


TIP

Network administrators should be able to detect and monitor the operation of unsanctioned apps, and to reduce or eliminate their impact on the system if they become a problem.

## Recognizing That the App Is King

Ultimately, the purpose of a computer network is to enable application communications among users and data. Consequently, nothing is more important than that applications run as quickly and as problem-free as possible. Some apps are more important than others, so perhaps it is more correct to say that critical apps are kings and queens, other useful apps are dukes and duchesses, and unsanctioned apps are commoners.

### Setting priorities

In order to make sure that the most important jobs get done in a timely manner, priorities should be assigned to all apps that utilize the network. These priorities should reflect each app's importance to the organization. An app's importance may vary with time, so it is important that priorities can be dynamically altered on the basis of changing demands.

Critical apps should have a higher priority than merely useful apps, and in turn, those apps should have a higher priority than unsanctioned apps. However, it is often important to have control of priorities that is more fine-grained than that.

Even among critical apps, some are more critical than others. You should be able to rank apps within a category and assign priorities. The most important app should get the resources it needs, even if it is at the expense of everything else.


REMEMBER

To ensure that the most important apps receive the bandwidth that they need, a network management system should provide policy-based shaping that prioritizes how and when users, applications, and web sites can consume bandwidth. The network manager should be able to control bandwidth usage by network location, users, and departmental groups.

## Safeguarding critical apps

It would be naive to assume that just because the apps on your network are running smoothly now, they will continue to do so in the future. Latent bugs have a habit of cropping up at the least convenient time. Malicious hackers may try to steal your information, alter it, or even destroy it. Beyond that, commercial applications are updated by their vendors on an ongoing basis. Every time this happens, you run the risk that a new vulnerability will be introduced or that out-of-date software will run less effectively or perhaps not run at all.


TIP

To guard against these problems, which can be a major threat to your organization, it is wise to have a system that eliminates vulnerabilities and bugs with a patch management system, as well as a facility to scan your system on a regular basis for new vulnerabilities. Once a potential vulnerability has been detected, a network administrator can decide how to deal with it. In addition to bugs in your operating system or your applications, vulnerabilities can exist in the form of compromised USB devices, smartphones, tablets, software packages, open shares, open ports, and weak passwords, as well as users and groups that are no longer active.

It's unfortunate that you have to worry about what people with malicious intent might do to disrupt the operation of critical apps on your network. However, that is present-day reality. Highly sophisticated hacking tools exist, and they are in the hands of

people who are adept at using them. If one of your most critical apps goes down because of the exploitation of a vulnerability in your network or the apps running on it, you have a major problem.

REMEMBER

It makes sense to take preemptive action by employing a security system that sniffs out and deals with threats before they can do major damage.

## Adapting to network changes

In today's dynamic business environment, the one thing you can count on is that things are going to change. The competitive landscape will change, the organization will change in response, technology will change, and demand for the organization's products and services will change. The network must be able to evolve in response to these external changes. Network management must be agile and responsive to these changes so that the network's quality of service never diminishes. This means that network management tools must have the flexibility to accommodate changes in all these areas.

## Visualizing app execution

As the size and complexity of a network grows, it becomes harder for a network administrator to stay aware of the metrics that describe how efficiently the network is running.

TIP

This is where visualizations of how traffic is flowing, as well as other changing aspects of the system, can provide a quick overview of how well everything is functioning. Dashboards can instantly show the state of operations, flagging potential problems as they appear.

Dashboards should show at-a-glance performance in three key areas:

- Network
- Applications
- Users

With your finger on these three pulse points, you can anticipate and manage almost any business-network issue.

IN THIS CHAPTER

- Comparing networks of past and present
- Looking at app evolution
- Seeing that the cloud adds complexity
- Dealing with unsanctioned apps

# Chapter 2
# Surveying a Constantly Evolving Landscape

Thanks to the relentless advance of technology, the business world is in a state of flux. The people who were your most important customers in the past may be less relevant than newcomers in the future. The technologies that delivered the performance you needed last year may be overtaken by new ones that drive your tried and true solutions into obsolescence. You need to be ready to react to changes that come at you from any unexpected quarter.

For this reason, achieving an in-depth understanding of your network, including its strengths and weaknesses, is critical to responding appropriately to challenges.

## Comparing Networks of Past and Present

In the earliest days of electronic computers, networks did not exist. Computers were so large, and required so much infrastructure, that few entities had more than one. At best, a weaker processor could act as an intelligent I/O device for a stronger one. The software that would enable computers to interoperate on a peer-to-peer basis likewise did not exist.

Technology advanced and costs declined. It became feasible to connect computers in peer-to-peer networks in which peripheral devices could be shared, and later, computational load could be distributed. This development produced a major advance in productivity over the older, siloed approach in which each computer had its own peripheral devices and storage. However, network management was primitive and very much a high-maintenance task.

Networks today are larger and considerably more complex. Local area networks cover large business and academic campuses, and wide area networks girdle the world. Some networks even have nodes in space. Adding to the complexity are links to private and public clouds. As understanding and controlling these networks has become progressively more difficult, doing so has become more important than ever.

REMEMBER

Monitoring network status and being able to respond to performance slowdowns or unusual activity are necessary defenses against lost productivity and potential malicious attacks.

## Looking at App Evolution

Just as networks have evolved into larger and more complex forms, applications have undergone a similar transformation. In the early days, even the most expensive and sophisticated computing systems had a small fraction of the processing power, memory, and communication bandwidth of what today is not considered to be noteworthy. Because resources were comparatively limited on those early systems, the apps running on them couldn't be very complex, either. Apps were limited in what they could do because of resource limitations. As a result, managing a network that was running those relatively simple apps was much simpler than running a system today; not nearly as many things could go wrong.

As improvements have been made in the processor speed, memory, storage capacity, and data transmission capability, apps have grown in power and complexity to match.

Critical applications such as finance, human resources, and supply chain have always been core enterprise resource planning (ERP) systems and are the way enterprises have typically found and

defined competitive advantage. These applications have evolved, and new models have emerged that are more nimble, enabling new companies to disrupt older ones that have not kept pace.

As soon as new capacity becomes available, ways to make use of it are found. The additional work, of course, adds to the responsibilities of the network manager, who must become familiar with the normal operation of more and more complex applications, as well as be able to spot and deal with any deviations from normal operations.

Today's basic operations — and often, tomorrow's strategic direction — depend on it.

## Seeing That the Cloud Adds Complexity

You would think that the added complexity to be found on a contemporary proprietary network would be bad enough. However, many networks now make use of resources available on the public and private cloud. This trend compounds the complexity and adds new security concerns. When a network is connected to the cloud, a window opens in the firewall, through which data can both enter and exit the LAN. Either case can be problematic.

The network manager has now surrendered some of the control that she previously had to the cloud provider. More things can go wrong, and thus the network manager has more things to monitor and potentially take action against.

Finally, it becomes easy for users to install unsanctioned apps. In extreme cases, users might pick up SaaS apps and create their very own *shadow IT* department.

## Dealing with Unsanctioned Apps

You have sanctioned and unsanctioned applications running on your network. What's the difference?

**Sanctioned apps** are approved by the organization's IT department and are typically purchased with a license. Office 365, Slack, and Salesforce are examples of sanctioned apps.

**Unsanctioned apps** are unlicensed, unmanaged applications that the IT department does not know or explicitly approve of. Such apps may not cause overt harm but may lead to problems anyway, perhaps by soaking up bandwidth. Even if they do not use excessive bandwidth, they add an unknown factor behind the firewall, sometimes interacting with sensitive data. Browser extensions, instant messaging clients, and pirated apps that look like trusted known apps are all potential sources of malware. If people bring their own devices to work (BYOD), the organization is in the Wild West. IT has no authority over the apps present on employee-owned devices.

Sometimes even sanctioned apps can be a problem if they are augmented with unsanctioned third-party add-ons. For example, there are an average of 26 cloud apps for every implementation of Salesforce. Data can leak from highly protected and monitored sanctioned apps to third-party add-ons, compromising the integrity of confidential data.


TIP

Not all third-party add-ons are malicious, but if you have no visibility into them, you can't be sure that your data is safe. You need to know where your network traffic is coming from and where it is going. Software tools such as Exinda Network Orchestrator are designed to give you that visibility.

IN THIS CHAPTER

- Addressing end-users' quality of experience
- Caring about effective use of apps and personnel
- Keeping customers happy and staying on budget

# Chapter 3
# Understanding That Different Stakeholders Have Different Concerns

Different groups of people, each of whom has a stake in the success of an organization's network, have different concerns about what the network should deliver. Each of these constituencies needs its concerns addressed.

The people who use the network every day to do their jobs have expectations of what the network will do for them. Less directly involved, but equally important, the upper management of the organization considers the network to be a strategic asset and has expectations that are different from those of the regular users. Finally, the IT department is tasked with maintaining the network and correcting problems that arise. IT's main concern is that the network be robust and resilient in the face of heavy loading and other challenges.

# Addressing End-Users' Quality of Experience

Workers in enterprises of all types and sizes have jobs to do. These days, many of those jobs depend critically on the worker's ability to operate on information stored in the computational resources located on the organization's network. Whether the worker's experience is enjoyable, merely tolerable, or outright frustrating depends on how smoothly the system is operating.

The quality of a user's experience depends directly on the quality of service (QoS) delivered by the network. QoS depends on such things as:

- Bit rate
- Throughput
- Transmission delay
- Delay variation
- Availability
- Jitter
- Packet loss
- Bit error rate

Managing the bandwidth you already have can be just as effective as buying more capacity, with the bonus that you are saving money on capital equipment that you don't have to buy.

REMEMBER

Application run time can be affected by the factors in the preceding list, but also by capacity limitations, changes in the mix of jobs run on the system, apps that are more demanding of system resources than had been the case in the past, or a multitude of other conditions that have the ability to gum up the works.

## Slow or unresponsive apps

Probably the condition that affects a user's productivity and frustration level most often is having to deal with interactive applications that are slower than a human. What's up with that? Computers are supposed to operate a thousand times faster than the wetware inside a human's skull.

TIP

The most efficient, most productive users are more likely to be bothered by slow or unresponsive apps than are their less productive peers. If you decide to go for coffee or play a little Spider Solitaire while you wait for your app to return a result, your motivation and productivity are bound to suffer.

### Apps unavailable when you want them

When an app is unavailable, the impact on productivity can be devastating. If the app you need is on the critical path for an entire project, an outage can have repercussions far beyond one worker's individual production. Advance warning of an impending problem with an app can enable an administrator to redirect resources or make other arrangements that bypass the problem app.

TIP

Network and application monitoring software can give you the ability to see trends that somewhere down the line may cause an app to stop working as it should.

## Caring About Effective Use of Apps and Personnel

Applications and personnel are both important organizational assets. It is important to have a positive return on investment in both cases. If people are not making effective use of the sanctioned applications that have been purchased, the organization is not getting full value out of either the applications or the personnel.

### Users not using apps effectively

Businesses acquire computing environments, tools, and applications with the expectation that employees will use them effectively, thus deriving value that exceeds the cost of those resources. If employees are not using those resources, either because of inadequate training or personal biases, management is not getting an adequate return on the investment in them.

Perhaps the employees are not using apps because the apps are slow or unresponsive. If that is the case, monitoring of app usage with application management software can pinpoint the problem area and suggest a solution that will give the affected employee a more satisfying and productive experience, as well as give the

business managers a return for the investment they have made in the application in question.

If you introduce a new application and employees have a poor experience with it, they may return to whatever more familiar solution they had previously. For example, you may want to reduce mobile phone charges by installing Skype for Business. However, if calls are dropped or call quality is poor, people will quickly find alternatives without telling you.

This tendency may not affect just voice communications applications. If a new app shares data between suppliers and manufacturers but crashes at critical synchronizing times, you may lose productivity time. Your teams will find workarounds to do their jobs without the app that you spent so much to purchase.

### Moving data to the cloud can have unintended consequences

Storing data on the cloud rather than locally can provide substantial advantages. Users everywhere have equal and relatively frictionless access to it. However, for data that is only used locally at one site, adding the transmission delay inherent in remote cloud storage can reduce productivity. You also introduce a potential security vulnerability that does not exist when your LAN has no connection to the Internet.


TIP

Although management, to save money, may decide that data should reside on the cloud rather than on local hardware, enforcing this policy across the board may result in a performance hit that frustrates some users and delays the completion of important work.

## Keeping Customers Happy and Staying on Budget

Just as networks have evolved into larger and more complex forms, applications have undergone a similar transformation. In the early days, even the most expensive and sophisticated computing systems had only a small fraction of the processing power, memory, and communication bandwidth that a relatively inexpensive system has today. Because resources were comparatively limited on those early systems, the apps that were running on

them couldn't be very complex either. Apps were limited in what they could do because of resource constraints. As a result, managing a network that was running those relatively basic apps was much simpler than running a system today. There were not nearly as many things that could go wrong.

## The same user operational problems keep occurring

Elusive, intermittent problems that crop up without warning are among the most frustrating of challenges to the IT department. IT is tasked with keeping things running smoothly, but that's hard to do when a problem cannot be consistently reproduced, let alone tracked down and resolved. As long as such problems persist without an effective solution, users will continue to experience frustration and delay.

## No visibility of the source of problems

It's hard to fix a problem that you cannot see. You may experience the consequences of a problem, in terms of slow operations, failure to launch an app, or inaccessible data, but what is causing those problems can be much harder to pin down. The need for tools that point you in the direction of the source of a problem becomes apparent when such a cryptic problem arises.

## Problems consume staff time, leaving none for required maintenance

The IT department has important responsibilities that go beyond just fixing things when they break. IT's primary responsibility is delivering the quality of service that users have every right to expect. This means that computational and networking resources must be tuned to satisfy the changing demands that are placed upon them. Additionally, new equipment must be integrated into the overall setup as the need arises. Maintaining existing equipment is also a large part of the job.

REMEMBER

If IT spends most or all of its time chasing down problems that users are having, no time will be left for the department's other responsibilities, such as addressing security vulnerabilities or planning for future needs. Either of these tasks, if not allotted enough time, can have a major impact on continuing operations.

## Disconnect with business management over cloud usage

The IT department wants to keep its customers — the users — happy by delivering dependable, timely performance. It wants to do this despite all the challenges that it must address in maintaining a complex collection of hardware devices, the connections among them, and the software that is running on them. Including the cloud in the mix adds even more complication.

You need to be able to manage your private/public cloud networks as easily and securely as if they were inside your organization. You need to ensure security and accessibility for your users so the cost advantage of cloud is not overshadowed by business cost risks.

You also need to be able to take full advantage of cloud-based technologies and infrastructure. Rather than buying your own separate T1 pipe from a service provider, you can create a network backbone that has the same capacity but made of multiple technologies, transport media, service providers, and service-level agreements (SLAs). To support your business, you need to reduce the risk disadvantages while maximizing the opportunity advantages of using the cloud in your network and applications.

REMEMBER

Integrating a network with the cloud puts a stress on IT resources. Business management must understand this and be willing to give IT the additional resources it needs to successfully incorporate the cloud into its area of responsibility.

IN THIS CHAPTER

- Using apps effectively
- Maintaining productivity by keeping apps functioning
- Being proactive: Staying ahead of the curve

# Chapter 4
# Solving Problems

The problems described in Chapter 3 go beyond the fact that apps with performance issues are not delivering the desired return on investment. If those apps prevent the enterprise from operating efficiently, much more can be lost than just the cost of the app.

## Using Apps Effectively

The organization spends a significant amount of money every year subscribing to, developing, and maintaining applications in the course of doing business. Management expects a positive return on investment from the effective use of those applications. If people are not using the apps, continuing to pay for them is a waste of money. If people *are* using them, but they are not taking full advantage of the app's capabilities, the organization is still wasting money.

For example, if the quality of experience that users are having with an application is not good, they are likely to avoid using it. If the app is slow and unresponsive — jittery and slow to load — that

can be frustrating. Nobody wants to feel they are spinning their wheels.

If the users do not trust the application to produce accurate results, that is another reason to try to work around using the app. Users want to do their jobs efficiently, but they also want to do them accurately. Work that turns out to be misleading or incorrect reflects badly on the employees who produced it, even if the fault lies completely with the app they were running.


TIP

Sometimes, when application performance is subpar, it is not clear whether the problem is the application or the network. Tools that focus on the performance of applications alone, or the network alone, may not enable you to zero in on the source of the problem as quickly as a tool that gives an integrated view of both the application and the network that is hosting it. For example, Exinda Network Orchestrator provides the insight and bandwidth control that an application like Skype for Business requires to ensure true QoS and user adoption. It provides unified visibility, offers real-time monitoring, and gives actionable recommendations on what to do to address any problem it encounters.

## Maintaining Productivity by Keeping Apps Functioning

If ineffective or inefficiently used applications are a source of frustration for the users, they are even more problematic for the business. Funds are wasted on apps that are not producing the results that were envisioned when they were purchased or developed. A backlog of problem tickets keeps the tech support department busy and reduces its responsiveness to problems as they arise. The longer a problem remains unresolved, the more it costs.

Underuse or inefficient use of software can cost the organization money, as well as increasing the expense of supporting that software. This tendency reduces productivity, which ultimately causes a drain on the bottom line. If a problem prevents employees from doing their jobs, swift resolution of the problems becomes critical. This is where fine-grained visibility of both the software and

the network hardware must be available so that the organization can perform corrective action as quickly as possible.


TIP

Even better than reacting quickly to problems that reduce productivity is to be proactive. By taking a proactive stance, you can prevent productivity-sapping problems from occurring in the first place.

## Being Proactive: Staying Ahead of the Curve

Being proactive implies that you have a good idea of from where performance problems are likely to arise. To have that foresight, you need application and network management tools that show you how the system is operating on an instantaneous basis. You need to see trends in progress and be able to anticipate problems. Then you can make adjustments that will keep the system operating smoothly and efficiently.


TIP

An example of a tool that gives you that kind of visibility is Exinda Network Orchestrator. One of its dashboard views of system traffic, both inbound and outbound, is shown in Figure 4-1.

You can take positive steps to anticipate problems that are about to manifest themselves. You can start the process of taking those steps by asking questions about the network, the apps that run on it, and the users:

- **Network:**
  - Which apps are using the most bandwidth?
  - What percentage of traffic is unsanctioned?
- **App:**
  - What are my critical apps?
  - What is their usage?
  - What are the key QoS metrics for the critical apps?

» **User:**

- Which users (or set of users) are using the most bandwidth?
- Peak rates of usage on network — when is most bandwidth being consumed?

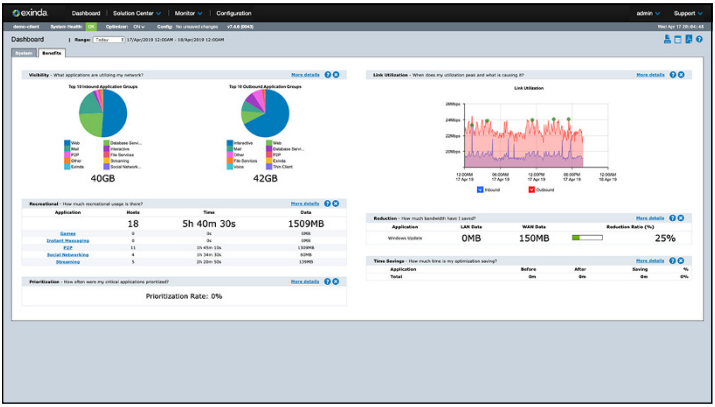



**FIGURE 4-1:** Application usage of network resources.

IN THIS CHAPTER

- Identifying what is causing the problem
- Coping with unsanctioned apps
- Dealing with bring-your-own-device (BYOD)
- Protecting against users bypassing your safeguards

# Chapter 5
# Identifying Problems

Once you suspect that a problem exists, either because of trouble tickets or excessive help desk traffic, the next step is to track down the cause. Usually, you need to do some detective work. Many factors can reduce network or application performance:

- Network throughput can be slowed by excessive traffic.
- An application may be hogging resources.
- A network user may be hogging resources.
- Traffic volume can spike at busy times.

Whatever is causing the problem, your job is to identify it, deal with it, and return the system to a nominal condition.

## Identifying What Is Causing the Problem

The cause of a performance problem usually is not obvious. There are many potential causes. The only way to deal consistently with network and application problems when they arise is by having deep visibility into everything that is going on. This means monitoring system status and behavior on a continuous basis.

TIP

Problems may appear and then disappear intermittently. Network and application real-time monitoring software can catch such occurrences and notify the network administrator when they occur. Problems that are more predictable, such as bandwidth saturation at times of heavy use, can also be identified by such software and brought to the attention of an administrator who can analyze the situation through an intuitive dashboard that gives visibility into the activities of all users, applications, devices, and locations.

Figure 5-1 shows an Exinda Network Orchestrator dashboard. You can tell at a glance which categories of applications are generating the most inbound and outbound traffic.

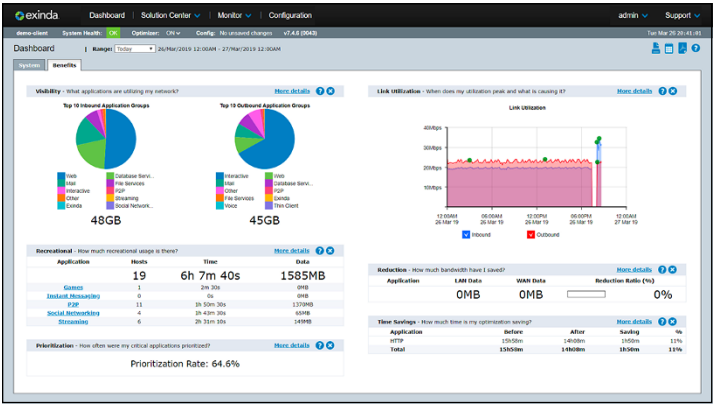



**FIGURE 5-1:** Network usage by application groups.

The pie charts show that web applications are generating the most inbound traffic and interactive applications are generating almost two-thirds of the outbound traffic. The information below the charts breaks out recreational usage into games, instant messaging, P2P, social networking, and streaming. On the right, a day's worth of link utilization is shown, with outbound utilization exceeding inbound during normal operation, with a brief flip to inbound exceeding outbound at about 8 p.m.

## Coping with Unsanctioned Apps

It would be great if network and application managers could control all the applications that appear on the network. This kind of tight control can be maintained in some places, but not others.

Users often download and run applications that consume large amounts of system resources. In many cases, these bandwidth hogging apps degrade the performance of sanctioned apps that are much more important toward reaching the organization's goals. Recreational apps, which are commonly found on academic networks, among others, can reduce performance of research and instructional applications.


TIP

Detecting low priority, but nonetheless resource-consuming apps, is one thing, but doing something about the situation is another. The solution is a policy shaping tool that enables the administrator to prioritize applications, restricting the amount of bandwidth that lower priority apps can consume and/or generate.

## Dealing with Bring-Your-Own-Device

Adding to the problems generated by users installing unsanctioned apps on network workstations, they are increasingly bringing their own laptops, tablets, and phones, and tapping into the network with them. The result of the bring-your-own-device (BYOD) trend is that unsanctioned hardware, in addition to unsanctioned software, adds uncertainty to the network. That's not even giving a thought to potential security vulnerabilities that may be introduced by these shadow IT devices. Speaking of unsanctioned software, any software on a BYOD device is unsanctioned by definition. Apps on such devices have not been cleared by IT.

## Protecting against Users Bypassing Your Safeguards

Users of your network can be diabolically clever. Regardless of how many safeguards you put in to protect your network from performance-robbing applications or from malware that is roaming in the wild, they will find a way to get around your safeguards, run the apps that they want to run, and connect to the sites that they want to connect to. This fact of life is unfortunate, but you likely will have to deal with the resulting problems when they arise. Your weapon of choice in that battle will be network and application management software and hardware that gives you visibility into what is happening at multiple levels.

IN THIS CHAPTER

- Excluding low priority traffic
- Buying more capacity
- Throttling incoming low priority traffic
- Gaining efficiency with SD-WAN
- Applying quality of service (QoS) criteria to applications

# Chapter 6
# Looking for Solutions

When a network and the applications running on it start suffering performance problems, network managers can take several approaches to free up saturated bandwidth. Each of these methods has advantages and disadvantages.

## Depending on the Firewall

One simple approach is to selectively block incoming traffic at the firewall. This frees up bandwidth, if the problem traffic is inbound rather than outbound, and if the sources you choose to block are the major sources of the problem. If, on the other hand, the traffic is coming from a multiplicity of dynamically changing sources, this strategy is like a game of whack-a-mole and may prove ineffective. Additionally, this solution does not address the source of the problem. Low priority traffic does not decide on its own to enter the network. It must be invited in by a user who asks for it.

## Throwing Bandwidth at the Problem

The "blunt instrument" approach to the problem is to buy and add more bandwidth. This solution is rarely effective in the long run, although it might help for a little while. As soon as increased

capacity becomes available, users find ways to use it. This approach is like adding another lane to the Interstate 405 freeway in Los Angeles. The increased capacity makes it attractive for even more people to take the 405. The result is more people wasting time and burning gas in the stop-and-go traffic. Nobody gets to their destination any sooner.

## Employing Filters

Another idea is to filter out the bad actors, the nodes out on the web that are the sources of problematic traffic. This can be effective for whatever is clogging your network right now, but unfortunately, the situation is dynamic rather than static. As new sources of unsanctioned content appear, the filters must be constantly updated. You cannot update the filters until you know what content to exclude and where it is coming from. You must constantly monitor the incoming traffic to see what is taking up an inordinate amount of bandwidth. After that, you must determine whether that traffic deserves the bandwidth it is consuming.

## Managing a Software-Defined WAN

If you have a data center at a central location and branch offices at geographically remote locations, you need a wide-area network (WAN) to connect those facilities. Traditionally, this job has been accomplished with a complex collection of routers and other hardware, along with some potentially very long communication lines. Routers, as the name implies, are not very intelligent devices. Their job is to send the signals they receive to their intended destinations. They don't offer much of a role for software.

More recently, it has become feasible at the network edge to replace dumb routers with smart X86 computers (a *PC-based network edge).* Because X86 processors, due to tremendous economies of scale, have become inexpensive, a smart, software-driven device (the X86 processor) can provide a simpler, easier to understand user interface, while providing a less expensive solution to the problem of managing a WAN.

REMEMBER

A device called an *orchestrator* communicates with the X86-based edge devices and communicates events coming in from them to the central network management system. The network administrator can monitor and control the network from the orchestrator's simple browser-based graphical user interface (GUI).

## Applying QoS Management to Applications

You might think that you have an intuitive understanding of what the term QoS (quality of service) means. It seems logical to see it as the performance of a service, as seen by the users of that service. That's a valid assumption, but the quality of service of a computer network is judged by different criteria than the quality of service of, for example, a telecommunications network or a pizza restaurant.

As mentioned in Chapter 3, for a computer network, QoS depends on such things as:

- Bit rate
- Throughput
- Transmission delay
- Delay variation
- Availability
- Jitter
- Packet loss
- Bit error rate

REMEMBER

For an application, QoS depends on all those things, but also on the demands of other applications that are contending for the same resources. Some applications that run on a network are more important to the organization, or more time critical. To manage the QoS of such an application, a mechanism must exist to assign a high priority to it. Thus, you maintain a guaranteed level of performance, regardless of whatever else is running at the same time. That's what QoS means in the context of computer networks.

IN THIS CHAPTER

- Getting an overview of a network
- Optimizing network resource allocation
- Recommending management actions
- Reporting on network status
- Monitoring network status in real time
- Combining the monitoring and the managing functions
- Making network management easy to understand

# Chapter 7
# Finding a Better Way

Chapter 6 talks about various ways of assuring that important applications receive the resources they need in order to deliver the performance that is required of them. Some of the proposed solutions in that chapter alleviate the problem of degraded performance temporarily, but then become less effective as users adapt to the new situation.

A more effective, integrated approach would give the network manager the following:

- Fine-grained visibility into what's happening on the network
- Recommendations on how to shape traffic so that the most important applications receive their fair share of resources
- The ability to take those recommendations and act on them to provide the maximum benefit to the organization.

# Providing Visibility across the Network

In order to take effective action to remedy a performance problem, you need to see where the problem is coming from. Perhaps one user or a small group of individuals is consuming an inordinate amount of bandwidth. Or perhaps a particular application slows the network to a crawl whenever it runs. Maybe the excessive traffic is being generated by one remote location, or perhaps the bottleneck is a single device.


TIP

To track down the problem quickly, the network manager needs an overview of these disparate, possible sources of the problem. This requirement is best served by network management software giving you visibility into all the potential sources of the problem from one centralized, easy-to-understand user interface.

The ideal solution to this requirement is to provide dashboards that enable real-time monitoring of:

- Network traffic
- Network interfaces
- Network throughput
- Network users
- Network conversations
- Service levels
- Applications
- Host traffic volume
- Subnets
- Virtual circuits
- The effects of controls
- Optimization reports


REMEMBER

Access to these sources of information from a single console enables the network manager to zero in quickly on the cause of a performance slowdown.

## Managing Bandwidth

In a contentious world where your users demand more bandwidth than you can deliver to them, you must be able to allocate the bandwidth you have, equitably and consistent with the overall goals of your organization. This need calls for policy-based shaping, with which you can control the maximum amount of bandwidth that can be consumed by traffic coming in from a designated source, the amount that can be consumed by a single user, or by a single departmental group.


TIP

With visibility of system usage from an integrated network management dashboard, you can equitably assign priorities to users, groups, or traffic sources.

## Employing a Recommendation Engine

Wouldn't it be great if your network examined the traffic flowing across it and, for example, noticed when an application that was not on the radar before was suddenly using a lot of bandwidth? The first step to solving a problem is knowing that one exists. The second step is identifying the source of the problem.

Only after you know what is reducing your network throughput are you in a position to do something about it. A recommendation engine would be a great tool for this, letting you follow these steps:

1. Analyze all the traffic that passed through during the most recent 24-hour period.
2. Check to see if any recreational apps had suddenly risen to become top bandwidth-consuming apps.
3. Recommend that you establish a policy to limit the amount of bandwidth such applications can consume when higher-priority apps are being negatively affected.


TIP

The Exinda Network Orchestrator appliance includes a recommendation engine. Run daily, it can keep you up on new, low-priority applications that appear, giving you the opportunity to deal with them before they become a problem.

## Generating Detailed Reports

To keep your network operating as close to its optimum performance level as possible, you need to know, at a highly detailed level, the nature of the traffic it is carrying as well as the effects that groups of applications are having on the system.

To obtain the actionable information needed, you must continuously collect network traffic data. Once collected, the data must be grouped in meaningful ways and then displayed in charts, tables, and graphs.

To determine whether the network is experiencing an abnormal load, you must first know what a normal load is. Take data for some time interval to establish a baseline for operations. Once you have a baseline, reports can show deviations from the baseline that may warrant investigation.

Ideally, any performance report that can be displayed on a monitor screen should be easily converted into a report in .pdf format as a permanent record, or to present to management and other interested parties.


TIP

One useful report shows how much bandwidth your top-ten hungriest applications are consuming. If all is well, these are the same applications that were the top ten when you established your performance baseline. If a new application suddenly appears in the top ten, and has not been a major bandwidth consumer before, it likely bears investigation. Is it a recreational or other low-priority app that is now reducing performance for apps that are business-critical? Such a report can give you early warning of a potential problem before it becomes a real problem.

Speaking of recreational applications — games, instant messaging, peer-to-peer file transfers, social networking, and streaming — such apps are appropriate in some places and not others. For example, recreational apps are likely appropriate on a college network that provides service to student dorms. That may not be the case for a business network. However, because some of the apps in these groups may have a legitimate application even in a business context, you may not want to ban them completely. This is where a prioritization system using policy-based shaping can allow these applications to run, but not at the expense of higher-priority apps.

## Monitoring in Real Time

Weekly or monthly reports on network operations serve an important purpose. However, to maintain a high quality of service, the network must be monitored in real time. The network is a highly dynamic piece of critical infrastructure, with applications and users coming and going at unpredictable times, changing the loading on the system as they do so. It's important to be able to recognize a peak loading situation while it is happening and to be able to deal with it by reallocating resources to the places where they are most needed.

## Having a Single Tool That Monitors and Manages

Monitoring a network and managing that same network are two distinct functions, but they are closely related. You must do the managing, based on what you learn by doing the monitoring. If you use the same tool to both monitor and manage your network, there is no "impedance mismatch" between the two functions. The two work seamlessly together.

## Gaining Productivity with an Easy-to-Understand Interface

If you have a single, intuitive user interface for a tool that performs both the monitoring and the managing functions for a network, users come up to speed faster and make use of the full functionality provided by the tool quickly. You spend less time training new operators, who can then become productive right away.

IN THIS CHAPTER

- Setting priorities
- Providing solutions
- Assigning users to groups
- Assigning resources to users
- Managing multiple locations

# Chapter 8
# Working with Advanced Network and Application Management

Beyond the basic task of managing a network and the applications running on it, you can take advanced actions to make the network more than just acceptably productive. This chapter discusses several factors that can provide a significant productivity boost.

## Setting Policy Dynamically

From a network manager's point of view, it makes sense to prioritize the applications that are running in a way that allocates the most resources to the most important applications, fewer resources to less important applications, and minimal resources to the least important applications. The problem is that priorities change over time. New applications appear for the first time. Where should they be placed in the priority ladder? Existing applications become less important, but they retain their initial priority unless you change it.

The dynamic nature of business means that adjustments to priorities must be made on an almost continuous basis, taking up a significant amount of the network manager's time. More importantly, throughput is degraded as capacity allocated to a retired application goes unused, while another app that needs that capacity is choked.

The obvious answer is to establish an adaptive rather than a static bandwidth allocation policy, based on a variety of characteristics. One aspect of such a policy is to commit to a minimum and a maximum amount of bandwidth for a particular application or user, and to provide a higher burst bandwidth allocation when free capacity is available. Some applications, such as Skype for Business, require a certain minimum amount of bandwidth to be usable at all. Setting the right minimum threshold is important in such cases. A maximum threshold is important too. You don't want to degrade important business processes with a cluster of simultaneous Skype calls. An adaptive approach can reduce video quality to ensure continuous, low-latency throughput.


TIP

A valuable distinction of the Exinda Network Orchestrator is that it supports an adaptive rather than a static bandwidth application policy.

## Employing a Solution Center

Of all the things that could possibly cause performance problems on a network, a relatively small number will likely be the culprit most of the time. If you can easily keep an eye on those few things, it's unlikely that you will be caught off guard by a problem that seriously degrades your network's performance. Problems are most likely to arise in four areas:

- Application performance
- Network governance
- Project readiness
- WAN planning


TIP

If you have a centralized place where you can view the status of these areas, you will be able to stay on top of any emerging issues.

In the area of **application performance**, a small number of apps likely consume most of the capacity of your network most of the time. If your solution center links directly to performance

monitors for these heavily used apps, you can check how each one is doing with a single mouse click.

**Network governance** has to do with making sure that the network is being used to accomplish the objectives of the organization and is not being used for purposes that would be harmful. Under this category is managing recreational usage, which should never impede the execution of operations that are important to the organization. Another aspect of network governance is monitoring traffic to ensure that illegal downloading of "pirated" or illicit content or other copyrighted material is not taking place. The organization may be exposed to liability if such activity is occurring.

**Project readiness** is what you do when something goes seriously wrong. Are you prepared for an equipment failure, a major power outage, or sudden change in traffic demands that bring the network down? You should have plans in place for foreseeable events, and a link to those plans should be present in the solution center.

Before introducing a new application, make certain you have the bandwidth to support it, based on how it is likely to be used. Be prepared for events that place unusual demands on the network. You don't want an epic fail when the CEO is addressing the organization over a live stream. A network assessment will ensure that such an event goes smoothly.

**WAN planning** involves asking whether you should buy more capacity. Before you place that order, check on the bandwidth usage of your most heavily used apps. You may find that the usage of those apps is legitimate and reasonable. Or you might find that a big chunk of bandwidth is being consumed by streaming or some other low-priority application. In that case, you can correct the situation without spending a dime by restricting the errant activity with policy shaping.

## Placing Users into Priority Groups

In any organization, some jobs are more important to the achievement of organizational goals than others. People holding those jobs should have better access to system resources than others. You can give this to them by placing people into groups and then setting a priority for the group. Everyone in the group will have the same priority, and they will have a higher priority than the people in another group to which you have assigned a lower priority.

## Allotting Users' Resource Quotas

You can allot resources on an equal basis to the members of a priority group or you can allot those resources on an individual basis. Perhaps users at remote locations will have different needs for system resources than people at the main office. You need to be able to allot resources according to what people need.

## Centrally Managing Multiple Locations

In even a small network, you have a lot to monitor and manage. You need to perform those monitoring and managing tasks as easily as possible. That means taking care of everything from a single, centralized location. In one place, the network manager will have an overview of the entire system, with visibility into all the far-flung parts of it, as well as the ability to establish and enforce policies as needed.

This capability is of special concern when you have a network spanning branch offices and a head office. Data connections between an enterprise headquarters facility and branch offices are often unreliable, not fast enough, and expensive. Enterprises that have a headquarters facility (such as a main office or data center) and various branch offices need to be able to communicate between all offices as well as with devices and servers on the public Internet. With the proliferation of cloud services based on private and public clouds, as well as services that are heavily dependent on reliable and high-performance applications, you may have hit the limits of available WAN (wide area network) services.

Although it may be economically feasible to provide high bandwidth Internet connectivity to the main office, providing the same speed connection to each branch office is prohibitively expensive.

Network management of the WAN, incorporating bandwidth from multiple sources, is one key way to manage this concern.

REMEMBER

When performance is critical, you need to be able to intervene in a timely manner when problems arise. Centralized management makes that possible.

IN THIS CHAPTER

- Creating a more efficient network
- Keeping users happy and productive

# Chapter 9
# Ten Points to Remember

Your business operations depend on applications and data. Your applications and data depend on your network. The network manager's job is vital and challenging, with many things to think about. Here are ten important ones.

## Keep Users Happy

The network and the applications that run on it are tools. The primary purpose of those tools is to enable the users to accomplish the organization's objectives. To do that, the apps that they are using and the network they are running them on must deliver productive, dependable, hassle-free operation.

## Don't Overload IT Staff

Automate operations to the extent possible. The direct attention of a human operator should not be needed until an off-nominal condition occurs. At that point, it should be easy for an IT staffer to determine quickly what is wrong and what to do about it, ideally based on easy-to-use and proactive information available on the management console. More automation reduces the chance of human error and also reduces staffing costs.

## Get Your Money's Worth Out of Purchased Applications

The organization has purchased or subscribed to a collection of sanctioned applications. To maximize the return on investment in these apps, it is important that users are properly trained in their use and are actually using them. Training resources on applications should be available to everyone who might need them.

## Give Critical Applications High Priority

Any network and application management solution must have the capability of understanding the needs of, and assigning different priorities to, the variety of applications or groups of applications you have. You need to assign the highest priority for network resources to your most important apps.

## Identify and Prohibit Dubious Applications

Applications that are not materially helping meet the objectives of the organization have a way of finding their way onto the organization's network. Even those installed by employees to help do their jobs must be monitored, managed, and decided upon. The network management system must be able to spot such apps and deal with them, either by severely restricting the amount of bandwidth they can consume or by eliminating them from the network.

## Reduce Strain on the Help Desk

The best way to reduce strain on the help desk is to anticipate performance problems that will affect users and to mitigate them before those users detect reduced performance. This requires a monitoring system that notices a problem early, informs the network manager about it, and enables action to be taken quickly to solve it.

## Reduce Data Center Costs

The first instinct of many network managers when they start to run up against bandwidth limits is to buy more bandwidth. This is the "throwing more bandwidth at the problem" brute force solution. This may relieve the problem for a while, but ultimately traffic will grow to consume the additional capacity. A more enlightened approach would be to reduce the traffic being transported across the network or, through management, ensure critical applications have the network resources they need to ensure organizational success.

One reason why network traffic builds up is redundant transfer of data. Chances are, if a user at a branch office needs a particular data item, either she or one of her coworkers will likely need it again soon. Rather than choke the network with that traffic, a more efficient solution is to cache incoming traffic at the branch office so that it is immediately available when it is requested again, without crossing the network at all. Depending on the application that is running, this idea can save significant bandwidth, making the capacity freed up available to other traffic. Delaying or even obviating the need to upgrade the capacity of the entire network by caching at the network edge can yield major cost savings.

## Monitor and Control Everything from One Place

The person filling the role of network manager at any point in time must have broad visibility of what is happening across the entire network. It must be possible to monitor the following:

- Network traffic in real time
- Network interfaces
- Network throughput
- Service levels
- Applications
- Network users
- Traffic volume of hosts

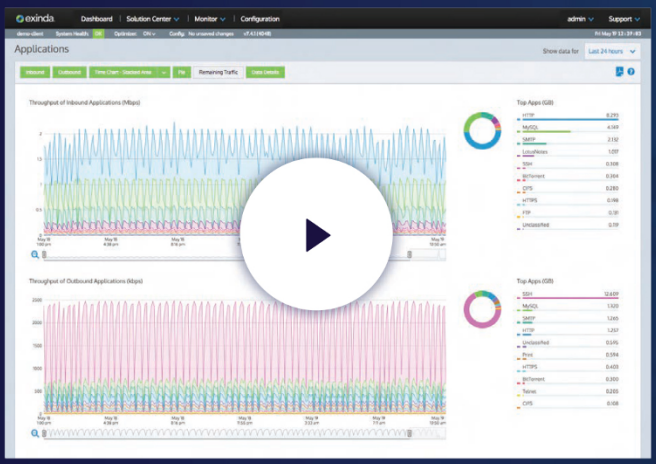
- Network conversations
- Subnets
- Virtual circuits
- The effects of control interventions
- Optimization reports
- Performance of network management appliances
- Statistics of monitored quantities

All these monitoring tasks should be overseen by the network manager, located at a single console. The only way to have a comprehensive, overall view of network and application performance is to have the information available to the responsible individual, in one place.

## Recognize Problems Before They Affect Users

The advantage of having an array of monitoring functions and reports at your fingertips, delivering up-to-the-minute, real-time information on the health of your network, is that you can take remedial action as soon as you see a troublesome trend developing. An integrated network management system consisting of hardware appliances and appropriate software, at both the data center and the branch office, gives you this capability.

# Manage the Performance of Your Network & Applications




## Boost user satisfaction and cut user complaints

Accelerate, shape and cache application traffic in a single solution. Ensure your most important applications perform without having to buy more capacity.

Four demo videos available

See how Exinda can put you in control of your network and traffic

Learn how to solve network issues without throwing bandwidth at the problem

**Get Your Exinda Demos**

## Keep your network and apps running smoothly

Managing a network and the applications that run on it is a demanding job. To keep things running smoothly and provide the level of service that users and the organization expect, network managers need an approach and tools that can help them meet those expectations. This book looks at the challenges that network managers face, some of the tactics that managers use to meet those challenges, and some of the reasons why those tactics often don't produce the desired result.

## Inside...

- Understand networks and applications
- Stay ahead of evolving technology
- Address stakeholder concerns
- Be proactive about performance
- Diagnose and solve problems
- Adopt an integrated approach to network and application management



**Allen G. Taylor** is the author of more than 40 books, including the best-selling *SQL For Dummies 9th Edition* and *SQL-All-In-One For Dummies 3rd Edition*. He tweets as @SQLwriter and lives in Oregon City, Oregon. You can contact Allen at www.allengtaylor.com.



**ISBN: 978-1-119-62410-3**
**Not For Resale**

# WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.