Compliments of riverbed

2nd Riverbed Special Edition

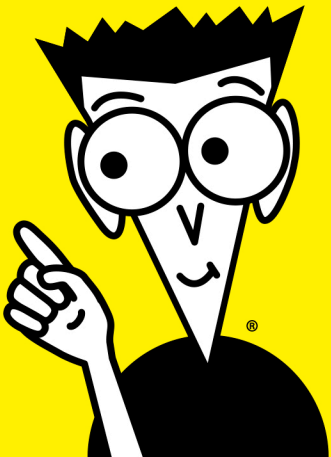
Network Monitoring & Troubleshooting

FOR DUMMIES®

A Wiley Brand

Learn to:

- The best practices for network monitoring and troubleshooting
- The top benefits and what ROI to expect
- The must haves for superior monitoring and troubleshooting



Mike Talley

Riverbed Performance Management

Your infrastructure and network exist for one reason — to deliver the applications that matter to your business. You need to understand dependencies between your applications and network, be alerted to issues before business is impacted, and accelerate troubleshooting. With an integrated approach, you can understand the critical impact the network has on application performance.

At Riverbed, our unique combination of End-User Experience Monitoring, Transaction Tracing & Component Monitoring, and Network & Infrastructure Management maximizes the performance, availability, and productivity of critical application for:

- **End-to end visibility:** Manage the complete performance picture. Leverage cloud, mobile, and virtual environments without compromising visibility and intelligence.
- **End-user aware:** Deliver quality end-user experience. Understand end-user experience and productivity, shifting focus from infrastructure to applications and users.
- **Analytics:** Increase IT effectiveness and productivity. Automated expert analysis to empower your IT teams, as well as increase application availability and user productivity.
- **Streamlined troubleshooting:** Dramatically reduce downtime. Navigate from business-level views to performance metrics to the root-cause of performance problems.
- **Intelligence:** Eliminate blind spots and plan for change. Understand holistic views of your users, their application ecosystems, and the infrastructure it relies on.

Riverbed Performance Management: Because insight is better than hindsight!

For more information about what Riverbed Performance Management can do for you, visit www.riverbed.com/npm.

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

Network Monitoring & Troubleshooting

FOR DUMMIES®

A Wiley Brand

2nd Riverbed Special Edition

by Mike Talley

FOR DUMMIES®

A Wiley Brand

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

Network Monitoring & Troubleshooting For Dummies®, 2nd Riverbed Special Edition

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

Copyright © 2014 by John Wiley & Sons, Inc., Hoboken, New Jersey

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the Publisher. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at www.wiley.com/go/permissions.

Trademarks: Wiley, the Wiley logo, For Dummies, the Dummies Man logo, A Reference for the Rest of Us!, The Dummies Way, Dummies.com, Making Everything Easier, and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates in the United States and other countries, and may not be used without written permission. Riverbed and the Riverbed logo are registered trademarks of Riverbed. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc., is not associated with any product or vendor mentioned in this book.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

For general information on our other products and services, or how to create a custom For Dummies book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the For Dummies brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN: 978-1-118-87250-5

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Acquisitions, Editorial, and Vertical Websites

Project Editor: Carrie A. Burchfield

Editorial Manager: Rev Mengle

Business Development Representative: Karen Hattan

Custom Publishing Project Specialist: Michael Sullivan

Special Help: Rebecca Salie, Heidi Gabrielson, Anne Merkert, Liz Padula

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

Introduction

The purpose of this book is to introduce you to common network performance management (NPM) issues and give you a new way of looking at solving them. This perspective allows you to see your network from your users' point of view, namely, the services and applications they use and their experience with them. Of course, you can still get down to the other flow and packet levels, but macro-level visibility is a key differentiator in your ability to monitor and troubleshoot network performance efficiently.

About This Book

In this book, you find an overview of the challenges of maintaining a diverse network and a new way to think about how you monitor your network, troubleshoot issues, identify security threats, and plan for changes to your network and your IT infrastructure. You also discover how to select a network performance management solution that allows you to get to resolutions quicker and have better visibility and information about your network and your applications when you need to upgrade hardware, consolidate branch office services into the datacenter, virtualize application servers, or move some functions to the cloud.

Because this book is a *For Dummies* book, the info comes to you in an easy-to-read, easy-to-find manner, and you can skip around to find what you're most interested in and read that first.

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

If you're on the front lines in IT and are constantly fighting network performance problems, you find useful information in this book to help you think more clearly about how to solve those problems. This book also gives you the ammunition to successfully lobby your boss for better tools, and if you're in management, and particularly if you have a "C" in your title, you'll gain some insight into the challenges your IT team faces with respect to one of the most important pieces of technology that keeps your business rolling — your network.

We need to make one last point: We've decided to use the terms *visibility, monitoring,* and *troubleshooting,* but you sometimes see this set of functions called *application-aware network performance management* (AANPM).

Icons Used in This Book

You find a few icons used in this book — they alert you to useful information and things to pay special attention to. They are as follows:

These tips may save you time or provide some additional information to you about a particular topic.

The remember icon gives you little pieces of information to jog your memory or keep in mind.

When you see this icon, pay special attention so you know where you need to take caution.

You can skip this info, but you techies out there just may love it!

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

Chapter 1

Say Hello to Your Network

In This Chapter

- Realizing the challenges of managing your IT infrastructure
- Fighting outages and performance fires
- Thinking about your approach to solving problems

Take a minute to step back and ponder what crucial service you, as the IT network guy or gal, provide to your company. Your role is huge — you're responsible for the lifeblood of the company — the network.

Managing a network comes with its very own challenges. This chapter discusses those challenges while the next chapter, Chapter 2, covers ways to meet these challenges.

Networking in the Real World

The network — and the applications and services running on it — represents the means by which you get work done. E-mail, SharePoint, VoIP, CRM, ERP, SAP, Salesforce.com, and every imaginable custom or off-the-shelf software solution runs on a network. Sure, people still use their phones to communicate, but

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

today even that doesn't work if the network is slow or — gasp! — out of commission. You know your company can't function without the network, but keeping it running in top-notch form is easier said than done.

Seriously, how do you manage it all?

Do you start your morning reading through network availability, outage, and threshold reports? These may give you a vague idea of your network hotspots that need to be addressed today, but what about those nagging questions you have in the back of your head? You know — those things that you think about and then wonder if you'll ever have the time to find the real answer. Like, why is the branch office in Kansas City, where payroll is processed, always showing up on problem reports at the end of the month? Why don't the users in Seattle ever use the unified communications application that was supposed to reduce conferencing costs? And what in the world are those guys in Dubai doing with the process modeling servers?

Face it; you'll never have the time to answer those questions unless you have a monitoring and troubleshooting solution that can effortlessly gather data for you. From traffic dashboard-level monitoring to packet capture and protocol analysis, this type of system can give you the user's view of network availability and performance, and help you get the answers you need. With those answers you can solve current problems and confidently plan upcoming network and application upgrades.

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

To complicate those expectations and responsibilities, you have some major challenges to deal with. More direct-to-Internet or hybrid network scenarios have emerged, and to top it off, parts of applications or entire applications themselves now reside across the public Internet in cloud infrastructures. Sensitive and thin unified communications and real-time virtual computing traffic are required to run over those same network paths, which require real-time quality of service (QoS) monitoring — yet another component to manage and maintain. Lastly, with end-users accessing business critical applications on a more diverse set of mobile devices every year, the network can never be taken for granted.

But that's exactly what people do. Just like they expect to be able to plug something into an electrical outlet and have it work, the network and the services on the network are always expected to just work and be fast, too.

Having It Out with Outages and Performance Incidents

You know the scenario: The phone rings . . . the person on the other end says the network is slow again. Suddenly the e-mails and calls start coming in with multiple users having the same problem. The network is fine — you know it is — but what's causing the problem? The next few minutes are your *mean time to innocence* (MTTI) — or how long you have to prove that it's not the network causing the application degradation. But this doesn't actually help solve the problem with the *you-name-it* critical service. Taking a defensive posture doesn't help answer the question about

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

why customer orders can't be placed or filled, why the manufacturing floor is stalled for lack of components because the just-in-time inventory system isn't working, or why the emergency room doctor can't get the test results for a critical patient.

What if you could move beyond the blame game, the finger-pointing, and the defensive line-up, and start putting together a system that reduces average downtime incidents by a third and decreases the duration of incidents by 65 percent? With a network monitoring and troubleshooting solution like Riverbed Performance Management, you can identify and even solve problems before they start impacting your users.

Problem? What problem?

If your company thinks that Simple Network Management Protocol (SNMP) solutions that tell you if the status of devices on the network are green or red, or if sifting through gigabytes of packet data provides sufficient information to troubleshoot your network, that's probably why troubleshooting is still so difficult! At best, you feel like a competent, experienced firefighter who can be the hero of the day and get people working again, but you never have the time to set up more proactive and strategic systems because you're always out fighting the fires.

At worst, you feel like a clumsy circus clown trying to juggle too many things at once and always dropping the ball. Although it may sometimes be rewarding to work like this, it's not even close to being an ideal situation over the long term.

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

Imagine that instead of learning about performance issues and outages from the help desk, you have powerful behavioral analytics working on your behalf to identify issues early so you can address them before their impact becomes noticeable. Just because your network is complex doesn't mean your monitoring and troubleshooting tools should be, too. For more information about monitoring and troubleshooting, see Chapter 2.

Reducing MTTR

The mean time to resolution (MTTR) — the time it takes to diagnose and resolve a problem after it's been identified — can have a significant impact on your budget. If it takes you days or even weeks to identify and resolve even minor performance issues, maybe it's time to give your operations team a shot in the arm — you know, give 'em the tools that allow them to find the problem faster and quickly get to a resolution.

Products like Riverbed Cascade, together with the leading protocol analyzer Wireshark, give you the ability to solve tough network-related issues in half the time. A productivity boost of that magnitude can absolutely affect your bottom line.

In addition to cutting MTTR by half, you'll also see the number of help desk calls reduced by more than half. Your support guys are going to be able to solve problems faster and take fewer calls because you're able to monitor and troubleshoot the ultimate measure of application performance: the end-user's experience.

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

So, if you have to sell this type of solution to upper management and argue for new capital expenditure, you can start building your case right now. You'll find more information on the benefits and ROI of network monitoring and troubleshooting solutions in Chapter 5 and a list of capabilities to look for in a visibility solution in the appendix of this book.

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

Chapter 2

Visibility Is Gold

In This Chapter

- Seeing the tradeoffs between the broad view and the deep view
- Discovering what's running on your network
- Gaining visibility to improve monitoring and troubleshooting

The IT industry is filled with buzzwords. *Cloud computing. Synergy. Paradigm shift.* The meaning of these terms and even the merits of using them can be debated, but one thing is for sure: If you think the term *visibility* is a buzzword, think again.

In the world of application-aware network performance management (NPM), providing visibility anywhere is a key aspect of any solution that you may be using or evaluating. Visibility anywhere can mean visibility into

- Remote sites, WAN, and deep into data centers
- Across physical, virtual, optimized environments and cloud
- From end-user devices to servers

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

A system that offers good visibility is all about getting you to the right level of information needed to solve the problem quickly. This chapter is about how the visibility anywhere can help you meet the challenges set out in Chapter 1. Flip to Chapter 1 for more information on those challenges.

You don't know Jack!

The biggest problem most companies have is that they don't know what they have. If you have a solution that can provide multiple, unified views of your network, application traffic, and actual end-user experience and does its own discovery, dependency mapping, and behavioral analysis, you have a pretty good solution. Congratulations!

If you don't, you have a difficult time reconstructing the crime scene, so to speak, when something goes wrong. Put on your best Sherlock Holmes hat, put a curved pipe to your lips, and answer these questions:

- What's on your network?
- Who's using it?
- How are they using it?
- Where are they accessing it?
- When did this all take place?

If you have difficulty answering these simple questions, you're in desperate need of a solution that gives you these answers.

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

Going Deep or Going Broad

In any network, the *packet* is the ultimate source of the truth, so a network management solution must provide the ability to go deep to capture and analyze those packets. But when you think about it, *flow* is also critical to understanding how the network behaves and provides that broad, end-to-end visibility.

To recap, two important mechanisms help gain visibility:

- **Monitoring flow data** is a cost-effective and scalable way of collecting performance metrics from routers, switches, and other network devices. Flow data provides end-to-end visibility across the network without having to install probes everywhere, but it lacks lower-level details. This type of data is great for trending, high-level analysis, and some troubleshooting.

If you select a solution that de-duplicates and correlates flow data from multiple locations, you won't be overwhelmed with all this data capture. This reduction in the amount of data has a direct benefit on storage costs and analysis performance.

- **Examining packet data** is required for detailed visibility into application performance. Only the packets contain the complete conversations that took place on the network. There may be some sections on your network (like in the data center) where using continuous packet capture is essential for retrospective or back-in-time analysis. Packet data is also necessary to view web-page response time for a true end-user perspective.

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

When choosing an NPM solution, some companies pick one that goes deep or goes broad. This choice can be a big mistake because it only gives you part of the bigger picture. A solution that only goes deep doesn't let you see the forest for the trees, and a broad solution doesn't let you know that the forest is full of poison ivy.

The ultimate solution is one that integrates packet data *and* flow data into a single record. This integration enables broad visibility with minimal instrumentation as well as the seamless transition between flow-based information and packet-level information. This combination is important because it reduces the time it takes to identify, diagnose, and resolve complex performance issues.

In the end, an integrated architecture provides you with greater visibility and management, and as an added bonus, typically demands a lower upfront and operating cost than separate solutions that address only packet or flow data.

Digging for Gold

Flow data provides another type of visibility that's often overlooked. It's the ability to discover application dependencies — what applications are running on the network and how they relate to each other and the network hardware.

When it comes time to consolidate data centers or simply move a server, this information is also extremely useful. The visibility into dependencies allows you to make more reliable project plans and

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

reduces the inherent risks involved in changing the infrastructure.

This information is also essential to building robust application or service-level dashboards. How can you monitor an application if you don't know all the working parts — the users, web servers, application servers, load balancers, DNS and authentication servers, and databases — involved in delivering a single application to users?

This critical step may be skipped by some companies, but you absolutely have to know what you have on your network in order to monitor and troubleshoot it. How can someone trust a network management system that can't even identify what it's going to manage?

Getting from dashboards to packets — fast

Everyone likes to use a dashboard to see what's happening, but people also need to drill into problems fast. Optimally, this functionality would be integrated into a solution that allows you a high-level view of your network and enables you to progressively drill down to deeper layers of detail in a flexible and easy-to-use manner.

Consider the analogy of a telephoto lens on a top-of-the-line camera. You can look through it and see a panoramic view, but with a turn of the lens, you can zoom in on a single object.

Apply this analogy to network monitoring and troubleshooting, and you've just gone from the dashboard view, to flow-level details, to the packet view, almost instantaneously.

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

Moving from problem to resolution

Uptime is critical when it comes to networks, so the faster you can uncover the source of a problem and get to the resolution, the happier you, your users, and your boss are going to be.

With a solution that works like a telephoto lens, you can cut the time it takes from an intelligent alert to the root cause without getting caught thrashing through the weeds (or packets, as the case may be). It's much faster and more efficient to start broad and then focus in on the details.

Reaping the Visibility Bounty

When you have more visibility into your network's operations, your common network management tasks become easier. Who doesn't like easier?!

Monitoring and troubleshooting a network without adequate visibility can be tedious at best. Having a single, consolidated view of the network that seamlessly combines the best of flow and packet data with end-user experience monitoring not only makes monitoring easier but also improves the efficiency at which you can troubleshoot problems.

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

Chapter 3

Network Analysis Paradise

In This Chapter

- Monitoring network health through dashboards
- Putting analytics to work for you
- Discovering and mapping dependencies
- Being mindful of security and compliance issues
- Getting visibility even with optimization
- Reducing your MTTPP

A good network performance management (NPM) solution isn't only about troubleshooting problems. A good solution allows you to analyze and measure performance, generate alerts without having to set thresholds, and get an overview of what users are experiencing at any time.

Monitoring Health via Service Dashboards

Service dashboards provide a quick view into the end-to-end health of an application or service. With dashboards, executives can get a quick status check of what's happening with critical business applications

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

across the entire network, and network folks will find it's a logical starting point for accelerated analysis and troubleshooting.

Would you rather go to your primary care doctor or the ER?

When people have a critical health issue (like a heart attack) that sends them to the emergency room, doctors, nurses, and specialists mobilize to stabilize them.

Other people will go in for regular checkups to their general practitioner, who may run a bunch of tests such as a blood panel, EKG, x-ray, and the like, to check on their overall health. If the doctor discovers a problem, like high blood pressure, he'll treat it so it doesn't lead to a bigger problem.

The first approach — the ER — is stressful, scary, and expensive. The other — continuous, preventative care — is more measured and controlled, and usually allows you to avoid any stressful visits to the ER.

Extend this example to your network. What approach are you taking now? Do you operate like an emergency room trying to stabilize your critical patient — the network — or like a general practitioner who spends a little time each day dealing with the small issues before they become catastrophic?

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

Putting Analytics to Work for You

Your dashboard status indicators — those red, yellow, and green lights — may look simple, but they should have advanced analytics behind them to give you a true sense of how things are running and provide the initial details — the who, what, where, and how — of the developing issue.

Advanced behavioral analytics examine what's normal for your network and alert you to changes. It's a learning process. Network and application metrics — such as response time, throughput, and connection rates — are measured and tracked over time to develop a baseline of what's typical. Building and updating the measurements that make up this baseline allow an NPM solution with analytics to know the difference between typical network activity and a sudden change in activity that potentially indicates a problem.

The great thing about Riverbed Performance Management analytics is that they're completely automatic and dynamic. You don't need to set any hard-coded thresholds that are destined to become obsolete next week or are impossible to determine in today's complex networks.

False positive alerts can really drag you down, mostly because you start losing trust in the system that's sending them. It's like the spam in your junk e-mail folder. Occasionally there's something of value in there, but emptying it without even looking at its contents is usually safe. Make sure the vendor you select has perfected analytics.

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

End-User Experience Monitoring

What are end-users actually experiencing as they interact with the application? Whether you're using web or thick client applications, and regardless if users are local, around the world, or mobile, you must be able to monitor and troubleshoot the ultimate measure of application performance: the end-user's experience.

Riverbed AppResponse Xpert monitors and analyzes end-user experience to give you visibility into:

- Application usage
- Response times
- Transaction analytics
- Real-time usage and historical trends
- Network and server delays

With these types of end-user experience metrics, you can detect problems earlier and troubleshoot application performance issues faster.

Automated Discovery and Dependency Mapping

A solution that automatically and passively identifies all the components involved in delivering an application service — the users, servers (application, web, DNS, authentication), load balancers, databases, and so on — and maps the way applications interact on your network pays handsomely in the end. It pulls everything together in a way that gives you visibility into

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

- How each piece fits into the bigger picture
- Which assets are really critical
- The interdependencies among all the pieces

Understanding this information is essential to monitoring service performance end to end and for building accurate application definitions for service dashboards. It's also an important first step in planning for major IT projects, such as data-center consolidation, virtualization, cloud initiatives, and more, so when it comes time to make a change, you don't need to spend hours, days, or even weeks getting the project plan in place.

The great thing about Riverbed Cascade's automated discovery is that it doesn't require scans, agents, or credentials. It passively monitors historical flow conversations to determine everything that application has recently "spoken" with. All you need to get started is the name, IP address, URL, or CIDR range of the server in question. Then you can just sit back and wait for the inventory to be done.

For any project that requires a change in the infrastructure, such as server consolidation, virtualization, and moving to the cloud, you need to know what applications and assets are going to be affected by the proposed change. If you don't know for sure, you could miss something and put the project at risk.

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

Security and Compliance

Some solutions use network behavior analysis (NBA) to detect and alert you to potential security threats. These threats may come from inside the network by trusted employees or partners such as network misuse, policy violations and data leakage; it may be an emerging (a.k.a. zero-day) threat that isn't yet recognized by blacklists or signature sets; or it could be a botnet or denial of service (DOS) attack.

Traditional perimeter-based security solutions can't defend against internally instigated attacks and are typically too expensive to implement on highly-meshed networks. They can also introduce performance bottlenecks and miss many of the threats they're intended to stop.

Leveraging analytics for network security

Your network can be attacked in an infinite number of ways that avoid your traditional perimeter defenses of firewall, virus scanners, or intrusion detection systems. But, the network itself can be a primary source of information about an attack. Are you safe from the following scenarios? Can your current solution identify the following:

- Surges in bandwidth utilization that may indicate a DOS attack?
- The addition of new servers or server ports on the network that could indicate an outside agent is controlling them?
- A significant increase in connections that typically result from the spread of a virus or worm?

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

These scenarios, and more, represent security problems and you should investigate right away.

Solutions that alert you to potential security problems use data about what's occurring on the network to signal that further analysis is recommended. They can also provide you with the scope of the security breach and may also automatically take action to prevent further damage. Continuously capturing and storing packet data (think DVR for your network) gives you the chance to go back in time to review evidence if and when you need it.

Compliance

Perhaps *you* don't worry much about compliance, but you know that *someone* has to. Keeping personally identifiable information (PII) private is important to many businesses. The right network monitoring and troubleshooting solution helps you meet regulatory, and sometimes business-mandated, compliance issues by

- Establishing and enforcing network usage and access policies (for example, making sure no one but a handful of finance managers have access to customer credit card information)
- Identifying all the components that must be secured or monitored in order to meet compliance standards

These two things help you identify where security may be weak or where you may be vulnerable to infiltration.

Having a visual diagram of actual application dependencies is an ideal way of seeing compliance violations. Seeing, for example, an

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

instance where your credit card processing system is accessing an unsecured development server instead of the production server is a great verification that you can't know it all, and you need a solution that automatically discovers compliance issues for you.

Look for a solution that offers the ability to do forensics analysis on any number of network events, in real time or in the past. Also, having a solution that helps you quickly research and piece together a user's activities is worth every penny.

WAN Optimization Analysis

Optimized or not, wide area network (WAN) performance is a constant headache to maintain decent performance for remote employees. Whether it's latency, congestion, low bandwidth, chatty applications, or contention with other applications, many network admins rightly turn to optimization to solve these issues. But in doing so, they can unintentionally lose the ability to monitor and troubleshoot problems over those connections.

You're probably already optimizing WAN performance, and, if you aren't, it's likely to be on your roadmap, so choosing a solution that still gives you visibility into how your network is functioning is a win-win situation. Look for a solution that eliminates this loss of visibility due to optimization — in particular, one that supports QoS reporting and can reconstruct response times across optimized links, as well as tell you how your organization benefits from optimization.

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

Did you know that Riverbed Steelhead WAN optimization appliances can also function as remote application monitoring and troubleshooting devices for Riverbed Cascade? Cascade takes deep packet inspection instrumentation of applications and continuous packet capture data from Steelhead, for increased application visibility and troubleshooting. Without increasing your branch office footprint, Cascade delivers a deep enterprise wide view of application utilization and insight among all locations in your enterprise.

Getting a clearer picture with Riverbed Cascade

Cascade offers a range of built-in reports for monitoring Riverbed Steelhead appliances in WAN optimized environments, including

- Overall WAN Analysis
- Optimization Benefit Analysis
- Optimization Candidate Analysis
- Site Capacity Analysis
- WAN Site and Intersite Optimization
- Quality of Service (QoS)

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

Last but Never Least, Reporting

What is your *mean time to a pretty picture* (MTTPP) that you can show your boss and your boss's boss? Maybe you're about to walk into that budget meeting and you need to have your facts and arguments documented and presentable. Or maybe you're getting a call from headquarters about a new initiative that needs some data, and fast, or else it's going to end up on the cutting floor. With a solution that offers advanced reporting capabilities over and above what the run-of-the-mill solutions offer, you can deliver this information.

Add to these capabilities the ability to build custom, template-based reports, and your MTTPP just got a lot shorter.

Look for built-in reports that target different audiences, such as executive and technical, and reports that can jump-start your decision making by providing instant analysis of your network. Also, make sure you have the ability to create on-demand reports that you can instantly share with colleagues to aid in troubleshooting and that document your successful conclusion to a troublesome issue.

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

Chapter 4

Picking the Right Solution

In This Chapter

- Understanding packet capture and analysis
- Leveraging what you already have
- Using the best packet protocol analyzer
- Perusing the ups and downs of virtualization

In this chapter, you take a look at the common solutions to choose from when trying to resolve your networking, monitoring, and troubleshooting problems.

Defining the Source of Network Truth

When you need to troubleshoot really complex or intermittent network problems, you need packet-level data. Like a football commentator, *packets* give you a play-by-play description of what's happening on the network in real time. You can capture the packets you need for analysis in two ways:

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

- Temporarily connect to whatever link you suspect the problem is occurring on and start recording ("on demand")
- Permanently instrument key spots on your network with an appliance that continuously captures and stores large amounts of data for several days at a time. (How long you can store the data depends on how much disk the appliance has, how big the link is, and how much data is flowing over it.)

The limitation with on-demand packet capture is that, if the problem is intermittent, by the time you hook up your laptop and start recording, you've probably missed the problem. The other problem is that if the problem occurs in a remote office with no IT staff, it could take hours before you can get to the site.

Alternatively, packet capture appliances continuously record all the packets so they're always available for back-in-time analysis when you need them. It doesn't matter if the problem is intermittent or the branch office is half-way around the world.

When deploying continuous capture appliances, make sure that the packet analysis is done directly on the remote appliances so only the specific packets of interest are sent over the network to Wireshark for decoding. You don't want to be sending gigabits of packet trace files across the network, which can potentially create or add to performance problems.

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

When's a terabyte of storage not a terabyte of storage?

When talking about continuous packet capture appliances, storage is fairly expensive. You want to balance the amount of disk storage (for example, the length of time you can store information) with the costs to deploy. Make sure the solution you choose can maximize storage by providing the following capabilities:

- **Pre-capture filters:** Record only the traffic you're concerned with (for example, just VoIP traffic), saving significant storage capacity.
- **Multiple capture jobs:** Enable IT staff to dedicate different amounts of storage to each job to flexibly extend storage time for critical applications. For example, one job records only ERP data and is allotted 3TB of storage; a second job records all Internet traffic on the remaining 1TB.
- **Selective recording:** Makes recording just a portion of the packet possible (for example, just the header, or the head plus the first "x" bits of the payload). It extends the amount of data that can be recorded and the length of time it's available.

Leveraging What You Already Have

Take a moment to consider how your new network monitoring and troubleshooting solution fits with what

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

you already have. Can you leverage third-party networking equipment as instrumentation points? Can you send performance alerts to your MOM (manager of managers) for single pane-of-glass viewing? Can you integrate with Active Directory to resolve IP addresses to actual user names? Don't look at your network performance management solution in a vacuum.

Working with the Best: Wireshark

Averaging half a million downloads per month, Wireshark is the de facto standard for packet protocol analyzers. Chances are your network engineers are already using Wireshark to decode trace files. Why make your engineers switch to another, inferior product or learn another interface? Make sure the monitoring solution you choose integrates with the best technology available.

Riverbed Cascade seamlessly integrates with Wireshark. In fact, it has the tightest integration on the market.

Getting a clearer picture with Cascade

When using Cascade, you can analyze network data whether it's a live capture or you're doing some historical research from a saved trace file. To do this, you click Send to Wireshark. You can then view the packets from the filtered data that you were just analyzing in Cascade.

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

The Virtualization Black Hole

Virtualization can cause a visibility black hole for network managers. Application traffic goes into the virtualized environment, but then you lose track of it and never see it come out — same problem with load balancers. Understanding how services are interacting among virtual servers within a physical device is key to optimizing and troubleshooting application behavior across the *entire* network. Make sure the solution you choose provides visibility into virtualized, WAN optimized and load-balanced environments.

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

Chapter 5

Ten Benefits of Implementing a Network Monitoring and Troubleshooting Solution

In This Chapter

- Learning the top benefits of a network monitoring and troubleshooting solution
- Evaluating your return on investment

In this chapter, you discover the ten benefits of a good application-aware network performance management (AANPM) solution. These may help you estimate your return on investment (ROI), because every time your network is down, your organization may be unable to manufacture goods or provide services to your customers or employees. Either way, this has the potential to translate into lost revenue. The right solution helps preserve revenue by protecting productivity and the user experience, regardless of the industry.

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

Improved Availability, Responsiveness, and Predictability

With a best-of-breed network monitoring and troubleshooting solution, you should expect to see

- Improvements in the general availability of applications and services on a network that's actively managed
- Better and more predictable response times, on average, because you have the knowledge needed to tune your network to better handle applications and services
- Improvements in application performance because you have a better understanding of whether quality of service settings are meeting expectations

Accelerated Problem Resolution

Whether it's a problem with a mission-critical application or a stubborn network performance issue affecting a branch office's productivity, the quicker you resolve it, the happier your users — and your CEO — are going to be. Accelerating mean time to innocence (MTTI) and mean time to resolution (MTTR) makes you look like a hero to your IT colleagues, management, and users. For more information on the reduction of MTTR, see Chapter 1.

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

Minimization of Downtime

When the network is slow or out of commission, business doesn't get done — period. Products can't be sold, customers grow unhappy, employees are unproductive — and the list goes on. Minimizing downtime has a direct impact on the bottom line.

According to Charles Naut, author of the book Risk-Free Technology, the cost of downtime for the average enterprise is 3.6 percent of annual gross revenue. It's not a hard cost, per se, but the cost of lost labor. The closer you can get your network to utility-grade, meaning the network is as ever-present and available as delivery of electricity from the utility company, the more productive your users are going to be.

Reduced Help Desk Calls

A solution that actively monitors and alerts on meaningful changes in performance provides early warning so you can head off potential problems before they become bigger issues. The conundrum is, if you fix a problem before anyone actually notices it and calls the help desk to complain, was it actually ever really a problem?

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

More Accurate Planning

The better the picture you have of what's currently happening on your network, the better you're going to be able to plan for future needs and expansions of the network. Planning for a new service roll-out, bandwidth growth, and data-center consolidation projects are much easier, and far less risky.

Reduced Costs

The right solution can help you reduce both operational and capital expenditures. Don't throw more bandwidth at a slow WAN link until you know whether congestion is caused by business-critical applications or unauthorized recreational traffic.

Leverage existing network equipment for remote visibility so you don't have to shell out unnecessary funds for traditional hardware-based probes and to avoid the expense of flying IT staff to remote branch offices to perform emergency troubleshooting.

Simplified Management

You may be looking at a network monitoring and troubleshooting solution because you're struggling to manage your network. This issue is common in today's businesses that have global networks that have grown organically and sometimes sporadically as telecommunications and technology have improved around the world. Getting a global view of your global network is key to understanding, managing, and improving your investments.

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

Tool Consolidation

If your global network has grown organically, the tools used to monitor your network have probably followed in those same tracks. A good network monitoring and troubleshooting solution should simplify the number of tools you use to monitor and troubleshoot your network, and it should reduce the number of dependencies you have on getting the right data from your network.

Improved IT Productivity

Easier monitoring and quicker troubleshooting allow your IT staff to be more productive and to focus on higher-level projects versus troubleshooting day-to-day operations. With an integrated, simplified set of tools, IT can plan, monitor, and resolve issues faster and with greater competence than before — which increases your department's reputation and your company's bottom line.

Improved Collaboration

Powerful service dashboards allow everyone to be on the same page. From the CIO and IT management to application managers to the security and network teams, everyone has access to the same data and can see a unified picture of the network and the applications and services on the network.

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

Measuring the ROI of Riverbed Cascade

The IDC whitepaper "Realizing the Business Value & ROI of Application-Aware Network Performance Management," published in July of 2012, summarizes the ROI of the Cascade line of products:

- On average, Cascade customers achieve a three-year ROI of 519 percent and a payback period of 5.1 months.
- Cascade customers experience 65 percent fewer downtime incidents per month, restoring 73 hours of productive time to each user annually.
- By automating network management operations, Cascade reduced operations time by 12,000 hours or $5,497 per 100 users.
- The duration of the average help desk call was cut by 92 percent.
- Customers saved an average of $12,047 per 100 users of annual IT expenses with improved server utilization, bandwidth efficiencies and reduced number of IT staff to solve problems.

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

Appendix

Evaluating Network Monitoring and Troubleshooting Solutions

In This Appendix

- Evaluating key aspects of network monitoring and troubleshooting solutions
- Thinking about your current and future investments in solutions

When evaluating your investment in a network monitoring and troubleshooting solution, many criteria exist that you can use as your guide. Each section in this appendix provides additional information and a demonstration that depicts how the solution must meet these specifications. This appendix should help you objectively compare different solutions to figure out which one best meets your needs.

Application Monitoring

Application monitoring is critical to figuring out how users are experiencing network performance and a

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

solution that's application-aware gives you a much better snapshot of that experience. Use Table A-1 to compare how your application-aware network performance monitoring (AANPM) solution ranks.

Table A-1 Application Monitoring Checklist

Application Monitoring	*Yes*	*Partially*	*No*
Application delivery path knowledge versus interface by interface reporting			
Accurately identify application type and its performance across any environment — WAN optimized, virtual, remote locations, even those with ADCs			
Application Performance Metrics: Actual end-user experience, response time, network round-trip time, server delay, client delay			
TCP health metrics: Connection rates, throughput and duration, application throughput, resets/ retransmits			
Quality of Service (QoS) levels by application type and class			
VoIP quality			

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

Network Monitoring

Network monitoring is the bread and butter of NPM, but all solutions aren't created equal — especially when you add in WAN optimization and virtualization. How does your NPM solution stack up? Use Table A-2 to compare your solution to others.

Table A-2 Network Monitoring Checklist

Network Monitoring	*Yes*	*Partially*	*No*
Network Performance Metrics: Packet rate, bandwidth, interface/link utilization, conversations, top-talkers, protocol errors			
QoS reporting and service level performance			
Switch port discovery			
QoS visibility for WAN-optimized environments			
Support virtualized environments (Virtual LANs, virtualized servers)			
SNMP reporting on utilization and errors related to network performance			
Identification of least used assets and bottom talkers			

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

Alerting and Behavioral Analytics

Accelerated fault detection isn't just about sending alerts when a threshold is crossed; it has more to do with behavior analytics and intelligent alerting when something suspicious occurs on the network. Use the checklist in Table A-3 to see how your solution stacks up.

Table A-3 Alerting and Behavioral Analytics Checklist

Alerting and Behavioral Analytics	*Yes*	*Partially*	*No*
Behavioral analytics: Non-threshold-based anomaly detection and alerts			
Support for user-defined usage, security, and performance policies			
Integration with security/vulnerability management solutions			
Threshold-based alarms			
Forwarding of alerts to third-party systems			
Automatic, expert analysis to help identify the root cause when events are detected			

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

Usability

Is usability really that important if users can be trained how to use a piece of software? Absolutely! If users are able to more intuitively use the software, they're more likely to be successful. From the architecture of the solution down to the right type of information displayed at the right time, a product with greater usability and familiarity means higher productivity. Use Table A-4 to see how your solution ranks.

Table A-4 Usability Checklist

Usability	*Yes*	*Partially*	*No*
Service-level dashboards			
Automated discovery and dependency mapping			
On-demand and scheduled reporting on any gathered metric			
User identity integration (associate a username with an IP address)			
Support grouping of IPs/subnets to provide independent views (for example, by location or function)			
Support seamless pivot and drill down to packets			

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

NetFlow Support

Support for a variety of NetFlow types shouldn't be taken for granted with any NPM solution, so check to make sure the solution you're considering provides what you need now and potentially down the road long term.

It's also wise to evaluate whether your solution provides a way to reduce the amount of data stored locally, remotely, and anyplace in between in order to keep ongoing costs under control. Use Table A-5 to determine what NetFlow support and de-duplication requirements you have and will need later.

Table A-5 NetFlow Support Checklist

NetFlow Support	*Yes*	*Partially*	*No*
Support for all flow sources: NetFlow (v 5, 7, & 9), Sampled NetFlow, IPFIX, NetStream, jFlow, cflowd, sFlow			
De-duplicate records of the same flow but from different exporters			
The ability to support millions of de-duplicated flows per minute			

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

Troubleshooting

When you're troubleshooting, use a packet analysis tool that provides the greatest flexibility. Use Table A-6 to determine whether your packet analysis tool is up to the task.

Table A-6 Troubleshooting Checklist

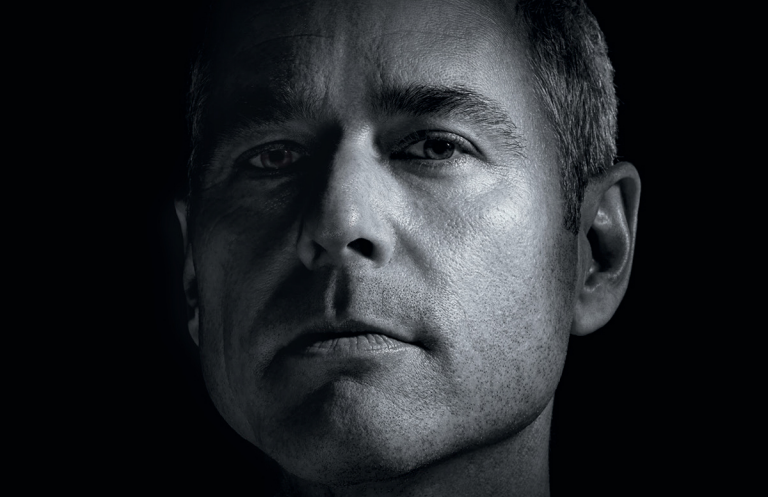
Packet Analysis	*Yes*	*Partially*	*No*
Continuous packet capture and storage			
Mix and match 1GbE and 10GbE interfaces on the same appliance			
Ability to analyze trace files directly on remote capture appliances			
Multiple concurrent capture jobs			
Pre-capture filters			
Selective recording of the packet payload			
Multi-segment analysis			
Integration with Wireshark			

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

KISS

NETWORK PERFORMANCE PROBLEMS GOODBYE BEFORE THEY SAY HELLO.



What if you had the tools to monitor every component and every application across your WAN, LAN and datacenter? Then you could troubleshoot and solve problems in hours, not days, and deploy IT resources where and when they're needed most. This "what if" can become reality with one introduction. Meet Riverbed.

WAN optimization • cloud storage delivery
cloud acceleration • application delivery
network performance management

riverbed.com/kiss

riverbed®

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.

Networks are complex. Your network performance management shouldn't be.

Today all networks are extremely complex. Monitoring and trouble-shooting performance problems with limited resources and in cost-effective and efficient manners can feel overwhelming. This book can help identify the best-of-breed network performance management solution that's right for your business.

- ***Discover the best practices — for proactive network monitoring and fast troubleshooting***
- ***Enjoy the top benefits and ROI — automatic discovery, end-to-end visibility, faster MTTR, and more***
- ***Study the helpful evaluation checklist — ensure you're getting the best solution for your needs***

Open the book and find:

- **Ways to reduce your mean time to resolution (MTTR)**
- **How to minimize downtime**
- **How to align IT and business priorities**

Go to Dummies.com®
for videos, step-by-step examples, how-to articles, or to shop!

FOR DUMMIES®
A Wiley Brand

ISBN: 978-1-118-87250-5
Not for resale

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.