

WHITE PAPER

Better IT Planning for Tight Budgets:

The Right Tools to Make
the Right Decisions

riverbed[®]

Think fast.[™]

Executive Summary

Making the best decisions possible for your IT environment is critical in these tough times. You have fewer resources to manage an increasingly complex infrastructure and problems can have a severe business impact. Network Behavior Analysis (NBA) systems can provide you with vastly improved information about your infrastructure and its usage to improve the information you have and enable better planning.

The key capabilities that NBA systems offer to improve your IT planning include:

- Discovery and dependency mapping
- Historical usage with layer 7 and port 80 visibility
- Unified data collection and retention
- Reports that pivot on any data element

Additionally, NBA systems offer:

- Cost-effective deployment and management
- Value across the entire IT organization to improve performance, availability, and security

A financial services company deployed an NBA system and within a couple of weeks was able to:

- Identify and eliminate underutilized servers for significant operational cost savings
- Reschedule backups to free up significant WAN bandwidth during peak business hours
- Identify and fix a mis-configuration that was consuming 570 GB of WAN bandwidth every week, freeing up significant capacity

Times are Tough and Making the Right Decisions is Even Tougher

In today's economy, budgets are tight and businesses are cautious. As a result, vendors are busy repositioning and repackaging their products, white papers, and advertising around saving money and increasing ROI. As an IT executive, you need to wade through buzzword marketing and vendor spin to find the tools and technologies that meet your needs.

Making IT decisions — whether about changing the infrastructure, adding new applications or services, or deploying new management tools — is difficult in the best of times.

Making IT decisions — whether about changing the infrastructure, adding new applications or services, or deploying new management tools — is difficult in the best of times. When you are facing budget cuts and uncertainty, it can be nearly impossible. All you can do is take the best information you can get and use it to make the best decisions you can for your organization. But in this economic climate, making the right IT decisions has become more important than ever to support revenue, operations, and employee productivity.

One way to improve your ability to make the right IT decisions is to improve the information you have about your infrastructure and its use. There are many tools out there that give you valuable information, but often that information is limited. Either it provides a snapshot, which does not reflect what happens over time, or you get comprehensive information that covers only a portion of the infrastructure.

While there is no technology that will give you complete information for every decision you need to make, there is one technology that provides you with vastly improved information about your infrastructure and its usage: network behavior analysis (NBA) systems.

Better Information for Better Planning

Because NBA systems offer cost-effective deployment and management, they won't require significant capital and operational expenditures to install and maintain.

NBA systems provide a new way of managing application performance and security by analyzing the interactions of users with the applications, systems, and network devices that comprise the application delivery infrastructure. They passively collect network flow data and enhance it with application and user identification, behavioral analytics, and network performance metrics. Pre-defined and customizable behavioral analytics enable users to identify performance, availability, and security issues before they disrupt business services. Complete and accurate usage and dependency data provide the key inputs for making the right optimization and change management decisions.

The key capabilities that NBA systems offer to improve your IT planning include:

- Discovery and dependency mapping
- Historical usage with layer 7 and port 80 visibility
- Unified data collection and retention
- Reports that pivot on any data element

Because NBA systems offer cost-effective deployment and management, they won't require significant capital and operational expenditures to install and maintain. Furthermore, because NBA systems provide capabilities beyond those discussed in this paper, they can be used across the entire IT organization to improve performance, availability, and security.¹

¹ White papers that detail the other capabilities that NBA systems offer — including increased performance, availability, and security — are available at www.riverbed.com/cascade

Complete, Automated Discovery and Dependency Mapping

Unlike other discovery systems that focus on the characteristics of individual systems, NBA systems use flow-based discovery to provide information on the relationships among systems across the network. NBA systems collect network flow data to provide detailed knowledge of how every application is being used, by whom, and when on a continuous basis. (See the sidebar for more information on flow.) Unlike other approaches, flow-based discovery is pervasive, continuous, and passive:

What is Flow?

Network flow records are outputs of routers and switches that contain summary information about the network conversations. Flow was originally designed as an accounting mechanism to capture data for network "chargeback." There are a number of flow protocols, one example being Riverbed Steelhead™.

The format of a flow record may vary depending on flow type and version, but the contents typically include:

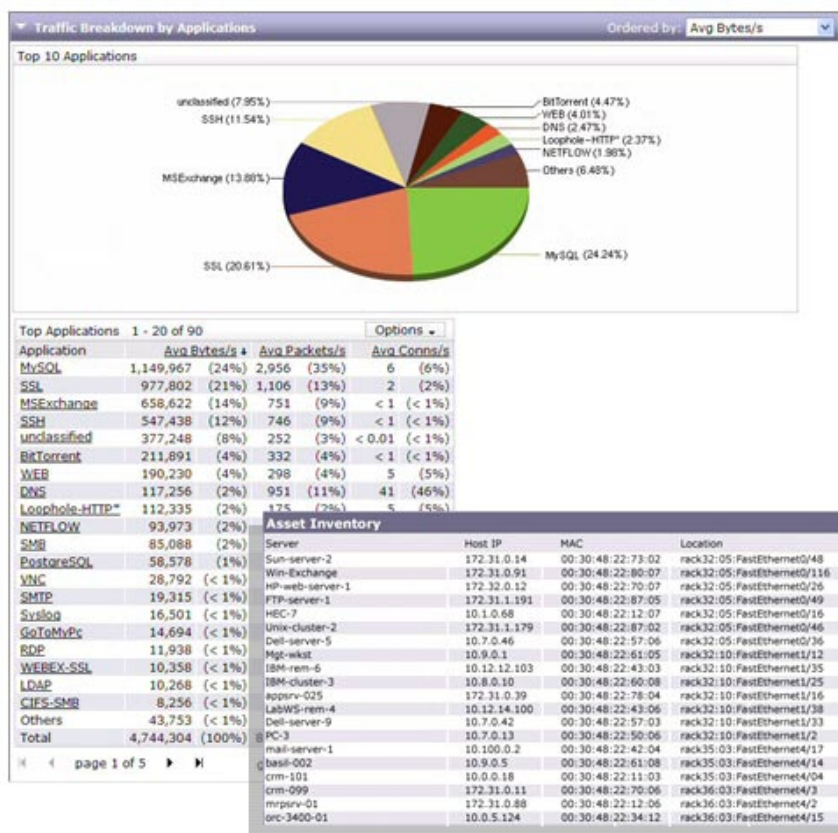
- Source and destination IP addresses
- Source and destination ports
- IP protocol
- Ingress interface label
- Timestamps for flow start and finish times
- Number of bytes and packets observed in the flow

Enabling flow data from your network infrastructure is an extremely efficient way to see network conversations.

- **Pervasive** — All devices transmitting any traffic over the network are included in the discovery, ensuring that the data collected is complete regardless of whether they are instrumented. This also means you can discover information about systems that are not internally deployed, such as SaaS or third-party applications, as well as applications you don't know are on the network.
- **Continuous** — Always-on discovery enables you to understand actual dependencies based on real-time usage across business cycles regardless of when or for how long applications run.
- **Passive** — Passive discovery uses data from existing routers and switches for fast and cost-effective deployment without affecting performance. This approach also enables data collection without credentialing problems.

Why it Matters. An understanding everything that you have on the network and how it interconnects is traditionally very difficult to obtain. Having this information enables you to make changes to the infrastructure without breaking dependencies and causing outages. It is useful for identifying unauthorized systems on the network, and for identifying underutilized servers to be consolidated or eliminated.

NBA systems enable you to automatically identify all the applications running on the network by name including details on utilization. You can also get a complete asset inventory including physical (switchport) location.



With NBA systems, it's easy to run a report to show you the dependencies of any system or group. In this case, a report is being run to show the dependencies of "Thumper."

Report Criteria

Hosts, subnets or groups: [Browse...](#)

Report by: Break out MAC-IP assignments

▶ Additional Traffic Criteria

▶ Report Format

Run now Run in background...

Time frame:

Last: Days

From:

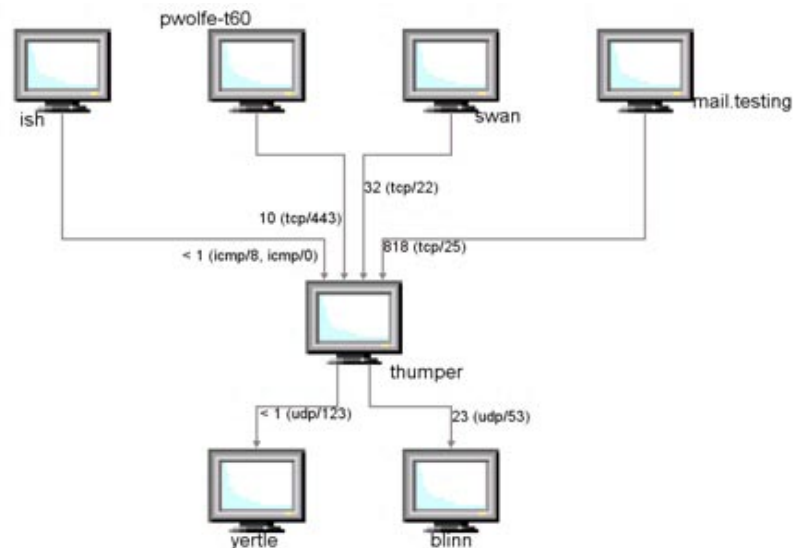
To:

Data resolution:

Host Pair and Port 1 - 7 of 7 Options ▾

Server	Server Group	Client	Client Group	Port	Avg Bytes/s *	Avg Server Delay (ms)	Client Switch Info
thumper	Boston	mail.testing	DataCenter1	tcp/25 (smtp)	818 (93%)	5	camb-core-sv01:GigabitEthernet3/24
thumper	Boston	swan	Dallas	tcp/22 (ssh)	32 (4%)	12	camb-core-sv01:GigabitEthernet3/10
blinn	DataCenter1	thumper	Boston	udp/53 (domain)	23 (3%)		camb-core-sv01:GigabitEthernet3/12
thumper	Boston	pwolfe-t60	DataCenter1	tcp/443 (https)	10 (1%)	7	camb-core-sv01:FastEthernet4/5
thumper	Boston	ish	DataCenter1	icmp/8 (echo)	< 1 (< 1%)		camb-core-sv01:GigabitEthernet3/24
thumper	Boston	ish	DataCenter1	icmp/0 (echo-reply)	< 1 (< 1%)		camb-core-sv01:GigabitEthernet3/24
yertle	DataCenter1	thumper	Boston	udp/123 (ntp)	< 1 (< 1%)		camb-core-sv01:GigabitEthernet3/12
Total					883 (100%)		

The resulting tabular report shows you the client/server pairs where Thumper is involved, port information for the server, activity for the server, and switch port location of the server.



You can also get a graphical view of dependencies which includes Thumper (the server of interest in this case), its clients, and the servers on which Thumper depends.

Historical Usage with Layer 7 and Port 80 Visibility

The broad range of network monitoring tools available today offers a number of ways to identify applications. Many systems identify applications by port/protocol combinations. This is a dated technical view; while it does provide useful information, it doesn't provide complete or accurate information in a business-centric context. And sometimes, host/port mapping simply is not enough. For example, it's easy to identify SMTP email, which uses port 25/TCP. But how do you identify Exchange Web mail, which uses port 80? If you wanted to identify all the mail traffic in the organization, using port 25 would not capture the Web-based mail. Simply including traffic from both ports 80 and 25 provides no way to distinguish the Web mail traffic over port 80 from other port 80 traffic.

NBA systems collect layer 7 application data and merge that data with the flow data from the network. NBA systems have built-in libraries of known application "fingerprints;" you can update the library with fingerprints from custom client/server or Web applications. This means that you can look at usage based on the way you think about the network: by application. NBA systems provide this information in real time and also allow you to view usage over any desired time frame.

Why it Matters. Understanding actual usage by application is extremely useful for capacity planning as well as for making decisions about future application changes. It can also help identify use of unauthorized applications that are consuming expensive bandwidth and reducing employee productivity.

Even custom Web-based applications can easily be identified by name. In this case, applications associated with the URL <https://intranet.riverbed.com> are called "Intranet."



Traffic Breakdown by Application Ordered by: Avg Bytes/s

Application	Avg Bytes/s	Avg Packets/s	Avg Conns/s	Avg Net. RTT (ms)
Web	2,707 (100%)	57 (100%)	< 1 (100%)	119
LDAP	582 (100%)	3 (56%)	< 1 (100%)	59
Gmail	139 (45%)	< 1 (18%)	< 1 (100%)	129
SSH	103 (33%)	< 1 (11%)	< 0.01 (5%)	435
SMB	78 (25%)	< 1 (7%)	< 1 (21%)	35
DNS	29 (9%)	< 1 (6%)	< 1 (100%)	
YahooMsg	26 (8%)	< 1 (8%)	0 (0%)	
MSNMMsg	17 (6%)	< 1 (8%)	0 (0%)	
Corporate	4 (1%)	< 1 (< 1%)	< 0.01 (5%)	130
TheOnionRouter	3 (1%)	< 1 (1%)	< 1 (16%)	30
aDirectory	2 (< 1%)	< 1 (< 1%)	< 0.01 (11%)	22
Intranet	2 (< 1%)	< 1 (< 1%)	< 0.01 (11%)	34
Total	308 (100%)	5 (100%)	< 1 (100%)	

Reporting is simplified by having applications — even Web-based applications — identified by name rather than by port/protocol.

Application names are used throughout the system including, as shown here, in the behavioral analytics. This ensures that the system looks at the network the same way you do: by application name, not port/protocol combination.

Unified Data Collection and Retention

NBA systems coalesce flow, application, and user data together into one meaningful record. Unlike other systems that might see one “conversation” as multiple individual connections, NBA systems can give you an end-to-end view. Unlike other systems that save only summarized data over time, NBA systems can store these detailed records for as long as you require based on your retention policies.

Why it Matters. The coalesced records give you an accurate picture of what happened on the network at any given time without the “noisy” duplication of a single event as it moves through the network. Storage of this detail over the long term ensures that you have the complete information to help with your planning.

Reports that Pivot on any Data Element

Having complete historical data is critical, but it only helps if you can easily find the information you need. NBA systems provide complete, flexible reporting capabilities that enable you to pivot on any data element and to click for increasing levels of detail.

Why it Matters. You need to get at exactly the information you need quickly and easily in order to make the right decisions. Easy access to detail provides even more information and context to inform or validate your decisions.

NBA systems provide an easy-to-use interface for setting up reports to look at any aspect of current or historical activity.

Host Pair 1 - 14 of 14									Options
Server	Server Group	Client	Client Group	Avg Bytes/s	Avg Packets/s	Avg Conns/s	Avg Net. RTT (ms)	Avg Server Delay (ms)	
webmail	MSEExchange-srvr	t60-larry	desktop-users	6	(43%) < 1	(42%) < 0.01	(38%)	31	< 1
exchange	MSEExchange-srvr	belverson-t60	desktop-users	7	(43%) < 1	(42%) < 0.01	(38%)	3	< 1
webmail	MSEExchange-srvr	t61-stevec	desktop-users	4	(38%)	< 1	(38%)	3	< 1
exchange	MSEExchange-srvr	t61-stevec	desktop-users	5	(38%)	< 1	(38%)	2	< 1
webmail	MSEExchange-srvr	t60-suzan	desktop-users	6	(38%)	< 1	(38%)	1	< 1
exchange	MSEExchange-srvr	t60-dlashlev	desktop-users	6	(38%)	< 1	(38%)	1	< 1
webmail	MSEExchange-srvr	t60-carthur	desktop-users	4	(38%)	< 1	(38%)	1	< 1
webmail	MSEExchange-srvr	t61p-podsielzki	unassigned	15	(38%)	< 1	(38%)	< 1	< 1
exchange	MSEExchange-srvr	t61-podsielzki	unassigned	15	(38%)	< 1	(38%)	< 1	< 1
exchange	MSEExchange-srvr	m3							
webmail	MSEExchange-srvr	t60							
webmail	MSEExchange-srvr	t60							
webmail	MSEExchange-srvr	m3							
exchange	MSEExchange-srvr	m3							
Total									

Host information report	
User Report	
External links	
Vulnerability Scan...	
Notes...	
Traffic for this host	
Traffic for this host in context	
Traffic between these hosts	
Traffic between these hosts in context	
Packets for this host	
Packets between these hosts	
By applications	
By application ports	
By application port QoS	
By ports	
By hosts	
By peers	
By host pairs	
By host pair ports	
By protocols	
By port groups	
By devices	
By interfaces	
By flows	
By host groups	
By peer groups	
By group pairs	
By group pair ports	
By QoS	
By interface QoS	
By network segments	

NBA systems enable you to easily drill down into reports for increasing levels of detail. In this case, you can drill down from a view of conversation (host) pairs by right-clicking to pivot on an interface-centric view.

Cost-Effective Deployment and Management

Because NBA systems use the flow data from your existing infrastructure and supplement that with layer 7 application and other information, you get the all the capabilities described here with minimal deployment of devices such as network probes. The lightweight deployment model scales by number of data centers as opposed to by WAN links or remote sites. This delivers savings by significantly reducing capital expenditures required to reach full deployment and eliminating operational expenses related to maintaining remote hardware and agents.

Why it Matters. The value you get from any tool must be greater than the cost to deploy and maintain it. Because NBA systems are cost effective to install and manage, they provide immediate value. Furthermore, when NBA systems are used for more than planning — such as for improving performance, availability, and security — they deliver significant value to the organization without significant incremental cost.

Financial Services Company Case Study

A major financial services company deployed an NBA system and in a matter of weeks was able to provide IT management with information to help them more efficiently manage their IT infrastructure. The NBA system identified, among other things, underutilized servers that could be eliminated or consolidated to significantly reduce costs, as well as opportunities to improve bandwidth management.

Identify and Eliminate Underutilized Servers

The NBA system was used to identify all the servers in a particular segment of the network and their activity including number of connections and number of bytes transmitted. Of the approximately 100 servers that the NBA system identified, however, 13 were generating 93 percent of the total number of network connections and eight were generating 92 percent of the total number of bytes transmitted. Just this information alone showed them that there were a lot of underutilized servers in this segment and that there was enormous opportunity to save significant costs through server elimination and consolidation.

When you look at the network connectivity, support personnel, space/power/cooling, and maintenance costs, the average \$10,000 server costs \$7,500 to operate on an annual basis. Each server eliminated through removal or consolidation will save the company money that quickly adds up.

The NBA system also gave them complete information they could drill into to determine exactly which servers could be eliminated and or consolidated.

Improve Bandwidth Management

The NBA system was able to identify two areas in which the company could improve its bandwidth utilization without requiring any further investment.

First, by analyzing historical traffic, the company quickly found that backups were responsible for almost 95 percent of the total bandwidth on two links during peak business hours. By implementing policies that require backups to be run during non-business hours, they were able to free up a significant amount of bandwidth on those links. They were able to use the NBA system to alert them when backups are performed during normal business hours.

Second, there was a mis-configured application server that was attempting to push a 500 MB file to an SMTP relay every 15 minutes and had been doing so for the past fifteen months! This was consuming 570 GB of network capacity every week.

Without this information, the company might have invested in additional bandwidth. But because they were able to reschedule backups and eliminate a long-standing mis-configuration, they were able to free up significant amounts of bandwidth.

Other Resources

Learn how NBA systems can be used by network operations and security teams to improve performance, availability, and security by downloading white papers at:

www.riverbed.com/cascade/resources

Find out how much your company can save by eliminating underutilized servers, improving performance and availability, reducing security breaches, or using NBA instead of internal firewalls/IDS; download ROI calculators at:

www.riverbed.com/cascade/roi

About Riverbed Technology, Inc.

Riverbed is the IT infrastructure performance company whose industry-leading WAN Optimization solutions give organizations an order-of-magnitude increase in the performance and value of their existing network, application, and storage infrastructure. With Riverbed, organizations no longer need to sacrifice IT strategy when cutting costs.

Riverbed frees business from common IT constraints by arming CIOs with WAN Optimization solutions that increase network throughput and application performance by up to 100 times; provide enterprise-wide network and application visibility; store three-to-10 times more data; and support distributed users better. Further, Riverbed lets companies achieve all this with the same amount of network bandwidth, storage and servers they have today. In fact, customers can often reduce their current IT infrastructure footprint after deploying Riverbed's products.

These capabilities may sound "unbelievable," yet they are market-proven by thousands of successful enterprise deployments. Riverbed helps budget-constrained CIOs extract more value from their IT infrastructure without requiring significant upgrades to support operations in their data centers, remote offices or for their mobile users. With Riverbed, CIOs can effectively navigate this era of tight or shrinking budgets while continuing to support today's fluid, ever-changing, and increasingly dispersed enterprises.

Thousands of the world's most demanding businesses, including half of the Forbes Global 100, trust Riverbed to make their IT infrastructure faster, less expensive and more responsive – by an order of magnitude.

Riverbed: Believe it.



Think fast.™

Riverbed Cascade

125 CambridgePark Drive
Cambridge, MA 02140
Tel (617) 354-9292
Fax (617) 354-9272
www.riverbed.com/cascade

Riverbed Cascade EMEA Office

Farley Hall
London Road
Binfield
Bracknell
Berks
RG42 4EU
UNITED KINGDOM
Tel: +44 (0) 1344 401900
Fax +44 (0) 1344 401903