

## Practicing Defensive Network Driving

AAA East Central Relies on Observer® for Advanced Troubleshooting

When a problem arises on the network, the first steps in troubleshooting are the most critical. By following a proven troubleshooting methodology, IT professionals can promptly address critical problems instead of letting them fall through the network cracks. Although advanced network troubleshooting tools are readily available, many IT professionals continue to take the old “trial and error” approach to solve problems. This is bad for users, customers, and the bottom line: while administrators are wasting time, employees can’t use the network effectively or at all, resulting in poor or negligible customer service. The American Automobile Association (AAA) East Central shows how following a proven troubleshooting methodology that takes advantage of advanced, proactive tools to manage the network translates into cost savings (and happier users and customers).

### Monitoring Roadways Since 1902

AAA East Central, a not-for-profit organization founded in 1902, is an advocate for motorists and travelers alike. Known primarily for providing emergency road service, maps, and travel publications, AAA East Central also provides a broad range of travel services, member benefit programs, and engages in many public service activities.

AAA East Central is headquartered in Pittsburgh, Pa., and has over 56 remote offices across New York, Ohio, Pennsylvania, and West Virginia. The club is also growing tremendously—it is scheduled to open 17 more offices within the next year alone. More than 1,500 employees depend on the East Central network, which includes a fiber backbone, Gigabit Ethernet connecting switches, and 10/100 end-user connections.

### Roadside Protection

AAA East Central was a Network General™ customer, having deployed Sniffer on the main backbone to monitor traffic at the corporate headquarters. This left AAA East Central blind to most remote traffic, meaning the IT team often found themselves responding to problems at branch offices rather than preventing them. To get better coverage for the entire network and still stay within budget, AAA East Central CIO Portia Ulinski deployed Network Instruments’ Observer Suite along with 60 probes across the entire network infrastructure. IT staff now have comprehensive visibility and functionality club-wide, and are thus able to prevent most user complaints, and quickly troubleshoot any problems that do come up.

“We realized how important it was to monitor all network communication at the time destructive viruses such as sobig and mydoom were hitting companies around the world,” Ulinski said. “Fortunately we never got hit but we didn’t want to take that chance again. That’s why we chose Observer. This way we can see problems as they emerge and eliminate them before they have a chance to affect the network.”

### Finding and Prosecuting Road Hogs

Understanding who is producing loads of traffic is important for any company whose mission depends on the network. Whether there are security threats, network inefficiencies, network misuse, or application problems, knowing something as simple as what device is causing an unusual amount of activity can be the key factor in resolving the situation.

Observer’s Top Talkers feature shows the current activity for every device on the network in real time. Senior Network Engineer Coleman Jennings regularly uses this feature at AAA East Central to address a number of issues.

“We consistently use Top Talkers to track the total amount of stats for each office to see if there is any unusual activity,” Jennings said. “It’s a big problem when a device other than servers, routers or anyone in the IT department ranks high on Top Talkers.”

There could be a number of reasons someone at AAA East Central tops the list. One explanation Jennings gives is due to employees transferring an unusually high number of files across the network. In one case, he identified an end user transferring a large number of files to a server. He investigated further and discovered that an employee was backing an entire hard drive to that server, which is not an acceptable or necessary club practice.

“Through Top Talkers I was able to track down the person who was transferring all that data to the server,” Jennings said. “Had I not stopped that person, all the activity would have overloaded the server. That is not acceptable under club policy. I was able to enforce the policy and assist that employee in alternative options to protect the data.”

Observer Suite - Top Talkers											
MAC (by hardware address)		IP (by IP address)		Packets							Util %
Alias	IP from Address Book	Address	Rx	Tx	Total	%	/sec				
WebServer	193.189.247.11	Cisco [50:B5:86]	7485	8626	16111	11.664	41.31	25.46			
BackupS	207.108.87.16	3Com [76:E1:CC]	4216	3186	7402	5.359	18.98	18.14			
WEB Server	207.108.87.1	WD [0F:09:D2]	3286	6383	9669	7.000	24.79	14.01			
NT	207.108.87.2	WD [6E:02:9C]	9611	7522	17133	12.404	43.93	9.121			
Richard		GVC [34:AC:F7]	1065	1062	2127	1.540	5.45	5.417			
Eric	128.223.2.8	DEC [04:E6:A5]	2148	960	3108	2.250	7.97	5.337			
Tomas	128.223.2.11	3Com [80:AC:82]	960	2148	3108	2.250	7.97	5.225			
Harry		3Com [9F:42:C1]	9658	5382	15040	10.888	38.56	4.847			
Ian		Intel [C8:F6:57]	2125	2103	4228	3.061	10.84	1.994			
Sara		Intel [DB:6E:EB]	2103	2125	4228	3.061	10.84	1.879			

Observer’s Top Talkers feature shows the current activity for every device on the network in real time.

In summary...

### About AAA

AAA East Central is a non-profit organization founded in 1902 known primarily for providing emergency road service, maps, and travel publications. AAA East Central is headquartered in Pittsburgh, Pa., and has over 56 remote offices across New York, Ohio, Pennsylvania, and West Virginia. More than 1,500 employees depend on the East Central network.

### Challenge

AAA East Central needed a way to proactively monitor network communication in order to prevent problems from affecting customer service.

### Solution

By deploying Observer Suite and 60 probes, the IT team could easily detect problems as they started to emerge, allowing AAA East Central to eliminate problems before they wreaked havoc on the network—ensuring customers were receiving the best possible service.

“Observer is like having an employee on site at all hours to manage the network. We’ve been very satisfied with its capabilities. So far Observer has prevented us from experiencing any downtime.”

Portia Ulinski  
CIO  
AAA East Central



### Putting the Brakes on Hackers

In Top Talkers, every device on the network is identified by its MAC address, IP address, and alias name, easily leading to the source of potential problems. If there is an unknown device topping the Top Talkers list, it could mean that a hacker is infiltrating the network. Jennings has found this to be the case multiple times.

"When we get an unknown IP address scanning through the system, I'll first run a packet capture to determine what it is doing," Jennings said. "Typically, it is a hacker and in that case I will block the IP address at the router."

### Stalled Applications

When employees complain about a slow network at AAA East Central, it is very easy for Jennings to use Observer to determine whether the network or a particular application is at fault. In one case, the application responsible for providing AAA East Central's Emergency Road Service (which includes roadside assistance such as a jump start, a tire change, gas delivery, and a tow to a service station) stalled. Without that application, services get delayed, which can leave customers stranded at the roadside for an extended period waiting for help. Jennings immediately pulled up Top Talkers and noticed that the road service application was creating an unusual amount of activity. From there he drilled down even further with Observer's Connection Dynamics for a packet-by-packet display of the application's communication with each client.

"Through Connection Dynamics, I could monitor the communication between the road service application and the rest of the network," Jennings said. "The time analysis clearly showed there was a problem with the application, which I was able to immediately address—restoring full service to our customers."

### Observer: The Eye in the Sky for Real-Time Network Traffic Reports


Jennings cannot efficiently identify and resolve network problems without a comprehensive understanding of all the activity on the AAA East Central network. To ensure that he can see every segment of the network, Jennings deployed 60 probes at AAA East Central's regional branch offices. Each probe reports back to an Observer Suite console and is equipped with all the tools Jennings needs to monitor the network, including Top Talkers.

"Comprehensive visibility is crucial to stay on top of the network," Jennings said. "With Observer it's like looking in 60 directions at once. The IT team couldn't possibly be as effective if we didn't have that many 'eyes.'"

By implementing Network Instruments® probes at remote offices, an IT professional not only gains visibility into those sites, but Network Instruments Distributed Network Analysis (NI-DNA™) architecture makes it just as easy to monitor those sites as it is to monitor the local LAN. NI-DNA provides uniform functionality and seamless integration across the entire Observer family of products.

### Working Around the Clock

Although employees may leave at the end of the day, business goes on. Observer monitors network communication around the clock to ensure that AAA East Central constantly receives the information resources needed.

"Observer is like having an employee on site at all hours to manage the network," Ulinski said. "We've been very satisfied with its capabilities. So far Observer has prevented us from experiencing any downtime." 

### About Top Talkers

The Observer Top Talkers display offers a heads-up view of bandwidth utilization by all stations on the network. It also shows detailed traffic flow statistics that can indicate a runaway station, a broadcast/multicast storm, or an unbalanced switch. With this information, network administrators can determine network usage patterns, detect faulty network hardware, and determine what percentage of the network's bandwidth potential each system is using—all from one comprehensive display.

### About Connection Dynamics

Connections Dynamics shows a selected conversation graphically, illustrating the inter-packet delay as spacing between packets. Packet-to-packet delay times are shown graphically, allowing instant identification of long latency and response times. Retransmissions and lost packets are flagged in red for quick identification. The packet display can contain either a brief or detailed view of each packet's contents.

### About Network Instruments, LLC

Network Instruments is the industry-leading developer of distributed, user-friendly and affordable network management, analysis and troubleshooting solutions. The award-winning Observer family of products combines a comprehensive management and analysis console with high-performance probes and network TAPs to provide integrated monitoring and management for the entire network (LAN, 802.11 a/b/g, gigabit, WAN). All Network Instruments products are designed utilizing a Distributed Network Analysis (NI-DNA™) architecture. With NI-DNA, the Observer solution set simplifies network troubleshooting and management, optimizes network and application performance and scales to meet the needs of any organization. Founded in 1994, Network Instruments is headquartered in Minneapolis, Minnesota with offices in London, Munich, Paris, Toronto, and multiple cities throughout the United States with distributors in over 50 countries. More information about the company, products, innovation, technology, NI-DNA, becoming a partner, and NI University can be found at: [www.networkinstruments.com](http://www.networkinstruments.com).

### About AAA East Central

Since its founding in 1902 as the American Automobile Association, this association of independent clubs has been an advocate for the motorist and traveler. It has fought motorists' legislative battles, protected them against unduly restrictive legislation, and worked against harsh and unjust prosecutions. AAA has been in the forefront of the movement for adequate roads and safe use of those roads. It has fought for equitable taxation and stood constant watch over the rights and prerogatives of America's travelers.

A not-for-profit, fully tax-paying organization with more than 48 million members, AAA is well respected for its credibility and integrity. Known primarily for providing emergency road service, maps and travel publications, AAA also has a broad range of travel services, member-benefit programs and public service activities. AAA East Central is a not-for-profit association with 56 local offices in Pennsylvania, West Virginia, Ohio and New York. For more information about AAA East Central, go to [www.aaa.com](http://www.aaa.com).

"Comprehensive visibility is crucial to stay on top of the network. With Observer it's like looking in 60 directions at once. The IT team couldn't possibly be as effective if we didn't have that many 'eyes.'"

Coleman Jennings  
Senior Network Engineer  
AAA East Central

**Corporate Headquarters** Network Instruments, LLC • 10701 Red Circle Drive • Minnetonka, MN 55343 • USA

toll-free: (800) 526-7919 • telephone: (952) 358-3800 • fax: (952) 358-3801 • [www.networkinstruments.com](http://www.networkinstruments.com)

**European Office** Network Instruments • 7 Old Yard • Rectory Lane • Brasted, Westerham • Kent TN16 1JP • United Kingdom

telephone: +44 (0) 1959 569880 • fax: +44 (0) 1959 569881 • [www.networkinstruments.co.uk](http://www.networkinstruments.co.uk)

