THE
Network Monitor™
A PUBLICATION OF NETWORKING ISSUES

Vol. 6 No. 4

In this issue:

Industry Focus: Colleges and Universities

Higher education these days is big business and colleges and universities have some of the most complex, diverse, and conflicting set of network requirements around. They must support retail operations, protect student personal information, limit access to other sensitive data, provide a high level of connectivity, significant bandwidth, and support large numbers of people. Gone are the days where the campus network was run by a group of computer science or engineering students. Today's higher education networks are a significant asset that influences admissions as well as regular business operations. By incorporating a process of Audit, Analysis, and Automation, colleges and universities are able to operate large networks with small teams.

Audit, Connectivity & Capacity

A typical campus will encompass several buildings at a minimum. Many colleges and universities also have remote teaching facilities, so the network will also include a rather significant WAN component. A good network audit will identify the network infrastructure devices, their connectivity, and the clients and servers connected to the network. This is the first step of a smoothly running network.

The LAN environment is typically a large switched network, hopefully following vendor design guides to increase reliability and efficiency. When problems occur in a switched environment, they can be difficult to track down, so tools that show connectivity of end stations and the operational configuration of spanning trees are very useful.

Gone are the days where the campus network was run by a group of computer science or engineering students. Today's higher education networks are a significant asset that influences admissions as well as regular business operations.

Students and faculty are taking advantage of online collaboration, performing research for papers, sharing files, creating web sites, and making phone calls. This puts a tremendous load on the network. The network staff must keep a close eye on what the network is doing and making sure that important services are not starved of network bandwidth due to lower priority applications.

(continued on page 2)

Knowing Your Network – Event Analysis

By Terry Slattery

When a significant network event occurs, the network equipment often sends a message, using either Syslog or SNMP Trap format, to a pre-configured network management station. Events are much like fire alarms - something important has happened, possibly impacting the business. These messages are asynchronous; that is, the network management station receives them without polling. The content of the messages, defined by the vendor, identifies the event that caused the message to be generated. Events typically have varying severity levels, from informative to critical. The vendors attempt to classify the severity according to how much impact the event will have on the network. Obviously, critical events will warrant a higher level of attention than an informational event.

Needle In The Haystack

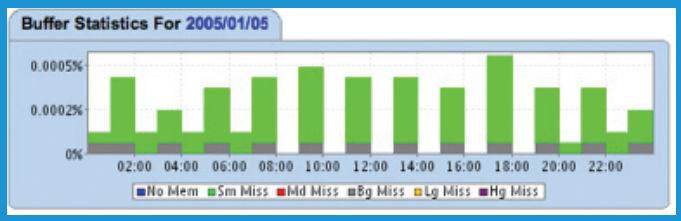
Most every network of any reasonable size uses an event collector to collect and store event logs. The volume of messages collected each day means that manual processes for searching and identifying critical messages don't work with large logs. Therefore,

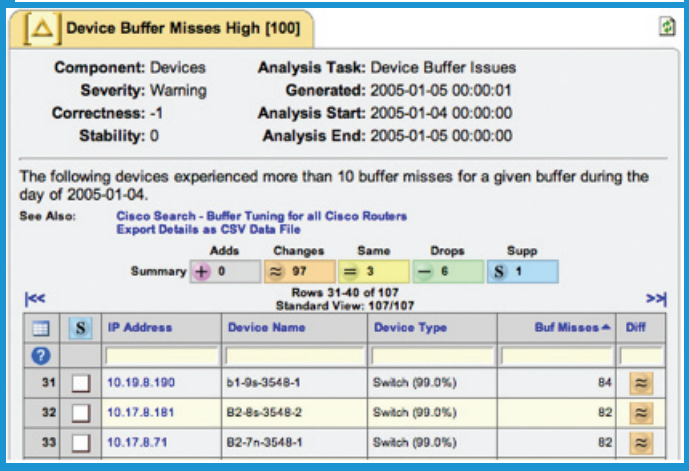
(continued on page 3)

Cisco Buffer Tuning

tech tip

Unnoticed packet loss in networks can adversely affect the applications using the network and one potential source of packet loss is the store-and-forward buffering used in Cisco routers. Cisco routers generally do an excellent job at handling network traffic, but sometimes a bit of buffer tuning will improve the process. In some rare cases, an IOS bug will never release buffers, eventually consuming all memory. Watching buffer creation and the total number of buffers (or memory) in use will alert you to places in the network where buffer tuning may be helpful.





Cisco divides system buffers into multiple sizes, which are used to hold packets being process switched, routing updates, telnet and ssh, and other purposes:

Buffer Type	Size (in bytes)
Small	104
Middle	600
Big	1524
Very Big	4520
Large	5024
Huge	18024

Each buffer type can have a number of permanent buffers, as well as minimum and maximum free buffers. The router will create new buffers as needed to handle the packet flows.

Automated systems such as NetMRI monitor buffer misses, failures, and no memory counters on a daily basis and identify routers where these counts are excessive. It is also useful to know what time of day the buffer counters changed so that you can determine the type of traffic involved and the application that is likely to be affected. NetMRI creates an issue when a router is experiencing excessive buffer misses or failures, or when there are any no memory counts.

In the above example, the maximum number of buffers exists in the pool, so it would be reasonable to increase the max count by a small percentage, say 20%, or 30 more buffers. The number of failures is .15% of the total number of buffer hits, so increasing the number of permanent buffers to 50 would be reasonable, given the buffer size of 600 bytes. The following commands would perform this change:

```
buffers middle permanent 50
buffers middle min-free 20
buffers middle max-free 180
```

Be careful when tuning buffers. You can exhaust system memory by allocating too many buffers, impacting routing protocols, telnet/ssh access, and other internal functions. At least a megabyte of free system memory is necessary in most routers for normal operation.

Look for our tech tip library at www.netcordia.com/resources **TNM**

continued from page 1

Even with high speed LAN interfaces, a lot of campus network teams are finding that the Internet connections are a major bottleneck. Open source packages like MRTG and Cricket have been the staple of watching link utilization. But the configuration of QoS across a network makes these tools a lot less useful (Cisco's Class-Based QoS MIB – CBQOSMIB is one of the most complex MIBs we've seen and is difficult to monitor with these tools). Just monitoring link utilization isn't sufficient in modern networks. The network is a big system and must be monitored and analyzed as such. The challenge is finding tools that provide a system level view of the network.

Analysis & System-Level Views

In any large network, there are many operational parameters that should be checked on a regular basis. Many parameters interact with one another in one way or another. A simple example is that HSRP may be properly configured on two routers, but because of a cabling problem, only one is operational. Quite often, a failure that shouldn't have happened was the result of redundancy failure that was not identified. More complex examples involve the interaction between QoS settings and application performance. Both examples are configuration and operational characteristics that go beyond device level management and into

(continued on page 6)

continued from page 1

vendors have built complex mechanisms for filtering log files.

Event logs also force you to be reactive. When the notification is received, the event has already occurred and you're in the position of trying to respond to the event to limit downtime or brown-outs. Wouldn't it be better to prevent significant network events rather than reacting to them?

Finally, what happens if the needle never makes it into the haystack? When network congestion or re-convergence occurs due to a significant network event, packets may be discarded by the network equipment. If an important event message was discarded then you must use other data sources to determine that an event occurred. One source is that your end users start calling to inform you of some service that's no longer available on the network.

The network is a big system and must be monitored and analyzed as such. The challenge is finding tools that provide a system level view of the network.

The end result of the above is that log files tend to be most often used for postmortem analysis, long after the business has been impacted by the event. That's why it is preferable to use SNMP and CLI as the primary sources for network management – it is better to find early symptoms or to detect latent problems through these data sources and apply corrections before a major event occurs. Even so, there are some events that are only observable through log file analysis, making log file analysis imperative.

What Is Event Analysis?

A good log analysis system relies on more than just log data for its analysis. The network is a system and its analysis must encompass the entire system. Event analysis must:

- Allow easily searching and filtering event logs.
- Correlate between various data sources, including other events messages, audit information, configuration information, and operational data.
- Don't trigger an alert on repetitions of the same message.
- Trigger other actions such as collecting additional data via the CLI or SNMP.
- Provide links to other data referenced by data within the message.
- Automatically clear events when the system can detect its resolution.
- Create a user forum to share event processing definitions with other network managers. Even though it isn't strictly a part of event analysis, sharing is an important capability.

Ideally, the event analysis system can be configured so that only a few messages are important enough to generate an alert each day, because if the volume is too high, then the network staff will be overloaded. One symptom of overload is when the staff can't determine which events should be handled first. (Much like a router without QoS, most people will resort to FIFO handling of events because of the perception that there's no time to prioritize them.)

NetMRI Event Analysis

I've not encountered an event log system that took into account enough variables to make its output very useful. So when we looked around at systems prior to starting to build one for NetMRI, we found Splunk. They index event messages and store them in a way that makes it easy to use their GUI to quickly filter messages (yes, it can be faster and easier than grep). It also has the advantage that it can handle multi-line messages correctly, which grep can't do. At a recent site visit, I was able to quickly filter through about 10MB of messages and find the one message that was important.

What about the other requirements I stated above? Some of them are being addressed in our first release. There is basic correlation between devices and events. For example, you might have a set of important routers on which you want to be notified of any routing adjacency changes while other routers have more unreliable and less important WAN & VPN interfaces. By correlating events with device groups it is possible to filter out the

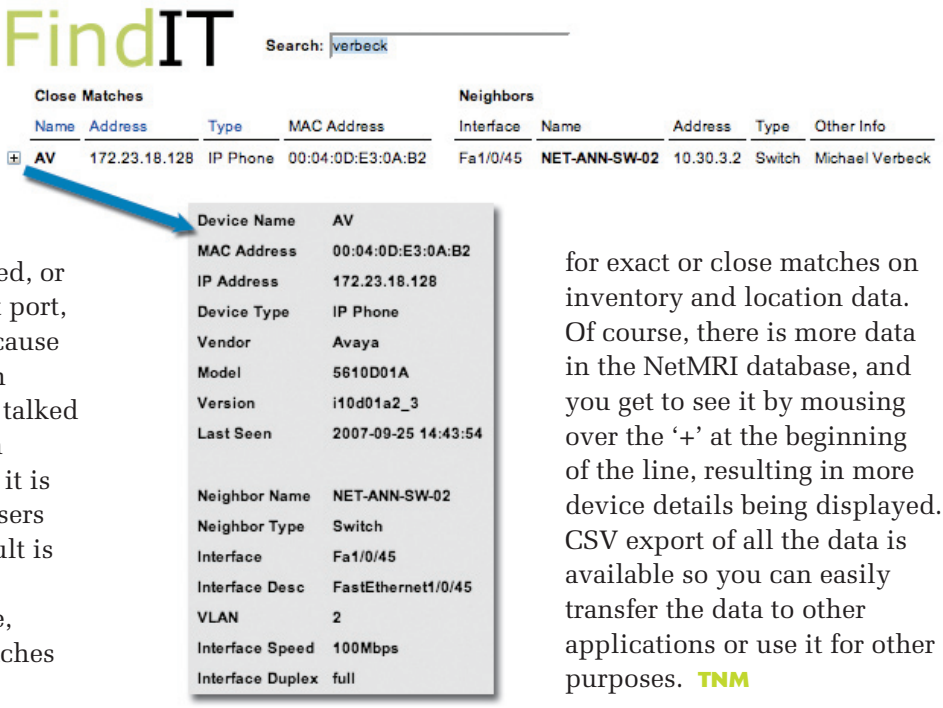
A good log analysis system relies on more than just log data for its analysis. The network is a system and its analysis must encompass the entire system.

(continued on page 4)

NetMRI Did You Know...?

Many organizations need a tool for their help desk or operational support team to use to determine the logical location of an end user workstation. The typical use is to find the switch port to which a user's workstation is connected, either for checking operational characteristics like duplex mismatch or speed, or to monitor traffic on that port, or to disable the port because the workstation has been infected. People that we talked with called this function "user tracking", because it is typically used to track users on the network. The result is NetMRI's FindIT™.

This person's IP Phone, defined in the Close Matches section, is connected to the switch identified in the Neighbors section. The search field can contain user names, device names, IP addresses, MAC addresses. Entering portions of search strings may match multiple systems, such as finding all systems within a given subnet by specifying the first characters of the subnet number. (No, it doesn't do binary math to match on subnet prefixes. Think Google-style matching and you're closer to how it works.) The input string is used to search for exact or close matches on inventory and location data. Of course, there is more data in the NetMRI database, and you get to see it by mousing over the '+' at the beginning of the line, resulting in more device details being displayed. CSV export of all the data is available so you can easily transfer the data to other applications or use it for other purposes. TNM



Knowing Your Network – Event Analysis

continued from page 3

noise of routing protocol adjacency changes on VPN and Frame Relay links and see the important adjacency changes on core routers and important links.

Generate a single alert when multiple events of the same type occur. But also allow the creation of alerts when the number of events increases, with the severity depending on the number of events within a time period. For instance, clusters of environmental errors that indicate overheating of a wiring closet. The alerting mechanism lets you determine when one mechanism should be preferred over the other.

Some events provide an early alert of something starting to happen, but more details are needed by executing CLI commands or collecting other SNMP data. A simple example is to collect the new configuration file after a configuration modification event message is received. Another is to use the CLI to collect more details about a Pinnacle error or CBUS error in a Cisco device. We're starting with a few examples of these event-based triggers and will be expanding them as we learn what functionality customers want.

Event messages often contain hints at offending systems within the text of the message. In the below sample message, wouldn't it be nice to automatically know more about the end station identified by the MAC address that's reported?

```
%STANDBY-3-DUPADDR: Duplicate
address 10.1.2.2 on Vlan2,
sourced by 000b.60ab.cdef
```

Some events generate an OK message when the problem is resolved, or other data can be used to determine that

(continued on page 6)

Customer Spotlight

Texas A&M University

Texas A&M is the nation's sixth largest university in enrollment and boasts one of the largest campuses in the nation with 5,200 acres, including a 434-acre research park. Unlike most universities of this size, Texas A&M has one centralized IT group for networking—the Computing and Information Services (CIS) Network Group—which is responsible for the entire campus network backbone and LANs spanning over 340 buildings, including student residence halls, student labs, and data centers.

Texas A&M's network management group relied on a conglomerate of tools to maintain the network backbone. Managing multiple tools was time consuming and required a significant use of manpower to learn the tools, manage them, and try to make sense of the disparate data provided by each tool. The group needed a way to simplify the management of the network and spend the time saved on more productive, strategic tasks.

"Writing scripts for multiple tools takes an excessive amount of time and energy, and with the backbone being continuously modified and changed, we needed a way to streamline these tools in order to efficiently manage the network," said Matthew Almand, Chief Network Engineer for Texas A&M University.

After reviewing several options, Texas A&M chose NetMRI, a proactive network management solution, to manage its vast multi-vendor network as one whole system. With its built-in expert rules engine, NetMRI monitors, detects, and reports on network issues before they become problems for Texas A&M's IT staff. After installing NetMRI, Texas A&M was able to replace most of its monitoring tools, resulting in an enormous reduction in overall network management and maintenance time. This dramatic reduction enables the Network Group to be proactive instead of reactive.

"The initial hook was that NetMRI contained all our best practices in a box." — *Matthew Almand, Chief Network Engineer, Texas A&M University*

"The initial hook was that NetMRI contained all of our best practices in a box," said Almand. "It is very easy to install and simply understands how the internal network infrastructure works. NetMRI is truly a unique solution and I haven't found another product that is able to carry out the functions and tasks that it performs."

One of the biggest benefits for Texas A&M was NetMRI's Policy Management capabilities. This feature enables them to catalog configurations, monitor changes, enforce policy and standards, and even execute changes whenever necessary-quickly and easily. Now, they can make rapid changes across multiple devices from different vendors without requiring significant programming time.

NetMRI also makes configuration modification of devices on the network simple and hassle free. It formalizes Texas A&M's best practices before the IT staff rolls out new pieces of equipment. NetMRI also maintains copies of current and previous configurations, which enables the network group to revert to an earlier configuration at any time. By comparing Texas A&M's currently running configurations with its previous configurations, NetMRI also serves as an excellent backup tool.

Overall, NetMRI has greatly simplified and streamlined Texas A&M's overall network management, which enables the network engineering staff to work more efficiently. NetMRI simplifies everything by providing Texas A&M with one solution that unifies control of key aspects of its infrastructure. Most importantly, the Network Group now has the time to proactively manage the network, rather than constantly running multiple tools. TNM

Knowing Your Network – Event Analysis

continued from page 4

the resolution has occurred. In these cases, use this data to automatically remove the notification, reducing the network staff work load in handling important events. Reducing human workload is probably the most important factor in making network management systems usable. NetMRI Event Analysis includes the ability to clear an event on receipt of another event or to clear it if the sequence of messages stops over some period of time (not a perfect mechanism, but useful nevertheless).

Finally, we're starting a user forum on which customers can share their definitions for handling events. Like the open source community, sharing definitions and reasoning behind the rules reduces the work that each of us has to perform to create a really good set of event analysis rules.

In summary, the NetMRI Event Analysis system is looking to me to be a really nice system, filling a lot of the holes I've encountered in handling event messages in operational networks. TNM

Industry Focus: Colleges and Universities

continued from page 2

system-level management. It is looking at collections of devices that are providing a service on the network and whether that service is configured and operating correctly.

University network staffs that take advantage of tools that perform automatic analysis of the operational data that's collected from the network have an advantage here. They get to spend more time implementing corrections ahead of time instead of after a failure (pro-active vs reactive) and also have more time to work on new designs that significantly improve the network. The data collection and system-level analysis performed by such tools is the functionality that enables this approach.

Automation & Security

Network security is a big problem in campus networks. Portable computers that have been infected are attached to the network every day. Even one mis-configured subnet could allow a virus into the

(continued on page 7)

Upcoming Events

Netcordia News

Community Server

Our growing user community asked that we provide a user forum where they can share experiences in using NetMRI to improve their networks. At connection.netcordia.com, you'll find the user forums where you can learn about NetMRI's use as well as blogs we write on a variety of topics. You'll find a link to the community server on the Netcordia web site, in the upper right hand menu, labeled 'Netcordia Connection'.

NetMRI 2.3 and Event Analysis

We've recently announced NetMRI 2.3, which adds more real-time analysis, support for additional devices, and device location capability (see FindIT description elsewhere in this issue). The NetMRI Event Analysis (NEA) product is an appliance-based syslog and snmp trap collector that interfaces with a NetMRI network analysis appliance. A software module provides the interface from NetMRI to the NEA appliance. The advantage is that correlation between data that NetMRI has collected and events that NEA has collected can be performed. You continue to view all the data through NetMRI's "single pane of glass" user interface, greatly simplifying the process of incorporating network events with configuration and operational data collected by NetMRI. TNM

continued from page 6

campus network, creating a major slow-down and a lot of work for the network staff. Making sure that the network is properly configured to isolate, scan, and remediate infected systems is a big challenge, probably on par with that for compliance, as noted below.

Automated tools are required to check network device configurations daily. The best method for doing this verification is to verify that device configurations reflect the security policies designed into configuration templates. Any configuration change should result in a new copy of the configuration being archived and making sure that the change is compliant with the network's policies.

Automation & Compliance

Today's compliance regulations affect much of the operation of a university network. There are retail operations for the bookstore, cafeterias, and other student functions. These must comply with the Payment Card Industry Data Security Standard (PCI) to protect credit card data from theft and fraud. Student grades, billing records, and financial aid information access and modification should be treated the same as public corporation's financial data, which is subject to Sarbanes-Oxley Act compliance regulations. Student health records are certainly subject to the Health Insurance Portability and Accountability Act (HIPAA). Some universities perform sensitive research for federal organizations and this data must also be protected from unauthorized access and modification.

Making sure that a large university network is secure from unauthorized modification and that the defined policies are properly implemented is a big task. Manually checking hundreds of routers and switches is not feasible. Automated processes are required.

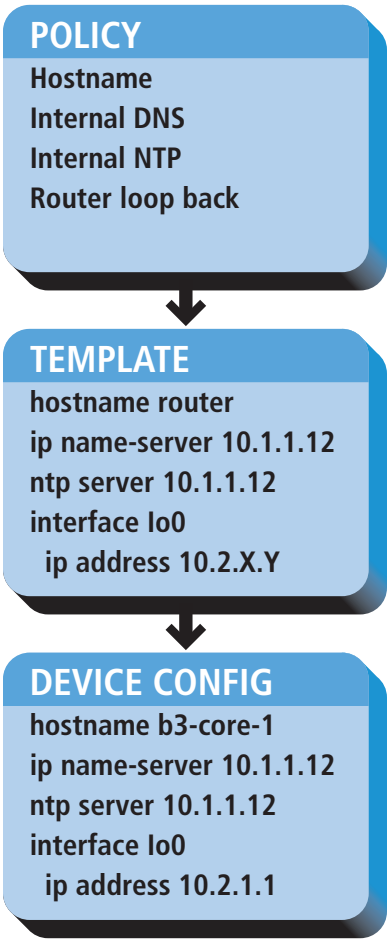


Figure 1

The normal method of implementing network configuration policies is to define the policy, then create templates for each class of device, and finally install the device-specific configurations in the network equipment (see Figure 1).

By checking the templates against the installed configurations, the installed network policies can be regularly validated. There are at least three places where this mechanism pays for itself. One is when new devices are installed in the network. The policy check makes sure that the installed configuration matches the approved policies. Another is to detect any unauthorized changes made to the network. Finally, one that isn't often considered ahead of time, is to track which devices need to have their configurations updated when the policy changes.

Summary

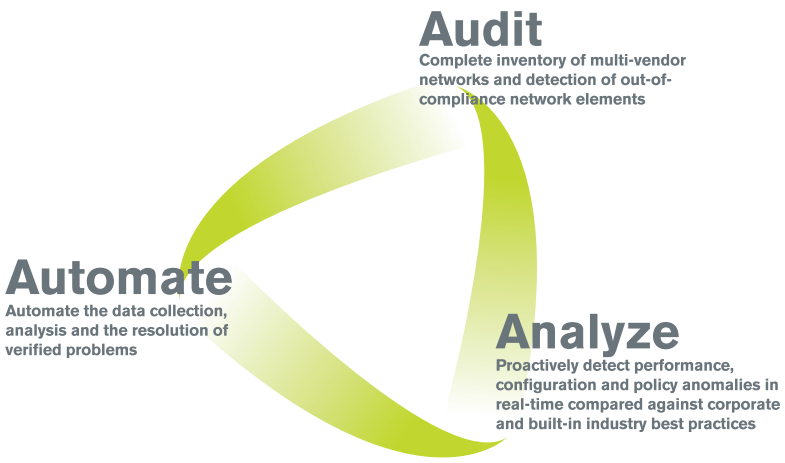
Audit: the big, complex networks used by higher education requires a complete audit to know what's on the network and how it is connected.

Analyze: collect configuration and operational data and analyze it from a system-level perspective to identify current and potential problems that should be corrected.

Automate: the repetitive process of auditing and collecting data and doing the analysis must be automated to the greatest degree possible. Provide mechanisms to allow the network staff to automate the tasks that consume large amounts of staff time.

The Customer Focus on Texas A&M University contains a few hints into why they see value in Netcordia's approach to network management. TNM

**Participate in our online community forum.
Share your thoughts, ideas and learn from others at:
connection.netcordia.com.**



For more information on Netcordia and our full range of automated network management solutions, please call +1-410-573-2271 or visit netcordia.com.

**Want to see NetMRI in action?
Join us for a live demo at www.netcordia.com/demo/**

Don't miss out!

We hope you enjoy this free quarterly publication and encourage you to visit us online to ensure you receive the next issue. Please visit us at www.netcordia.com/tnm to sign up.

Any comments, suggestions ideas? Please e-mail TNM@netcordia.com.

The Network Monitor is published quarterly by Netcordia.

Terry Slattery
CTO and Founder

Don Pyle, CEO

Jay Ennis,
V.P., Product Development

Jon Bierman
Executive V. P., Worldwide Sales and Marketing

Contact:
Netcordia, Inc.
2431 Solomons Island Road,
Suite 302
Annapolis, MD 21401

Phone: 410-266-6161
Fax: 410-573-0774
Customer Support: 410-573-2271
sales@netcordia.com

Netcordia™
Simply a better way to manage

Netcordia™
Simply a better way to manage

2431 Solomons Island Road
Suite 302
Annapolis, MD 21401

PRSRT STANDARD
U.S. Postage
PAID
Permit No. 273
Annapolis, MD

ATTN Mail Room: If not deliverable to addressee, please route to Network/Communications Department.