



Applying Performance Metrics to an Application Centric Network Management Scheme

A Whitepaper on PATROL DashBoard 6.4.00, PATROL
Visualis 1.2.00 and PATROL Integration for DashBoard 1.2.00

By:
Wes Noonan, MCSE/MCT/CCNA/CCDA/NNCSS
Senior QA Rep.
BMC Software, Inc.
(713) 918-2412
wnoonan@bmc.com
<http://www.bmc.com>

Introduction

As technology has continued to evolve, there has been a trend of convergence for the network and the applications that run on that network. The network has moved from being something small and relatively low impact on business processes, to being a vital component of the architecture of the business processes. Today's business applications have moved from a monolithic design model to a distributed design model, which relies heavily on the performance and stability of the network. Simply put, if the network fails to function properly, the applications that rely on the network fail as well. At the end of the day, whether it was the network or the applications that failed doesn't matter – the users couldn't do their jobs.

BMC Software, Inc. recognizes this situation as an important aspect of the day-to-day business functions of a company, and to this end has developed an initiative named "Application Centric Network Management" (ACNM). Where as many vendors can monitor your network, or your applications, BMC Software, Inc. is taking it's proven track record with PATROL for application management and integrating it's network management product lines, including PATROL DashBoard and PATROL Visualis, to provide a singular network aware intelligence to our extensive enterprise management capabilities.

PATROL Visualis and PATROL DashBoard – The foundation of ACNM

The grail of network management, and indeed application management, has always been to forecast potential downtime allowing the administrators to address the issue before it becomes a problem. The problem is that most management tools do not provide the kinds of comprehensive information that allows an administrator to forecast the reliability of the network. An aspect of the network that has always been able to shed light onto reliability and forecasting however has been performance statistics. This is where PATROL Visualis 1.2.00 and PATROL DashBoard 6.4.00 and PATROL Integration for DashBoard 1.2.00 come together.

PATROL DashBoard 6.4.00 is a management application which specializes in collecting and reporting on performance related data and metrics. PATROL DashBoard collects on numerous performance thresholds including: workload, drops, CPU-load, memory-usage, and non-unicast on the device and input, output, drops, non-unicast, errors and collisions on the device interface. PATROL Visualis 1.2.00 is a management application that collects and reports on application and traffic flows. PATROL Visualis provides graphical modeling capabilities to this collected data, delivering a topological map that can be used to overlay and clarify the impact that data on your network has on any given segment or device.

Using PATROL DashBoard and PATROL Visualis to collect these performance statistics provides the insight an administrator needs to know how their network behaves. They provide insight into the consistency and quality of individual and overall network services and applications. In network monitoring, perception is reality and the effective collection and use of performance related data can shape that perception.

PATROL DashBoard and PATROL Visualis assist in shaping that perception by looking at the performance of all of the aspects of your network infrastructure – routers, switches, hubs, bridges and servers, to deliver information to the administrator allowing them to analyze application performance, capacity planning and proactive fault management. How does it do this? Let's take a look.

The Application Impact on Network Performance

The network impact of the applications can be measured in PATROL DashBoard and PATROL Visualis by leveraging network statistics, network probes and RMON as well as numerous Cisco proprietary instrumentations such as Service Assurance Agents, NetFlow and Class of Service information to accurately report on the application impact to the network. By looking at the application trends and traffic modeling, as well as the network reaction to the application traffic, the administrator can build an effective baseline defining the normal traffic patterns on the network. Armed with this information the administrator can then make much more informed diagnostic decisions in the event of a problem. This also facilitates the administrator being able to take the application performance data and use it to make better capacity planning and fault management decisions.

Capacity Planning

Knowing the application performance statistics allows the administrator to forecast with a much greater degree of accuracy what effect an application or network change may have on the application performance perception. The reason for this is simple. Knowing what the network is doing now allows you to extrapolate the impact a change will have. For example, if you know that having 200 clients running application X puts a workload of 3000pps on your network and you need to add 100 clients, you know you will need to make sure that the network has enough workload headroom to support an additional 1500pps at a minimum. This allows the administrator to be more judicious in what they need to buy and when they need to buy it, moving away from the expensive “throw more bandwidth at it” philosophy and to a much more cost effective network management policy without needing to sacrifice long term goals for short term solutions.

Capacity planning is something that everyone knows they need to do, but day to day troubleshooting and firefighting often compromises the amount of time the administrator has to spend on forward looking projects. Through the use of the extensive reporting capabilities of PATROL DashBoard and PATROL Visualis the ability to make proactive, informed decisions about capacity planning becomes a much easier task for the administrator to perform. Instead of needing to spend hours wading through complex systems and log files correlating data, the administrator can use the weekly, monthly and even yearly reporting and logging capabilities to quickly and effectively recognize trends and limitations allowing the administrator to spend more time taking care of problems and less time planning for the future – without sacrificing quality.

Fault Management

The reality is that application management and capacity planning, while vital to the overall health and well being of the network, play a secondary role to fault management. Let’s face it; no one cares how the network will work when change Y is made if the network is down right now. Fault management is the linchpin to an overall network management philosophy. BMC Software, Inc. provides this capability via the PATROL Integration for DashBoard product line. PATROL Integration for DashBoard contains an SNMP based reachability parameter that uses SNMP get functions to check device reachability. The concept is pretty simple, if the KM gets a response, the device is up, if it doesn’t the devices is considered unreachable and goes into alarm. One of the strongest benefits of this capability is ability to integrate this data into your singular network management console, instead of needing a separate, and often times incompatible, application for managing your network’s up/down state.

Performance Measurement to Fault Management

Fault management is a must in any network management platform. However, the problem with most fault management products is that they only tell you when a problem has occurred. That is fine for firefighting and reactive management, but it does little to help an administrator get ahead of the curve and address issues before they become problems. BMC Software, Inc. recognizes this and incorporates its mature and robust alerting capabilities of the PATROL Console and PATROL Agent with PATROL DashBoard’s comprehensive data collection capabilities. Using the PATROL Integration for DashBoard KM, we take the network data already being collected by PATROL DashBoard for application performance and capacity planning and integrate it with the PATROL namespace. This allows the PATROL Agent to actually use performance related metrics as alertable network management metrics.

Many times indicators on your network equipment precipitate a network failure or outage. For example, an interface that is beginning to fail might start dropping more packets. With conventional fault management, you might not know this until the interface actually failed and data started getting lost. With ACNM however, as PATROL DashBoard is collecting the data on the interface, including the increase in dropped packets, this data is being integrated with the PATROL Agent via the PATROL Integration for DashBoard KM allowing the administrator to see that packets are being dropped – including potentially alarming on the situation so the administrator doesn’t even need to go looking for the data, but rather the administrator can get paged prior to actual failure.

Another example of using performance management for fault management is the case of saturated network links. In a world where perception is reality, if a user can’t access an application because the network link is saturated, the user doesn’t care what is causing it they simply know that “the application is down”. By integrating performance metrics into network management metrics, the administrator can get alerted as the bandwidth on the link starts getting consumed instead of being alerted when the link has reached it’s saturation point preventing the users from working. Now, instead of being informed “a link is down”, often times by the users themselves, the administrator

gets informed “a link is becoming saturated” by PATROL, allowing the administrator to potentially address the issue *before* it becomes a problem. The administrator is now in control of the perception of the network, and can shape the perception of “no problems”, thus keeping the user community satisfied.

This capability of using performance metrics as a threshold that can be managed and maintained is known as “brown-out” notification, and is an integral component of the integration between PATROL DashBoard and the classic PATROL foundation.

Intelligent Alerting

One of the best things about today’s technology is how easy it is to stay connected. One of the worst things about today’s technology is how easy it is to stay connected. A common tool for a network administrator is a pager so the administrator can stay informed of network situations. Unfortunately that often means wading through countless pages that require time to investigate only to discover that there really wasn’t a problem. BMC Software, Inc. addresses this by applying intelligence to it’s alerting. Through robust thresholds, alerting and recovery actions, PATROL can qualify the data being collected to make sure that when the administrator gets a page, it’s because the situation has met conditions the administrator configured. PATROL pages the administrator when the administrator thinks it’s necessary. For example, let’s say a link normally operates at 20-25% capacity. As the administrator you have determined that you want to be notified when the link begins operating in excess of 60% of capacity, however you don’t want to get a page because of a fluke instance where the link jumped to 70% utilization and then dropped back to normal again. With PATROL you can configure threshold to go into an alarm condition, and thus alert you, only after 2 consecutive instances above the 60% threshold.

BMC Software, Inc. has also designed the ACNM products with this in mind. A common indicator of network performance is non-unicast percentage of traffic. With traditional products however, they just look at the raw non-unicast percentage as an indicator. The problem arises when the link or interface in question has very low over all utilization. On an Ethernet network, if a device is sending very little traffic, the majority of the traffic that is going to be observed on that interface is going to be non-unicast, for example the ARP traffic that normally occurs. Unfortunately, using traditional non-unicast percentage, even though you might have a 100Mbps link that is only using 1Kbps of bandwidth, since almost all of the actual traffic is non-unicast, the interface would be in alarm. Let’s face it; this probably isn’t a problem. In fact, at the rate of 1Kbps of traffic it probably doesn’t matter what the non-unicast is, the link is fine. BMC Software, Inc. addresses this issue by using a “Non-Unicast Proportion” parameter in addition to the traditional non-unicast percentage. This parameter works by looking at the actual bandwidth being used on the interface before alerting on non-unicast issues. For example, let’s say you have a 100Mbps link. You can configure the Non-Unicast Proportion parameter to only look at the amount of non-unicast traffic after the actual bandwidth in use on the link exceeds a certain threshold (configurable by the administrator) let’s say 20%. So when the link is running at a capacity that is less than 20Mbps, Non-Unicast Proportion isn’t going to worry at all what the non-unicast percentage of traffic is. If the traffic capacity exceeds 20Mbps however, the Non-Unicast Proportion will actually look at how much of the 20Mbps is non-unicast, and if it exceeds the administrator-defined threshold for non-unicast percentage, will alarm accordingly. Now, instead of getting “false positive” alarms about non-unicast percentage on links that are performing fine, the administrator can get meaningful alerts that could well jeopardize the network performance perception.

Forensic Tasks

As networks have matured and become more complex, a need has developed for the network administrator to be able to quickly figure out “what happened” in an attempt to prevent future such occurrences. This “forensic” work can often times be very difficult to accomplish due to the amount of data that might need to be reviewed. Unfortunately, this leads to administrators following a policy of “I don’t know what caused it, but it is working now” as they move on to the next problem on their list. This short term methodology is harmful for the long term health and stability of your network. BMC Software, Inc. helps to address this by making it much easier to isolate, or exclude portions of the network from the problem by looking back at the data that was collected in a very expeditious manner. A great example of this occurred with the “Code Red” outbreaks of 2001.

When Code Red hit, many companies struggled to figure out (a) what was happening and (b) how it happened. Using ACNM, this task was much easier to determine. Because PATROL collects data about performance and integrates it with network management, PATROL Visualis and PATROL DashBoard were able to see the tell tale

signs of Code Red, increased overall and non-unicast traffic, and as a result of the integration with the classic PATROL foundation were able to alert the administrator to a situation occurring that needed to be addressed. Sure, we didn't know that the problem was Code Red – but we knew that a problem was occurring. We could see that because of the increased abnormal network traffic and non-unicast traffic on the network. This was able to alert the administrator that something was going on that needed their attention, thus dramatically reducing the amount of time spent diagnosing the problem. Once the problem was addressed, the administrator was then able to use PATROL Visualis' topological maps and ability to playback captured data to actually watch the Code Red traffic as it entered the network, specifically where it started, and see how it spread from location to location and segment to segment. What is a very complex task to undertake has now been made much easier and less time consuming, allowing the administrator to take the time to look at the data and thus not sacrifice long term goals at the cost of short term firefighting.

Summary

There are a number of critical success factors in monitoring and managing the performance of your network. You need to have a baseline for your network and your application data. You need to perform a what-if analysis on the network and applications to know the result of potential changes you might make. You need to perform exception reporting to address capacity issues that might arise. You need to review the data you have collected and use it to help develop and design upgrade and tuning procedures on both a reactive and long-term basis. By coupling the strengths of PATROL DashBoard and PATROL Visualis, which are collecting the performance related metrics of your network and your applications, as well as the established capabilities of the PATROL foundation, which is collecting your application data in great detail as well as performing fault management functions, BMC Software, Inc. is able to provide the Application Centric Network Management you need to effectively, and with much greater ease, manage your network, and thus control the perception of your users. After all, the best network in the world is of little worth without applications to take advantage of it.