> **SearchNetworking**

NETWORKING MONITORING BEST PRACTICES: SETTING A NETWORK PERFORMANCE BASELINE

TechTarget

> SearchNetworking

W

HY THE NEED for a network performance baseline? A network performance baseline is a set of metrics used in network performance monitoring to define the normal working conditions of an enterprise network infrastructure. This expert E-Guide highlights the necessity for a network performance baseline, potential challenges and how to overcome them.

SPONSORED BY **ixia**

> Search**Networking**

HOW TO SET A NETWORK PERFORMANCE BASELINE FOR NETWORK MONITORING

WHY THE NEED FOR A NETWORK PERFORMANCE BASELINE?
In the simplest terms, a network performance baseline is a set of metrics used in network performance monitoring to define the normal working conditions of an enterprise network infrastructure. Engineers use network performance baselines for comparison to catch changes in traffic that could indicate a problem.

Setting a network baseline also provides early indicators that application and network demands are pushing near the available capacity, giving the networking team the opportunity to plan for upgrades. Aligning network performance baselines with existing network service-level agreements (SLAs) can help the IT organization stay within capacity parameters and identify problem areas that are falling out of compliance.

The network monitoring challenge for engineers, however, is to define what is normal for their organization's infrastructure.

NO INDUSTRY STANDARD FOR NETWORK MONITORING OR METRICS

For IT organizations that have adopted the Information Technology Infra-
structure Library (ITIL) framework for best practices, there are ITIL-specific
monitoring tools available. These tools are designed to take advantage of the
device configuration databases and applications built to support the IT service
management process. Beyond ITIL, however, there is not an industry standard
approach to setting performance baselines. Support for monitoring tools and
the breadth and depth of information made available can vary greatly among
manufacturers, devices and operating systems, ultimately preventing a com-
mon set of metrics from being used in monitoring.

A good first place to start might be the networking vendors themselves.
Every vendor has, at minimum, a list of the monitors a given device supports.
Given the ubiquity of monitoring protocols such as SNMP, many vendors also
have their own recommendation or best practices for monitoring and defining
thresholds for their products. Armed with this information, administrators can
initially focus on a narrow subset of available monitors and grow as needed.
Cisco, for example, recommends not exceeding 60% of CPU utilization on its
routers and has published an SNMP message to monitor that statistic.

NETWORK PERFORMANCE MONITORING: TAKING STOCK AND CONSIDERING VIRTUALIZATION

While building up your inventory of network devices to monitor, be sure to include both physical and virtual devices on your list. With the current trends in appliance and server virtualization, virtual switches (vSwitches) and virtualized application accelerators are important considerations when looking at network performance. Serving as network ports within the environment, vSwitches enable virtual machines to communicate with each other without having to traverse physical network adapters. While vSwitches speed inter-server communication, they don't enable a network monitoring tool to report these paths or receive application performance data. Fortunately, the networking industry has recognized the problem and is working to improve the situation, either with more intelligent vSwitches or through virtual server standards such as Virtual Ethernet Port Aggregator (VEPA), which would enable exposure of virtualized network traffic to traditional network monitoring tools.

COLLECTING DATA TO SET A NETWORK PERFORMANCE BASELINE

After taking inventory of network devices, the next phase is analyzing the traffic running across the infrastructure. While an overall network utilization is

a reasonable indicator of the overall health of the network, that single metric provides no context for what the users are actually doing on the network. In order to gain insight into how the network is being used, monitoring tools must collect and open actual packets of data.

There are two approaches to collecting network data for traffic analysis, each with its own pluses and minuses. Data capture or sniffing tools capture the entire stream of network data, giving administrators a full view of what is moving around the network at a given moment in time. Sniffing the network offers a complete view of what is going on. While this is vital for network forensic analysis and troubleshooting, it might be overkill for ongoing network monitoring and baseline analysis. For network performance monitoring, the metrics of application and network utilization are key, not necessarily the information within the individual packets. In these situations, network sniffing tools could provide the required information, but would do so with significant overhead.

GET SAMPLES WITH SFLOW/NETFLOW MONITORING
Alternatively, protocols such as NetFlow or sFlow are designed to be less storage intensive by capturing traffic at assigned intervals. Built into many enterprise routers, NetFlow and variants can pass along sampled data to a monitor

without the overhead of sniffers, providing a reasonable overview of which applications are running across the network. By performing packet analysis, administrators can see trends in application usage and assign a percentage of utilization for each application against total network usage.

Digging in deeper, most tools can also help parse out Internet traffic, separating, for example, use of cloud-based applications from general Web browsing. Knowing how much of the network each application consumes not only identifies the source of response time problems, but also enables administrators to see the impact of new applications and services as they are deployed on their networks.

HOW LONG MUST YOU MONITOR TO SET A NETWORK PERFORMANCE BASELINE?

With all of the desired monitors in place, the next step is to let the monitors run and build up data points. Many experts cite seven days as an effective monitoring window to allow performance trends to appear.

It is important to consider the context of when the traffic was captured. Cyclical usage patterns exist in most organizations and any traffic analysis should be sensitive to those patterns. A large retailer, for example, would no doubt see

network and application use spike during the holiday season. A manufacturer might actually see the opposite effect with plant shutdowns significantly lowering network utilization during the same holiday period. If the analyst does not account for these business cycles, network performance baseline results could vary widely in either direction.

Any significantly high or low spikes in the numbers must be identified and a determination must be made as to why they occurred and if they are indeed part of the network norm. If you see occasional spikes because of an identified problem, build the baseline on the remaining data points. If the spikes are identified as a common occurrence, include them in the average for the metric. It's also possible that the network experienced a significant problem during your monitoring cycle. In that case, it would be safer to toss those data points and rerun the metrics after the situation has been addressed.

When a reasonable amount of monitoring data has been collected and radical shifts have been accounted for, a baseline for each of the metrics can be assigned. The ultimate result is determining the typical range of values for each of your defined monitors. The combined set of ranges is the current network performance baseline.

The final point to consider is that the network performance baselines you

Home

How to set a
network perfor-
mance baseline for
network monitoring

set today are only good until something changes. Network equipment upgrades, new servers and new applications will have an impact on today's baselines and will require some care and feeding of the monitoring solution on an ongoing basis. The good news, however, is that in most cases, not everything changes at once, so a few tweaks can be made as applications, services or devices are added or removed.

FREE RESOURCES FOR TECHNOLOGY PROFESSIONALS

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

WHAT MAKES TECHTARGET UNIQUE?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.