Realtime publishers

The Essentials Series: Network Troubleshooting and Problem Identification

Bandwidth Monitoring and Traffic Analysis

sponsored by solarwinds

by Greg Shields

SUPER-CHARGE YOUR NETWORK WITH SOLARWINDS ORION POWER PACK!

The **Orion Power Pack** combines three of our most popular products to take your network management to the next level!

- **Orion NPM** delivers comprehensive fault and performance management across multi-vendor networks of any size.
- **Orion APM** extends Orion NPM's powerful monitoring capabilities to applications and servers.
- **Orion NTA** provides deep visibility into network traffic behavior and trends by leveraging NetFlow, J-Flow and sFlow data.

solarwinds

Bandwidth Monitoring and Traffic Analysis 1
Different Perspectives for Different Needs 1
Flow Analysis Provides a Big Picture View 3
Finding Resolutions to Common Problems 4
Focusing on the Right Features 5
Looking Forward 5

Copyright Statement

Bandwidth Monitoring and Traffic Analysis

Your company's network lines and the interstate freeways have a lot in common. Each is a necessary component of an overall system. When well designed, each provides a high-speed connection between two points within that system. And each, when oversubscribed, results in a less-than-desirable experience for its users. You can use this freeway analogy in many comparisons between what is considered good network performance—high speed, low latency, few collisions—and performance that doesn't meet acceptable levels. To put it simply, when there are too many cars on the road, nobody gets to their ultimate destination very quickly.

Taking the analogy a step further, monitoring and measuring both network and vehicular traffic works in much the same way. There are multiple ways in which network traffic can be monitored and measured for performance. Traditional packet-based monitoring tools enable peering into individual packets to determine their contents, the transactions between systems, and the details of communications being passed along that network. Yet the packet-based approach is a lot like attempting to determine the cause of a traffic jam by peeking into each individual vehicle. Knowing what people and cargo are travelling within each vehicle may be helpful in answering some questions, but it's not likely to illuminate the cause of the system-wide slowdown.

Different Perspectives for Different Needs

Bandwidth monitoring and traffic analysis are two key activities for every business environment. Performing each correctly assists the network administrator with identifying areas of bottleneck. It helps the admin identify the network needs and uses of servers and their hosted applications, as well as how the network needs of one IT service impacts another. It also delivers hard data that objectively verifies the ability of the network to meet stated Service Level Agreements (SLAs).

And yet the perspective gained through these two activities is different than what we nominally think of as *packet analysis*. Whereas packet analysis tends to look at network conditions from a very close-in perspective, bandwidth monitoring and traffic analysis step back to see conditions on the system as a whole. To help you understand the differences in perspective here, let's take a look at common ways used to measure traffic on a network:

- *SNMP monitoring of network devices*. Device monitoring using the Simple Network Management Protocol (SNMP) provides a very device-centric view of network conditions. Using SNMP, counters on a device such as a router, switch, or firewall can be measured and forwarded to a network management system for review. This data is useful for understanding performance conditions that are specific to that device such as processor or memory utilization; however, analysis suffers when attempting to see conditions that occur across multiple devices or on the system as a whole.
- *Protocol analyzers.* Protocol analyzers take a look at network conditions from the perspective of the packet. These tools analyze conversations between devices on the network from the location where the analyzer is measuring. This information gives the network administrator an extremely detailed view of individual transactions between two computers and the specific data being transferred between them. But this perspective also suffers when attempting to gather information across the entire environment.
- *Hardware probes and distributed analyzers.* Hardware probes and distributed analyzers are an early attempt to overcome the limitations of an individual protocol analyzer. These tools can be positioned all across the network for the gathering of information. They go far in providing the whole-system perspective that is so difficult to gather through the previous two perspectives. Yet because each individual probe requires separate management, administration, and maintenance, their use suffers from scalability issues as the network grows.
- *Traffic flow analyzers.* These tools overcome the administration headaches of hardware probes and distributed analyzers by leveraging the data flow capture capabilities of the network device itself. Generically referred to as NetFlow or NetFlow data due to the prevalence of Cisco equipment in most IT environments—NetFlow is a Cisco protocol—there are, in fact, multiple manifestations of these protocols: SFlow, JFlow, and IPFIX to name a few. Traffic flow analyzers receive flow data directly from monitored devices and analyze that data to gain the high-level perspective needed for troubleshooting incidents across the network system.

Flow Analysis Provides a Big Picture View

Consider the situation in which you, the network administrator, are notified that there appears to be a problem with the network. When you sit down to troubleshoot the problem and look through your available tools, which of them provides the best picture of the situation? Depending on the problem at hand, flow analysis tools can be superior to the others for a number of reasons:

- *Easy to use and understand.* The big picture perspective of flow analysis tools tends to result in visualizations that are easy to understand. Traffic patterns between devices are regularly gathered, allowing for the visual mapping of network capacity compared to network consumption. With the high-level view of the network map readily available and with drill-down capabilities into problem areas, you can quickly identify system-wide behaviors that might relate to the problem at hand.
- *High-level traffic flows rather than packet-level inspection.* Although packet-level inspection is exceptionally useful for identifying the specific communication between two or more computers, network issues are most often reported at a higher level. Having the ability to see high-level flows helps the troubleshooting administrator quickly isolate the problem before digging deeper into its resolution.
- *Common vendor support.* Flow analysis tools tend to support multiple vendor networks. This is especially critical considering that most networks are not completely homogeneous. With devices from multiple network vendors being positioned around the network, crossover support for the flow analysis tools of each means that a Cisco router can be monitored by the same tool that looks after a Juniper device or an application firewall.
- *Low cost and low administrative overhead.* Unlike the use of probes or distributed analyzers, individual devices typically include native flow capture capabilities. Enabling these capabilities and directing them towards network management systems for data collection involves little additional work, virtually all of which is completed during the device's initial installation.
- *Provides rapid answers to critical questions.* Although deep packet-level inspection capabilities are handy for some network problems, the most often questions usually asked of the network administrator often relate to "What is consuming my bandwidth?" and "Why is the network slow today?" Quickly finding answers to these questions requires a holistic understanding of the network, its connections, and the types and levels of traffic being experienced across network links. Information gathered through high-level tools can usually be later leveraged for a deeper discovery once the larger initial questions have been answered.

Finding Resolutions to Common Problems

To further explain how flow analysis improves a troubleshooting administrator's efficiency, let's take a look at three common issues seen on most business networks today. The first of these relates to resource overuse by a specific application. When an application on the network begins consuming more than its fair share of network bandwidth, its use will impact the capacity available for other network services. The problem with identifying these incidents using other types of network tools is that the reporting of problems tends to focus on the network service being impacted. For example, when the problem occurs, the network administrator usually starts with knowledge that Application B "is slow today." The job is then theirs to determine why the service is slow and what is inhibiting its desired level of performance. Using effective flow analysis tools, the administrator can easily view the traffic and usage patterns across the entire network to identify that Application A is actually the culprit. Conversely, using tools with a closer perspective may incorrectly focus the administrator's troubleshooting on Application B, while ignoring the impact of Application A.

A second and similar issue occurs when a specific protocol overconsumes network resources. Streaming protocols are an excellent example of this type of constant and predictable network flow. When users on a network make use of streaming applications, their consumption typically occurs at a constant level over an extended period of time. Different than transaction-based protocols, streaming protocols have the tendency to saturate available network resources due to the additive effect of multiple streams. One user making use of one stream may not be likely to cause a network problem, but 50 or 100 users employing an equal number of streams quickly begins saturating the network. Unlike packet-based tools that analyze individual pieces as they go by, flow analysis tools enable the identification of the source, destination, and protocol of streams across the network. The end result is the ability to craft effective network policies that enable streaming protocols where necessary while preventing those that negatively impact the functionality of the network.

A final area for which flow analysis tools are particularly well suited is during LAN and WAN optimization activities. In both the case of LANs and WANs, there occasionally comes the need to stand back from the network architecture and look for where improvements can be made. With the constraints of limited time and funding, these activities need to focus on solving the network's biggest problems first. Flow analysis tools, especially those with the ability to see historical traffic and usage patterns, deliver quantitative information to the network architect that allows them to make educated improvement decisions.

Focusing on the Right Features

To this point, this article has attempted to illustrate the differences between the vision gained through the use of flow analysis tools compared with others available to the network administrator. In much the same way that you don't measure the efficiency of interstate highway traffic by looking at the each vehicle's cargo, different network tools illuminate a different view of the network. The right tools include the right set of features for assisting with problem resolution and network management. When looking for products that fulfill your needs for flow analysis, consider those that include

- *Multiple vendor and protocol support.* Although the term *NetFlow monitoring* is often used to describe the kinds of flow analysis activities discussed here, NetFlow is only one of many protocols available on network devices today. An effective flow analysis tool will include the support for all currently available forms of network flow analysis irrespective of vendor (jFlow, sFlow, IPFIX, etc.). This ensures that your environment is not later forced into using network devices of a single manufacturer down the road.
- *Real-time and historical analysis capabilities.* Although most problems in network administration directly relate to how the network operates *right now*, the only effective way to ascertain today's behaviors is to view them in comparison with yesterday's or last week's. Effective flow analysis requires the capability to store and later review statistics over an extended period of time. This ability enables the network administrator to identify long-term traffic patterns and plan for growth.
- *Visualizations accessible from anywhere.* As a network administrator, you're not always sitting in your office. Problems and issues tend to pop up all across the network, some of which require on-site support. In these cases, having visualizations that can be accessed from anywhere—for example, using a standard Web browser—gives you the ability to take your toolset to wherever the problem exists.
- *Drill-down support.* With drill-down support built-in to flow analyzer's visualizations, it is possible to quickly move from the highest-level view down into specific problems as needed. Drill-down support reduces on-screen clutter, enabling a single-glimpse and high-level view of the network during periods of nominal activity.
- *Affordability.* Lastly, any toolset used in troubleshooting and resolving network issues must cost less than the amount of benefit it provides. Expensive solutions take longer to pay for themselves and may be more difficult to obtain in a time of shrinking IT budgets. Finding the tool that meets your needs at an acceptable cost is important to gaining the biggest return on your investment.

Looking Forward

The second article of this series will delve specifically into one difficult topic for many network administrators—namely, isolating the source of problems between the network and its hosted applications. As you'll find, the flow analysis capabilities discussed in this article are one of many tools used by troubleshooting administrators in determining the source of the problem.