Using NetFlow for Real-Time Performance Management

Introduction

Network managers must constantly balance the need to maximize network resources with the ability to foresee any potential negative performance impacts on critical business applications. This balancing act requires not only expertise but also the best possible suite of tools. By listening carefully to the needs of network professionals, SevOne has created a performance management solution that leverages the unique strengths of both SNMP monitoring and flow monitoring to provide real-time performance management, troubleshooting, and network reporting for a fraction of the cost of a traditional packet inspection-based system. And because this system uses a distributed, peer-based architecture for monitoring and reporting, it is more scalable, easier to implement, and more affordable to operate than any competing solution.

NetFlow Evolution

In the twelve-plus years since Cisco introduced its NetFlow IP traffic flow monitoring capability, it has grown to become one of the most widely adopted technologies for managing the huge array of devices and interfaces involved in modern enterprise-level networks. While NetFlow offers most of the functionality of traditional, expensive, resource-intensive packet inspection-based monitoring, it can be inexpensively implemented. This fact, combined with NetFlow’s scalability and the relative ease with which it can be deployed and maintained, has made it an attractive option for enterprise and service provider organizations around the world.

With the advent of NetFlow v9, the technology has seen significant improvements in functionality and customization. Most notably, users can now choose among 200+ fields to generate customized reports that meet their unique requirements. Based on the market adoption of earlier versions and the standardization of NetFlow v9 by the IETF as Internet Protocol Flow Information eXport (IPFIX), other firms have built their own unique “flavors” of flow-based monitoring, including J-Flow, sFlow, cFlow and NetStream.

How SevOne Leverages Flow-Based Monitoring

While NetFlow is an excellent tool, most implementations still involve some degree of manual synchronization between flow-based monitoring and other network monitoring systems. The SevOne Performance Appliance Solution (SevOne PAS™) was designed from the ground up to leverage the unique strengths of both high-capacity NetFlow-based collection and SNMP-based monitoring, unifying both approaches in a single user workflow. In practical terms, this means that users can react instantly to utilization spikes and other performance alerts from any polled data source, seamlessly drilling down through NetFlow to determine what applications, devices, and addresses are involved.

The NetFlow approach to traffic analysis is an alternative to packet-sniffing systems since NetFlow-based systems focus on network traffic accounting – examining information about flows of packets instead of examining the content of packets. The SevOne solution is far more scalable and cost-effective than packet-based monitoring solutions that require probes for each node on a network. SevOne can monitor the most complex global networks, encompassing tens of thousands of interfaces, with fewer than a dozen appliances.

“One of the major challenges facing any Application-Aware Network Performance Management solution is scalability for data collection, analysis, and presentation/reporting. I was impressed by SevOne’s best in class scale for flow record collection and lightning-fast viewing and reporting enterprise-wide.”

Jim Frey, Enterprise Management Associates
Integrated Monitoring, Alerts, Troubleshooting and Analysis

As mentioned above, SevOne provides one-click navigation between alerts and the relevant NetFlow data for the network device in question, a capability SevOne calls “Universal Metric to Flow”. In practice, this allows users to retrieve rich, detailed reports within seconds of being alerted about a change in a key performance indicator. The reports yield information on every aspect of the event, including all associated devices and users. By instantly generating reports that allow network engineers to trace the issue back to its source, the system greatly reduces troubleshooting time, and helps identify and diagnose problems before they have a significant impact on network performance.

To further understand Universal Metric to Flow the following case study explains a typical workflow. The SevOne Alerts dashboard provides a notification indicating that the core data center switch has exceeded the threshold set by the network administrator. The administrator then generates an instant graph of the network traffic data during the timeframe of the alert, illustrated in the subsequent diagram.

Once the event has been identified, the administrator can highlight the specific time of the event to zoom in for more detail resulting in the next graph.

By selecting a more granular time period and then clicking on the NetFlow button, the administrator can immediately generate a report based on NetFlow data displaying the top talkers during the highlighted period of degraded performance, as shown in the next report.
The top talker report reveals one very high and several high bandwidth consumers; however, further investigation requires more information. The administrator clicks on the drill down button to identify the destination IP address for the traffic as shown below.

The administrator now sees that all of top talker traffic has the same destination IP address and can drill down again to view the type of service and next hop.
Now the administrator sees a series of high port numbers from multiple residential addresses all terminating at the same destination address. Many readers will no doubt recognize the familiar signature of BitTorrent traffic in this chart. From here, the user in question may be due for a (potentially awkward) conversation about unauthorized downloading during business hours, or a report may be exported in PDF format and e-mailed to the user or manager.

**Deep Flow Inspection**

Deep Flow Inspection is, as some SevOne engineers have dubbed it, “a techie’s dream.” In essence, the system is designed to provide as much detail and depth as users could possibly want from a flow-based solution. For example, users can take individual NetFlow fields, dissect them, and extract information in ways that are simply beyond the capabilities of other tools. Take for example, the NBAR field, which provides information on application recognition. This field is composed of both engine ID and application ID. Using SevOne, a user can actually break up this field into its components, storing and examining them as two separate SevOne fields. This best-in-class level of user control lets users gain a deeper understanding of what they consider most important for the proper functioning of their networks.

**Maximize the Expanded Functionality of NetFlow v9**

One of the significant improvements that Cisco has made to version 9 of its NetFlow system is the inclusion of user-definable fields for collection templates. With over two hundred customizable data ranges that can be monitored and reported on, network managers have a unique opportunity to generate custom templates that deliver precisely the information that they need.

Of course, sifting through hundreds of options can also make generating those templates a significant investment of time and effort. With an eye toward saving users’ valuable time, SevOne has included a library of pre-defined templates that leverage some of the most useful and interconnected fields in NetFlow. By tweaking SevOne’s templates, instead of generating new ones from scratch, engineers can leverage industry best practices and save significant time and effort.

**Reporting**

SevOne’s reporting interface is designed to maximize the ease and customizability of use. As mentioned above, a single click is sufficient to generate a flow-based report synchronized to an SNMP alert. But the interface truly shines when it comes to turning
those reports into compelling, easy-to-grasp documents. Each report generated via the system can be detached, and then appended to a unified reporting document generated on the fly based on each user’s specifications. Users can quickly create a report, analyze, chop, and reconfigure data, place it side-by-side for maximum impact (for example, aligning SNMP and flow-based reports of the same event on a single page), and convert it quickly to a PDF or other document format. Within minutes, users can both identify the source of a network issue, and generate a concise, rich, and colorful report that explains their findings to others.

From the customizable SevOne dashboard, network managers may choose from Instant Graphs, a Network Overview, Report Manager or Telephony-specific reports.

When selecting Instant Graphs, network managers may choose a pre-defined report provided by SevOne, a previously saved user-defined report, or a new report may be defined with a few clicks of the mouse. In the diagram below, a new report maybe created by choosing from the NetFlow fields on the left, and adding them to the report fields on the right.
In this case, the network manager selects four items and saves the template successfully.

The resulting report is shown below.

Distributed Architecture

With most monitoring solutions, reporting bottlenecks are nearly inevitable, as a host of monitoring appliances must all feed information to a central reporting hub. On the other hand, SevOne’s peer-to-peer-based architecture means that every collector handles its share of any reporting requirements, avoiding potential bottlenecks. When a user logs into SevOne from any point on the network, he or she can issue a reporting query, and each device will handle the subset of the query that relates to the devices in its area. All reports are then returned to the peer appliance that issued the request, which assembles the final report, delivering it to the user’s browser.
In effect, this peer-based system means that the SevOne system has no practical limits. Given that each additional networked collector expands the system’s reporting and storage capabilities, the system can scale in a linear fashion as a network grows. A single appliance can handle up to 15 million flows per minute.

**Data Retention**

In its standard configuration, SevOne’s system is designed to collect raw, unaggregated flow data, sampled at one-second intervals, for up to seven days at a time. Beyond that point, the system stores aggregated data, and top 200 results per template at one-minute, fifteen-minute, sixty-minute, and one-day intervals. Obviously, clients with storage requirements in excess of these parameters can have those needs met through expansion of standard storage devices.

The raw flow data retention period is a unique and particularly useful aspect of SevOne’s approach. Whereas many other tools wouldn’t be able to offer insight into micro-spikes, DNS storms, or other brief events that can cause network disruptions, the SevOne system provides sufficient granularity over the short term to allow real-time analysis. Even in aggregated form, the system stores 99.8% of data—representing the highest degree of granularity in the industry.

To illustrate the value of granular data retention, consider the following use case. A network administrator examining a graph of traffic summarized to 1-minute granularity observed a spike up to 5.23 megabits in network traffic.

The graph below examines the same time period at 1-second granularity. Notice that the spike actually peaks at 8.07 megabits.
Thanks to the system’s retention of granular data, network administrators can ensure that critical, near-term troubleshooting information will not be missed. Bursts of short but intense traffic often occur in seconds or milliseconds. Resolution of these issues, which may be caused by improper QoS settings, can only occur with the most granular reporting possible.

In the case of such common problems as clicks and noises on voice over IP calls or pixilation during video conferencing, the only way to determine the cause is raw, unaggregated data provided by SevOne.

Conclusion

The SevOne NetFlow solution for network performance monitoring, reporting and troubleshooting provides network managers with a best-in-class product that reduces the time required to identify and resolve network issues that impact business productivity, while at the same time providing global, scalable, integrated SNMP and NetFlow monitoring. And all of this is achieved at a fraction of the cost of a packet-based monitoring solution.

About SevOne

SevOne, Inc. delivers the industry’s fastest, most scalable, and comprehensive real-time network monitoring, troubleshooting and performance reporting solution. SevOne created a proprietary, next-generation distributed technology, called the SevOne Cluster™, that combines the cutting edge principles behind peer-to-peer sharing and big data clusters to scale smoothly so that millions of network elements, across all monitoring technologies, can be monitored and provide a single view to the user. Hundreds of customers, including the top cable companies in North America, wireless network and managed service providers, and top financial services institutions rely on SevOne. Visit www.sevone.com.