



# Network Traffic Analysis Using Cisco NetFlow

*Taking the Guesswork Out of Network Performance Management*



# Network Traffic Analysis Using Cisco NetFlow

*Taking the Guesswork Out of Network Performance Management*

## EXECUTIVE SUMMARY

Many enterprise networks are being pushed to the limit, forced to accommodate more business-critical applications, more users and more data than ever before. As a result, network administrators are under increased pressure to improve availability, optimize application performance and solve performance problems faster.

Adding bandwidth isn't necessarily the answer: Many organizations over-provision bandwidth to minimize performance bottlenecks, but often that only serves to increase costs while masking underlying problems.

Network slowdowns are frequently symptoms of more serious concerns, including:

- non-mission-critical traffic taxing network resources — end-users downloading MP3 or video files
- network configuration problems
- internal and external security breaches, malware and denial-of-service (DOS) attacks

Administrators need complete visibility into the network in order to resolve these problems as well as to optimize the network infrastructure and make informed infrastructure investment decisions. Unfortunately, most administrators lack the tools they need to truly understand network traffic behavior.

Now, SolarWinds' Orion NetFlow Traffic Analyzer enables administrators to leverage the existing infrastructure for sophisticated measurement and analysis of traffic across the enterprise network. Providing a holistic view of network bandwidth usage, Orion NetFlow Traffic Analyzer helps you:

- improve availability and performance
- speed problem resolution
- align network capacity to business requirements
- support new services to meet business objectives
- identify the source of security breaches

## THE NETWORK PERFORMANCE CHALLENGE

In many organizations, network performance management is largely a matter of guesswork. However, this approach can be quite costly in terms of IT resources, business productivity and end-user satisfaction. Organizations often spend thousands of dollars each year simply identifying and isolating network problems — not fixing them.

In fact, many organizations have decided that it's less expensive to provision a larger circuit than to try to diagnose what's going on inside the network. But while bandwidth is cheap and getting cheaper, an increasing number of latency-sensitive applications are changing the network performance equation. It's no longer enough to throw bandwidth at the problem — administrators need quantifiable network performance data that shows them which users and applications are consuming network bandwidth.

In the past, gaining such insight required the use of expensive and complex hardware probes to gather network traffic data. Network probes can be configured to capture data on a wide range of protocols in real time with no additional load on the network. However, such probes require a significant capital investment and incur ongoing support costs because administrators must maintain the probes at strategic points throughout the distributed network. Network probe solutions aren't readily scalable — probes must be added to monitor different types of traffic and upgraded as network bandwidth increases.

Network administrators need solutions that minimize the effort and cost of gathering network traffic data. Cisco NetFlow traffic analysis can provide a granular understanding of bandwidth usage without the overhead associated with hardware probes.

### What Is NetFlow?

NetFlow is an open protocol developed by Cisco Systems for collecting IP packet information without the cost and complexity of hardware-based network probes. Built into routers and switches from Cisco and other vendors, NetFlow captures detailed information on streams of data that share a common source, destination and protocol — so-called network traffic flows.

Utilizing Cisco NetFlow generally requires no capital investment as most networks already include NetFlow-capable devices. NetFlow is easy to deploy and configure — administrators need only turn on the NetFlow data and enter a few commands to begin measuring all IP traffic across the network. And NetFlow is automatically scaled and upgraded as the organization maintains its Cisco router infrastructure.

---

**Organizations often spend thousands of dollars each year simply identifying and isolating network problems — not fixing them.**

---

## ORION NETFLOW TRAFFIC ANALYZER

A typical enterprise network will have thousands of connections generating massive amounts of NetFlow data in only a short period of time. SolarWinds' Orion NetFlow Traffic Analyzer collects and consolidates raw NetFlow data and transforms it into useful graphs, charts and tables that help administrators understand what's going on inside the network. With Orion NetFlow Traffic Analyzer, network administrators can more effectively:

- improve overall network performance
- support latency-sensitive applications such as voice over IP (VoIP) and video
- better manage traffic spikes
- enforce network policies
- expose traffic patterns that point to malicious activities

Orion NetFlow Traffic Analyzer also helps administrators understand what percentage of network resources is being consumed by each data type at any given time. The network engineer can see at a glance how much bandwidth is being used by e-mail, accounting and ERP systems, and other applications, as well as how many users are watching YouTube videos or making Internet phone calls during the work day. Orion NetFlow Traffic Analyzer also helps pinpoint unauthorized activities so administrators can address them very quickly, reducing the impact of potential security breaches.

Orion NetFlow Traffic Analyzer utilizes a top-down approach to help administrators isolate problem areas and then drill down to find a particular chokepoint on the network. This combination of broad overview and detailed analysis enables network engineers to diagnose problems faster and easier than ever before.

### Unique Value Proposition

A number of companies offer network traffic analysis solutions based upon NetFlow data. However, many of these products place significant limitations on an administrator's ability to identify and resolve network performance problems. Orion NetFlow Traffic Analyzer transcends these limitations to create an intuitive, real-time analysis tool that provides unique insight into the network.

Orion NetFlow Traffic Analyzer presents NetFlow data in a consumable form that enables administrators to easily drill down into more details. Network engineers can examine traffic flows by user, application, department, conversation, interface and protocol via a unified console that provides

---

**Orion NetFlow Traffic Analyzer also helps administrators understand what percentage of network resources is being consumed by each data type at any given time.**

---

point-and-click access to comprehensive charts and detailed reports. This information becomes available within minutes of starting the software. While competitive products deal with the massive amounts of NetFlow data by preprocessing it, Orion NetFlow Traffic Analyzer provides information in real time. Administrators get NetFlow data on demand, whenever they need it, rather than on a prescheduled basis.

Many applications only store NetFlow data for a few days, but SolarWinds places no limitations on NetFlow data storage. An optimized storage engine intelligently summarizes large amounts of raw NetFlow data, giving administrators quick access to historical data while reducing storage costs. The solution is Windows-based and data is stored in an open SQL database, resulting in a stable, reliable tool that requires minimal maintenance.

### Fully Integrated Solution

Given the growing complexity of today's networks, administrators need tools that can correlate traffic analysis with performance, configuration and other information. Orion NetFlow Traffic Analyzer is tightly integrated with the entire suite of SolarWinds products to create a top-down and bottom-up view of the network.

It is available as an add-on module to the Orion Network Performance Monitor platform, enabling network engineers to drill down from broad views of performance data to detailed views of traffic patterns. Orion Network Performance Monitor alerts administrators of areas of heavy traffic, and NetFlow Traffic Analyzer helps the engineer determine the root cause of such traffic spikes.

Orion NetFlow Traffic Analyzer can be utilized in conjunction with SolarWinds' Cirrus Configuration Manager to increase availability, improve security and ensure policy adherence. Cirrus is a comprehensive, intuitive solution designed to streamline and automate network configuration management.

SolarWinds offers free evaluation versions that can be downloaded from [www.solarwinds.net](http://www.solarwinds.net).

---

**Many applications only store NetFlow data for a few days, but SolarWinds places no limitations on NetFlow data storage.**

---

## **SOLVING REAL-WORLD PROBLEMS**

SolarWinds customers can use Orion NetFlow Traffic Analyzer to resolve many of the real-world problems that plague today's complex, heterogeneous networks. Network engineers can address network slowdowns in real time, better understand cyclical issues, application-specific traffic spikes and performance trends, and make informed decisions regarding capacity planning and security.

### **Real-Time Diagnostics**

*Example:* Voice over IP calls to the Dallas office are either failing or the voice quality is very poor and broken.

*Analysis:* After reviewing the data collected by Orion and the NetFlow Traffic Analyzer, it became apparent that the VoIP issues were related to variations in latency (jitter) caused by a lack of available bandwidth. Further investigation revealed that several users in the Dallas office were logged into YouTube.com viewing videos.

*Solution:* Using Cirrus Configuration Manager, the network administrator created an access list to temporarily block access to YouTube and similar sites from within the Dallas sales office. Telephone operation immediately went back to normal.

### **Cyclical Issues**

*Example:* A backup process for the account database fails at the same time each day, apparently due to network problems.

*Analysis:* Using the Orion NetFlow Traffic Analyzer, the network administrator determined that, all of the largest databases within the enterprise were trying to complete their daily backups across the same network link during this same 30-minute window.

*Solution:* The administrator offset the database backups by 30 minutes each so that bandwidth is not over-utilized.

### **Impact Study**

*Example:* After the new ERP system was deployed, several network users who rely on the network for voice and data transfers noticed network performance degradation.

*Analysis:* Upon reviewing statistics collected by the Orion NetFlow Traffic Analyzer, it became apparent that while the total amount of traffic on the WAN link was not normally exceeding the committed available bandwidth, there was no prioritization of time-sensitive data vs. non-time-sensitive data on the network.

*Solution:* The network administrator implemented QOS and weight fair queuing on all WAN circuits to alleviate the problem.

### **Capacity Planning**

*Example:* A planned acquisition will add dozens of users and several applications to the network overnight.

*Analysis:* By reviewing data within the Orion NetFlow Traffic Analyzer the network administrator was able to estimate the additional load that these users and applications will create on the network by comparing them to similar activity already on the network.

*Solution:* The network administrator recommended that the organization order additional bandwidth in order to maintain current service levels.

### **Security**

*Example:* Internet connectivity from one of our remote offices is sporadic and network performance is awful.

*Analysis:* Through a review of data collected via NetFlow, the network administrator is able to see that a disgruntled employee was scanning the network from several remote hosts, searching for a way in and creating a DOS attack.

*Solution:* The network administrator uses Cirrus to block the IP range that the ex-employee was sending data from and all was good.

## CONCLUSION

Due to the high cost and complexity of traditional hardware probes, organizations often add bandwidth to alleviate network slowdowns rather than invest in traffic analysis and reporting tools. Unfortunately, adding bandwidth is a band-aid at best. As more latency-sensitive applications such as voice and video are added to the network, administrators need tools that enable them to effectively troubleshoot performance problems as well as plan for future growth and expansion.

Network traffic analysis using Cisco NetFlow data provides needed visibility into the network utilizing the existing network infrastructure. Armed with detailed performance data, administrators no longer have to rely on end-user finger-pointing and “best guess” analysis for network troubleshooting. Network engineers locate problems and determine their root cause.

SolarWinds’ Orion NetFlow Traffic Analyzer is a powerful tool that gives network engineers a centralized, comprehensible view of real-time and historical NetFlow performance data. Its easy-to-use interface and top-down approach enables administrators to productively and cost-effectively address network performance challenges. With Orion NetFlow Traffic Analyzer, organizations are better positioned to meet business objectives through optimized network performance and availability.