NetFlow Tips and Tricks

Introduction

Managing enterprise networks is a huge responsibility and with today's organizational environment, network administrators are now tasked with deploying advanced network services, maintaining network performance, and reducing costs with fewer resources. With these new challenges, administrators are facing tremendous pressure to maintain network uptime and prevent any organization-wide operational loss due to network problems.

One of the biggest factors impacting your network performance is network traffic and bandwidth usage. With more personal devices hogging enterprise network bandwidth, network managers are deploying new policies to maintain the quality of service. Although there are multiple ways to manage your network, flow-based network monitoring is the most sought after approach to managing todays' networks. By understanding these technologies, network administrators can take advantage of the flow technology that's built into routers and switches. Now, IT professionals can **monitor, troubleshoot, and solve bandwidth related problems** rather easily compared to earlier processes.

NetFlow and other Flow Technologies

Network problems seem to be a never-ending condition for administrators who are charged with both maintaining network performance and delivering advanced network services to their organizations. Couple this with the restraint in IT budgets, increasing pressure to ensure constant uptime, the need to manage existing resources, and the need to control costs. For network engineers, troubleshooting network related problems and solving bandwidth issues can be achieved by understanding more about NetFlow and other flow technologies.

What is NetFlow?

NetFlow is a network protocol developed by Cisco® Systems for collecting IP traffic information. It has become the universally accepted standard for traffic monitoring and is supported on most platforms. NetFlow answers the questions of who (users), what (applications), and how network bandwidth is being used. Some of other flow technologies include:

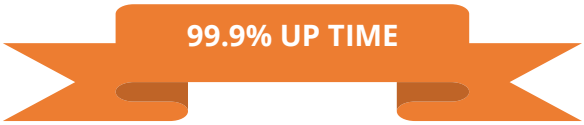
Flow Format	About
IPFIX	IETF standard for flow export. Customizable and template based like NetFlow. Available on Barracuda®, Extreme® Switches®, Sonicwall®, etc.
sFlow®	Sampling based 1 in N 'packets' captured by traffic analytics. Supported by most vendors, namely Alcatel®, Brocade® – Foundry, Dell® – Force 10, Enterasys®, Extreme XOS®, Fortinet®, HP® ProCurve, Juniper®, Vyatta®, etc. (http://sflow.org/products/)
J-Flow™	Juniper's proprietary protocol for flow export from Juniper routers, switches, and firewalls.
NetStream®	A variation of NetFlow supported on Huawei®/3COM devices.

NetFlow Tips and Tricks

By using NetFlow, monitoring your network traffic not only becomes much easier but also provides greater visibility by collecting and analyzing the flow data in your network. In this document we will discuss some everyday use cases that you may not have considered.

Tech Tip – 1: Troubleshooting Network Issues

Network uptime is critical to an organization's revenue. Understanding your network traffic behavior helps you maintain uninterrupted service. Excessive use of network bandwidth by users and applications can be controlled by identifying the top talkers from real-time and historical flow data. Because NetFlow data contains information about network traffic, it helps network administrators to attend to issues related to application slowness and network performance degradation.



Using NetFlow you can:

- Identify the hosts involved in a network conversation from the source and destination IP addresses, and its path in the network from the Input and Output interface information.
- Identify which applications and protocols are consuming your network bandwidth by analyzing the Source and Destination Ports and Protocols.
- Analyze historical data to see when an incident occurred and its contribution to the total network traffic through the packet and octet count.
- Ensure the right priorities to the right applications using ToS (Type of Service) analysis.

Flow data helps keep track of interface details and statistics of top talkers and users, which can help determine the origin of an issue when a problem is reported. Type of Service (ToS) in NetFlow records helps you understand traffic pattern per Class of Service (COS) in a network. By verifying Quality of Service (QoS) levels, optimizing bandwidth to your network requirements becomes much easier.

Additionally, NetFlow data helps you to analyze usage patterns over a particular time, find out who or what uses most of the network bandwidth, and provides support to **quickly troubleshoot application and performance related problems** in the network. You can manually collect flow data from each switch or router but the analysis of the data becomes increasingly difficult as your network size and complexity grows. By using a NetFlow analyzer, you can automatically capture NetFlow data from different points in your network and convert them into easy-to-interpret information that will help with better management of your network.

Tech Tip – 2: Network Anomaly Detection

One of the biggest threats that organizations face today is related to network security. Many network security issues are caused by Malware, Distributed Denial of Service (DDoS) attacks, and unknown applications running on well-known ports—all of which can be difficult to detect. To combat these security threats, Network Administrators can use NetFlow and other flow technologies to monitor and detect abnormal network traffic patterns that can affect their network's performance.

What can cause Network Anomalies?

Two common ways that network anomalies can be introduced into your network are telecommuting and Bring Your Own Device (BYOD). Both increase the risk of malware being introduced directly into your network after having been infected through an external

source. Additionally, the network could be hosting a bot that was introduced through one of these sources.

Anomaly Detection

In an enterprise, administrators try to secure their network by having an Intrusion Detection/Prevention System (IDS/IPS) which collects data and operates based on signatures to identify the threats, while routers and firewalls work based on access control rules defined by users. As explained in the image above, if a zero-day malware enters the network, it can be very hard to detect by routers, firewalls or even by IDP/IPS systems. A bot, hosted on a network, won't be detected by firewalls or IDS/IPS because they track only the inbound traffic, whereas bots contribute more to the outbound traffic. A non-signature IDS/IPS system is an expensive alternative.

Finding an anomaly in your network can be difficult, but there are symptoms that can be identified such as a sudden rise in network traffic, off-baseline network traffic behavior, unusual peaks, and traffic abnormally focused on certain parts of network/ports/IPs, and new applications hogging most of the bandwidth or generating abnormal traffic patterns. Some specific cases you should watch for are a high volume of outbound SMTP traffic, intermittent and short bursts of UDP packets, conversations from one host to many on the same port, traffic on unknown ports, too many TCP SYN flags, traffic from and to IANA reserved IP Addresses, etc...

By collecting flow data from all devices at a single point, analyzing the traffic patterns, and looking out for unexpected traffic behavior, network administrators can detect anomalous

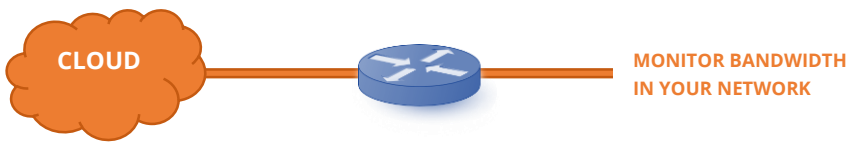
network traffic behavior. One can diagnose specific time periods in the NetFlow records to find what caused an outage that occurred, for example, during the weekend or when everyone was away from the office.

Tech Tip – 3: Tracking Cloud Performance

The growing demand of cloud based applications and its increased rate of adoption has resulted in massive pressure on network administrators. When implementing cloud services, it's imperative that enterprises have continuous network uptime for necessary operational processes. Any issues with the network or the speed of service can have an adverse business effect. One of the biggest impacts of cloud applications and services is on a network's bandwidth. Cloud and Software as a Service (SaaS) based approaches mean you need to ensure enough bandwidth is available for business critical applications to run uninterrupted processes 24x7. Any network downtime can cause a huge enterprise-wide operational loss and potentially affect the organization's bottom line. Some of the problems that network administrators face while using cloud applications include:

- Impact on bandwidth by cloud applications
- Operational loss if a mission critical cloud application is down
- Bottlenecks in the enterprise network
- Bandwidth hogs by other applications
- Unauthorized protocol and application usage

Ensuring continuous cloud application usage



Analyzing NetFlow data helps to monitor the network performance as continuous uptime is an absolute necessity for the enterprises who use or host cloud applications. It's important for network administrators to lookout for bottlenecks, bandwidth hogs, and unauthorized protocol and application priority. NetFlow data carries information on:

- Cause of traffic bottlenecks
- Different end points using enterprise bandwidth
- Applications being used in the network
- Conversation priority within the network

NetFlow gives network administrators insight and helps them prioritize hosted applications and deploy Quality of Service (QoS) policies. It provides the means to track the cumulative usage of a given application in an aggregate manner, down to specific regions, if necessary. As a result, NetFlow information can be used to verify whether the cloud usage behavior matches your service level agreement by mapping your actual activity between the cloud and your network. Measuring latency is challenging while operating on the cloud, but by using flow exporters like nProbe™, you can identify bottlenecks by analyzing the data through NetFlow collectors and demand that cloud providers deliver the promised service.

Tech Tip – 4: Monitoring BYOD Impact

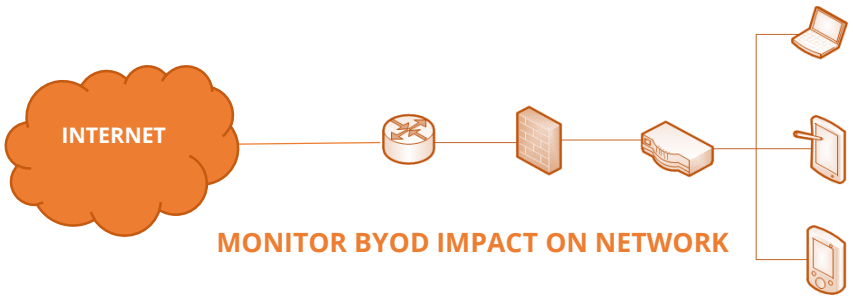
The trend of Bring Your Own Device (BYOD) has complicated even further the already complex nature of today's networks. In order to increase productivity, many organizations now encourage the usage of BYOD and telecommuting. With that, network administrators have added another burden to the list of problems that they already face. With an increase in personal devices, businesses of all sizes are trying to solve bandwidth problems caused by BYOD.

Managing BYOD without concrete policies can create significant issues for network administrators. Some of these include:

- Increased usage of BYOD for personal reasons
- Compromise in security and network integrity
- Bandwidth bottlenecks
- Increase in access by unauthorized applications
- Problems with existing QoS policies

How NetFlow helps to monitor BYOD

BYOD is going to add more traffic to your network and understanding its impact on your network's bandwidth is imperative. Blocking unauthorized applications from hogging your network bandwidth is essential to having more optimal network usage as these unknown applications compete with business applications.

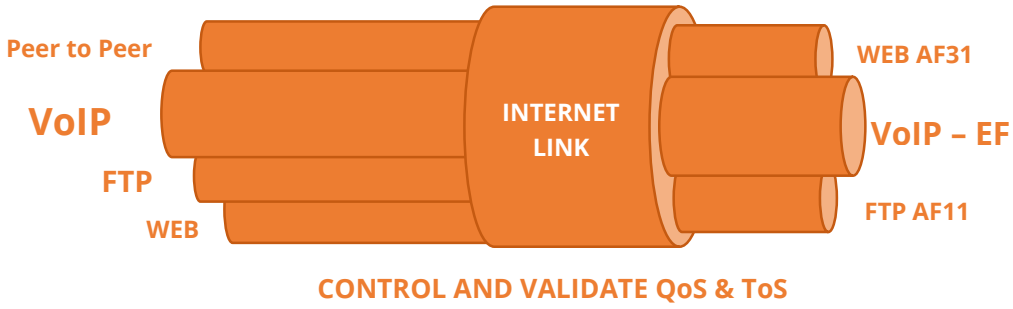


NetFlow helps breakdown the BYOD bandwidth usage by monitoring what kind of applications are being used, and by identifying the sources and destinations of the increased traffic. In depth tracking through NetFlow provides real-time information on network traffic and BYOD monitoring begins at the access layer, closer to the traffic source. By Implementing QoS policies across the network and looking at data from NetFlow, you

can find where all the traffic is heading to and restrict bandwidth to applications which have low priority.

Tech Tip – 5: Validate QoS and ToS

Rogue applications can block network bandwidth, which in turn could result in an interruption of important business applications. Because of this, it's important to define Quality of Service (QoS) and set priorities for various applications. Prioritizing bandwidth according to your needs is a critical strategy for network managers. As an example, 50% of your bandwidth can be set to VoIP applications that are business sensitive, while other non-critical applications are allocated lower bandwidth. Thus by defining QoS classes and assigning policies, network administrators can set predefined actions to be triggered under specific cases.



.

As explained in the image above, applications will compete with each other when traversing the WAN and because bandwidth is neither infinite nor free, it only makes sense that you'll want to see how your bandwidth is being used. Since NetFlow data reports on Type of Service (ToS) and DSCP fields from traffic conversations, you can monitor your bandwidth usage by application and measure the effectiveness of your QoS policies.

Tech Tip – 6: Capacity Planning

NetFlow helps administrators plan network capacity more accurately—by deploying greater bandwidth for advanced networking services—as organizations scale up. Using NetFlow, one can easily check if bandwidth growth is aligned with resources utilized in the current environment and plan for the future. This will allow network managers to more easily monitor bandwidth consumed by applications.

Capacity planning using NetFlow can also help network administrators implement QoS policies and prioritize mission critical applications by characterizing traffic. By distinguishing different types of network traffic like voice, email and other applications, administrators can analyze and understand the QoS policies they have implemented. Top applications and conversations based on NetFlow data can be stored for reference unlike PCAP, which requires extensive storage.

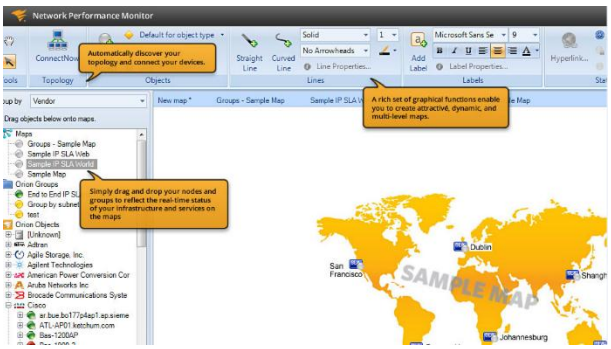
Capacity Planning will help enterprises collect more NetFlow historical data and compare the trends with the organization's network. This helps to allow enough bandwidth for critical applications and prevent any anomalies to enter the network. Having NetFlow for capacity planning will also assist in scaling up the network according to needs and utilize the available bandwidth in a better way, ensuring good resource alignment and capacity planning.

About SolarWinds Bandwidth Analyzer Pack

SolarWinds Network Bandwidth Analyzer Pack includes everything you need to monitor network availability, performance, bandwidth and traffic. It's a comprehensive Network Bandwidth Analysis & Performance Monitoring solution which can detect, diagnose, and resolve network performance issues; track response time, availability, and uptime of routers, switches, and other SNMP-enabled devices; monitor and analyze network bandwidth performance and traffic patterns; identify bandwidth hogs and see which applications are using the most bandwidth; and graphically display performance metrics in real time via dynamic interactive maps.

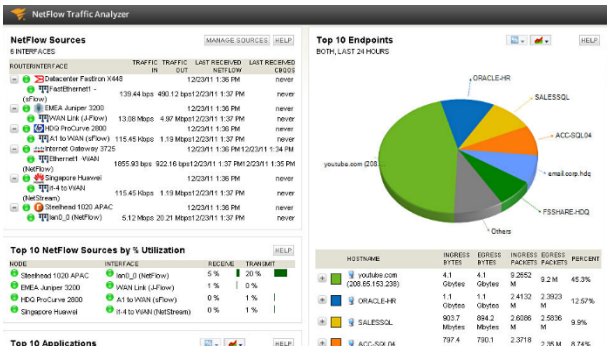
Product Highlights:

SolarWinds Bandwidth Analyzer Pack features Network Performance Monitor and NetFlow Traffic Analyzer. With **Network Performance Monitor**, you can quickly detect, diagnose, and resolve performance issues and deliver real-time views and dashboards that enable you to visually track network performance at a glance.



- Simplifies detection, diagnosis, and resolution of network issues.
- Tracks response time, availability, & uptime of routers, switches, and other SNMP-enabled devices.
- Shows performance statistics in real time via dynamic, drillable network maps and includes out-of-the-box dashboards, alerts, and reports.

With **NetFlow Traffic Analyzer**, you can leverage flow technology to get insight on network bandwidth performance and traffic patterns with real-time visibility into whom and what are consuming network bandwidth.



- Find network bandwidth hogs.
- See which applications are using the most bandwidth.
- Discover traffic patterns & device performance.
- Prioritize business critical applications.
- Validate effectiveness of CBQoS policies.

About SolarWinds

SolarWinds (NYSE: SWI) provides powerful and affordable IT management software to customers worldwide from Fortune 500 enterprises to small businesses. In all of our market areas, our approach is consistent. We focus exclusively on IT Pros and strive to eliminate the complexity that they have been forced to accept from traditional enterprise software vendors. SolarWinds delivers on this commitment with *unexpected simplicity* through products that are easy to find, buy, use and maintain while providing the power to address any IT management problem on any scale. Our solutions are rooted in our deep connection to our user base, which interacts in our online community, **thwack**, to solve problems, share technology and best practices, and directly participate in our product development process. Learn more today at **http://www.solarwinds.com/**.

Learn More

For product information or to purchase SolarWinds products, visit solarwinds.com, call, or email:

Americas
Phone: 866.530.8100
Fax: 512.857.0125
Email: **sales@solarwinds.com**

APAC
Tel : +65 6593 7600
Fax : +65 6593 7601
Email: **sales@solarwinds.com**

EMEA
Phone: +353 21 5002900
Fax: +353 212 380 232
Email: **sales@solarwinds.com**

3711 South MoPac Expressway, Building Two, Austin, Texas 78746