



 eBOOK

Go With the Flow Crash Course

What You Need to Know About NetFlow (And Other Flow Data)

Table of Contents

1	CHAPTER 1: FLOW DATA – WHAT IS IT? HOW CAN IT HELP?	3
	What is flow data?	3
	How do I use it?	4
	Homework	4
2	CHAPTER 2: TROUBLESHOOTING NETWORK ISSUES	5
	Homework	5
3	CHAPTER 3: TRACKING CLOUD PERFORMANCE	6
	Ensuring continuous cloud application usage	6
	Homework	7
4	CHAPTER 4: VALIDATING QUALITY OF SERVICE POLICIES	8
	Homework	8
5	CHAPTER 5: CAPACITY PLANNING	9
	Homework	9

Go With the Flow - Crash Course

Whether you've been monitoring networks for years or are just starting out in the industry, check your methods against our tips and tricks to getting the most out of your flow data. We've also assigned some homework for each crash course to help you dive deeper into the material and/or put these lessons into practice.

CHAPTER 1: FLOW DATA – WHAT IS IT? HOW CAN IT HELP?

Managing enterprise networks is a huge responsibility. In today's organizational environment, network administrators are tasked with deploying advanced network services, maintaining network performance, and reducing costs, often with fewer resources. Administrators are facing tremendous pressure to maintain network uptime and reduce operational loss due to network problems. Among the biggest factors that affect network performance are network traffic and bandwidth usage.

What is flow data?

Flow data export is configurable on almost all network gear, making it an inexpensive option to gain visibility into application traffic. Network administrators can use flow data to more easily monitor, troubleshoot, and solve bandwidth-related problems.

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 routing platforms. NetFlow answers the questions of who (endpoints), what (applications), and how much (network bandwidth) is being used. There are different flow export technologies, such as IPFIX, J-Flow™, and NetStream®, which are used by other network hardware vendors, as well as sFlow®, which is traffic sampling-based and also supported by most vendors.

Fast fact: You may hear flow data referenced as "NetFlow" even when data from other vendors is included. This is because Cisco drove the industry standard for flow data with NetFlow, but the flow type available is dependent on the hardware vendor. Be sure to confirm that any flow data traffic analyzer you consider can handle multiple types of flow data so you have full visibility into the traffic across your network.

How do I use it?

Once your device is configured to send flow data, you can use a flow data analyzer to gain deeper insights into the traffic and bandwidth use on your network. You may be able to see which applications are the top consumers of bandwidth, or find out what caused a bandwidth spike yesterday. With more visibility into the traffic on your network, you can make informed decisions on whether you need to procure more bandwidth to support the business, or if stricter traffic prioritization could help ease bandwidth concerns for critical business services.

Homework:

- » [Watch SolarWinds Lab Bits™: What is NetFlow?](#)
- » Visit the sFlow Consortium site: [Network Equipment that Exports sFlow](#)

CHAPTER 2: TROUBLESHOOTING NETWORK ISSUES

Whether you are trying to meet uptime SLAs or ensure network downtime isn't affecting revenue, understanding your network traffic usage helps you guard against service interruptions due to excessive bandwidth use. Because NetFlow and other flow data contains information about network traffic, it helps network administrators address issues related to application slowness and network performance degradation. By identifying the top talkers from current and historical flow data, you can easily identify the top consumers of network bandwidth.

Using flow data, 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. Additionally, NetFlow data helps you analyze usage patterns over time and find out who or what uses most of the network bandwidth, so you can quickly troubleshoot application- and performance-related problems in the network.

Homework:

- » [Learn more](#) about finding network bandwidth hogs

CHAPTER 3: TRACKING CLOUD PERFORMANCE

The growing demand of cloud-based applications and their increased rate of adoption have resulted in massive pressure on network administrators to have continuous network uptime for necessary operational processes. Any issues with the network or the speed of service can have an adverse business effect. Cloud and SaaS (Software as a Service) based approaches mean you need to ensure enough bandwidth is available for business-critical applications to run uninterrupted 24/7, particularly during peak business hours when the network is most stressed. Any network downtime can cause a huge enterprise-wide operational loss and potentially affect the organization's bottom line.

Ensuring continuous cloud application usage

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

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

It provides the means to track the cumulative usage of a given application in an aggregate manner, down to specific regions, if necessary. SolarWinds® NetFlow Traffic Analyzer (NTA) even allows you to create custom views based on applications, devices, IP groups, and other filters, so you can easily see the information that's important to you. NetFlow information can then be used to verify whether the cloud usage behavior matches your service level agreement by mapping the actual activity between the cloud and your network.

Measuring latency is challenging while operating in the cloud, but identifying bottlenecks by analyzing the flow data can help you ensure that cloud providers deliver the promised service.

SOLARWINDS NETFLOW TRAFFIC ANALYZER CUSTOMER TESTIMONIAL

My favorite feature of NetFlow Traffic Analyzer is:

“ The application-wise traffic data. It helps us to see the top applications consuming bandwidth.

— **Abhishek Sharma, Systems Engineer, Encore Capital Group, Inc.**

Source: Abhishek Sharma, Systems Engineer, Encore Capital Group, Inc.



✓ Validated Published: Feb. 1, 2018 TVID: BA5-AFD-8BB

Homework:

- » Check out how you can track cloud and on-premises network performance with [SolarWinds Network Performance Monitor and NetFlow Traffic Analyzer](#)
- » Walk through the interface utilization resource in the [Network Traffic Analyzer online demo](#)

CHAPTER 4: VALIDATING QUALITY OF SERVICE POLICIES

Bandwidth is neither infinite nor free, so it only makes sense that you want to see how it is being used. Prioritizing bandwidth according to needs is a critical strategy for network managers. By distinguishing different types of network traffic like voice, email, and other applications, administrators can define Quality of Service (QoS) and set priorities for various applications. For example, 50% of the bandwidth can be set to VoIP applications that are business sensitive, while other non-critical applications are allocated lower bandwidth.

By defining QoS classes and assigning policies, network administrators can set predefined actions to be triggered under specific cases. After implementing QoS policies across the network, you can review flow data to measure the effectiveness of the policies and, if needed, further restrict bandwidth to low priority applications. Prioritizing mission-critical applications by characterizing traffic can also help network administrators understand the bandwidth needs for capacity planning. (More on this in the next lesson!)

SOLARWINDS NETFLOW TRAFFIC ANALYZER CUSTOMER TESTIMONIAL

My favorite feature of NetFlow Traffic Analyzer is:

“ The Types of Service (ToS) summary. It has helped me to prioritize and identify traffic and confirm the proper classification of traffic from different endpoints.

— Michael Sprandel, Network Administrator, Glencoe Regional Health Services

Source: Michael Sprandel, Network Administrator, Glencoe Regional Health Services

solarwinds 

 TechValidate

✓ Validated Published: Feb. 2, 2018 TVID: 93B-157-3D8

Homework:

- » [Learn more](#) about network QoS reporting and monitoring
- » Explore the CBQoS monitoring and shaping capabilities in the [Network Traffic Analyzer online demo](#)
- » Download a 30-day free trial of [SolarWinds® Bandwidth Analyzer Pack](#)

CHAPTER 5: CAPACITY PLANNING

As organizations scale up and add users and tools, the network capacity can be tested. How do you know if an increase in bandwidth is truly necessary to support critical business services? Analyzing flow data can help administrators plan network capacity more accurately. Using flow data, you can verify bandwidth growth is aligned with resources utilized in the current environment and plan for the future.

Monitoring flow data can help identify when you are nearing bandwidth capacity. You can then confirm that the usage is for critical business applications, and add bandwidth to accommodate the needs of your users. If the usage is not for critical business apps, an adjustment to QoS policies may correct the issue and save you from spending on additional bandwidth that isn't needed. With this information, you can utilize the available bandwidth in a better way, helping ensure good resource alignment and capacity planning.

SOLARWINDS NETFLOW TRAFFIC ANALYZER CUSTOMER REVIEW



5/5 Stars

How our organization uses NTA:

“ We use NTA to troubleshoot issues when end-users report network problems for their buildings. NTA allows us to see what types of activity are taking place so that we can quickly zone in on potential culprits for the end-users. We've also been able to identify when we've approached steady, heavy usage at a building to weigh the needs of increasing bandwidth in certain locations.

What would you tell another network admin or engineer about NTA?

“ It's a valuable tool.

Source: Network Engineer, Large Enterprise Educational Institution Company

 

 Published: Feb. 1, 2018 TVID: 53C-E58-47F

Homework:

- » Start troubleshooting bandwidth issues and monitoring flow with [SolarWinds® Bandwidth Analyzer Pack](#)

ABOUT SOLARWINDS

SolarWinds provides powerful and affordable IT management software to customers worldwide, from Fortune 500® enterprises to small businesses, MSPs, government agencies, and educational institutions. We are committed to focusing exclusively on IT, MSP, and DevOps professionals, and strive to eliminate the complexity that our customers have been forced to accept from traditional enterprise software vendors. Regardless of where the IT asset or user sits, SolarWinds delivers market-leading products that are easy to find, buy, use, maintain, and scale while providing the power to address all key areas of the infrastructure from on-premises to the cloud. Our solutions are rooted in our deep connection to our user base, which interacts in our THWACK® online community to solve problems, share technology and best practices, and directly participate in our product development process. Learn more today at www.solarwinds.com.