

# Enterprise Network Traffic Informatics

————— A CIO's hand guide —————

**White Paper**






## Summary

---

*This paper puts forth the importance of having an enterprise wide network traffic analysis tool in today's global enterprises. By harnessing the data contained in the flow exports (NetFlow / sFlow/cflowd / J-Flow / Netstream / IpFix) from the routers/switches one can get deep insights in to the network traffic – especially the who, what, why aspects of the bandwidth usage. Such knowledge is vital for IT heads to take the right strategic decisions that can benefit the whole organization. In discussing the various methodologies, this paper brings out the advantages of deploying a flow-based pure-software solution that uses distributed-collection technique. Unlike the hardware probe-based monitoring, the flow-based software-solution has the advantage of lower investment, easiness of installation, and delivery of value in a matter of hours.*





## Table of Contents

<b>1. The end of Business, as we know it.....</b>	<b>4</b>
<b>2. Enterprise Bandwidth Monitoring - A Strategic Requirement.....</b>	<b>5</b>
<b>3. Typical Approaches to Bandwidth Monitoring.....</b>	<b>7</b>
<b>4. The Flow based software solution.....</b>	<b>9</b>
<b>5. The Flow-based distributed monitoring solution.....</b>	<b>10</b>
<b>6. Conclusion.....</b>	<b>11</b>



## 1. The end of Business, as we know it

In today's world, where the business landscape is changing fast, computer networks play a vital role. No longer is business confined to the four walls of the enterprise. Large enterprises today, need to pursue strategies like offshoring, outsourcing, smart-sourcing etc to be competitive. Under this, the nature of work gets globalized and work gets done across geographies and time zones. Welcome to the "Distributed Enterprise"!

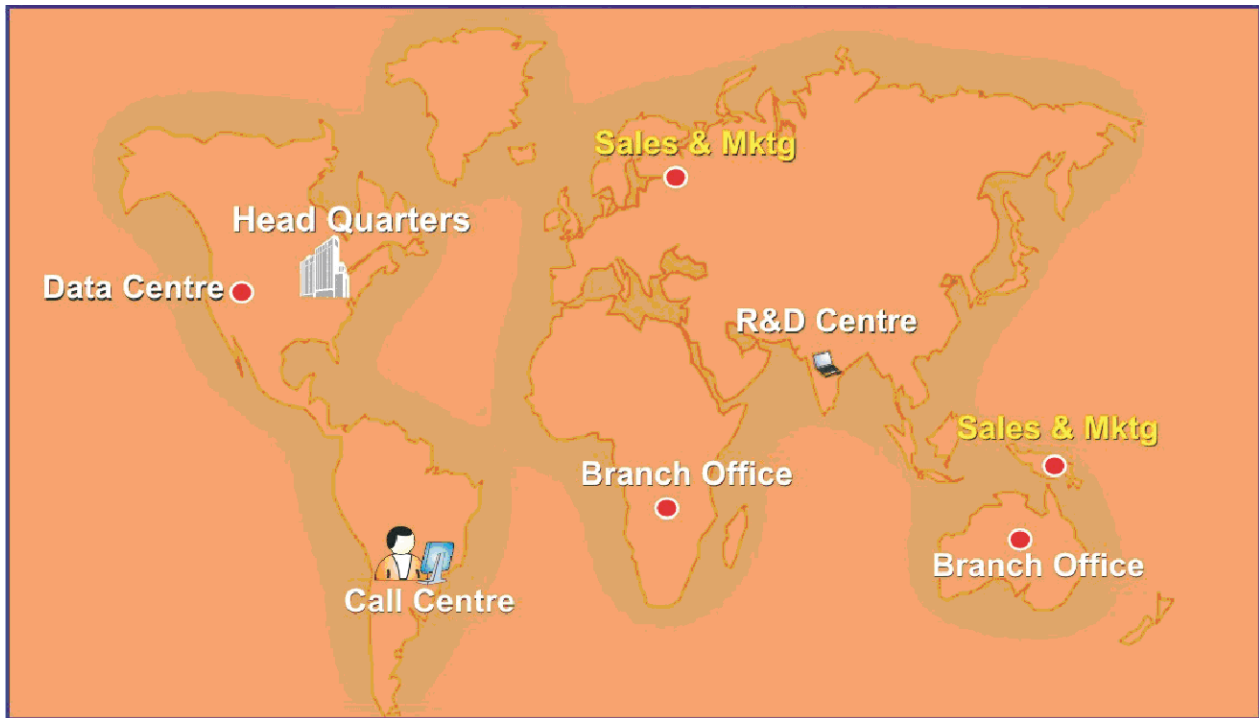



Figure 1: The Distributed Enterprise

Some of the strategies pursued by today's enterprises:

- It is common to see enterprises have their headquarters based out of UK, the suppliers of raw materials (supply chain) based out of China, Brazil and Norway, the knowledge workforce based out India, its road-warriors (sales & marketing staff) spread across the globe, and have all its sales happen the e-commerce way
- To avoid legal hassles and to comply with the growing emphasis on data integrity and security, (thanks to HIPAA, SOX and the like), enterprises today prefer to have their entire database on all aspects of their business in a secure central data center, mostly based in the US

- 
- To overcome the cost associated with deploying skilled network administrators at various distributed office locations and also to overcome the challenge of skilled finding personnel, enterprises prefer a centralized monitoring of their global networks
  - Every enterprise that wants to cut costs and remain competitive is doing away with the costs associated with acquiring proprietary software/applications. The emerging trend is enterprises moving towards the hosted or the SaaS (Software as a Service) model. This includes web-based applications like Salesforce.com for sales force automation, Zoho for enterprise productivity, etc.

In such conditions facilitating access/communication between the various constituents of the distributed network and ensuring access to the datacentre/SaaS application from the remote offices becomes crucial. Also to monitor the whole network from a centralized location having a unified view of the entire network becomes indispensable.


Enterprise bandwidth monitoring is today an indispensable core requirement, and quite a strategic one at that.

## **2. Enterprise Bandwidth Monitoring - A Strategic Requirement**

With such sweeping changes embracing the enterprises, has the network administrator's responsibility to ensure high level of WAN availability all the time, become very critical. Especially as enterprises get global, there comes the challenge of managing the health and performance of the entire network including the remote/branch office. Any degradation in the network performance anywhere in the network, could lead to significant productivity loss and employee frustration. It gets all the more important to be sure that no unwanted traffic / network abuse /network attack is happening at any point in time.

The main challenges in such a scenario include:

- Ensuring strong network connectivity and bandwidth availability at all times
  - Bandwidth should not be a limiting factor to a business' success

- 
- Ensuring optimal bandwidth for critical applications – ensure revenue generating applications take precedence over trivial applications
    - Being able to prioritize critical applications like access to SAP HRMS, Oracle Financials, Zoho CRM, Salesforce.com or access to the company's IBM mainframe at head office over trivial things like streaming videos, music downloads etc
  - Quickly troubleshooting any network incidents – pinning down the root cause of problem to fix it fast
  - In the event of a capacity planning doing it accurately – as the costs involved are huge when it comes to large enterprises
  - Having a tab on the globally spanning network
    - Be in the Know: is your enterprise network bandwidth being used or abused and also to be able to charge back to remote offices if needed.
    - The lack of availability of qualified network administrators need to be overcome by a centralized monitoring delivered to the Network manager
  - Ensuring the quality of the service delivered by the ISP is in line with the terms of the agreement

The only way to address these problems is by having a very strong enterprise wide bandwidth monitoring and traffic analysis tool. By having a knowledge of the traffic patterns in similar departments across offices / geographies and the causes of bandwidth consumption a Network Admin / CIO can take educated decisions. This information enables the network admin to enforce appropriate policies to restrict undesired bandwidth usage – like downloading music files or watching videos off you-tube during business hours.

At the CIO level, a unified collective view of the bandwidth consumption across the distributed enterprise can help in taking an accurate strategic decision - capacity planning (ordering more bandwidth), for instance. Also, having access to historic data of traffic usage pattern helps to benchmark current usage levels



### 3. Typical Approaches to Bandwidth Monitoring

A cursory look at the solutions available in the market shows that there are solutions of various types to choose from. In general they can be classified based on the underlying technology (data acquisition technique)

#### **Based on the data acquisition technique:**


The solutions available in the market adopt one of these techniques: SNMP query, Test Access Ports (TAPs) or SPAN Ports, Packet Sniffing and analyzing Flow exports like NetFlow / sFlow / cflowd / J-Flow / Netstream / IPFIX.

SNMP or Simple Network Management Protocol uses SNMP queries on SNMP agents running in the network device, to get information on the bandwidth usage in the network. SNMP query gives a consolidated or bulk traffic figure. So, this needs to be complemented with in depth network traffic analysis that answers questions like who, when, what aspects of the bandwidth usage. Also, as it uses the "pull-technology" it may cause considerable load on the enterprise bandwidth.

Span ports (Switched Ports Analyzer) is a port designated on switches to mirror traffic received on other ports. Test access ports are traffic replicators placed in between two routers, firewalls or enterprise switches that sends a copy of all the network traffic flowing through them. Span or Tap ports can be used to forward network traffic to Software applications or hardware probes for traffic analysis. Network traffic can be tapped via them. The downside is the cost involved in procurement, deployment and management of these

Packet Sniffer intercepts and collects the local traffic by capturing the packets from the network that the sniffer is attached to. A "sniffer" is useful in network troubleshooting, network intrusion detection, monitoring network usage. The advantage is the ability it lends to account the actual traffic by IP address and the protocol. The downside is the heavy load caused on the monitoring system.

Flow based technology harness the information contained in the flow exports like NetFlow, sFlow, cflowd, J-Flow, Netstream, IpFix and present an in depth view of the traffic flow. They offer a scalable and a low cost approach to have deep insight into the network traffic based on layer 3 and layer 4 level, packet information. With them one can know the - who, what when aspects of bandwidth usage. Using the data extracted from the flows the following can be known:



- Who are the top talkers in the network?
- When did the traffic peak and why?
- How long was the bandwidth hit and why?
- The source- and destination involved in a Conversation

This approach provides the information necessary to make capacity planning decisions and to detect any form of network abuse, in monitoring QoS and to certain extent in identifying security attacks.

The below table lists the vendors, whose devices are capable of exporting one of – Cisco NetFlow, sFlow, cflowd, J-Flow, NetStream, IPFIX.

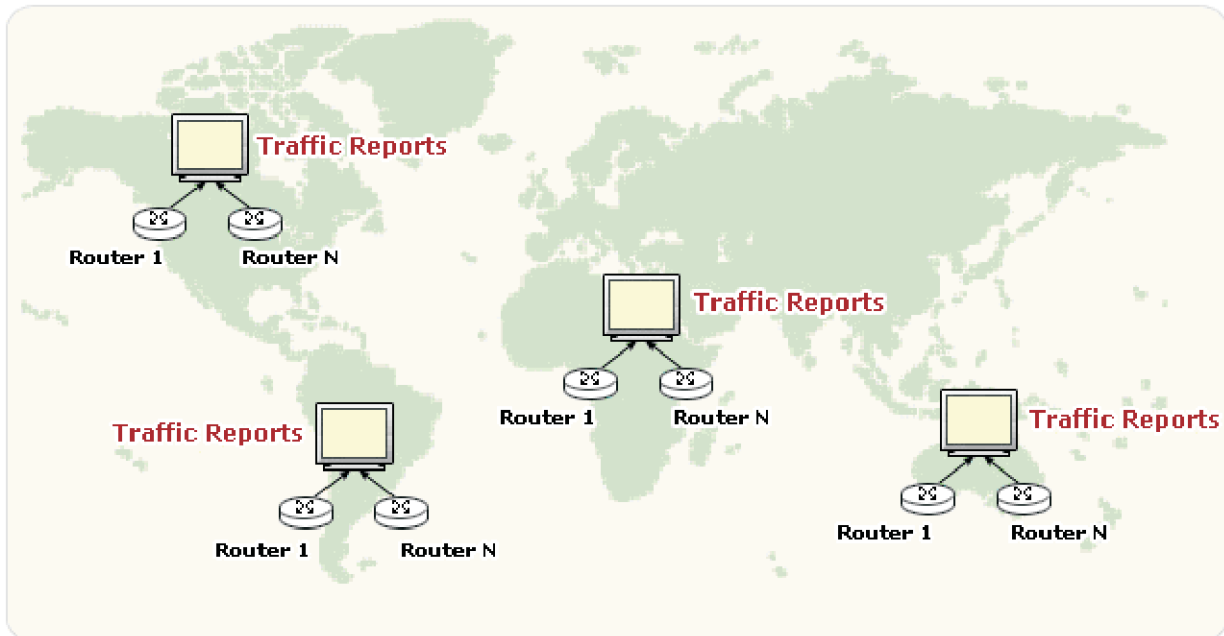
Type of Flow	Supporting Vendor Devices
NetFlow	Cisco Devices, Enterasys, Extreme Networks, Foundry Networks, 3com, Riverbed
sFlow	Alcatel, Extreme Networks, Foundry Networks, Hitachi, NEC, Alaxala Networks, Allied Telesis, Hewlett Packard, Comtec Systems, Force10 Networks
cflowd /J-Flow	Juniper
Netstream	Huawei, H3C
IPFIX	Nortel devices

*Table 1: Various Flows & Supporting Vendors*

Let us consider the case of a software solution that is based on harnessing the data contained in the “Flows” to monitor an enterprise network bandwidth.

## 4. The Flow-based software solution

When a global enterprise decides to use a flow based software solution for the purpose of monitoring its distributed global enterprise, the setup looks like the figure below. The software has to be deployed in each of the remote locations and the data gathered from the location is visible to the network admin at that level/ location only.



*Figure 2: A typical Flow based monitoring*

The report on the bandwidth usage in each of the office is visible only to the network administrator at that level. Here the data is in "silos". For a consolidated overall view the data available with each network admin has to be collated by the chief Network Administrator / CIO.

### **Drawback of this solution:**

- Lack of an unified view



A distributed monitoring solution can fix the drawback in the above model. By collating data from all the distributed locations and presenting it in a unified fashion, it brings greater control to the Chief Network Administrator/ Network Manager.

## 5. The Flow-based distributed monitoring solution

### Case In Point: The NetFlow Analyzer Enterprise Edition

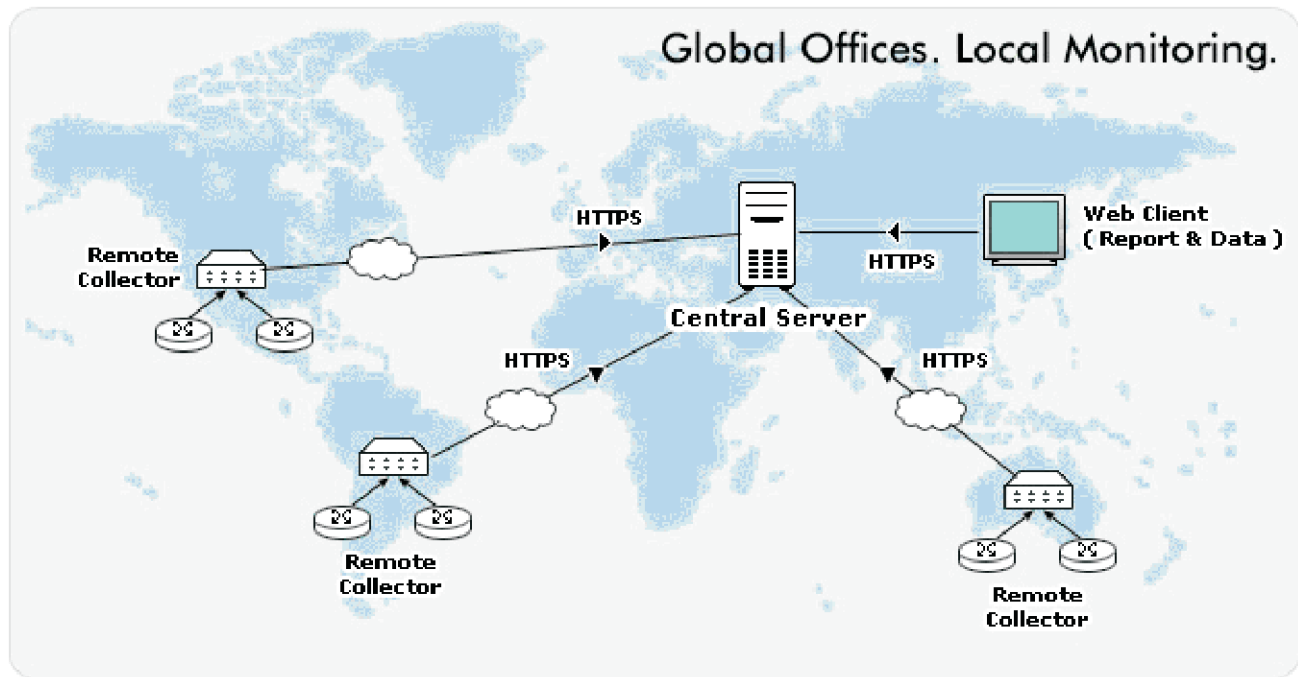


Figure 2: Flow based monitoring with Distributed collection

The NetFlow Analyzer Enterprise Edition is a flow based scalable software solution from AdventNet, ideal for large corporations with tens of thousands of interfaces. It uses distributed collectors (shown in the diagram), which are installed, in remote offices. The remote collectors collect the flow information from all the routers in the location. It processes the data and after compression sends it to the central server through a secure https link. This way the bandwidth that is consumed is just a fraction of what would be consumed otherwise.





The central server receives the compressed data exported by all collectors and does further analysis for the purpose of reporting. The central server is ideally located at the Head Quarters. A chief network administrator or CIO can access the reports generated by the Central Server through a web-client and get a unified view of the entire network.

Benefits of the NetFlow Analyzer Enterprise Edition:

- Suited for **large enterprises** with distributed networks
- **Scalable architecture** to support thousands of routers and switches
- Supports **centralized unified view** for easy management
- Supports Cisco **NetFlow v5/v7/v9** and **sFlow** technologies
- Supports **TOS, DSCP** and **TCP\_Flag**
- Https based **secure communication**
- **All-software solution** and does not require complex hardware probes
- Runs on Windows & Linux - both 32-bit and 64-bit
- Pricing starts as low as \$ 17,995
- Backed by a responsive support
- **Free 30-day** evaluation with **no restriction** on features made available


## 6. Conclusion


Take in to consideration the below key points before choosing your traffic analysis / bandwidth monitoring solution, in order to ensure that the investment delivers value, as expected.





## 9 Key Points for the CIO/Network Manager to consider in choosing the right solution

- Consider what kind of solution it is – Hardware / Probe / Packet Analyzer based or Pure-Software Based
  - Consider the cost of the solution – demand to know the likely cash out-flow to own the software over atleast a 5-year horizon
    - Clarify the cost associated with software upgrades, telephonic support
    - Costs associated with having a personnel deployed in case of eventualities
  - See the cash-outlay Vs ROI metrics.
    - A product that far outweighs the ROI it generates is never the right solution.
    - Bandwidth Monitoring is a function that is meant to add value to the enterprise' bottom line. It should not end-up casting the Network department the “cost-center” image
  - Evaluate the kind of support you are likely to get
    - Often more than the number of PhDs / Masters a company has on its rolls it is the number of responsive staff available that makes difference to you as the end-customer
  - Demand to know the legacy of the company/product
    - Typically a company that has been in the business for more than a decade and has managed to remain profitable is a good choice to go with
    - Typically a product / base-product that has had the support of thousands of customers from across the globe is a testimony to strong engineering ability and a rock-solid support
    - Factor the above two points when you have narrowed down to almost two vendors/solutions
- 

- 
- Choosing the vendor - See beyond today
    - Do not buy a solution considering today's requirement alone.
    - Typically opting for a company that has a whole range of network-management-allied products is a very good decision. In addition to monitoring your whole enterprise network bandwidth, you may want to monitor the performance of applications in your network or analyze your firewall logs etc tomorrow
    - Visualize the future needs of your network and chose the competent vendor
  - Evaluate at your pace
    - Seek extension of trial license as and when you need
    - A company that does not oblige to extend license or has cumbersome procedures may not be the best bet going forward
  - The "Forums" is the ultimate index
    - See how active and vibrant the forums is
    - It is an index of how popular and how responsive the product and the product teams respectively are
  - Finally don't fall prey to consultants and marketing gimmicks!
- 