StableNet® - WHITE PAPER

Netflow Monitoring and Analysis using Infosim StableNet®

Document Ref: - SN_NFLOW_WP_DP004_IV1

Author	David Poulton – COO Infosim (UK)
Document Reference	SN_NFLOW_WP_DP004_IV1
Version Number	1.0
Issue Date	6th December 2013

Document Request – Contact: - sales@infosim.net

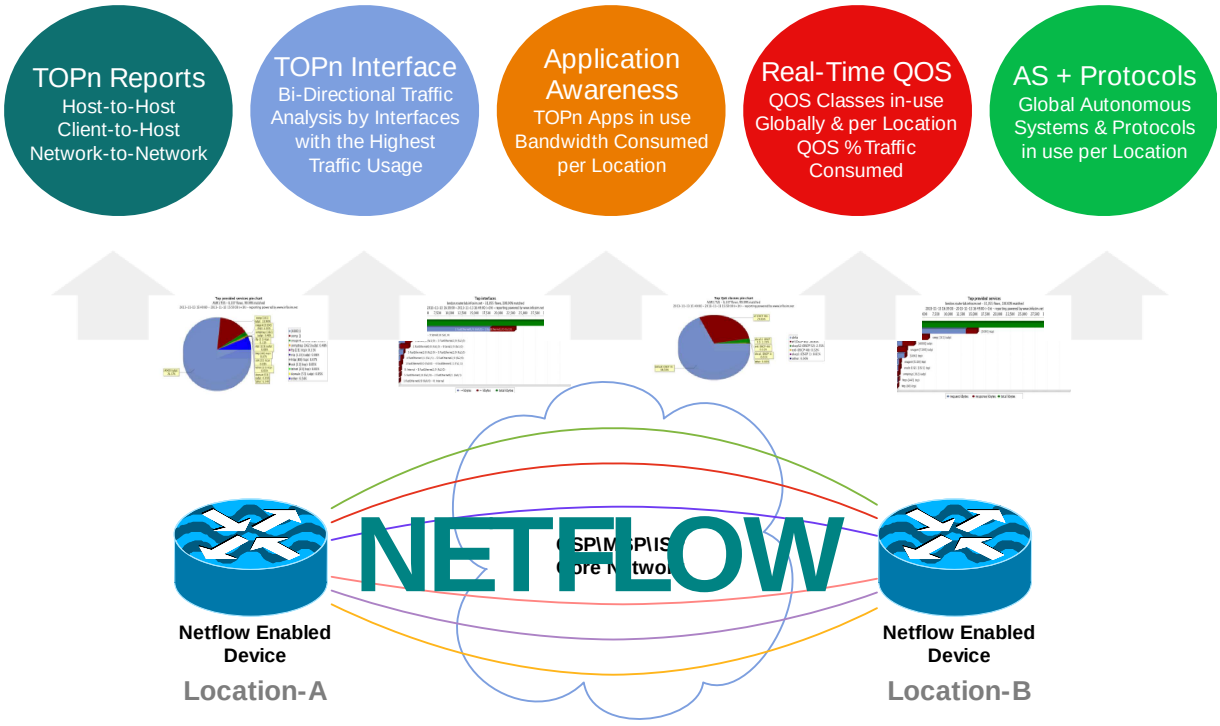
Contents

1 Netflow Management Overview

NetFlow is a Cisco-developed flow technology that allows flow-monitoring for a given network. StableNet® is a unified network management system available in two options; namely, 'Telco' version for CSP/ISP/MSP customers, and 'Enterprise' for Corporations, Service Integrators, and Managed Services Operators. The StableNet® NetFlow Analyzer is a functional capability of the unified management system that receives and processes the flow-data being sent from the configured flow devices in the network. The flow-data is then subjected to deep-flow-analysis that results in a series of statistical and graphical real-time reporting. The reporting can be manipulated to detail-specific date/time ranges to be displayed in order to assist with troubleshooting-specific events that may have caused performance degradation or service loss.

This document will provide insight into the StableNet® Netflow capability and detail when Netflow is appropriate to be used and in what context it should be deployed.

StableNet® Netflow Capability Framework



StableNet® incorporates the following flow collection technology:

- **Cisco NetFlow v5,7 & 9**
- **Juniper J-Flow**
- **IPFIX**
- **sFlow**
- **NetStream**

2 Netflow Monitoring

Enablement, or the turning on, of the Netflow capability within your network architecture will provide greater visibility of the data-flows traversing your network through deep-flow-analysis. Devices within your network that are NetFlow-capable can be configured to send the flow-data to a Netflow collector. StableNet® agents have Netflow collector capability to take the flow-data and process it for deep-flow-analysis reporting.

The growth in converged VoIP, IPTV, and mission-critical networks and applications is becoming more predominant and having the ability to understand and characterize the traffic on your network, from both a visualization and capacity viewpoint, is vital for future planning and security anomaly detection.

The following report types are supported with StableNet® Netflow and include flexible filtering:

- **TOPn Reporting with Flexible Filtering**
  - Client applications
  - Networks
  - Hosts
  - Protocols
  - Type of Service (TOS)
  - Applications in use
  - Filtered reporting
  - Export of Real-Time flows in *.csv* format for data customization and visualization purposes

- **TOPn Interface Statistics with Flexible Filtering**
  - Real-Time bandwidth usage
  - Bi-Directional traffic usage per interface
  - Filter-specific traffic type per interface
  - Filter-specific conversation type per interface
  - Export of Real-Time flows in *.csv* format for data customization and visualization purposes

- **Application Awareness with Flexible Filtering**
  - Real-Time global application usage + %Bandwidth usage statistics
  - Real-Time per-Netflow device Application usage + %Bandwidth usage statistics
  - Real-Time per-Netflow device per-selected interface Application usage + %Bandwidth usage statistics
  - Filter to specific conversation data with date/time selection
  - Export of Real-Time flows in *.csv* format for data customization and visualization purposes

- **Real-Time QOS with Flexible Filtering**
  - Real-Time global QOS class and DSCP markings + %Bandwidth usage on a global basis
  - Real-Time per-Netflow device QOS class and DSCP markings + %Bandwidth usage statistics
  - Real-Time per-Netflow device per-selected interface QOS class and DSCP markings + %Bandwidth usage statistics
  - Filter to specific QOS markings with date/time selection
  - Export of Real-Time flows in *.csv* format for data customization and visualization purposes

- **Autonomous Systems + Protocol Statistics with Flexible Filtering**
  - Real-Time global AS class and Protocol graphical dashboards + %Bandwidth usage on a global basis
  - Real-Time per-Netflow device AS class and Protocol graphical dashboards + %Bandwidth usage statistics
  - Real-Time per-Netflow device per-selected interface AS class and Protocol graphical dashboards + %Bandwidth usage statistics
  - Export of Real-Time flows in *.csv* format for data customization and visualization purposes

3 Baseline your Network using Netflow

A greater need for the baseline of a given network is now a necessity in today's modern data infrastructures. Time-critical applications rely so much on speed that delay, transient latency, inter-packet delay, End-to-End performance, and transactional response times are an essential business monitoring requirement. StableNet® Netflow will report the necessary baseline analysis to:

- Assess a Network Infrastructure for suitability of provisioning services *(e.g. VoIP, Wireless, IPTV)*
- Monitor, measure and trend the effect of infrastructure changes
- End-User performance experience, know what your 'normal modus operandi' is so that you can identify and alert on any deviation from the known state
- Application Awareness and Change
- Project future performance states based upon modeled current data collections

Netflow is a perfect tool for the initial baseline of a given network. Used in combination with a unified suite of functionality it will enable continuous baseline performance monitoring with proactive enablement via pre-configured threshold settings that can auto-trigger proactive awareness and self-heal mechanisms integrated within an OSS/BSS environment.

Historical baseline data can then be tracked and reported against specific performance thresholds, provide feeds into your capacity planning processes, creating the necessary historical performance statistics for predictive future bandwidth trend analysis.

Infrastructure Baseline Using StableNet® Netflow

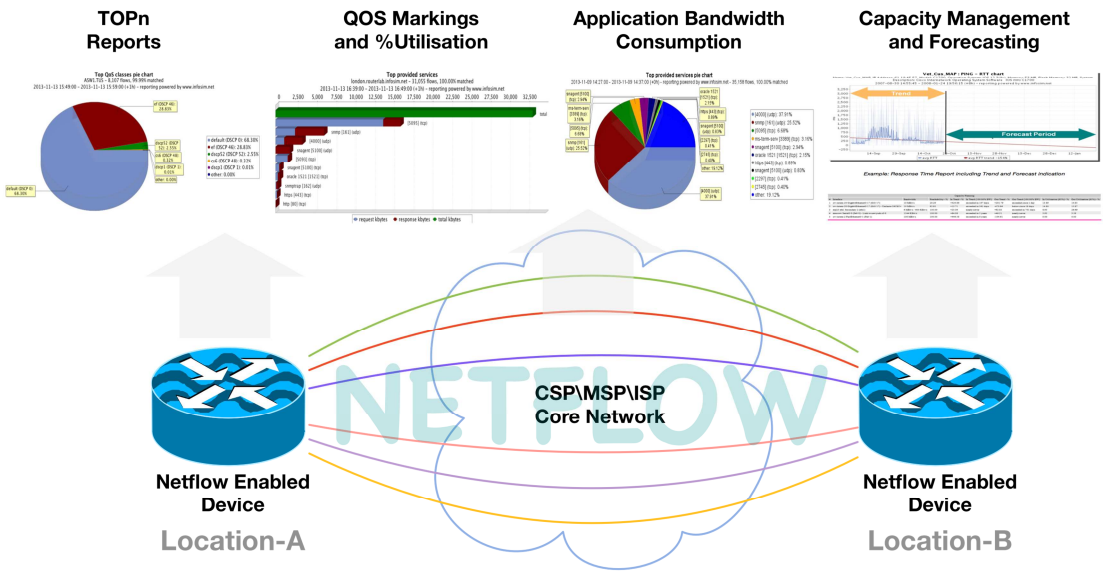
4 Netflow Performance & Capacity Management

Having the ability to visualize and characterize IP traffic and account for where it flows is critical for network availability and performance capacity monitoring. Being able to look at the flow-data from a particular site, or critical location, for example; a datacenter or call center, and seeing the real-time and historical flow-data on a per-application basis is principle to understanding who or what is consuming the bandwidth in/out of a specific location.

Enabling Netflow allows you to visualize what applications are being utilized the most from a global, and site-specific perspective. This in-turn builds an application usage picture of where your corporation's applications operate allowing you to accurately capacity plan site bandwidth usage and Quality of Service (QOS) prioritization for those applications deemed important, or critical to your corporation's business operation.

StableNet® is a unified management system that provides greater value-add through the use of a combination of integrated functionality. Using StableNet® Netflow in combination with StableNet® performance and fault management provides complete visibility and proactive manageability of the performance and capacity management of your entire global infrastructure.

StableNet® Netflow Performance & Capacity Unified Management Reporting



5 Security of your Network using Netflow

Enabling Netflow at the entry and exit points of your network increases visibility of the connection dynamics of the data-flows entering and exiting your corporate infrastructure, and extends the visibility features of your existing security systems providing a more comprehensive addition to compliment intrusion detection IDS/IPS systems, and security and information event management (SIEM) solutions eliminating potential network blind-spots.

Netflow assists in identifying traffic deviation from the normal, or baseline operating performance. This is why it is so important to baseline critical networks *(see section 4)* in order to understand in explicit detail:

- What the typical traffic types look like
- What are the acceptable levels of normal and peak operational utilization

- Configuring proactive-threshold management in order to alarm when breached, or when the traffic deviates from the known normal levels of operation

Infosim recommends the use of Cisco's six phase approach to security using StableNet® unified management:

1. **Phase 1 – Preparation** – Baseline your critical networks so as to understand what 'normal' network traffic operation looks like, then employ proactive-threshold management for alarm and alerting to potential traffic performance deviation.

2. **Phase 2 – Identification** – Through the enablement of Netflow identify and label the traffic TCP/UDP port types traversing the network for application recognition purposes, and capture the typical source/destination host networks for internal/external location identification.

3. **Phase 3 – Classification** – Once identification of the traffic types and source/destination host networks are completed, look to classify and group/sort where you expect the flow to come from e.g. internal/external groups of classified flow types. This will assist in rapid identification of any suspected threat.

4. **Phase 4 – Trace-Back** – Ensure sufficient historical flow-data is captured in order to perform any problem diagnosis on tracing back the source and path of any suspected attack. Identify where and when the change/event or traffic threshold deviation took place and if it appeared under any application type guise.

5. **Phase 5 – Reaction** – Identification, classification and trace-back of potential/real risks/threats or security holes from the flow information provided at the entry point within the infrastructure should then result in reaction with the use of appropriate ACL *(Access Control Lists)* to mitigate the risks. Configuration, distribution and policing of the ACLs within the entry points to the corporation's global infrastructure should be managed using StableNet® unified management as this can be performed in a completely automated way.

6. **Phase 6 – Post-Mortem** – IT and Service Management teams work together to identify and discuss the root-cause and have proven visibility of change and eradication of risk/threat, update policy and continue to police.

StableNet® Netflow can also be deployed to detect and prevent Denial of Service attacks and other undesirable traffic types. Corporations with a high-profile online presence are subject to potential attacks that are intended to flood networks with Denial of Services (DOS) packets. These untrusted source packets can be of varying packet sizes, and consist of single or varying destinations. StableNet® Netflow can detect these flows and identify the packet source, destination, protocol number, port number, and packet size etc. for anomaly detection. NAT (Network Address Translation) and PAT (Port Address Translation) are employed in a large number of internet instances where many non-internet-routable addresses and ports are effectively mapped to an internet-routable address thus entering your domain on publicly routable addresses. StableNet® Netflow has the capability to audit the NAT/PAT traffic to assist in troubleshooting and resolution of these event types.

6 Netflow Connection Forensics

StableNet® Netflow connection forensic reporting details the following information:

- Flow time-stamp *(Delta)*
- Flow interval *(Duration of flow)*
- Protocol used
- QOS/DSCP marking used
- Source IP address
- Source port
- Source AS *(Autonomous System)*
- Destination IP address
- Destination port
- Destination interface
- Destination AS *(Autonomous System)*

- #of Bytes *(per flow interval)*
- #of Packets *(per flow interval)*

Having the ability to capture the above detail from each flow in a given network, or on a particular interface, and being able to export the data for visualization and forensic analysis, enables deeper forensic inspection of your network for instance:

1. Ability to determine the distribution of packet sizes across the network allows you to understand what the normal packet-size-distribution is and therefore track for deviation in what the acceptable norm is to ascertain if packet sizes within the flows are increasing, which could lead to identifying early potential attacks.

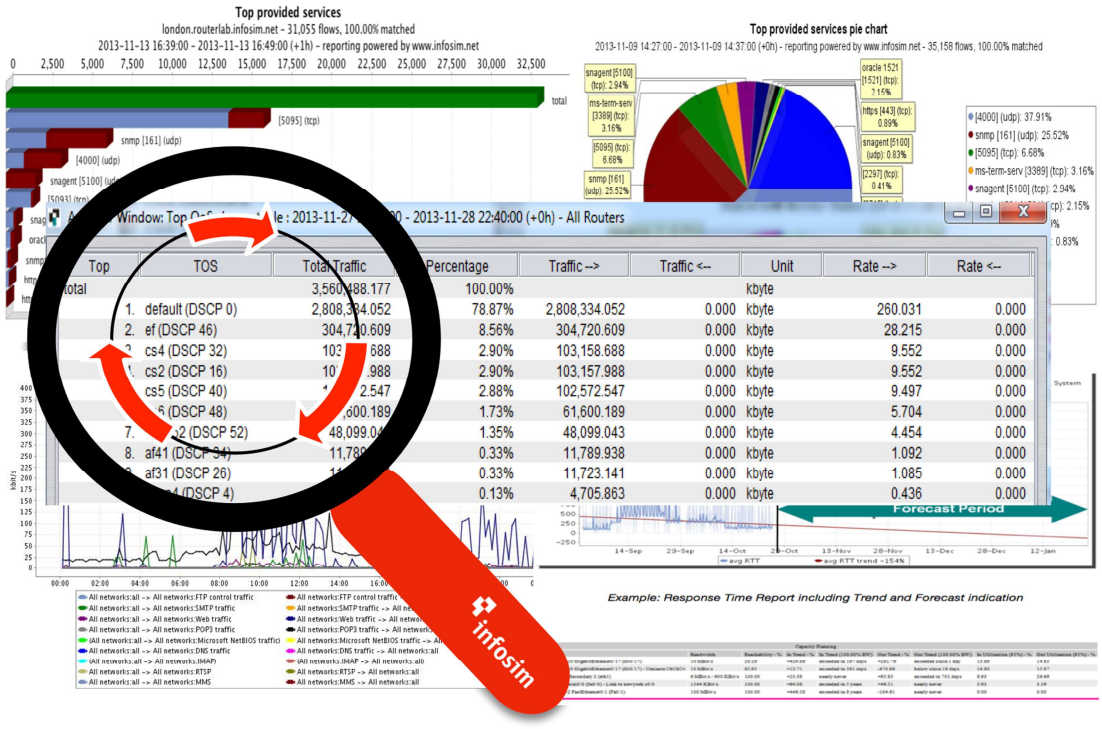
2. Baseline of flow distribution over a given network. Track deviation of excessive flow increases that could point to potential DDOS attacks.

3. Track, monitor and alert on the deviation of bi-directional flows in/out of specific interfaces.

4. QOS analysis – track global QOS markings and ensure deployment is in alignment with your corporation's QOS design policies. See what bandwidth each marking is consuming on a global and site-location basis. Go to specific site-location to visualize the QOS markings and track the bandwidth consumption per marking and police those corporate design QOS policies with the StableNet® unified management solution.

5. 95th percentile reporting is available when using the StableNet® unified management solution. This is normally used for billing purposes but can also be utilized for tracking and alerting on performance deviations for example; traffic bursts and spikes which may indicate an underlying issue or security attack.

StableNet® Netflow Forensic Analysis Reporting



7 Netflow Deployment & Scalability Considerations

Netflow, as we have discussed within this document, is an extremely useful functionality to enable on router and switching devices located within your corporation's infrastructure. However, you need to think about the mechanics and plan what you wish to achieve. For example:

1. Identify the locations within your infrastructure where you wish to enable Netflow functionality.
2. Identify where best to install the Netflow collection agents.
3. Think about the increase in bandwidth when enabling Netflow.
4. How long do you wish to keep Netflow data for?
5. Understand the storage requirements for long-term historical reporting and size your database accordingly.
6. Before enabling Netflow, check that the device has enough processing and memory to handle it being switched on, otherwise you may experience router/switch meltdown.

There are several things to consider when deciding what your Netflow collection architecture should look like. These factors include collector disk space, CPU power, exported Netflow packets per second, and network topology. If your environment is simple enough, a single collector may be sufficient, that is why it is very important to accurately plan the deployment of a Netflow solution.

Disk space and I/O speed is always one of the primary concerns when preparing to deploy Netflow. Because of the nature of Netflow, it is difficult to predict what a specific network will require for Netflow storage. A general rule of thumb is 1MB of storage for every 2GB of network traffic. This may not seem like a lot, but on an enterprise network this can add up quickly, especially given the fact that a single network transaction could potentially pass several devices exporting Netflow.

Network topology also needs to be considered when choosing where to physically deploy your Netflow collector(s). Sending Netflow records from a remote WAN device to a central collector can put additional strain on a link unnecessarily, especially during a Denial of Service attack. Netflow packets are UDP-based, so using high bandwidth connections can lead to exported flows being lost. If there are multiple routers exporting flows to a single collector, it can be beneficial to have multiple Netflow collectors running on different ports writing to different directory structures. Segmenting the data in this way will allow queries to be run that are specific to the network segment associated with a specific router.

Netflow can be exported from a variety of devices, including enterprise and small office routers, dedicated appliances, as well as passive monitors that work in the same manner as a network sniffer. Netflow should be exported from devices located at points of convergence, much like an IDS sensor. Having well-placed Netflow exporters reduces the number of devices needed to cover the entire network and reduces storage requirements.

It is highly recommended to use NTP and a common time-zone for time synchronization. Setting the time-zone of all your network devices to a common format such as UTC, takes very little effort and prevents the need to reconcile date and time issues during an incident.

***Note:** *Infosim has developed a Low-Cost-Agent (LCA) where we have made it very affordable to now deploy agents between every network hop throughout a corporation's network. Synthetic media scripts can now be employed to perform a series of continuous functional measurements that will report the real-time performance experience of your entire network between every hop so as to rapidly identify bottlenecks, degradation, packet loss, jitter etc. Infosim recommends that when used in combination with Netflow, enabled at strategic points within the network infrastructure, greater visibility of real-time performance and application awareness is realized and that storage and NetFlow collector costs are considerably reduced.*

8 Resources & Further Information

Follow the links below for further information about Infosim StableNet®.

1. Infosim Web Site: www.infosim.net
2. Infosim StableNet® Videos: http://www.infosim.net/resources/videos
3. Infosim StableNet® Case Studies: http://www.infosim.net/resources/case-studies
4. Infosim StableNet® Industry Reports: http://www.infosim.net/resources/industry-reports
5. Infosim StableNet® Webinars: http://www.infosim.net/resources/webinars
6. Infosim StableNet® Product Sheets: http://www.infosim.net/resources/product-sheets
7. Infosim StableNet® White Papers: http://www.infosim.net/resources/white-papers
8. Infosim StableNet® Solution Brief: http://www.infosim.net/cloud
9. Infosim StableNet® Request Trial: http://www.infosim.net/support/trial

For any additional information, demonstrations or webinar requests: http://www.infosim.net/about/contact

EMA Radar – Report Summary & Infosim Profile

An external report by Enterprise Management Associates® (EMA™) Radar Report for Enterprise Network Management Systems (ENMS): Q4-2012. A report summary and Infosim profile produced and written by Tracey Corbo, and Jim Frey October 2012 is available using the following link below:

http://www.infosim.net/fileadmin/user_upload/resources/industry_reports/EMA-ENMS-Q4-2012_RadarSummary-Infosim.pdf

9 About this Document

This document provides details on the Infosim StableNet® unified management system and how its multi-functional capabilities address a complete VoIP monitoring and reporting solution. Infosim StableNet® is the only all-in-one unified management tool capable of delivering and visualizing a complete End-to-End VoIP service solution monitoring system in a single product that has proven ROI *(Return-On-Investment)* in reducing capital *(CAPEX)* and operating *(OPEX)* expenditure, with conceivable savings in customer service credits through reduced MTTR *(Mean-Time-To-Repair)*, and increased service availability.

9.1 About Infosim

Infosim is a leading manufacturer of automated Service Fulfillment and Service Assurance solutions for Telcos, ISPs, Managed Service Providers and Corporations. Infosim develops and markets StableNet®, the leading unified software solution for Fault, Performance and Configuration Management. StableNet® is available in two versions: Telco (for Telecom Operators and ISPs) and Enterprise (for IT and Managed Service Providers). StableNet® is a single platform unified management solution designed to address today´s many operational and technical challenges of managing distributed and mission-critical IT infrastructures.

9.2 About Infosim StableNet® (Telco & Enterprise)

StableNet® Telco is a comprehensive unified management solution; offerings include: Quad-play, Mobile, High-speed Internet, VoIP (IPT, IPCC), IPTV across Carrier Ethernet, Metro Ethernet, MPLS, L2/L3 VPNs, Multi Customer VRFs, Cloud and FTTx environments. IPv4 and IPv6 are fully supported.

StableNet® Enterprise is an advanced, unified and scalable network management solution for true End-to-End management of medium to large scale mission-critical IT supported networks with enriched dashboards and detailed service-views focused on both Network and Application services.

StableNet® is a 3rd Generation highly-automated Network Management System. The key differentiation of StableNet® to other legacy type Operational Support Systems (OSS) is that StableNet® is a unified OSS system with three integrated functionalities that focus on Configuration, Fault and Performance Management, with automated Root-Cause-Analysis (RCA). StableNet® can be deployed on a Multi-Tenant, Multi-Customer or Dedicated platform and can be operated in a highly dynamic flex-compute environment.

9.3 Infosim Total Quality Management

Infosim StableNet® is a Total Quality Management solution that enables End-to-End automated Service Fulfillment and Assurance with flexible integration for service catalogue auto-provisioning. The Service-to-Provisioning-to-Customer process significantly reduces the Ready-for-Service *(RFS)* timescale and as a direct consequence enables Communication/Managed Service Providers *(CSPs/MSPs)* to reduce the time-to-bill on newly provisioned services thus maximizing revenues, whilst provisioning an automated repeatable quality customer service experience.

10 Disclaimer

END OF DOCUMENT