# Network Traffic Monitoring/Visibility Product/RFI Requirements

## Version 1.1

A white paper from the
ONUG Traffic Monitoring/Visibility
Use Working Group

May, 2015

TRAFFIC
MONITORING/VISIBILITY
WORKING GROUP
2015

Open Networking
USER GROUP

## Definition of Open Networking

Open networking is a suite of interoperable software and/or hardware that delivers choice and design options to IT business leaders, service and cloud providers. At its core, open networking is the separation or decoupling of specialized network hardware and software – all in an effort to give IT architects options in the way in which they choose to design, provision, and manage their networks. These technologies must be based on industry standards. The standards can be de-facto as adopted by a large consortium of the vendor community, open in the sense that they are community based, or defined as standards by the prevailing standards bodies. Open networking hopes to deliver on two promises:

1) Decoupling of network hardware and software which mitigates vendor lock-in and shifts network architecture structure options to users
2) Significant reduction of the total cost of ownership model, especially operational expense

## Scope

The scope of this document is to provide a set of tactical and strategic requirements aimed at guiding enterprise organizations in their design and selection criteria for traffic monitoring and traffic visibility solutions. Targeting a complete open interaction between varying solutions, the requirements listed include ranges from baseline architecture through data collection and capturing capabilities to data output from collector interchanges.

In detail, this white paper will address the following:

1. Identify the problems for today's enterprise network manager.
2. List current implementations and limitations.
3. Define the product requirement and expected baseline for collection and capturing of any network traffic.
4. Outlook on requirements for a product, which allows for flexibility and growth to mature in parallel with industry requirements.

In addition to the above, the following document will highlight existing limitations of currently available solutions, including their implications, which should be considered in future enhancements and new solutions.

To define a limit of this white paper, the user group will only evaluate an Ethernet protocol-based solution. Additional network traffic types may be evaluated in future revisions.

Not included in scope are end network design nor considerations regarding:

- Network security aspects,
- Network monitoring appliances for storing/processing traffic itself, and
- Network performance, trending and analysis.

## Executive Summary

The expected outcome for the Traffic Monitoring/Visibility Use Case Working Group adoption and usage in the enterprise market can be summarized, but is not limited to meeting this set of 10 product requirements for:

1. Commodity hardware based upon merchant silicon with either an open or propriety Switch Operating System (OS).
2. Granular filtering based on 5-tuple and/or even more, including application signatures, and Quality of Service (QoS) marking capability.
3. Capability to work with both underlay and overlay protocols, providing independent filtering on either, and/or correlate both traffic.
4. Process data without impact to production flow/processing flow (CPU/Memory/Bandwidth).
5. Horizontal scalability with the capability of resource management feedback.

TRAFFIC MONITORING/VISIBILITY WORKING GROUP
2015
Open Networking
USER GROUP

## Open Networking User Group (ONUG)

ONUG is one of the largest industry user groups in the networking and storage sectors. Its board is made up exclusively of IT business leaders, with representation from Fidelity Investments, FedEx, Bank of America, UBS, Cigna, Pfizer, JPMorgan Chase, Citigroup, Credit Suisse, Gap, and Symantec. The ONUG mission is to guide and accelerate the adoption of open networking solutions that meet user requirements as defined through use cases, proof of concepts, hackathons, and deployment examples to ensure open networking promises are kept.

The ONUG community is led by IT business leaders and aims to drive industry dialogue to set the technology direction and agenda with vendors. To that end, ONUG hosts two major conferences per year where use cases are defined and members vote to establish a prioritized list of early adopter, open networking projects that communicate propensity to buy and budget development. The vendor community stages proof of concepts based upon ONUG Use Cases, while standards and open source organizations prioritize their initiatives and investments based upon them. ONUG also hosts user summits and smaller, regional user-focused Fireside Chat Meet-Ups through the year. ONUG defines six architectural areas that will open the networking industry and deliver choice and design options. To enable an open networking ecosystem, a common multivendor approach is necessary for the following six architecture components::

1) Device discovery, provisioning, and asset registration for physical and virtual devices
2) Automated "no hands on keyboards" configuration and change management tools that align DevOps and NetOps
3) A common controller and control protocol for both physical and virtual devices
4) A baseline policy manager that communicates to the common controller for enforcement
5) A mechanism for sharing (communicating or consuming) network state and a unified network state database that collects, at a minimum, MAC and IP address forwarding tables automatically
6) Integrated monitoring of overlays and underlays

6. The ability to locally process data and create traffic signaling/alerting, while executing defined traffic-based actions.
7. Interoperability between vendors: integration and output that will support data collection integration and Open Application Programming Interface (API) for access and management (in/out).
8. Capability of Packet De-duplication/Packet Slicing/Data Masking and Application Recognition, including Packet Organization.
9. The ability to be Security and Compliance-aware.
10. Multilayer visibility between underlay and overlay protocol use for management/Service-Level Agreement (SLA), monitoring/alerting, troubleshooting and reporting capabilities.

## Problem Statement

Today, traffic usage of network infrastructure exponentially increases due to many factors. They include:

- Implementation of more cost-effective unified IP-based storage.
- Cloud orchestration capability, instantly creating computer resources.
- The movement of virtual infrastructure freely without fear of layer 2 fault domain due to the implementation of new technology, such as, Ethernet fabric, or any software-defined networking overlay and underlay capability.
- Big data implementation.

In short, the collection and capture of network infrastructure traffic data focusing on data network traffic analysis remains complex and costly.

In addition to the above challenge, information security has an increased need to collect the correct network traffic for security analysis, ranging from security threat analysis for any intrusion prevention mechanism, as well as real-time capability to assess any spread of unwanted traffic. This too, adds complexity.

Despite these factors, traffic visibility remains highly sought due to needs ranging from timely troubleshooting of performance issues, collecting applications analysis for capacity planning and forecasting capability that can be used for capital and operational expenditure planning. All of this relates to a requirement for better understanding of cost-effective network and infrastructure usage.

In order to provide the type of visibility above, most enterprise network management face many challenges, such as:

1. Proliferation of network packet inspection traffic-capturing tools, including the support infrastructure that creates another reliability challenge, manageability issue, additional costs, including capital and operating cost.
2. Sampling of traffic can lead to less accurate information.
3. Data loss due to oversubscription (SPAN Port – Switched Port Analyzer – limitation).

4. Technology limitations – SPAN port limitation, (Network) taps.

5. Bandwidth contention between production traffic and monitoring-related traffic.

6. Lack of flexibility around and beyond 5-tuple/marking-based filtering.

7. Security, Compliance and Control (PCI -Peripheral Component Interconnect, HIPAA – Health Insurance Portability and Accountability Act, PII – personally identifiable information, PAI – Privacy Act information) challenges due to requirements of capturing raw traffic data.

8. Challenges around capturing Encrypted Data.

The limitations described above traditionally had direct impact on root cause identification and remediation during network incidents or network security related incidents and other capability mentioned above. Furthermore, the tooling lacked proactive management of network availability and performance forecasting methods.

In addition, as software-defined network (SDN) implementation grow, for successful implementations with overlay and underlay networks, any of the outlined limitations need to be addressed and resolved to varying degrees.

## Current Environment

1. Traffic capturing devices are installed at select key network points and mirror the port/Virtual Local Area Network (VLAN) on the production switches. The production traffic flow is copied to the collector port and, then, analyzed separately. This implementation usually introduces security concern, due to the distributed nature of the tooling, including the overhead of the individual mirror port network devices. The proliferation of the tools itself is creating a burden of cost, scalability and manageability for the network manager. In addition, oversubscription of the traffic will be still a challenge on this implementation.

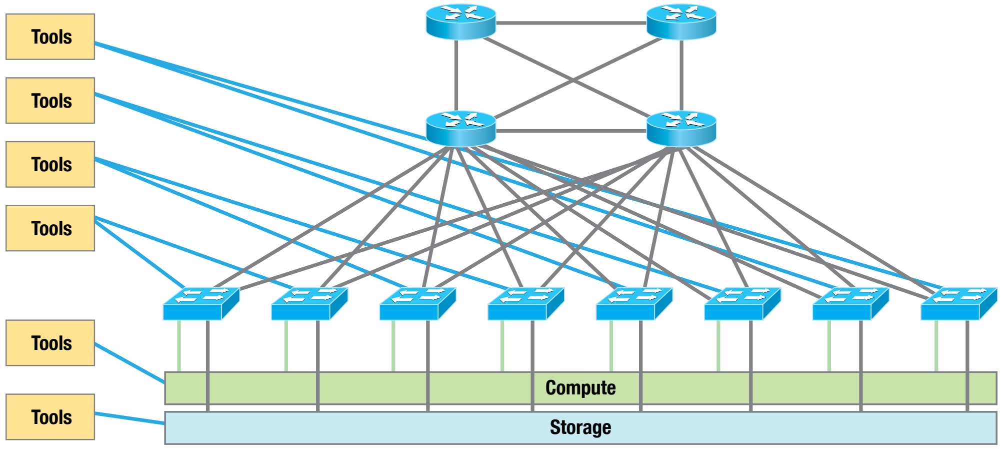

*Figure 1. Current Traffic Capture Approach*

2. To answer the limitation and challenge of point #1, usually, the network manager will try to centralize the tools and then, create a separate physical network to centralize the mirror data capture by the user of local or remote mirroring capability on the network devices. While this answers the proliferation of the tools

itself, the limitation of this approach includes the challenge of data loss due to oversubscription, and the lack of flexibility of the tools usage, due to the limitation of the current 5-tuple filtering capability and mirror/span port limitation.

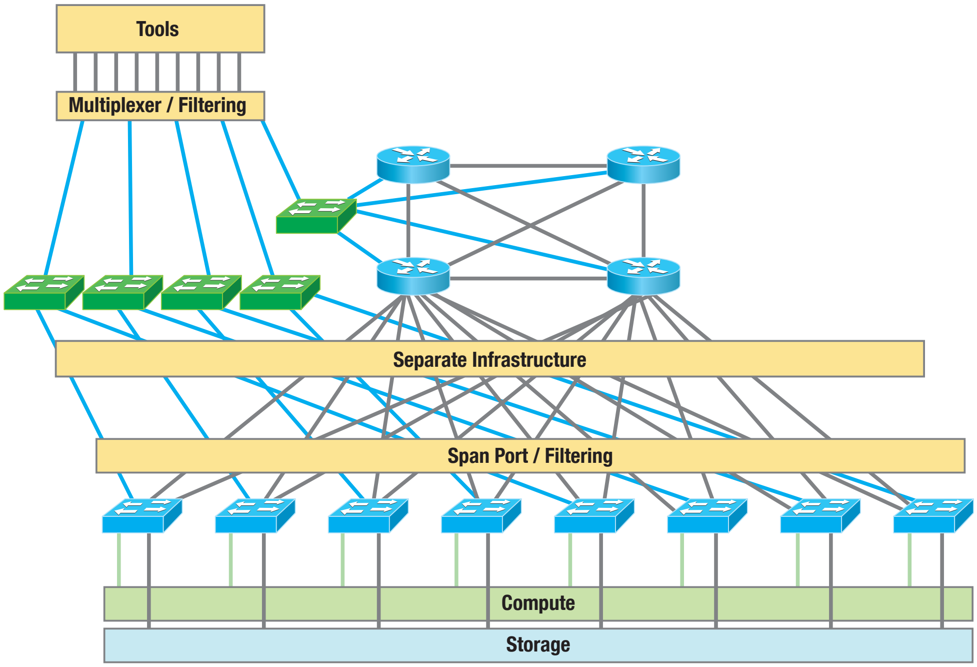

*Figure 2. Centralized Tools & Separate Network*

3. To reduce the limitation of point #2, especially related to data loss and oversubscription, the network manager will implement point #3, where, at each junction of the needed traffic visibility, network/mirror taps will be inserted to fully capture the entire flow of traffic without the challenge of oversubscription. While this implementation answers the challenge of full flow capture, this, however, does not solve the challenge of taps monitoring and the decrease of network reliability. Often this implementation also introduces proprietary encapsulation methods, and/or creating the overhead of forcing encapsulation awareness.

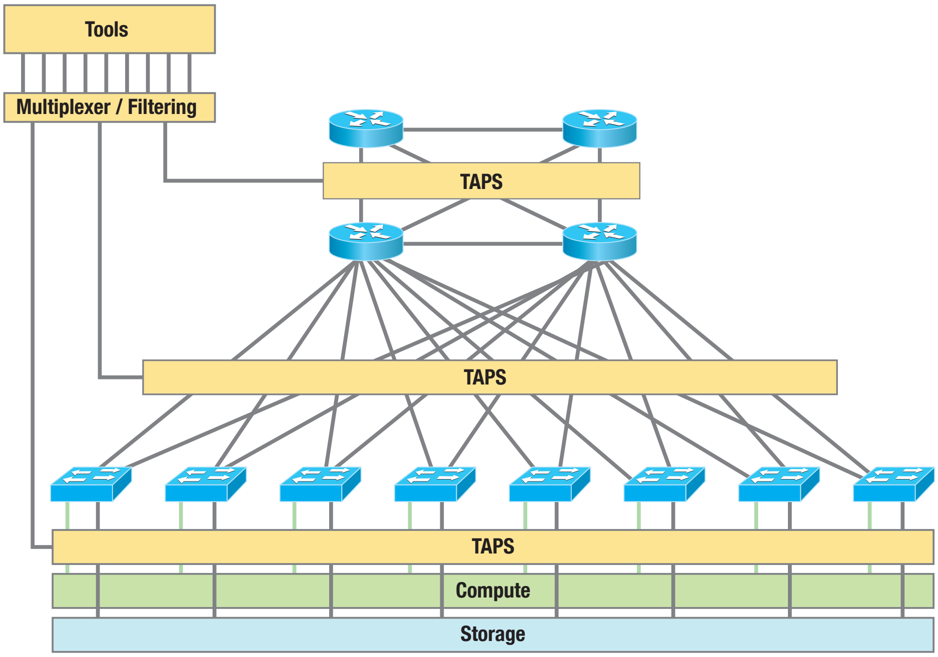

*Figure 3. Parallel taps Installed*

4. The last implementation is the hybrid of the above three implementations, where to work around the above limitation and challenges, multiple hybrid ways are implemented, including the usage of taps, span/mirror and distributed tooling. This implementation allows the reduction of oversubscription of the traffic captured, still keeping network stability and reliability in place, reducing the usage of proprietary encapsulation, and, without proliferating tools deployment. This implementation, however, has a high complexity and support challenge, including the higher cost of both capital and operation.

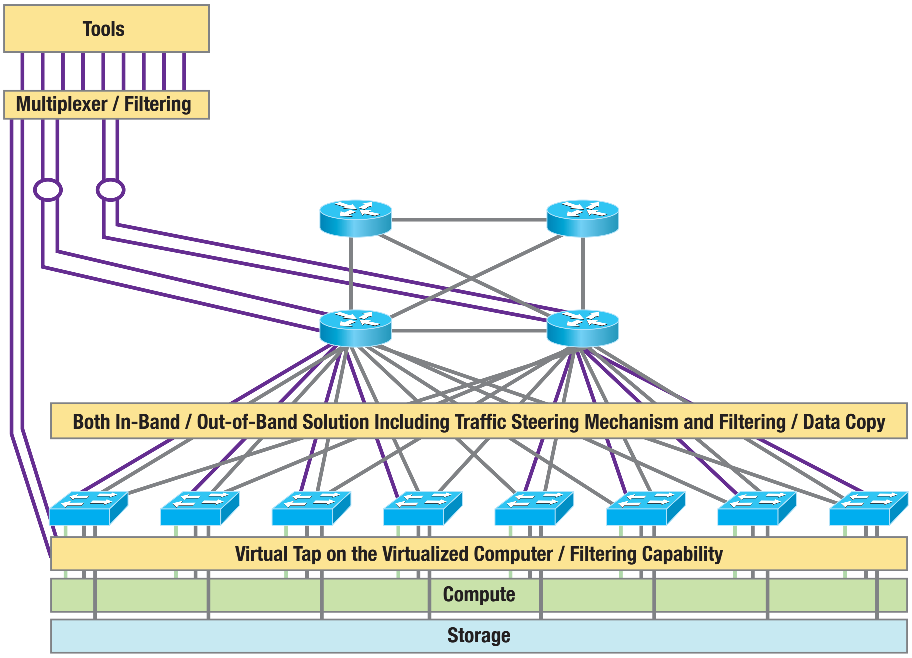
Tools
Multiplexer / Filtering
Both In-Band / Out-of-Band Solution Including Traffic Steering Mechanism and Filtering / Data Copy
Virtual Tap on the Virtualized Computer / Filtering Capability
Compute
Storage

*Figure 4. Desired ONUG Target Environment*

## Conventions

The following conventions are used throughout this document. The requirements that apply to the functionality of this document are specified using the following convention. Items that are REQUIRED (contain the words MUST or MUST NOT) will be labeled as [Rx]. Items that are RECOMMENDED (contain the words SHOULD or SHOULD NOT) will be labeled as [Dy]. Items that are OPTIONAL (contain the words MAY or OPTIONAL) will be labeled as [Oz]. In addition, a priority value of High (H), Medium (M) or Low (L) may be assigned to each item.

The priority will be labeled as [RHx], [DHy] or [OHz] for High priority, [RMx], [DMy] or [OMz] for Medium priority or [RLx], [DLy] or [OLz] for Low priority. The integer values {x, y, z} shall be unique across the document but are not required to be unique across the 3-tuple set {x, y, z}. For example, RM10 and DM10 are allowed whereas RM10 and RL10 are prohibited. Requirements in this document are numbered using increments of 10.

Where needed, related sub-requirements are numbered using increments of 1. The priority assignments are defined as follows.

- **High (H)**: Functionality that must be supported on day one and is critical for baseline deployment.
- **Medium (M):** Functionality that must be supported, but is not mandatory for initial baseline deployment.
- **Low (L):** Desired functionality, which should be supported, but can be phased in as part of a longer-term solution evolution.

## Product Requirement

### Baseline

**RH-10** Commodity hardware.

**RH-20** Granular filtering based on 5-tuple and/or even more., including application signatures, and QoS marking capability.

**RH-30** Capability to work with both underlay and overlay protocols, providing independent filtering on either, and/or correlate both traffic.

**RM-40** Process data without impact to production flow/processing flow (CPU/Memory/Bandwidth).

**RH-50** Horizontal scalability with the capability of resource management feedback.

**RM-60** Allow to run in-band and out-of-band (NetFlow vs. Deep Packet Inspection (DPI), Full DPI vs. Filter DPI, Green Field and Brownfield implementation).

**RM-70** Integrate with current protocol such as NetFlow/sflow or Internet Protocol Flow Information Export (IPFIX).

**RM-80** Provide flexibility to integrate with controller deployment.

**RM-90** Role-based access control and Identify and Access Management (IAM) integration.

TRAFFIC MONITORING/VISIBILITY WORKING GROUP 2015

Open Networking USER GROUP

**RL-100** Scalable across multiple infrastructure models (data center, distributed/branch, enterprise).

**RL-110** Both Virtual and Physical Form Factor.

### Collection

**RH-120** Need to be able to locally process the data and create traffic signaling/alerting, while executing defined traffic-based actions.

**RH-130** Interoperability between vendors: integration and output that will support data collection integration.

**RH-140** Capability of Packet De-duplication/Packet Slicing/Data Masking and Application Recognition, including Packet Organization.

**RH-150** Needs to be Security and Compliance aware.

**RM-160** Capability to integrate with the virtual compute information, such as software span on the virtual switch.

**RM-170** Capability to prioritize highly important monitoring traffic, like applying QoS on the Span (– controlled oversubscription).

**RM-180** Capability to handle SPAN port/monitor port traffic separate from production traffic.

### Processing / Presentation:

**RH-190** Open API for access and management (in/out).

**RH-200** Multilayer visibility between underlay and overlay protocol use for management/SLA, monitoring/alerting, troubleshooting and reporting capabilities.

**RH-210** Common output to assure interoperability between vendors.

**RH-220** Provide Application visibility through Application Signature capability, including custom application signatures for homegrown applications.

## ONUG Traffic Monitoring/Visibility Working Group

| | | | |
|---|---|---|---|
| Aryo Kresnadi | FedEx | Chairman | Contributor/Reviewer |
| Dominic Cafarelli | Gigamon | | Contributor/Reviewer |
| Dario David | ixia | | Reviewer |
| Sanjit Ganguli | riverbed | | Reviewer |
| Travis Griffin | FedEx | | Contributor/Reviewer |
| Shehzad Merchant | Gigamon | | Contributor/Reviewer |
| Zakir Mohideen | VISA | | Contributor/Reviewer |
| Sunay Tripathi | PLURIBUS NETWORKS | | Contributor/Reviewer |
| Sean Wang | UBC THE UNIVERSITY OF BRITISH COLUMBIA | | Contributor/Reviewer |

TRAFFIC MONITORING/VISIBILITY WORKING GROUP
2015
Open Networking
USER GROUP