

Network Working Group  
Internet Draft  
Intended status: Proposed Standard  
Expires: July 2014  
January 23, 2014

Youval Nachum  
Net Optics, an Ixia Company  
Linda Dunbar  
Huawei  
Tal Mizrahi  
Marvell

Network Smart Tapping (SmarTap)  
[draft-nachum-smartap-00.txt](#)

## Abstract

Tapping technologies provide traffic visibility to network analysis tools such as monitors, traffic recorders and security systems. Current tapping architectures and protocols are vendor specific and adapted to legacy networks.

Emerging networking such as large scale datacenters for cloud applications and Mobile backhaul networks demand accurate and fast network traffic visibility. These networks are built on Layer 2 technologies and infrastructure to support virtual machines mobility, growing number of devices including mobile users.

SmarTap architecture is designed to support emerging network requirements allowing network analysis tools to gain full visibility of network traffic. SmarTap technology monitors each link and each component of the network. It captures packets, classifies them and sends them to tools with relevant packet attributes. SmarTap can provide attributes such as flow-ID, tapping-location, tapping-time and statistics.

## Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

---

Internet-Draft

SmarTap

January 2014

The list of current Internet-Drafts can be accessed at  
<http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at  
<http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on July 23, 2014.

#### Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the [Trust Legal Provisions](#) and are provided without warranty as described in the Simplified BSD License.

Internet-Draft

SmarTap

January 2014

## Table of Contents

<a href="#">1.</a>	<a href="#">Introduction .....</a>	<a href="#">4</a>
<a href="#">1.1.</a>	<a href="#">SmarTap Motivation .....</a>	<a href="#">4</a>
<a href="#">1.2.</a>	<a href="#">Terms and Abbreviations Used in this Document .....</a>	<a href="#">4</a>
<a href="#">1.3.</a>	<a href="#">Existing Network Tapping Architecture .....</a>	<a href="#">5</a>
<a href="#">1.4.</a>	<a href="#">Network Analysis Tools Functionality .....</a>	<a href="#">7</a>
<a href="#">1.5.</a>	<a href="#">Emerging Networks .....</a>	<a href="#">7</a>
<a href="#">1.5.1.</a>	<a href="#">Emerging Networks characteristics .....</a>	<a href="#">8</a>
<a href="#">1.6.</a>	<a href="#">Networks Visibility Requirements .....</a>	<a href="#">8</a>
<a href="#">2.</a>	<a href="#">SmarTap Description .....</a>	<a href="#">8</a>
<a href="#">2.1.</a>	<a href="#">SmarTap Functionality .....</a>	<a href="#">8</a>
<a href="#">2.2.</a>	<a href="#">SmarTap Configuration .....</a>	<a href="#">9</a>
<a href="#">2.2.1.</a>	<a href="#">Tapping Location .....</a>	<a href="#">10</a>
<a href="#">2.2.2.</a>	<a href="#">Tapping Time stamping .....</a>	<a href="#">10</a>
<a href="#">2.2.3.</a>	<a href="#">Flow Digest .....</a>	<a href="#">11</a>
<a href="#">2.2.4.</a>	<a href="#">Packet Format .....</a>	<a href="#">11</a>
<a href="#">3.</a>	<a href="#">SmarTap Deployment Options .....</a>	<a href="#">12</a>
<a href="#">3.1.</a>	<a href="#">SmarTap with Network Analysis Tools .....</a>	<a href="#">13</a>
<a href="#">3.2.</a>	<a href="#">SmarTap with Layer-3 Networks .....</a>	<a href="#">14</a>
<a href="#">4.</a>	<a href="#">Security Considerations .....</a>	<a href="#">14</a>
<a href="#">5.</a>	<a href="#">IANA Considerations .....</a>	<a href="#">14</a>
<a href="#">6.</a>	<a href="#">References .....</a>	<a href="#">14</a>
<a href="#">6.1.</a>	<a href="#">Informative References .....</a>	<a href="#">14</a>
<a href="#">7.</a>	<a href="#">Acknowledgments .....</a>	<a href="#">14</a>

## 1. Introduction

Emerging networks such as large scale datacenters and Mobile backhauls demand the use of network analysis tools to enable stable and secure operation of the network. Network analysis tools such as Application Aware Network Performance Monitoring [[AA-NPM](#)], Intrusion Detection Systems (IDS) and Network Recorders (Such as financial transactions and phone calls) require visibility to the raw traffic, its tapping location and its exact tapping time.

Network visibility building blocks are network TAPs, SPAN ports and Network Packet Brokers NPB). TAP refers to a device located at the network which passes a copy of every packet to the monitoring tools. SPAN port, Switched Port Analyzer, mirrors what comes into the target port or out of the target port to the sniffer port for monitoring purposes. NPB device aggregates the monitored traffic from multiple ports to a single port or load balances the monitored traffic to multiple tools.

SmarTap, introduced in this memo, defines a protocol and an architecture that standardize the way network TAPs, SPAN ports and NPBs interact with network analysis tools. SmarTap provides high resolution network visibility by capturing raw packets with their exact tapping-time, tapping-location and relevant statistics and sends it to the tools in a standard form.

### 1.1. SmarTap Motivation

Network analysis tools require full and accurate visibility to the traffic that traverses the network. SmarTap standardizes the way tapping devices communicate with network analysis tools, specifies the information required by the tools and defines its data structure.

## [1.2.](#) Terms and Abbreviations Used in this Document

AA-NPM: Application Aware Network Performance Monitoring

IDS: Intrusion Detection System

NPB: Network Packet Broker

VM: Virtual Machine

Nachum, et al.

Expires July 23, 2014

[Page 4]

Internet-Draft

SmarTap

January 2014

## [1.3.](#) Existing Network Tapping Architecture

Common network tapping architectures consists of network TAPs and Network Packets Brokers (NPBs). All links that are subject to tapping are connected to network TAPs in the following manner. Figure 1 depicts a link between Router-1 and Router-2 that is subject to tapping. The network TAP is connected between router-1 and Router-2 as described by Figure 1.

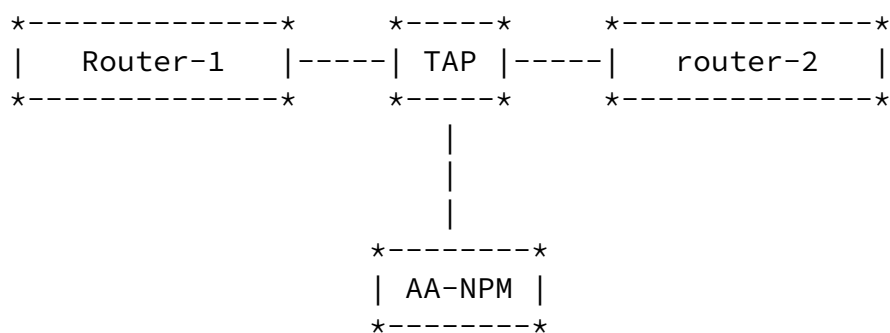


Figure 1 Tapping Device

The network TAP is transparent to Router-1 and Router-2 in all layers. It relays all packets from Router-1 to Router-2 and vice versa without any packet modification.

The network TAP also supports network high availability. In case of TAP failure, the network TAP can be bypassed and router-1 is

directly connected with router-2. In case of link failure at Router-1 or Router-2 the network TAP mimics the failure to the other router to enable network fast reroute.

The network TAP is also connected to the network analysis tools, for example Application Aware Network Performance Monitoring tool (AA-NPM) as described by Figure 1. The network TAP can either redirect the packets to the network analysis tools or just duplicate it, i.e. forward the original packet to the next router and transmit the copied packet to the tool.

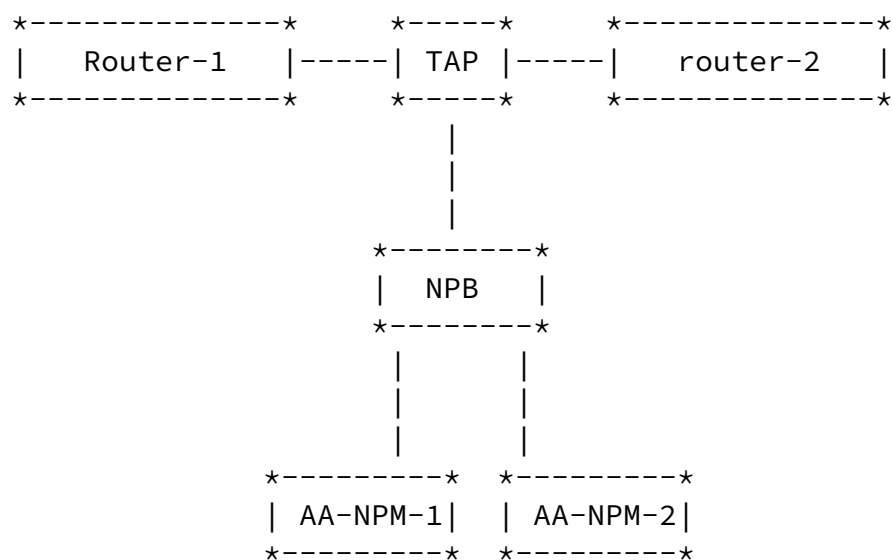


Figure 2 Tapping Device with NPB (regeneration).

Networks that monitor the traffic by multiple tools or monitor multiple links use Network Packet Brokers to aggregate or  
 REF \_Ref367009627 \r \h \\* MERGEFORMAT Figure 2 depicts an NPB duplicates all received packets from the network TAP to AA-NPM-1 and AA-NPM-2. Figure 3 depicts an NPB that aggregates traffic,

i.e., sends all received packets from TAP-1 and TAP-2 to the AA-NPM.

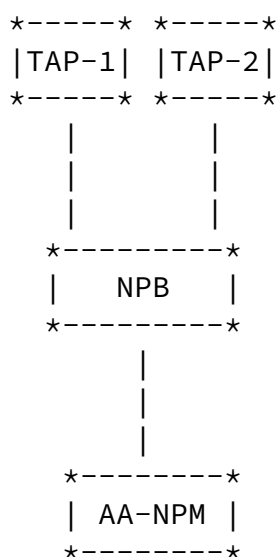


Figure 3 Tapping Device with NPB (aggregation).

#### [1.4.](#) Network Analysis Tools Functionality

Network analysis tools analyze tapped packets according to the packet fields and accompanied data such as:

- Tapping location
- Tapping time
- Packet transmitter and receiver location
- Packet next hop and previous hop
- Flow-ID
- Packet statistics

Network analysis tools in legacy networks deduce the tapping location of the packet from the received port. In networks where the TAP is directly connected to the tool, or using an NPB with a packet redirection, the received port at the tool indicates the

tapping location. Networks using an aggregation NPB mark the tapped packet at the NPB with a vendor specific indication to indicate the received port.

Network analysis Tools at Layer 3 networks deduce the next and previous hop of the tapped packets from the packet source and destination MAC addresses. The packet source MAC address refers to the previous hop router and the packet destination MAC address refers to the next hop router.

At Layer 3 networks the source and destination IP addresses of the tapped packet refer to the source and destination location of the packet transmitter and receiver.

Network analysis tools in legacy networks refer to the tapping time of the tapped packet as the time that the packet is analyzed by the tool or received by the NPB.

### [1.5. Emerging Networks](#)

SmarTap is designed to support emerging networks such as cloud computing, mobile Backhaul, large scale datacenters and finance computing. It also has huge advantages at the legacy Layer 3 networks.

#### [1.5.1. Emerging Networks characteristics](#)

Emerging networks such as mobile backhuls and large scale datacenters support mobile entities like virtual machines and cellular devices. Mobile entities move through the network while their connections remain stable at all networking layers.

Emerging network traffic is mostly Layer 2 based to allow efficient mobility while timing and performance become more critical and accurate.

### [1.6. Networks Visibility Requirements](#)

Some of the characteristic of emerging networks conflict with the behavior of network TAPs, as presented above. Network analysis



tools require full and accurate visibility to the tapped packet location, time and data.

In Layer 2 based network, IP addresses are not location oriented and MAC addresses remain unchanged throughout the packet route. Therefore, the location of the sender and the receiver of the tapped packet cannot be deduced from the IP addresses of the tapped packet, while last hop and next hop cannot be deduced from the tapped packet MAC addresses.

Analysis tools require the exact tapping time of the tapped packets. If the tapping time is measured by the NPB, the time at which a tapped packet is received by the tool or by the NPB includes network propagation delay and is thus not accurate enough.

Emerging networks provide tremendous rate of traffic to analyze in comparison to the processing resources of typical tools. The common way to overcome this gap is by using an NPB to load balance traffic between multiple tools. Emerging networks require additional actions to overcome the increasing gap.

## [2. SmarTap Description](#)

### [2.1. SmarTap Functionality](#)

SmarTap provides additional functionality beyond existing TAP technologies. It taps packets with their relevant metadata and sends it to the tools. Packet metadata includes: Timestamp, Location, related statistics and packet digest. The SmarTap device

is typically connected to a remote tool, and can send the tapped packets with their metadata encapsulated within a tunnel.

SmarTap supports multiple options to mitigate traffic load over the tools. It can truncate tapped packets to a preconfigured size (e.g., 64 or 128 bytes). Tapped packets can be sent to the tools statistically with a preconfigured ratio or rate. Traffic can be monitor by the TAP and sent to the tools conditionally. For example, SmarTap can filter the packets that are sent to the tools according to predefined filters or rate limits.

## 2.2. SmarTap Configuration

SmarTap is a tapping element that is connected to the target tapped link in the same manner as a TAP. Figure 4 depicts a target link between Switch-1 and Switch-2 that needs to be monitored.

The SmarTap is connected to Switch-1 and Switch-2 and is functioning as a regular TAP i.e. the SmarTap is transparent to Switch-1 and Switch-2 and has all TAP capabilities. Moreover, the SmarTap taps packets from Switch-1 to Switch-2 (and vice versa) and sends them to a preconfigured target port with the packets' metadata. The target port can be any port at the SmarTap. Figure 4 "Switch-3". In configuration A the tools or the NPB can be connected to any network element, switch or router, and receive all the tapped packets with their metadata by tunnels. Figure 5 depicts a SmarTap that is directly connected to the tool and sends the tapped packets with their metadata directly to the tool without the need to encapsulate them over tunnels.

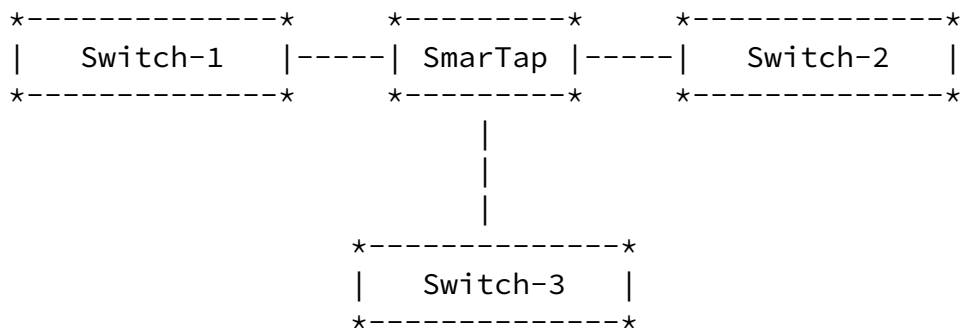
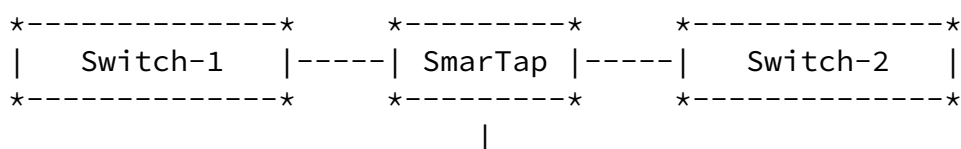


Figure 4 SmarTap Device Configuration A.



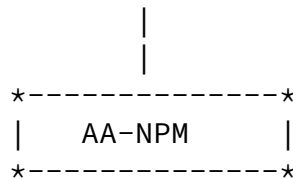


Figure 5 SmarTap Device Configuration B.

### [2.2.1. Tapping Location](#)

One of the tapped packet attributes is its tapping location, which indicates the link the packet was tapped from. In a simple scenario where the SmarTap is connected directly to the tool, the tapping location can be deduced from the received port. Otherwise, the tapping location, if needed, should be inserted to the tapped packet Metadata. There are a few options to describe tapping location:

- . Global Grid references
- . Tap-ID
- . Link-ID
- . Received tunnel

### [2.2.2. Tapping Time stamping](#)

There are several options for sending tapped packets with time stamping:

- . A tapped packet may be sent to the tools with the tapping time at the packet's metadata.
- . A packet may be sent with no packet modification (as it was received on the link).

- . Timestamp may be global or local to the network. Time synchronization and accuracy are determined by the tools.

### [2.2.3.](#) Flow Digest

Tapped packets are sent to the tool with a preconfigured statistic information embedded within the packet metadata, for example packet rate. The configuration of which packets to tap and what is the required statistic information is configured by the monitoring tool. Packet statistics is standard compatible for example sFlow, Netflow or RMON and is collected and provided by the tapping device.

### [2.2.4.](#) Packet Format

Packet format includes the tapped packet and its metadata. A tapped packet may be transmitted to the tool without any packet modification in the same way as it was transmitted on the tapped link. A packet can be also truncated to a predefined size, 64B, 128B.

Optionally, a metadata field is added to the packet. Metadata is in TLV format: Type, Length, and Value.

The tunneling protocol used for tapped packets is IP GRE.

Figure 6 and Figure 7 describe the tapped packet format and a tapped packet example. The packets start from left to right.

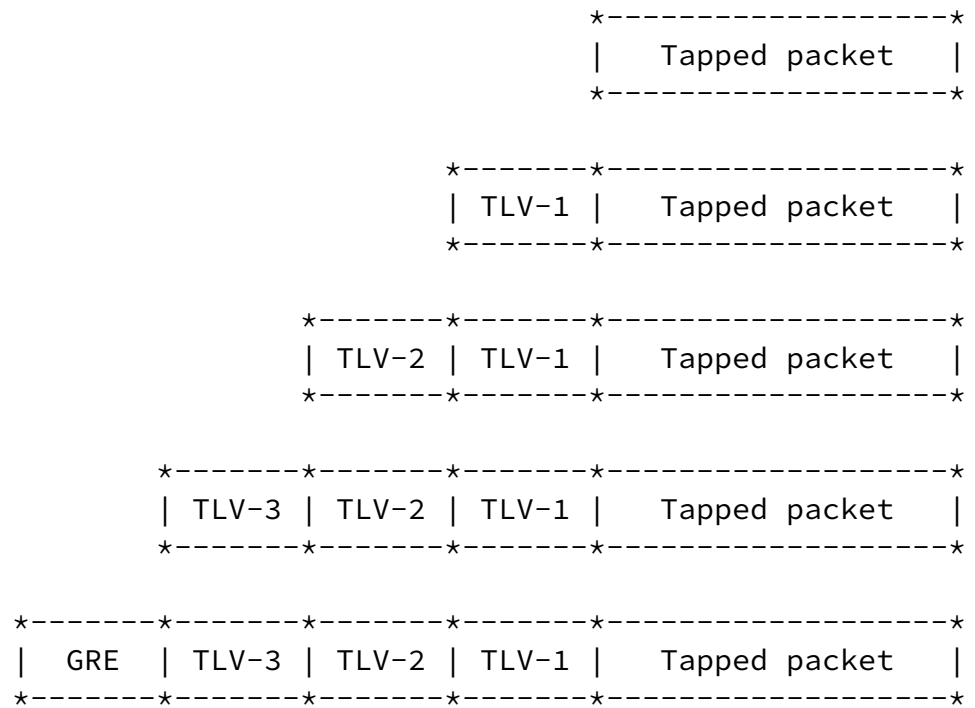


Figure 6 Packet Format.

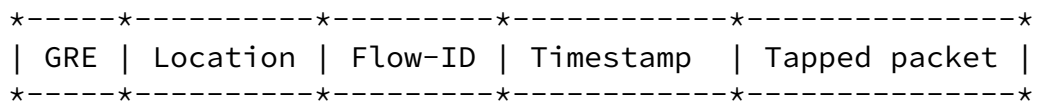


Figure 7 Packet example.

### [3. SmarTap Deployment Options](#)

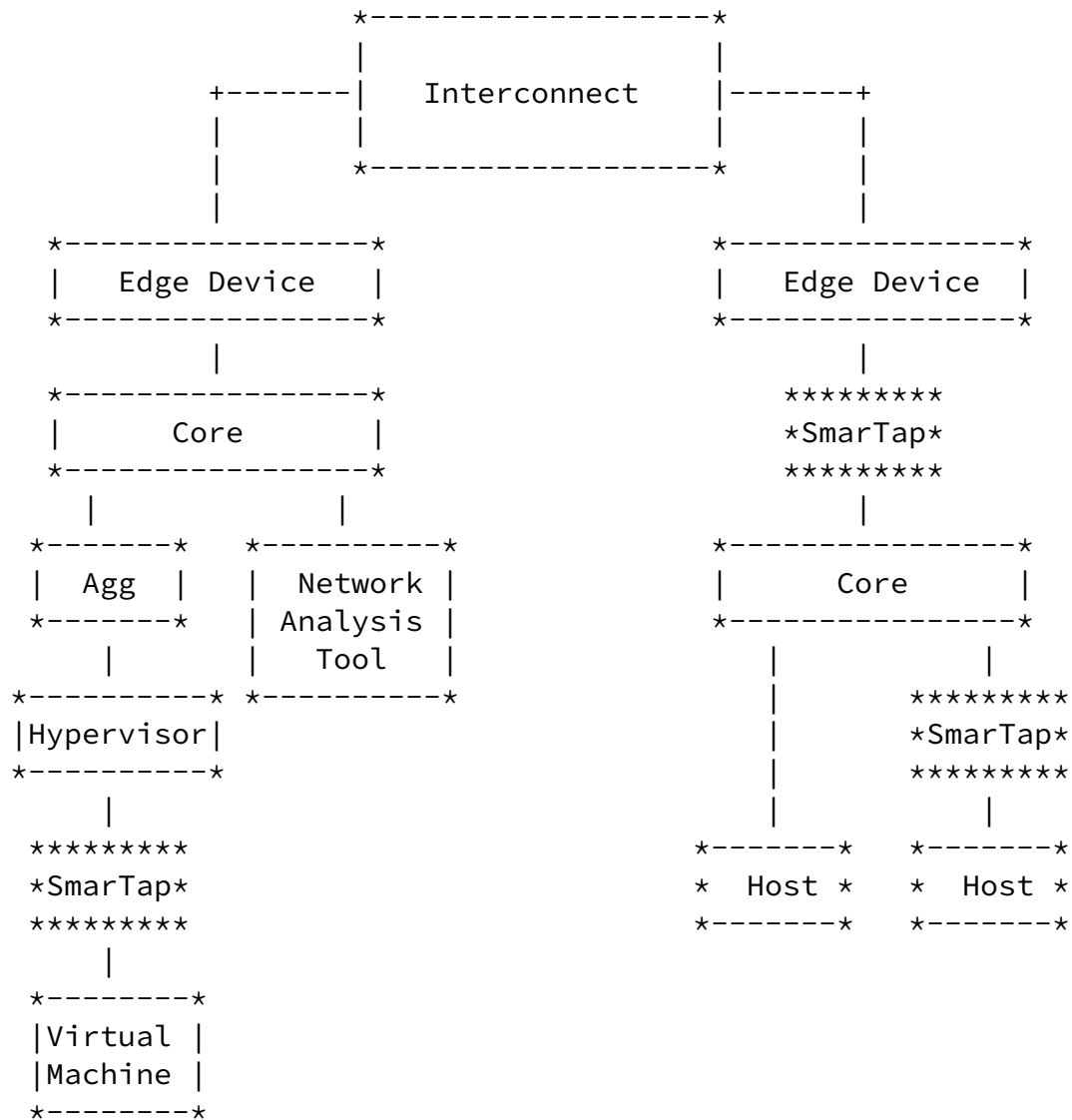


Figure 8 SmarTap deployment example.

SmarTap deployment is tightly connected to the network analysis tool and its visibility requirements. SmarTap is applied on each link that needs to be tapped whether it is a physical link or virtual switch on a hypervisor. Each SmarTap is configured with information such as which data to Tap, what is the required format of the packets and its metadata and the target tools.

### [3.1.](#) SmarTap with Network Analysis Tools

Network analysis tools are connected to all SmarTaps that are relevant to their application. The SmarTaps are either connected directly to the tools or by using tunnels. Each tool gets its

Internet-Draft

SmarTap

January 2014

required information in a central location and creates a networking picture.

SmarTap architecture can offload the tools by distributing the traffic classification and counting to the SmarTaps. In this option tools only get the digested data such as standard statistics with the relevant packets.

Offline tools have also full visibility to all the relevant data they need: the exact location, time and relevant statistics. In this scenario all information received from the SmarTaps is captured, stored and mapped to its exact time and location.

### [3.2](#). SmarTap with Layer-3 Networks

SmarTaps that are used at layer-3 networks are still functioning as TAPs with additional functionality. The tapping location of the received packet, its transmitter and sender location can still be deduced from the MAC and IP addresses of the tapped packet. All SmarTap advantages are also valid for layer-3 networks. SmarTap provides tapped packets with their Metadata, for example: location, tapping time and related statistics. With SmarTap architecture packet tapping location can be derived directly from the metadata which is simple and more accurate.

## [4](#). Security Considerations

To be updated in a future version of this draft.

## [5](#). IANA Considerations

There are no IANA actions required by this document.

RFC Editor: please delete this section before publication.

## [6](#). References

### [6.1](#). Informative References

[AA-NPM] Application Aware Network Performance Monitoring

## 7. Acknowledgments

This document was prepared using 2-Word-v2.0.template.dot.

Nachum, et al.

Expires July 23, 2014

[Page 14]

---

Internet-Draft

SmarTap

January 2014

### Author's addresses

Youval Nachum  
Net Optics, an Ixia Company, IL, LLC  
13 Amal Street, Building A  
Rosh Ha'Ayin, 48091 Israel  
Email: youval@netoiptics.com

Linda Dunbar  
Huawei Technologies  
5430 Legacy Drive, Suite #175  
Plano, TX 75024, USA  
Phone: (469) 277 5840  
Email: ldunbar@huawei.com

Tal Mizrahi  
Marvell  
6 Hamada St.  
Yokneam, 20692 Israel  
Email: talmi@marvell.com



Nachum, et al.

Expires July 23, 2014

[Page 15]