Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 2, 2016

B. Khasnabish
ZTE TX, Inc.
W. Meng
C. Wang
ZTE Corporation

July 1, 2015

Deep Stats Inspection (DSI) and its Applications to Dynamic Service Function Chaining (D-SFC)
draft-kmw-sfc-dsi-apps-00.txt

Abstract

This draft focuses on using Deep Statistics Inspection (DSI) for smart analytics in Service function chaining. DSI can be utilized for service chaining in multi-tenant (Data centers) environment, automated load balancing (ALB), and automated disaster recovery (ADR).

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on January 2, 2016.

Copyright Notice

Copyright (c) 2015 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.

Table of Contents

1. Introduction

Statistics can help SFC to make a right decision on packet forwarding behavior. For example, statistics about overload packets on one Service Function Instance will help SFC to switch path.

DSI is a method of statistics, it can help the service function forwarder (SFF) with additional smartness for analyzing packet-stream's (or flow's) path/routing/processing history, forecasted transit nodes, and destination. The SFF can be physical or virtual or a combination of both in the chained path.

Network/Service Function Grouping (N/SFG): Random grouping of network/service functions is commonly utilized for load distribution and balancing.

Network/Service Function Chaining (N/SFC): Sequential grouping of network/service functions is commonly utilized for service chaining (ordered processing).

Benefits: The comprehensive deep stats knowledge help achieve load balancing dynamically and efficiently. This ultimately will result in improved (a) resources utilization, and (b) user experience and satisfaction.

1.1. Scope

The scope of this document is inspection of deep stats and its utilization in service function chaining (SFC).

Ongoing discussions on virtualization and service chaining in network can be found in the following IETF and IRTF Websites: SFC [http://datatracker.ietf.org/wg/sfc/], I2RS [http://datatracker.ietf.org/wg/i2rs/], SPRING [http://datatracker.ietf.org/wg/spring/],and SDN-RG [http://irtf.org/sdnrg].

Traditional deep packet inspection (DPI) can help service chaining and load balancing only to a certain extent because the actions are taken only after inspecting the packet (header, trailer, payload, etc.)

The proposed deep stats inspection (DSI) invokes the concept of both historical and predicted (based on estimation, time series analysis, etc.) information about the life-cycle of packets and flows in the network.

The intelligence obtained from DSI and DPI can be utilized for cost-

effective and efficient management of (a) the time packets/flows spend in the network and (b) physical and virtualized network resources.

Virtual resources management in the context of Cloud and Data Center (DC) environment using unified API has been discussed in [I-D.junsheng-opsawg-virtual-resource-management].

1.2. Abbreviations

- ADR: Automated Disaster Recovery
- ALB: Automated Load Balancing
- API: Application Programming Interface
- AR: Auto Regressive
- ARIMA: Auto Regressive Integrated Moving Average
- ARMA: Auto Regressive Moving Average
- DC: Data Center
- DLB: Dynamic Load Balancing
- DPI: Deep Packet Inspection
- DR: Disaster Recovery
- DSI: Deep Stats Inspection
- I2RS: Interface to Routing System
- LB: Load Balancing
- MA: Moving Average
- NC: Network Coding
- NE: Network Element
- PDP: Policy Decision Point
- PEP: Policy Enforcement Point
- SDN: Software-Defined Network/Networking

- SE: Service Element
- SFC: Service Function Chaining
- VDC: Virtual DC
- VM: Virtual Machine
- VNE: Virtual NE
- VSE: Virtual SE

1.3. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

The following definitions and descriptions of terms are utilized throughout this draft. When applicable, descriptions of some of the terms are repeated here from other IETF/IRTF document for convenience.

- APP: This refers to Application and/or service. This could be as simple as a script or software package or a module of an executable for a specific application/ service.
- APP Interface: This refers to an interface (e.g., RESTful Java/Web interface) over which the Apps/Services interact with a control platform or an infrastructure element or a management domain or a combination of these.
- DPI: Deep packet inspection refers to inspecting beyond the contents of header of a packet for making policy enforcement and routing decisions.
- SFC: Service function chaining refers to serial (based on a set of pre-specified criteria) or random chaining of a set of service functions to be executed on a stream of packets or a flow of information.
- Multi-Tenant Service Chaining: This is similar to SFC except that the service functions are executed over streams of packets or flows of information of multiple tenants.
- I2RS: This refers to the interface to the routing system; an open interface for facilitating interaction of a client (in Apps/ Service domain) with routing agents resident to the routing

module.

- VNE: This refers to a virtualized network entity. Recently, VNE has been mentioned as virtualized network function (VNF) as well.

- VSE: This refers to a virtualized service (e.g., a firewall) function or entity. A VSE is commonly hosted in one or more virtual machines (VMs).

- PDP: This refers to a point (an entity or a host) that stores all of the policy decision rules.

- PEP: This refers to a point (an entity or a host) that enforces all of the policy decision rules.

- DSI: This refers to a gathering (pre-processing) and inspecting the first, second, and third order statistics related to a stream of packets or a flow in order to better manage routing, traffic, analytics, etc.

- LB: This refers to balancing the offered load to a host, server, or network/service function using one or more static rules.

- DLB: This refers to balancing the offered load to a host, server, or network/service function using one or more dynamic (evolves based on a set of criteria) rules.

- ALB: This refers to balancing the offered load to a host, server, or network/service function using one or more automated criteria and/or rules.

- DR: This refers to recovering from disasters by using redundant and/or standby local or remote "equivalent" resources.

- ADR: This refers to automated recovery from natural and/or man-made disasters.

2. Deep Stats Inspection (DSI)

The major differences between DPI and DSI:

Traditional deep packet inspection (DPI) can help service chaining and load balancing only to a certain extent because the actions are taken only after inspecting the packet (header, trailer, payload, etc.)

The proposed deep stats inspection (DSI) invokes the concept of both historical and predicted (based on estimation, time series analysis,

etc.) information about the life-cycle of packets and flows in the network.

Figure 1 describes a smart (with coded intelligence) flow (or packet stream) classifier. The intelligence about health, security, loading, etc. conditions of SFFs, SFs are gathered and stored in a database and then coded in manner that can be easily utilized by the flow classifier during inspection of the tags/stats of the incoming flows and can be adjusted accordingly without impacting user/service experience. This database provides inputs directly to the flow director/classifier for dynamically adjusting the tags/stats of the incoming flows.

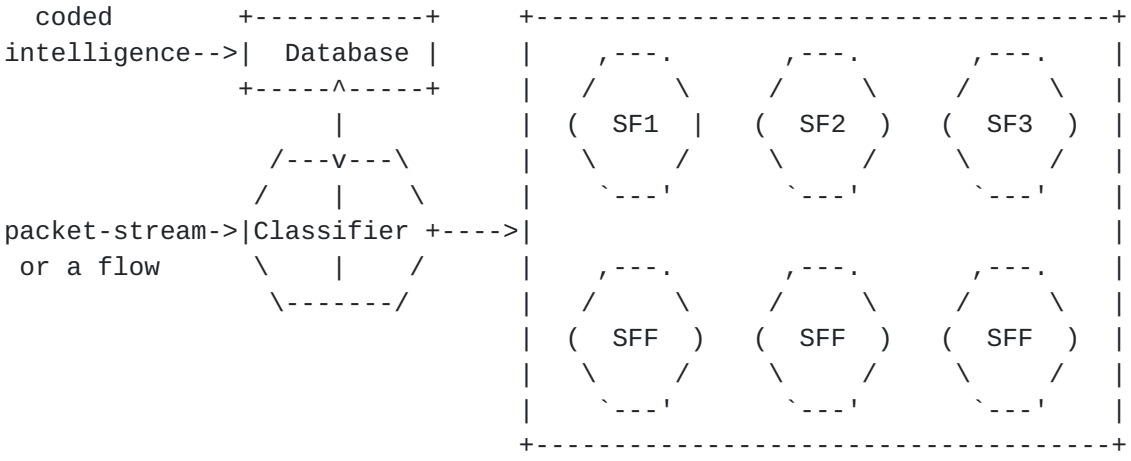

Figure 1: A Smart Classifier based on Deep Stats Inspection (DSI)

The classifier categorizes the incoming flows based on the tags associated with the flows. It may be also be possible to utilize some minor statistics that may be available in the flow!_s header. The categorized flows are sent through a series of service functions (SFs) or through the network functions (NFs) via the SFF/NF. Note that both SF/SFF and NF can be physical or virtual or a combination of both in the path of the service chain. The classifier usually does not have any knowledge of the loading or other conditions of any of the forwarders (SFF or NFF) which may cause serious performance and service bottlenecks or impairments in user experience.

if with a smart (with coded intelligence) flow (or packet stream) classifier, as mentioned before, the coded intelligence is derived from monitoring (health, loading, security, etc. conditions) the SFFs and NFFs.

The following is one possibility for defining the granularity of monitoring of the conditions.

SFF (or NFF) Health condition = {frail, modest, steady}

SFF (or NFF) Loading condition = {low, medium, high}

SFF (or NFF) Security condition = {at-risk, vulnerable, safe}

The monitoring frequency can be preconfigured to a default value or dynamically adjusted based on ay set of criteria.

A flow can be routed to an SF through an NF in addition to being routed directly from an SFF. The SFF can process the incoming flows in a round-robin fashion or on a first-come-first-serve basis or using any other intelligent incoming flow processing mechanism. The statistics tag of the flows can be utilized for intelligent servicing of the flows in the service function (SFs) which can be physical or virtual or a combination of both.

3. Management and Orchestration

TBD

4. API to Deep Stats Storage

The added flexibility (due to using an open API) will allow dynamic navigation of sessions/flows through a variety of network operations systems and physical/virtual infrastructure network/service elements. This will help achieve unified and seamless user experience irrespective of what the underlying network infrastructure is.

5. Deep Stats Lifecycle Management

TBD

6. Security Considerations

TBD

7. IANA Considerations

This document introduces no additional considerations for IANA.

8. Acknowledgments

The author(s) would like to thank many colleagues for their discussions and support.

9. References

9.1. Normative References

[I-D.junsheng-opsawg-virtual-resource-management] Chu, J., Khasnabish, B., Qing, Y., and Y. Meng, "Virtual Resource Management in Cloud", draft-junsheng-opsawg-virtual-resource-management-00 (work in progress), July 2011.

[I-D.karavettil-vdcs-security-framework] Karavettil, S., Khasnabish, B., Ning, S., and W. Dong, "Security Framework for Virtualized Data Center Services", draft-karavettil-vdcs-security-framework-05 (work in progress), December 2012.

[I-D.khasnabish-cloud-reference-framework] Khasnabish, B., Chu, J., Ma, S., So, N., Unbehagen, P., Morrow, M., Hasan, M., Demchenko, Y., and M. Yu, "Cloud Reference Framework", draft-khasnabish-cloud-reference-framework-08 (work in progress), April 2015.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement

Levels", BCP 14, RFC 2119, March 1997.

9.2. Informative References

[RFC3654] Khosravi, H. and T. Anderson, "Requirements for Separation of IP Control and Forwarding", RFC 3654, November 2003.

[RFC3746] Yang, L., Dantu, R., Anderson, T., and R. Gopal, "Forwarding and Control Element Separation (ForCES) Framework", RFC 3746, April 2004.

Authors' Addresses

Bhumip Khasnabish
ZTE TX, Inc.
55 Madison Avenue, Suite 160
Morristown, New Jersey 07960
USA

Phone: +001-781-752-8003
EMail: vumip1@gmail.com, bhumip.khasnabish@ztetx.com
URI: http://tinyurl.com/bhumip/

Wei Meng
ZTE Corporation
No.50 Software Avenue, Yuhuatai District
Nanjing
China

EMail: meng.wei2@zte.com.cn,vally.meng@gmail.com

Cui Wang
ZTE Corporation
No.50 Software Avenue, Yuhuatai District
Nanjing
China

EMail: wang.cui1@zte.com.cn