Network Working Group
Internet-Draft
Intended status: Informational
Expires: August 18, 2014

S. Lee
M. Shin
ETRI

February 14, 2014

Service Function Chaining Verification
draft-lee-sfc-verification-00

Abstract

This document addresses the possible conflicts among different service function chains. These conflicts may occur when 1) a traffic flow satisfies two or more classification rules of different service function chains; and 2) a service function cannot provide enough resource for a service function chain due to load of other service function chains. These conflicts need to be detected and resolved at deploying a new service chain.

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 August 18, 2014.

Table of Contents

1. Introduction

The current service delivery model is bound to static topologies and manually configured resources. This has motivated a more flexible deployment model which orchestrates the service delivery separated from the network. Service Function Chaining (SFC) [I-D.ietf-sfc-problem-statement] provides a new service deployment model that delivers the traffic along the predefined logical paths of service functions (i.e., service overlays or service chains). The service overlay provides a specific order of network services with no regard of network topologies. The traffic is classified with a set of rules in different granularity to select a target service overlay.

The service overlays are configured to be isolated from each other with virtualization of the network resources and different traffic classification rules. However, the service overlays can share the physical network resources (such as network links, service nodes, and service functions); and the traffic classification rules can overlap each other. This may cause unexpected QoS degradation in a composite network service due to network service overload; and service failure due to loops or interventions of the service overlays. It is required to detect and resolve these conflicts when deploying a new service function chain.

This document formulates these problems as two conflicts at deploying service function chains: rule conflict and resource conflict.

2. Problem Areas

The problem areas of the conflicts can be specified as follows:

1. Rule conflict:

An incoming traffic flow (i.e., a series of packets) is classified according to a classification rules to determine which service function chain will handle it. The classification is based on the contents of one or more packet header fields so that the classification rule may vary in different granularity. This may bring a problematic case that an incoming packet matches two or more classification rules of different service function chains, which can result in a service chain loop or intervention. For example, let's assume that there are two service function chains: SFC_A which handles the video traffics; and SFC_B which handles the packets sent by host H. Video traffic from host H satisfies both of SFC_A and SFC_B and this brings a rule conflict at service classification.

2. Resource conflict:

A service function chain constitutes a service-specific overlay that utilizes network resources such as service nodes, network links between service functions, and service function instances. These network resources may be shared by different service function chains. This brings an uncertainty in QoS of service function chains if there is no coordination for the use of network resources. For example, let's assume that a service function instance F is shared by the service function paths of SFC_A and SFC_B. If the service function instance F is fully loaded by the traffic over SFC_A, SFC_B cannot provide an expected service quality due to resource shortage.

3. Verification of Service Function Chains

The aforementioned problems arise from the conflicts between two or more service function chains. Thus, it is required to have a verification function to detect and avoid those conflicts.

The rule conflict can be detected by examining if there is any overlapping in a new classification rule with the existing classification rules when deploying a new service function chain. A bitwise comparison of target packet headers can be used for the examination. However, if the rules classify the packets with the header filed values in different layers (e.g., IP address and TCP port), then inclusive relationship between different classification rules should be also considered.

When a new classification rule is detected to have a conflict with the existing ones, then the new service function chain should be rejected to remove an uncertainty. While different priorities of the classification rules in a conflict can be used instead, it may bring higher complexity in rule matching and priority decisions.

The resource conflict can be detected by checking if the resource of the network and service functions is available enough for the new service function chain. An explicit request for the resources can be made beforehand by the service function chain or the resource usage can be dynamically determined by classified traffic over the service function path. When the resource is not available enough for a request, the new service function chain can be rejected to be deployed. An alternative service function path can be dynamically initiated instead to utilize different network resources or service function instances for the chain.

4. Security Considerations

TBD.

5. IANA Considerations

TBD.

6. References

6.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

6.2. Informative References

[I-D.ietf-sfc-problem-statement] Quinn, P. and T. Nadeau, "Service Function Chaining Problem Statement", draft-ietf-sfc-problem-statement-00, January 2014.

Authors' Addresses

Seung-Ik Lee
ETRI
218 Gajeong-ro Yuseung-Gu
Daejeon 305-700
Korea

Phone: +82 42 860 1483
Email: seungiklee@etri.re.kr

Myung-Ki Shin
ETRI
218 Gajeong-ro Yuseung-Gu
Daejeon 305-700
Korea

Phone: +82 42 860 4847
Email: mkshin@etri.re.kr