Service Function Chaining (sfc)
Internet-Draft
Intended status: Experimental
Expires: February 16, 2017

Yogendra Pal
Cisco
Venkata SRG
Citrix
Vikram Menon
Ericsson

August 16, 2016

DHCP option for NSH in Service Function Path (SFP)
draft-ypal-sfc-dhcp-option-for-nsh-for-sfp-02

Abstract

This draft specifies Dynamic Host Configuration Protocol option (both DHCPv4 and DHCPv6) for NSH aware clients participating in the service function path(SFP) of the service chaining. As part of this proposal SFF and SF will receive the SFP information containing Service Path Identifier(SPI), Transport protocol and Nexthop(NH) address of subsequent SFF/SF.

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 February 16, 2017.

Copyright Notice

Table of Contents

1. Requirements Language

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 RFC 2119 [RFC2119].

2. Introduction

In NSH aware service chaining model, SFF needs to be provisioned with SFP information. In the current environment, the operator manually provisions each network elements(SFF) with SFP information. This does not scale well when on-demand service functions are introduced and brought down in virtualized networks in cloud, datacenter, and so

forth deployments. This draft is trying to automate this network rollout of service chaining using the DHCP option. Each SFF willing to participate in NSH aware service chain model will indicate its interest to the DHCP server for SFP and gets provisioned accordingly from the DHCP server.

2.1 Terminology

This document uses the terminology defined in draft-ietf-sfc-nsh with respect to service function chain.

DHCP client: A DHCP [1] client is an Internet host that uses DHCP to obtain configuration parameters such as a network address.

DHCP server: A DHCP server is an Internet host that returns configuration parameters to DHCP clients.

Service Function Forwarder (SFF): A service function forwarder is responsible for delivering traffic received from the SFCNF to one or more connected service functions, and from service functions to the SFC network forwarder(SFCNF).

Service Function (SF): A function that is responsible for specific treatment of received packets. A service function can act at the network layer or other OSI layers. A service function can be a virtual instance or be embedded in a physical network element. One of multiple service functions can be embedded in the same network element. Multiple instances of the service function can be enabled in the same administrative domain.

Service Function Path (SFP): The instantiation of a SFC in the network. Packets follow a service function path from a classifier through the requisite service functions.

3. Model and Applicability

In service chaining model, SFC controller will provision SFF with details of service function paths SFP(s). In order to provision SFP details to SFF(s), controller needs some mechanism to configure the SFF. DHCP protocol is one of the existing mechanism for provisioning various network information to any DHCP clients.

Existing DHCP version 4 and 6 will be extended to incorporate option of provisioning dynamically SFP details to SFF. In this case, controller can be considered to act as DHCP server.

3.1 Example service chain network

See Figure 1, depicting SFF (DHCP clients) interacting with SFC controller (DHCP server) to register and getting provisioned with SFP details.

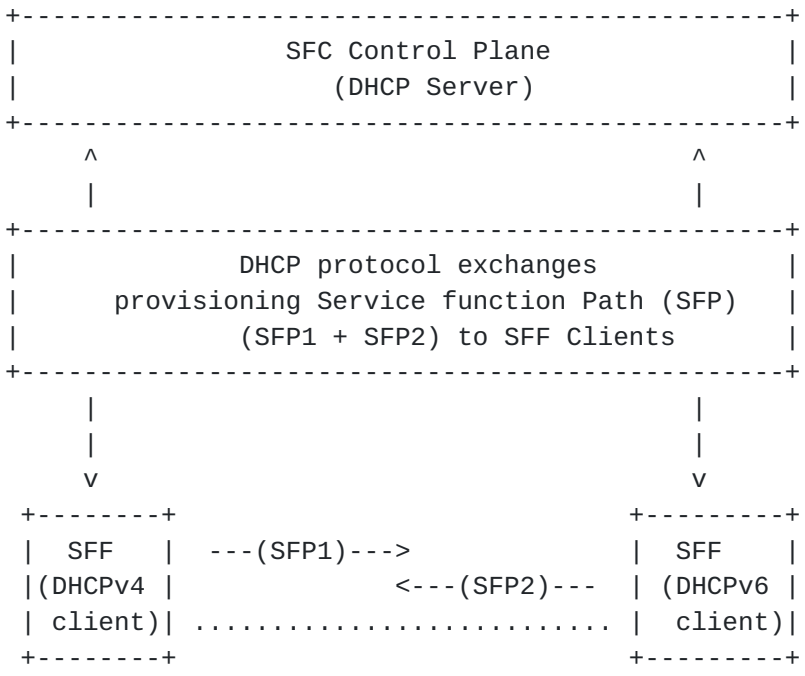

Figure 1: SFF enabled DHCP clients in service chaining

4. SFP DHCP Option Formats

The SFP information is composed of a generic SFP header, followed by one or more SFP entries, as shown in Figure 2.

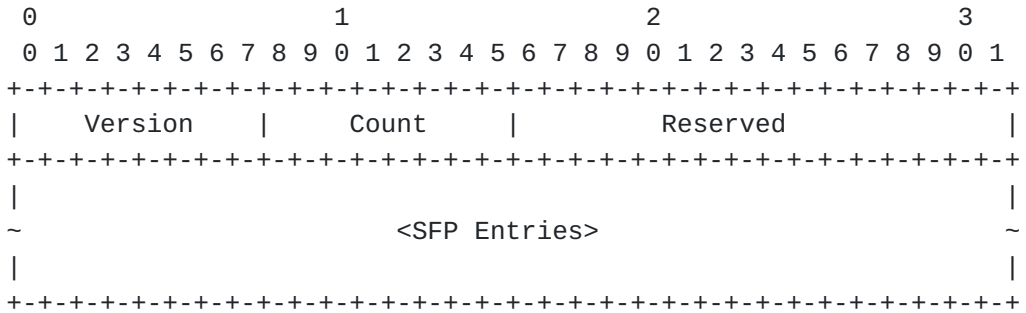

Figure 2: SFP Information

Version: SFP Information version (0), 1 Octet.
Count: This field indicates total number of SFP entries. This is 1 octet.
Reserved: MUST be set zero.
SFP Entries: One or more SFP entries, each composed Transport type, Protocol ID, SP header (SPH) and followed by one or more SFP-NH entries, as shown in Figure 3.

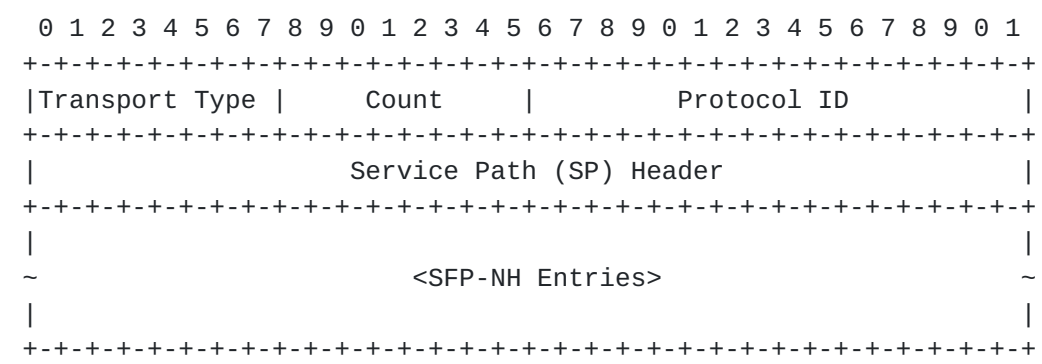

Figure 3: SFP Entry

Transport Type: This field indicates the type of transport layer attribute. Examples: L2, L3, L4. Values for transport type are following:

Transport Types	Value(in decimal)
L2	2
L3	3
L4	4

Table 1: Transport Types

Count: This field indicates total number of SFP-NH entries with the given Transport Type, Protocol ID and SP Header. This is 1 octet.

Protocol ID: This field indicates the actual protocol layer encapsulating the NSH. This is to be read and understood in accordance with Transport Type field. Values for this field are following:

Protocol ID	Value(in decimal)
Ethernet	35151
VXLAN-gpe	4790

| GRE | 47 |
| UDP | 6633 |

Table 2: Protocol ID

Example of {Transport Type, Protocol ID} SHOULD be seen as below:

Transport Type	Protocol ID
2	35151
2	4790
3	47
4	6633

Table 3: Association of Transport Type and Protocol ID

SP header is composed of Service Path ID and Service Index, shown in Figure 4.

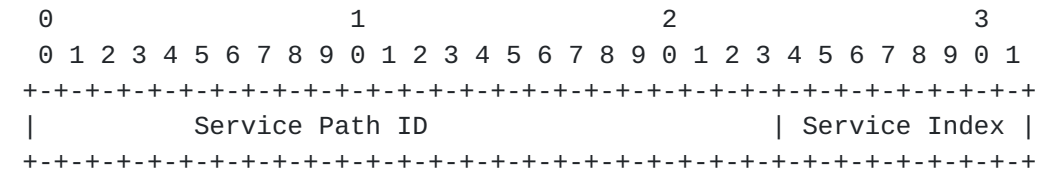

Figure 4: Service Function (SF) Header

Service Path ID (SPI): 24 bits
Service Index (SI): 8 bits
As defined in draft
[https://tools.ietf.org/html/draft-ietf-sfc-nsh-05#section-3.3]

SFP-NH Entries: One or more SFP-NH entries, as shown in Figure 5.

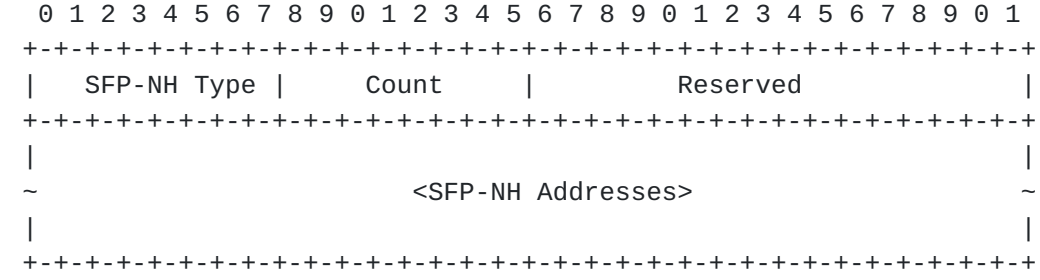

Figure 5: SFP-NH Entry

SFP-NH Type: Nexthop address types (1 Octet).

SFP-NH Type	Value (in decimal)
IPv4	1
IPv6	2
Ethernet	3

Table 4: SFP-NH Type Values

Count: This field indicates total number of SFP-NH addresses with the given SFP-NH type. This is 1 octet
Reserved: MUST be set zero.
SFP-NH addresses: One or more SFP nexthop addresses of same SFP-NH type.

4.1 DHCPv4 Options

4.1.1 DHCPv4 NSH SFP Option

The NSH SFP option can be used by DHCP servers to communicate SFP information to DHCPv4 clients, either in a stateful DHCPv4 address configuration or renewal transaction, or in a stateless information request (DHCPINFORM).

The format of NSH SFP option for DHCPv4 is:

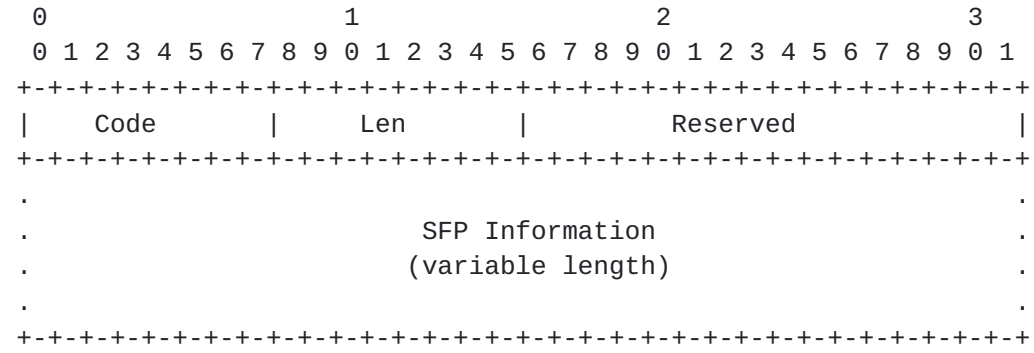

Figure 6: DHCPv4 NSH SFP option

Code: OPTION_NSH_SFP
(TBD1, 8 bit value, to be assigned by IANA).

Len: Length of SFP Information in 32 bit words.

Reserved: MUST be set zero.

SFP Info: Service function path details.

Refer Section 4 to see format and details of SFP information.

4.2 DHCPv6 Options

4.2.1 DHCPv6 NSH SFP Option

The NSH SFP option can be used by DHCPv6 servers to communicate SFP information to DHCPv6 clients, either in a stateful DHCPv6 address configuration or renewal transaction, or in a stateless information request (Information-request).

The format of NSH SFP option for DHCPv6 is:

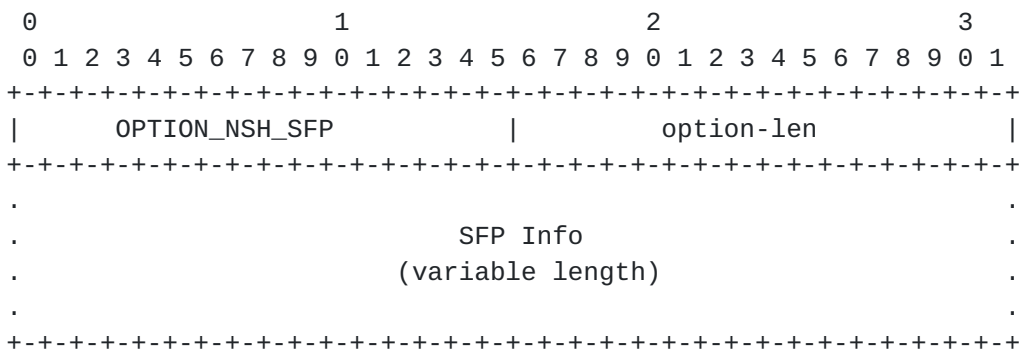

Figure 7: DHCPv6 NSH SFP option

option-code: OPTION_NSH_SFP
(TBD2, 16 bit value, to be assigned by IANA).

option-len: Length of SFP Information in octets.

SFP Info: Service function path details.

Refer section 4 to see format and details of SFP information.

5. Request and Processing DHCP SFP Option

In the service chaining model, SFF DHCP clients willing to participate in SFP can request SFP information from the DHCP server using the OPTION_NSH_SFP option. Details of this request in DHCPv4 and DHCPv6 are detailed in below sections.

5.1 DHCPv4 Client Behaviour

DHCPv4 client enabled with the capability of doing SFF/SF role in SFP MUST request for SFP information in DHCPDISCOVER and DHCPREQUEST of DHCPv4 protocol exchanges. Client behaviour is detailed below.

5.1.1 Requesting OPTION_NSH_SFP

SFF enabled DHCPv4 clients interested in SFP MUST send the OPTION_NSH_SFP option to the DHCPv4 server along with other

options in Parameter Request List (PRL). DHCPv4 clients supporting this option, should support FORCERENEW message exchange for any dynamic updates in SFP from DHCPv4 server.

DHCP clients that support the SFF option must handle the case where SFF functionality is configured after the client has been started. This can be handled by the client either by renewing its lease when SFF functionality is configured, or by sending a DHCPINFORM message.

5.2 DHCPv6 Client Behaviour

DHCPv6 client enabled with capability of doing SFF/SF role in SFP can request for SFP information at different stages of DHCPv6 protocol exchanges. Client behaviour is detailed below.

5.2.1 Requesting OPTION_NSH_SFP

SFF enabled DHCPv6 client interested in SFP MUST send the OPTION_NSH_SFP option to the DHCPv6 server along with other options in Option Request Option (ORO).

DHCPv6 clients that support the SFF option must handle the case where SFF functionality is configured after the client has been started. This can be handled by the client either by renewing its lease when SFF functionality is configured, or by sending a Information-request message.

DHCPv6 clients supporting this option, should support reconfigure message exchange for any dynamic updates in SFP from DHCPv6 server.

5.3 DHCP Server Behaviour

DHCPv4 and DHCPv6 server if configured to provide service chaining SFP parameters, SHOULD provision the SFF clients as per their administrative policy. DHCPv4 and DHCPv6 server can receive request for option OPTION_NSH_SFP from clients in Parameter Request List (PRL) and Option Request Option (ORO) respectively.

When a DHCPv4 and DHCPv6 server has been configured with different SFP parameters, the administrator or agent that updated the configuration should trigger FORCERENEW/DHCPINFORM and Reconfigure messages respectively for any DHCPv4 and DHCPv6 clients that now have stale configurations.

5.3.1 Processing OPTION_NSH_SFP Request

Clients do not send OPTION_NSH_SFP to servers; therefore, servers that receive this option should take no special action as a result of having received it.

5.3.2 Notifying update in SFP path to SFF

Any update to notify about change in service chain path is notified to SFF client using Reconfigure Message as defined in section 22.19 of [RFC3315] for DHCPv6 and FORCERENEW message exchange as defined in [RFC3203] of DHCPv4.

6. Security Considerations

Since there is no privacy protection for DHCP messages, an eavesdropper who can monitor the link between the DHCP server and requesting client can discover the SFP information.

To minimize the unintended exposure of SFP, the OPTION_NSH_SFP option SHOULD be returned by DHCP servers only when the DHCP client has requested this option in its request (Section 9.8 of [RFC2132]).

Networks where this option is used SHOULD use link-layer security and integrity protection. Additionally, such networks should filter out rogue DHCP messages (RFC 7610).

7. IANA Considerations

This document defines a new DHCP option, entitled "OPTION_NSH_SFP" (see Section 4.1 and 4.2) for DHCPv4 and DHCPv6 respectively. Assigned a value of TBD1 and TBD2 from the DHCPv4 [to be removed upon publication: http://www.iana.org/assignments/bootp-dhcp-parameters] [DHCP-OPTIONS] [DHCP-IANA] and DHCPv6 (Section 24.3 of RFC 3315) option space defined respectively.

Tag	Name	Data Length	Meaning
TBD1	OPTION_NSH_SFP	1 octet	DHCPv4 NSH SFP option
TBD2	OPTION_NSH_SFP	2 octet	DHCPv6 NSH SFP option

IANA is requested to create a new "DHCP NSH SFP parameters" registry. The following sub-sections request new registries within the "DHCP NSH SFP parameters" registry.

7.1 Transport types

Transport Type	Description	Reference
2	L2 transports	This document
3	L3 transports	This document
4	L4 transports	This document

Table 5

7.2 SFP Nexthop types

SFP-NH Type	Description	Reference
1	IPv4	This document
2	IPv6	This document
3	Ethernet	This document

Table 6

7.3 Protocol ID

Protocol ID values referenced in this draft Section 4, Table 2 is more towards using the values and no action is required from IANA towards it.

8. Acknowledgements

The authors would like to thank Ted Lemon, Youcef Laribi for the constructive comments to initial draft.

9. References

9.1 Normative References

[RFC0768] Postel, J., "User Datagram Protocol", STD 6, RFC 768, August 1980.

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

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[RFC2132] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, March 1997.

[RFC2939] Droms, R., "Procedures and IANA Guidelines for Definition of New DHCP Options and Message Types", BCP 43, RFC 2939, September 2000.

[RFC3203] T'Joens, Y., Hublet, C., and P. De Schrijver, "DHCP reconfigure extension", RFC 3203, December 2001.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C. and M. Carney, "Dynamic Host Configuration Protocol for IPv6", July 2003.

[RFC6225] J. Polk., M. Linsner., M. Thomson., B. Aboba, Ed., "Dynamic Host Configuration Protocol Options for Coordinate-Based Location Configuration Information", July 2011.

[I-D.ietf-sfc-nsh] Quinn, P. and U. Elzur, "Network Service Header", draft-ietf-sfc-nsh-00 (work in progress), March 2015.

9.2 Informative References

[RFC6335] Cotton, M., Eggert, L., Touch, J., Westerlund, M., and S. Cheshire, "Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry", BCP 165, RFC 6335, August 2011.

[RFC7348] Mahalingam, M., Dutt, D., Duda, K., Agarwal, P., Kreeger, L., Sridhar, T., Bursell, M., and C. Wright, "Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks", RFC 7348, August 2014.

[RFC7610] F. Gont, W. Liu, G. Van de Velde, "DHCPv6-Shield: Protecting against Rogue DHCPv6 Servers", BCP 199, August 2015

[RFC7665] Halpern, J., Ed. and C. Pignataro, Ed., "Service Function Chaining (SFC) Architecture", RFC 7665, DOI 10.17487/RFC7665, October 2015, <http://www.rfc-editor.org/info/rfc7665>.

[DHCP-OPTIONS]
Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, March 1997.

[DHCP-IANA]
Droms, R., "Procedures and IANA Guidelines for Definition of New DHCP Options and Message Types", BCP 43, RFC 2939, September 2000.

[I-D.draft-ietf-sfc-control-plane-06]
Li, et al., "Service Function Chaining (SFC) Control Plane Components & Requirements", draft-ietf-sfc-control-plane-06 (work in progress), May 2016.

Author's Address

Yogendra Pal
Cisco Systems, Inc.
Cessna Business Park,
Varthur Hobli, Outer Ring Road,
Bangalore, Karnataka 560103
India

EMail: yogpal@cisco.com

VenkataSubbaRao Gorrepati
Citrix R&D India Pvt Ltd,

Prestige Dynasty #33, Ulsoor Road
Bangalore, Karnataka 560042
India

EMail: venkatasubbarao.gorrepati@citrix.com

Vikram Menon
Ericsson India Global Services Pvt Ltd
Bangalore, Karnataka
India

EMail: vikram.menon@ericsson.com