Service Function Chaining (sfc)
Internet-Draft
Intended status: Standard Tracks
Expires: August 16, 2016

Yogendra Pal
Cisco
Venkata SRG
Citrix
Vikram Menon
Ericsson

February 16, 2016

DHCP option for NSH in Service Function Path (SFP)
draft-ypal-sfc-dhcp-option-for-nsh-for-sfp-00

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 August 16, 2016.

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.

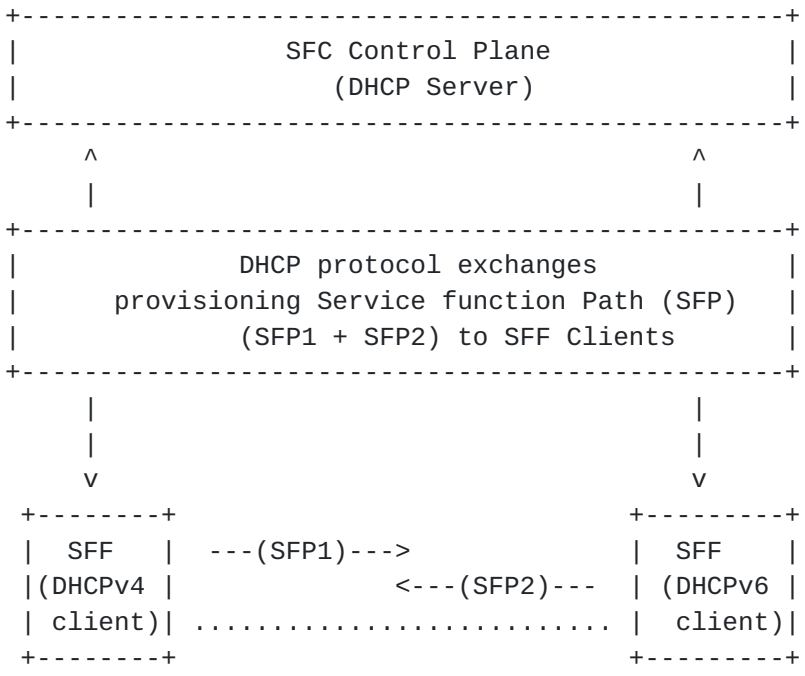

Figure 1: SFF enabled DHCP clients in service chaining

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.

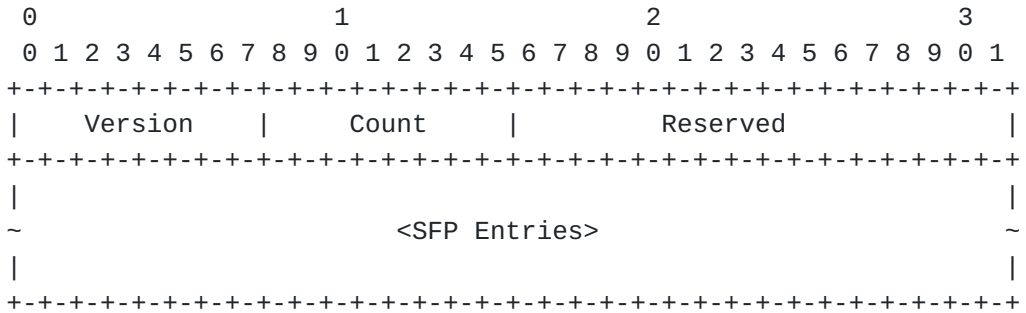

Figure 2: SFP Information

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.

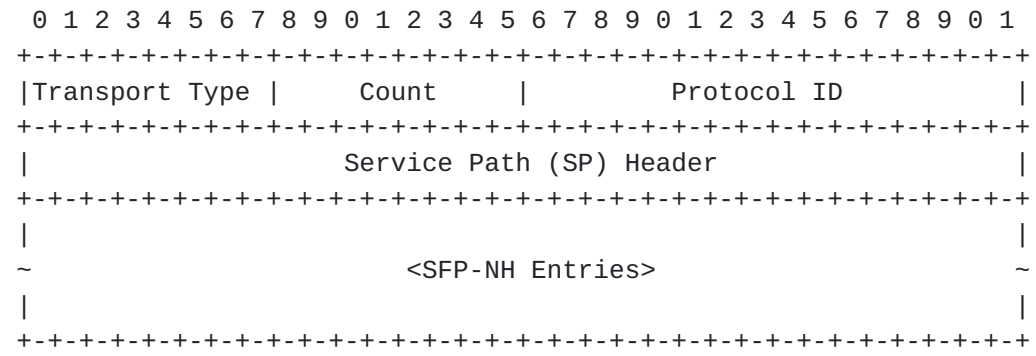

Figure 3: SFP Entry

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.

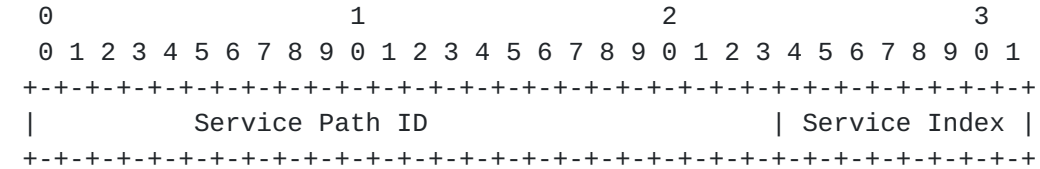

Figure 4: Service Function (SF) Header

Service Path ID (SPI): 24 bits
Service Index (SI): 8 bits
As defined in draft
[https://tools.ietf.org/html/draft-ietf-sfc-nsh-02#section-3.3]

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

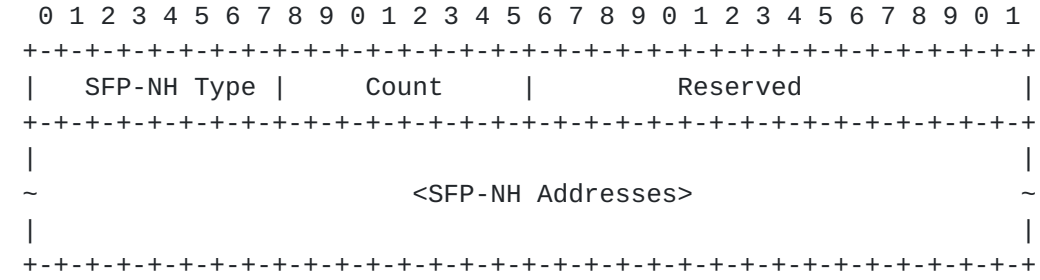

Figure 5: SFP-NH Entry

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 the client and server during the initial four message exchanges (DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, and DHCPACK) or during two message exchange (DHCPINFORM and DHCPACK) to configure the SFP details to SFF DHCP clients (i.e SFF will receive SFP details along with other DHCP configuration parameters).

The format of NSH SFP option for DHCPv4 is:

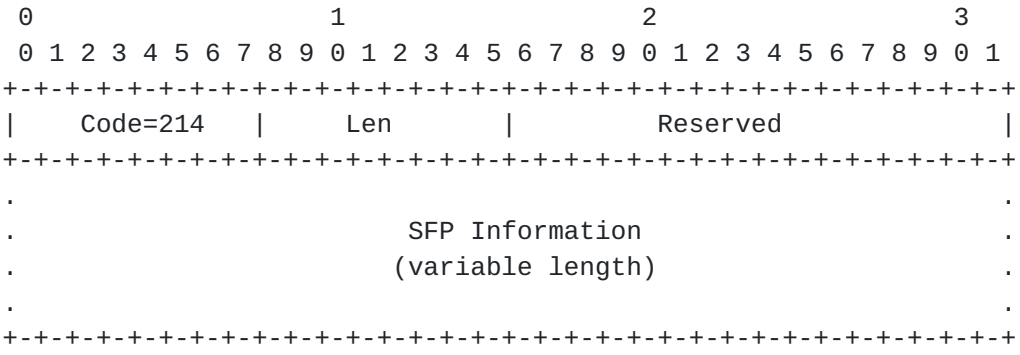

Figure 6: DHCPv4 NSH SFP option

Code: OPTION_NSH_SFP (TBD: IANA consideration)

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 is used by the server to configure the service function path details to SFF DHCP clients (i.e clients showing interest in participating in service chaining SFP as part of initial 4-way exchange or Rapid commit exchange).

The format of NSH SFP option for DHCPv6 is:

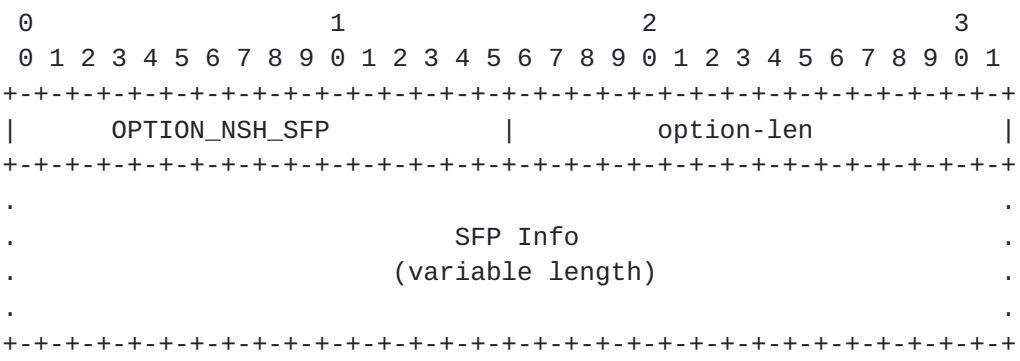

Figure 7: DHCPv6 NSH SFP option

option-code: OPTION_NSH_SFP (TBD: IANA consideration).

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 client interested in SFP MUST send the OPTION_NSH_SFP option to the DHCPv4 server along with other options in Parameter Request List (PRL).

A client configured from beginning to act as SFF MUST include the OPTION_NSH_SFP option in both DHCPDISCOVER and DHCPREQUEST to inform the server about the options client is interested in. Whereas, if the

client is configured latter to act as SFF after initial exchanges, it MUST include OPTION_NSH_SFP option in the DHCPINFORM message to inform the server.

5.2. DHCPv4 Server Behaviour

A DHCPv4 server if configured to handle service chaining, SHOULD provision the SFF clients with SFP, as per its administrative policy. A server can receive requests for OPTION_NSH_SFP option from clients in different message (DHCPDISCOVER and DHCPREQUEST) exchanges.

DHCPv4 server SHOULD inform the client with the option OPTION_NSH_SFP and SFP information in both DHCPOFFER and DHCPACK messages as a response to the DHCP client's DHCPDISCOVER and DHCPREQUEST respectively. If the DHCPv4 server receives the option OPTION_NSH_SFP during DHCPINFORM exchange, it SHOULD process and respond back as per administrative policy (server MAY choose to act as per the host requirement document). NSH SFP option sent to client is detailed in section 4.1.1

5.3. 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.

5.3.1 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).

A client configured from beginning to act as SFF MUST include an Option Request option in a Solicit, Request, Renew, Rebind, Confirm message to inform the server about options the client wants the server to send to the client. Whereas if the client is configured latter to act as SFF MUST include an OPO in the Information-request message to inform the server about options client wants server to send.

5.4. DHCPv6 Server Behaviour

A DHCPv6 server if configured to handle service chaining, SHOULD provision the SFF clients as per the administrative policy. A server can receive request for OPTION_NSH_SFP option from clients, in different messages (Solicit, Request, Renew, Rebind, Confirm or Information-request).

Whenever server detects any change is required in the SFP path, it will inform the clients using Reconfigure Message.

5.4.1 Processing OPTION_NSH_SFP Request

A server receiving the option OPTION_NSH_SFP in Solicit, Request, Renew, Rebind, Confirm or Information-request will process this request and SHOULD respond back to exchange with NSH SFP option as detailed in section 4.2.1

5.4.2 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].

5.5. Geolocation Based SFP

In certain cloud deployment scenarios, operator will like to know the details of SFF location to provide information to local authority towards integrity of resources and data moving across the SFF. In such scenarios, SFF sends option OPTION_NSH_SFP along with geolocation option to DHCP server.

In order to achieve this, the DHCP SFF clients SHOULD include the GeoConf option as per RFC6225 and OPTION_GEOCONF_CIVIC option as per RFC4776 for DHCPv4 and DHCPv6 respectively, along with the OPTION_NSH_SFP option in DHCPDISCOVER, DHCPREQUEST, DHCPINFORM requests of DHCPv4 and in Solicit, Request, Renew, Rebind, Confirm or Information-request in DHCPv6 exchanges.

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 included this option in its request (Section 3.5 of [RFC2131], Section 9.8 of [RFC2132]).

Where critical decisions might be based on the value of this option, DHCP authentication as defined in "Authentication for DHCP Messages" [RFC3118] and "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)" [RFC3315] SHOULD be used to protect the integrity of the DHCP options.

Link-layer confidentiality and integrity protection may also be employed to reduce the risk of location disclosure and tampering.

7. IANA Considerations

Request to IANA for assignment of values for following.

Table 1: Transport Types values.
Table 2: Protocol ID values.
Table 4: SFP-NH Type values.
Code: OPTION_NSH_SFP for DHCPv4.
option-code: OPTION_NSH_SFP for DHCPv6.

8. Acknowledgements

9. References

9.1. Normative References

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

[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.

[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.

9.2. Informative References

[I-D.ietf-sfc-architecture]
Halpern, J. and C. Pignataro, "Service Function Chaining (SFC) Architecture", draft-ietf-sfc-architecture-05 (work in progress), February 2015.

[I-D.draft-ietf-sfc-control-plane-00]
Li, et al., "Service Function Chaining (SFC) Control Plane Components & Requirements", draft-ietf-sfc-control-plane-00(work in progress), August 2015.

[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.

Author's Address

Yogendra Pal
Cisco Systems, Inc
India

EMail: yogpal@cisco.com

VenkataSubbaRao Gorrepati
Citrix
Bangalore
India

EMail: venkatasubbarao.gorrepati@citrix.com

Vikram Menon
Ericsson
Bangalore
India

EMail: vikram.menon@ericsson.com