Internet Engineering Task Force

Internet-Draft

Intended status: Informational Expires: September 20, 2018

J. Lemon, Ed. Broadcom F. Maino M. Smith Cisco

March 19, 2018

Group Policy Encoding with VXLAN-GPE and LISP-GPE draft-lemon-vxlan-lisp-gpe-gbp-00

Abstract

This document defines header companions for the Generic Protocol Extension for Virtual eXtensible Local Area Network (VXLAN-GPE) and for the Locator/ID Separation Protocol (LISP) Generic Protocol Extension (LISP-GPE) that are used to carry a Group Policy Identifier for the purposes of policy enforcement.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of \underline{BCP} 78 and \underline{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 https://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 September 20, 2018.

Copyright Notice

Copyright (c) 2018 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 (https://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

$\underline{1}$. Introduction
$\underline{1.1}$. Conventions
1.2. Abbreviations used in this document
2. Group Based Policy Sub-header
2.1. VXLAN-GPE GBP Sub-Header Format
2.2. LISP-GPE GBP Sub-Header Format 4
$\underline{3}$. IANA Considerations
$\underline{4}$. Security Considerations
$\underline{5}$. Normative References $\underline{6}$
Authors' Addresses

1. Introduction

This document defines the group-based policy (GBP) sub-header for VXLAN-GPE [I-D.ietf-nvo3-vxlan-gpe] and the GBP sub-header for LISP-GPE [I-D.ietf-lisp-gpe]. The GBP sub-header carries a 16-bit group policy ID that is semantically equivalent to the 16-bit group policy ID defined in [I-D.smith-vxlan-group-policy].

1.1. Conventions

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].

1.2. Abbreviations used in this document

GBP: Group-Based Policy

LISP-GPE: Locator/ID Separation Protocol Generic Protocol Extension

[I-D.ietf-lisp-gpe]

VXLAN-GPE: Virtual eXtensible Local Area Network, Generic Protocol

Extension [I-D.ietf-nvo3-vxlan-gpe]

2. Group Based Policy Sub-header

In the case of VXLAN-GPE, the Group-Based Policy (GBP) sub-header follows the VXLAN-GPE header, or a previous VXLAN-GPE sub-header. Similarly, in the case of LISP-GPE, the Group-Based Policy (GBP) sub-header follows the LISP-GPE header, or a previous LISP-GPE sub-header

Lemon, et al. Expires September 20, 2018 [Page 2]

2.1. VXLAN-GPE GBP Sub-Header Format

The format of the GBP sub-header in a VXLAN-GPE header is as shown below:

0		1									2										3										
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
+	⊢ – +	-		- -	+	+	 	+	- -	 	+	 	+	+	+	+ - +	- - +	- - +	-	+	- - +	-	H	- - +	- - +	+	+ - +	 	-	+	+-+
	Group Policy ID A D E Res Ver Next Protocol													L																	
+	+-+	- -	-	- -	+	+	 	+	+	+ - +	+	 	 	+	+	+ - +	H - H	H – H	- - +	+	+ - +	- - +	H - H	- - +	- - +	+	+ - +	 	H	+	+-+

- o Group Policy ID: 16 bit identifier that indicates the Group Policy ID being encapsulated by this GBP sub-header. The allocation of Group Policy ID values is outside the scope of this document.
- o Policy Applied bit (A bit): The A bit is set to 0 to indicate that the group policy has not (yet) been applied to this packet. Group policies MUST be applied by devices when the A bit is set to 0 and the destination Group has been determined. Devices that apply the group policy MUST set the A bit to 1 after the policy has been applied. The A bit is set to 1 to indicate that the group policy has already been applied to this packet. Policies that redirect the packet MUST NOT be applied by devices when the A bit is set. Policies that cause the packet to be dropped MAY be applied.
- o Don't Learn bit (D bit): The D bit is set to 1 to indicate that the egress VTEP MUST NOT learn the source address of the encapsulated frame.
- o End Destination bit (E bit): The E bit is set to 0 to represent the Group Policy ID associated with the source of the packet. The E bit is set to 1 to represent the Group Policy ID associated with the end destination of the packet. Note that if the packet carryies a destination group sub-header, it MUST also carry a source group sub-header.
- o Reserved (Res): the 3 bit field MUST be set to zero on transmission and ignored on receipt.
- o Version (Ver): indicates the Version of the Group Policy VXLAN-GPE sub-header. The initial version is 0.
- o Next Protocol: This 8 bit field indicates the protocol header immediately following this VXLAN-GPE sub-header. Next Protocol types are encoded as specified in [I-D.ietf-nvo3-vxlan-gpe].

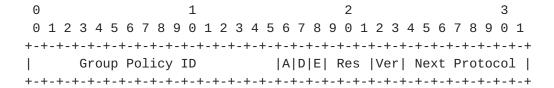
Lemon, et al. Expires September 20, 2018 [Page 3]

An example frame format is as shown below:

```
0
      1
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Outer Ethernet Header
Outer IP Header
Outer UDP Header
|R|R|Ver|I|P|R|0| Reserved |NP = GBP|
Virtual Network Identifier (VNI) | Reserved | |
Group Policy ID
         |A|D|E| Res |Ver| Next Protocol | GBP
Next Protocol
-----+
```

2.2. LISP-GPE GBP Sub-Header Format

The format of the GBP sub-header in a LISP-GPE header is as shown below:



- o Group Policy ID: 16 bit identifier that indicates the Group Policy ID being encapsulated by this GBP sub-header. The allocation of Group Policy ID values is outside the scope of this document.
- o Policy Applied bit (A bit): The A bit is set to 0 to indicate that the group policy has not (yet) been applied to this packet. Group policies MUST be applied by devices when the A bit is set to 0 and the destination Group has been determined. Devices that apply the group policy MUST set the A bit to 1 after the policy has been applied. The A bit is set to 1 to indicate that the group policy has already been applied to this packet. Policies that redirect

Lemon, et al. Expires September 20, 2018 [Page 4]

the packet MUST NOT be applied by devices when the A bit is set. Policies that cause the packet to be dropped MAY be applied.

- o Don't Learn bit (D bit): The D bit is set to 1 to indicate that the Egress Tunnel Router MUST NOT learn the source address of the encapsulated frame.
- o End Destination bit (E bit): The E bit is set to 0 to represent the Group Policy ID associated with the source of the packet. The E bit is set to 1 to represent the Group Policy ID associated with the end destination of the packet. Note that if the packet carryies a destination group sub-header, it MUST also carry a source group sub-header.
- o Reserved (Res): the 3 bit field MUST be set to zero on transmission and ignored on receipt.
- o Version (Ver): indicates the Version of the Group Policy LISP-GPE sub-header. The initial version is 0.
- o Next Protocol: This 8 bit field indicates the protocol header immediately following this LISP-GPE sub-header. Next Protocol types are encoded as specified in [I-D.ietf-lisp-gpe].

An example frame format is as shown below:

0		1				2						3		
0 1 2 3 4 !	5 6 7 8 9	0 1 2	2 3 4	4 5 6	7 8	9 0 1	1 2 3	3 4	5 6	7	8 9	0 1		
+-+-+-+-+	-+-+-+-	+-+-+-	+-+	-+-+-	+-+-+	+-+-+	-+-+-	-+-+	- - + -	+-+	+-	+-+-	+	
		Outer	Etl	nerne	t Hea	ader								
+-+-+-+-+	-+-+-+-	+-+-+-	+-+	-+-+-	+-+-+	+-+-+	-+-+-	-+-+	- - + -	+-+	+-	+-+-	+	
		(Oute	r IP I	Heade	er								
+-+-+-+-+	-+-+-+-	+-+-+-	+-+	-+-+-	+-+-+	+-+-+	-+-+-	-+-+	- - + -	+-+	+-	+-+-	+	
		Οι	ıter	UDP I	Heade	er								
+-+-+-+-+	-+-+-+-	+-+-+	+-+	-+-+-	+-+-+	+-+-+	-+-+-	-+-+	- + -	+-+	+-	+-+-	+ +	
N L E V I I	P K K	1	lonce	e/Map	-Vers	sion		1	NP =	GB	8P			
+-+-+-+-+	-+-+-+-	+-+-+-	+-+	-+-+-	+-+-+	+-+-+	-+-+-	-+-+	- - + -	+-+	+-	+-+-	+ LISF	-GPE
	In	stance	e ID	/Loca	tor-S	Status	s-Bit	ts						
+-+-+-+-+	-+-+-+-	+-+-+	+-+	-+-+-	+-+-	+-+-+	-+-+-	-+-+	- - + -	+-+	+-	+-+-	+ +	
Group	p Policy	ID		A	D E	Res	Ver	r N	Next	Pr	oto	col	GBP	
+-+-+-+-+	-+-+-+-	+-+-+	+-+	-+-+-	+-+-	+-+-+	-+-+-	-+-+	- - + -	+-+	+-	+-+-	+ +	
:		1	lext	Prot	ocol								:	
+													+	

3. IANA Considerations

IANA is requested to add a new value to registry of "Next Protocol", which is defined in [I-D.ietf-nvo3-vxlan-gpe]. The new value of 6 will signify a GBP sub-header as the next protocol.

IANA is requested to add a new value to registry of "Next Protocol", which is defined in $[\underline{\text{I-D.ietf-lisp-gpe}}]$. The new value of 6 will signify a GBP sub-header as the next protocol.

4. Security Considerations

The same security considerations applied to [I-D.ietf-nvo3-vxlan-gpe], [I-D.ietf-lisp-gpe], and to [I-D.smith-vxlan-group-policy] apply to this document.

Additionally, the security policy value carried in the GBP sub-header impacts security directly. There is a risk that this identifier could be altered. Accordingly, the network should be designed such that this sub-header can be inserted only by trusted entities, and can not be altered before reaching the destination. This can be mitigated through physical security of the network and/or by encryption or validation of the entire packet, including the GBP.

5. Normative References

[I-D.ietf-lisp-gpe]

Lewis, D., Lemon, J., Agarwal, P., Kreeger, L., Quinn, P., Smith, M., Yadav, N., and F. Maino, "LISP Generic Protocol Extension", draft-ietf-lisp-gpe-01 (work in progress), March 2018.

[I-D.ietf-nvo3-vxlan-gpe]

Maino, F., Kreeger, L., and U. Elzur, "Generic Protocol Extension for VXLAN", draft-ietf-nvo3-vxlan-gpe-05 (work in progress), October 2017.

[I-D.smith-vxlan-group-policy]

Smith, M. and L. Kreeger, "VXLAN Group Policy Option", draft-smith-vxlan-group-policy-04 (work in progress), October 2017.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
Requirement Levels", BCP 14, RFC 2119,
DOI 10.17487/RFC2119, March 1997,
https://www.rfc-editor.org/info/rfc2119.

Authors' Addresses

John Lemon (editor) **Broadcom Limited** 270 Innovation Drive San Jose, CA 95134 USA

Email: john.lemon@broadcom.com

Fabio Maino Cisco Systems

Email: fmaino@cisco.com

Michael Smith Cisco Systems

Email: michsmit@cisco.com