

Network Working Group
Internet Draft
Updates: [3031](#)
Intended Status: Proposed Standard
Expiration Date: June 2011

David J. Smith
John Mullooly
Cisco Systems

William Jaeger
AT&T

Tom Scholl
nLayer Communications

December 15, 2010

Requirements for Label Edge Router Forwarding of IPv4 Option Packets

[draft-ietf-mpls-ip-options-06.txt](#)

Abstract

This document specifies how Label Edge Routers (LER) should behave when determining whether to MPLS encapsulate an IP packet with header options. Lack of a formal standard has resulted in different LER forwarding behaviors for IP packets with header options despite being associated with a prefix-based Forwarding Equivalence Class (FEC). IP option packets that belong to a prefix-based FEC, yet are forwarded into an IP/MPLS network without being MPLS-encapsulated, present a security risk against the MPLS infrastructure. Further, LERs that are unable to MPLS encapsulate IP packets with header options cannot operate in certain MPLS environments. While this newly defined LER behavior is mandatory to implement, it is optional to invoke.

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), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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

Internet Draft LER Forwarding of IPv4 Options Packets December 2010

material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at
<http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at
<http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on June 1, 2011.

Copyright Notice

Copyright (c) 2010 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	Specification of Requirements	3
2	Motivation	3
3	Introduction	3
4	Ingress Label Edge Router Requirement	4
5	Security Considerations	5
5.1	IP Option Packets that Bypass MPLS Encapsulation ...	5
5.2	Router Alert Label Imposition	7
6	IANA Considerations	7
7	Acknowledgements	8
8	Normative References	8
9	Informational References	8
10	Authors' Addresses	9

Internet Draft LER Forwarding of IPv4 Options Packets December 2010

1. Specification of Requirements

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](#)].

2. Motivation

This document is motivated by the need to formalize MPLS encapsulation processing of IPv4 packets with header options in order to mitigate the existing risks of IP options-based security attacks against MPLS infrastructures. We believe that this document adds details that have not been fully addressed in [[RFC3031](#)] and [[RFC3032](#)], and that the methods presented in this document update [[RFC3031](#)] as well as complement [[RFC3270](#)], [[RFC3443](#)] and [[RFC4950](#)].

3. Introduction

The IP packet header provides for various IP options as originally specified in [[RFC791](#)]. IP header options are used to enable control functions within the IP data forwarding plane that are required in some specific situations but not necessary for most common IP communications. Typical IP header options include provisions for timestamps, security, and special routing. Example IP header options and applications include but are not limited to:

- o Strict and Loose Source Route Options: Used to IP route the IP packet based on information supplied by the source.
- o Record Route Option: Used to trace the route an IP packet takes.
- o Router Alert Option: Indicates to downstream IP routers to examine these IP packets more closely.

The list of current IP header options can be accessed at [[IANA](#)].

IP packets may or may not use IP header options (they are optional)

but IP header option handling mechanisms must be implemented by all IP protocol stacks (hosts and routers). Each IP header option has distinct header fields and lengths. IP options extend the IP packet header length beyond the minimum of 20 octets. As a result, IP packets received with header options are typically handled as exceptions and in a less efficient manner due to their variable length and complex processing requirements. For example, many router implementations, punt such IP option packets from the hardware forwarding (fast) path into the software forwarding (slow) path causing high CPU utilization. Even when the forwarding plane can parse a variable length header, it may still need to punt to the control plane, because the forwarding plane may not have the clock cycles or intelligence required to process the header option.

Multi-Protocol Label Switching (MPLS) [[RFC3031](#)] is a technology in which packets associated with a prefix-based Forwarding Equivalence Class (FEC) are encapsulated with a label stack and then switched along a label switched path (LSP) by a sequence of label switch routers (LSRs). These intermediate LSRs do not generally perform any processing of the IP header as packets are forwarded. (There are some exceptions to this rule, such as ICMP processing and LSP ping, as described in [[RFC3032](#)] and [[RFC4379](#)], respectively.) Many MPLS deployments rely on LSRs to provide layer 3 transparency much like ATM switches are transparent at layer 2. Such deployments often minimize the IP routing information (e.g., no BGP transit routes) carried by LSRs since it is not necessary for MPLS forwarding of transit packets.

Even though MPLS encapsulation seems to offer a viable solution to provide layer 3 transparency, there is currently no formal standard for MPLS encapsulation of IP packets with header options that belong to a prefix-based FEC. Lack of a formal standard has resulted in inconsistent forwarding behaviors by ingress Label Edge Routers (LERs). When IP packets are MPLS encapsulated by an ingress LER, for example, the IP header including option fields of transit packets are not acted upon by downstream LSRs which forward based on the MPLS label(s). Conversely, when a packet is IP forwarded by an ingress LER two undesirable behaviors can result. First, a downstream LSR may not have sufficient IP routing information to forward the packet resulting in packet loss. Second, downstream LSRs must apply IP forwarding rules which may expose them to IP security attacks.

IP option packets that belong to a prefix-based FEC, yet are forwarded into an IP/MPLS network without being MPLS-encapsulated, present a security risk against the MPLS infrastructure. Further, LERs that are unable to MPLS encapsulate IP packets with header options cannot operate as an LER in certain MPLS environments. This new requirement will reduce the risk of IP options-based security attacks against LSRs as well as assist LER operation across MPLS networks which minimize the IP routing information (e.g., no BGP transit routes) carried by LSRs.

4. Ingress Label Edge Router Requirement

An ingress LER MUST implement the following policy:

- o When determining whether to push an MPLS label stack onto an IP packet, the determination is made without considering any IP options that may be carried in the IP packet header. Further, the label values that appear in the label stack are determined without considering any such IP options.

Smith, et al.

[Page 4]

Internet Draft LER Forwarding of IPv4 Options Packets December 2010

This policy MAY be configurable on an ingress LER, however, it SHOULD be enabled by default. When processing of signaling messages or data packets with more specific forwarding rules is enabled, this policy SHOULD NOT alter the specific processing rules. This applies to, but is not limited to, RSVP as per [[RFC2205](#)], source routing as per [[RFC791](#)] as well as other FEC elements defined by future specifications. Further, how an ingress LER processes the IP header options of packets before MPLS encapsulation is out of scope since these are processed before they enter the MPLS domain.

Implementation of the above policy prevents IP packets that belong to a prefix-based FEC from bypassing MPLS encapsulation due to header options. The policy also prevents specific option types such as Router Alert (option value 148) from forcing MPLS imposition of the MPLS Router Alert Label (label value 1) at ingress LERs. Without this policy, the MPLS infrastructure is exposed to security attacks using legitimate IP packets crafted with header options. Further, LERs that are unable to MPLS encapsulate IP packets with header options cannot operate as an LER in certain MPLS environments as described above in [Section 3](#).

5. Security Considerations

There are two potential categories of attacks using crafted IP option packets that threaten existing MPLS infrastructures. Both are described below. To mitigate the risk of these specific attacks, the ingress LER policy specified above is required.

5.1. IP Option Packets that Bypass MPLS Encapsulation

Given that a router's exception handling process (i.e., CPU, processor line-card bandwidth, etc.) used for IP header option processing is often shared with IP control and management protocol router resources, a flood of IP packets with header options may adversely affect a router's control and management protocols, thereby, triggering a denial-of-service (DoS) condition. Note, IP packets with header options may be valid transit IP packets with legitimate sources and destinations. Hence, a DoS-like condition may be triggered on downstream transit IP routers that lack protection mechanisms even in the case of legitimate IP option packets.

IP option packets that belong to a prefix-based FEC yet bypass MPLS encapsulation at an ingress LER may be inadvertently IP routed downstream across the MPLS core network (not label switched). This allows an external attacker the opportunity to maliciously craft seemingly legitimate IP packets with specific IP header options in

order to intentionally bypass MPLS encapsulation at the MPLS edge (i.e., ingress LER) and trigger a DoS condition on downstream LSRs. Some of the specific types of IP option-based security attacks that may be leveraged against MPLS networks include:

- o Crafted IP option packets that belong to a prefix-based FEC yet bypass MPLS encapsulation at an ingress LER may allow an attacker to DoS downstream LSRs by saturating their software forwarding paths. By targeting a LSR's exception path, control and management protocols may be adversely affected and, thereby, a LSR's availability. This assumes, of course, that downstream LSRs lack protection mechanisms.
- o Crafted IP option packets that belong to a prefix-based FEC yet bypass MPLS encapsulation at an ingress LER may allow for IP TTL expiry-based DoS attacks against downstream LSRs. MPLS enables

- IP core hiding whereby transit IP traffic flows see the MPLS network as a single router hop [[RFC3443](#)]. However, MPLS core hiding does not apply to packets that bypass MPLS encapsulation and, therefore, IP option packets may be crafted to expire on downstream LSRs which may trigger a DoS condition. Bypassing MPLS core hiding is an additional security consideration since it exposes the network topology.
- o Crafted IP option packets that belong to a prefix-based FEC yet bypass MPLS encapsulation at an ingress LER may allow for DoS attacks against downstream LSRs that do not carry the IP routing information required to forward transit IP traffic. Lack of such IP routing information may prevent legitimate IP option packets from transiting the MPLS network and, further, may trigger generation of ICMP destination unreachable messages which could lead to a DoS condition. This assumes, of course, that downstream LSRs lack protection mechanisms and do not carry the IP routing information required to forward transit traffic.
 - o Crafted IP option packets that belong to a prefix-based FEC yet bypass MPLS encapsulation at an ingress LER may allow an attacker to bypass LSP Diff-Serv tunnels [[RFC3270](#)] and any associated MPLS CoS field [[RFC5462](#)] marking policies at ingress LERs and, thereby, adversely affect (i.e., DoS) high-priority traffic classes within the MPLS core. Further, this could also lead to theft of high-priority services by unauthorized parties. This assumes, of course, that the [[RFC3270](#)] Pipe model is deployed within the MPLS core.
 - o Crafted RSVP packets that belong to a prefix-based FEC yet bypass MPLS encapsulation at an ingress LER may allow an attacker to build RSVP soft-states [[RFC2205](#), [RFC3209](#)] on downstream LSRs which could lead to theft of service by unauthorized parties or to a DoS condition caused by locking up LSR resources. This assumes, of course, that the MPLS network is enabled to process RSVP packets.

The security attacks outlined above specifically apply to IP option packets that belong to a prefix-based FEC yet bypass ingress LER label stack imposition. Additionally, these attacks only apply to IP option packets forwarded using the global routing table (i.e., IPv4 address family) of a ingress LER. IP option packets associated with a BGP/MPLS IP VPN service are always MPLS encapsulated by the ingress LER per [[RFC4364](#)] given that packet forwarding uses a Virtual

Forwarding/Routing (VRF) instance. Therefore, BGP/MPLS IP VPN services are not subject to the threats outlined above [[RFC4381](#)]. Further, IPv6 [[RFC2460](#)] makes use of extension headers not header options and is therefore outside the scope of this document. A separate security threat that does apply to both BGP/MPLS IP VPNs and the IPv4 address family makes use of the Router Alert Label. This is described directly below.

[5.2](#). Router Alert Label Imposition

[RFC3032] defines a "Router Alert Label" (label value of 1) which is analogous to the "Router Alert" IP header option (option value of 148). The MPLS Router Alert Label (when exposed and processed only) indicates to downstream LSRs to examine these MPLS packets more closely. MPLS packets with the MPLS Router Alert Label are also handled as an exception by LSRs and, again, in a less efficient manner. At the time of this writing, the only legitimate use of the Router Alert Label is for LSP ping/trace [[RFC4379](#)]. Since there is also no formal standard for Router Alert Label imposition at ingress LERs:

- o Crafted IP packets with specific IP header options (e.g., Router Alert) and that belong to a prefix-based FEC may allow an attacker to force MPLS imposition of the Router Alert Label at ingress LERs and, thereby, trigger a DoS condition on downstream LSRs. This assumes, of course, that downstream LSRs lack protection mechanisms.

[6](#). IANA Considerations

This document has no actions for IANA.

7. Acknowledgements

The authors would like to thank Adrian Cepleanu, Bruce Davie, Rick Huber, Chris Metz, Pradosh Mohapatra, Ashok Narayanan, Carlos Pignataro, Eric Rosen, Mark Szczesniak and Yung Yu for their valuable comments and suggestions.

8. Normative References

[RFC791] Postel, J., "Internet Protocol Specification," [RFC791](#), September 1981.

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

[RFC3031] Rosen, E., Viswanathan, A., and Callon, R., "MPLS Label Switching Architecture," [RFC3031](#), January 2001.

[RFC3032] Rosen, E., Tappan, D., Fedorkow, G., Rekhter, Y., Farinacci, D., Li, T., and Conta, A., "MPLS Label Stack Encoding," [RFC3032](#), January 2001.

9. Informational References

[RFC2205] Braden, R., Zhang, L., Berson, S., Herzog, S., Jamin, S., "Resource ReSerVation Protocol -- Version 1 Functional Specification," [RFC2205](#), September 1997.

[RFC2460] Deering, S., Hinden, R. "Internet Protocol, Version 6 Specification," [RFC2460](#), December 1998.

[RFC3209] Awduche, D., L. Berger, D. Gan, T. Li, V. Srinivasan, G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels," [RFC3209](#), December 2001.

[RFC3270] Le Faucheur, F., Wu, L., Davie, B., Davari, S., Vaananen, P., Krishnan, R., Cheval, P., Heinanen, J., "Multi-Protocol Label Switching Support of Differentiated Services," [RFC3270](#), May 2002.

[RFC3443] Agarwal, P., Akyol, B., "Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks," [RFC3443](#), January 2003.

[RFC4364] Rosen, E. and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)," [RFC4364](#), February 2006.

Internet Draft LER Forwarding of IPv4 Options Packets December 2010

[RFC4379] Kompella, K., Swallow, G., "Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures," [RFC4379](#), February 2006.

[RFC4381] Behringer, M., "Analysis of the Security of BGP/MPLS IP Virtual Private Networks (VPNs)," [RFC4381](#), February 2006.

[RFC4950] Bonica, R., Gan, D., Tappan, D., and Pignataro, C., "ICMP Extensions for Multiprotocol Label Switching," [RFC4950](#), August 2007.

[IANA] "IP Option Numbers," IANA, February 15, 2007, <www.iana.org/assignments/ip-parameters>.

[RFC5462] Andersson, L., and R. Asati, "Multiprotocol Label Switching (MPLS) Label Stack Entry: EXP Field Renamed to Traffic Class Field," [RFC5462](#), February 2009.

10. Authors' Addresses

William Jaeger
AT&T
200 S. Laurel Avenue
Middletown, NJ 07748
Email: wjaeger@att.com

John Mullooly
Cisco Systems
111 Wood Avenue South
Iselin, NJ 08830
E-mail: jmullool@cisco.com

Tom Scholl
nLayer Communications
209 West Jackson, Suite 700
Chicago, IL 60606
E-mail: tscholl@nlayer.net

Internet Draft LER Forwarding of IPv4 Options Packets December 2010

David J. Smith
Cisco Systems
111 Wood Avenue South
Iselin, NJ 08830
E-mail: djsmith@cisco.com

