

MPLS Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 13, 2022

R. Gandhi
P. Brissette
Cisco Systems, Inc.
E. Leyton
Verizon Wireless
July 12, 2021

Encapsulation of Simple TWAMP (STAMP) for Pseudowires in MPLS Networks
draft-gandhi-mpls-stamp-pw-00

Abstract

Pseudowires (PWs) are used in MPLS networks for various services including carrying layer 2 and layer 3 data packets. This document describes the procedure for encapsulation of the Simple Two-Way Active Measurement Protocol (STAMP) defined in [RFC 8762](#) and its optional extensions defined in [RFC 8972](#) for PWs in MPLS networks. The procedure uses PW Generic Associated Channel (G-ACH) to encapsulate the STAMP test packets with or without an IP/UDP header.

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 <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 January 13, 2022.

Copyright Notice

Copyright (c) 2021 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

1.	Introduction	2
2.	Conventions Used in This Document	3
2.1.	Requirements Language	3
2.2.	Abbreviations	3
2.3.	Reference Topology	4
3.	Overview	4
4.	Session-Sender Test Packet	5
4.1.	Session-Sender Test Packet with IP/UDP Header	5
4.2.	Session-Sender Test Packet without IP/UDP Header	7
5.	Session-Reflector Test Packet	7
5.1.	Session-Reflector Test Packet with IP/UDP Header	8
5.2.	Session-Reflector Test Packet without IP/UDP Header	10
6.	Security Considerations	11
7.	IANA Considerations	11
8.	References	12
8.1.	Normative References	12
8.2.	Informative References	12
	Acknowledgments	13
	Authors' Addresses	13

[1.](#) Introduction

The Simple Two-way Active Measurement Protocol (STAMP) provides capabilities for the measurement of various metrics in IP networks [[RFC8762](#)] without the use of a control channel to pre-signal session parameters. [[RFC8972](#)] defines optional extensions for STAMP.

Pseudowires (PWs) are used in MPLS networks for various services including carrying layer 2 and layer 3 data packets [[RFC6658](#)]. The PWs are bidirectional in nature. The PWs can be point-to-point or point-to-multipoint. A PW Generic Associated Channel (G-ACh) [[RFC5586](#)] provides a mechanism to transport Operations, Administration, and Maintenance (OAM) and other control messages over MPLS data plane. The G-ACh channel types identify the various OAM messages being transported over the channel.

The STAMP test packets need to be transmitted with the same MPLS label stack that is used by the PW traffic to ensure proper validation of underlay path taken by the actual PW traffic. Also, the test packets need to follow the same ECMP path taken by the PW traffic. The STAMP test packets may be encapsulated over the PW

associated channel with or without an IP/UDP header. The requirements for the encapsulation of the STAMP test packets for the PWs in MPLS networks can be summarized as follows:

- o The PW associated channel MUST support STAMP test packets with IP/UDP header.
- o The PW associated channel MUST support STAMP test packets without IP/UDP header.
- o The Session-Sender test packets MUST follow the same underlay path taken by the traffic for the associated PW channel.
- o The Session-Sender test packets MUST follow the same ECMP underlay path taken by the traffic for the associated PW channel.
- o The Session-Reflector test packets MAY follow the same reverse underlay path taken by Session-Sender test packets.
- o The Session-Reflector test packets MAY follow the same reverse ECMP underlay path taken by Session-Sender test packets.

This document describes the procedure for encapsulation of the STAMP defined in [[RFC8762](#)] and its optional extensions defined in [[RFC8972](#)] for point-to-point PWs in MPLS networks. The procedure uses PW Generic Associated Channel (G-ACh) to encapsulate the STAMP test packets with or without an IP/UDP header. The procedure for point-to-multipoint PWs will be added in future.

2. Conventions Used in This Document

2.1. 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 [[RFC2119](#)] [[RFC8174](#)] when, and only when, they appear in all capitals, as shown here.

2.2. Abbreviations

ECMP: Equal Cost Multi-Path.

G-ACh: Generic Associated Channel.

GAL: G-ACh Label.

HMAC: Hashed Message Authentication Code.

MPLS: Multiprotocol Label Switching.

OAM: Operations, Administration, and Maintenance.

PW: Pseudowires.

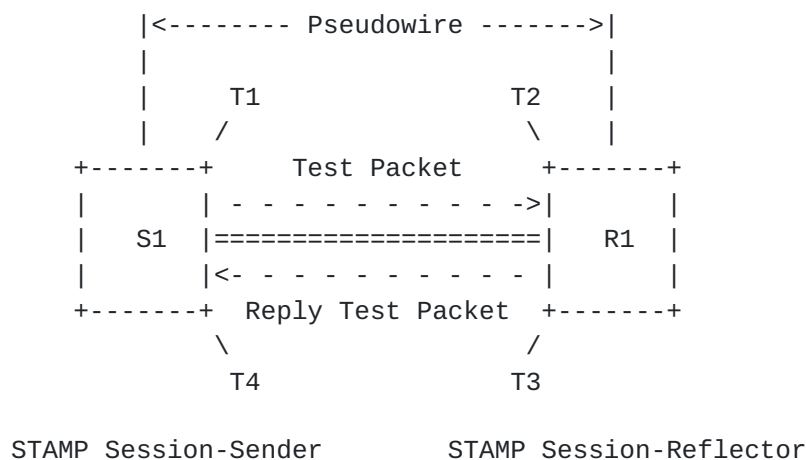
SHA: Secure Hash Algorithm.

STAMP: Simple Two-way Active Measurement Protocol.

TC: Traffic Class.

2.3. Reference Topology

In the Reference Topology shown in Figure 1, there exists a packet pseudowire to transport data between LSRs S1 and R1. The STAMP Session-Sender on LSR S1 initiates a Session-Sender test packet and the STAMP Session-Reflector on LSR R1 transmits a reply test packet. The reply test packet is transmitted to the STAMP Session-Sender on the same path (same set of links and nodes) in the reverse direction of the path taken towards the Session-Reflector.



T1, T2, T3, T4: Timestamps as described in [\[RFC8762\]](#)

Figure 1: Reference Topology

3. Overview

The STAMP Session-Sender and Session-Reflector test packets defined in [\[RFC8972\]](#) are transmitted over the PWs in MPLS networks. The base STAMP test packets can be encapsulated using IP/UDP header and may use Destination UDP port 862 [\[RFC8762\]](#).

The STAMP test packets are encapsulated with MPLS header using the same label stack as the PW traffic and the PW G-ACh header. The encapsulation allows the STAMP test packets to follow the same path as the PW traffic, and provide the same ECMP path selection on the intermediate nodes.

There are two ways in which STAMP test packets may be encapsulated over a PW associated channel, either using an IP/UDP header or without using an IP/UDP header.

For encapsulating the STAMP test packets over a PW associated channel with an IP/UDP header, IPv4 and IPv6 G-ACh types [[RFC4385](#)] are used for both Session-Sender and Session-Reflector test packets. The destination UDP port numbers in the Session-Sender and Session-Reflector test packets discriminate the test packets. The IP version (IPv4 or IPv6) MUST match the IP version used for signaling for dynamically established PWs or MUST be configured for statically provisioned PWs.

For encapsulating the STAMP test packets over a PW associated channel without an IP/UDP header, two new G-ACh types are defined in this document, one for the Session-Sender test packets and one for the Session-Reflector test packets. The different G-ACh types are required for the Session-Sender and Session-Reflector test packets as the STAMP test packet formats do not have a way to discriminate them.

The Time to Live (TTL)/Hop Limit (HL) and Generalized TTL Security Mechanism (GTSM) procedures from [[RFC5082](#)] apply to this encapsulation, and hence the TTL/HL is set to 255.

The G-ACh label (GAL) [[RFC5586](#)] is not added in the MPLS label stack.

4. Session-Sender Test Packet

4.1. Session-Sender Test Packet with IP/UDP Header

The content of an example STAMP Session-Sender test packet encapsulated over a PW associated channel using an IP/UDP header is shown in Figure 2. The STAMP G-ACh header [[RFC5586](#)] with G-ACh MUST immediately follow the bottom of the MPLS label stack. The payload contains the STAMP Session-Sender test packet defined in [[RFC8972](#)].

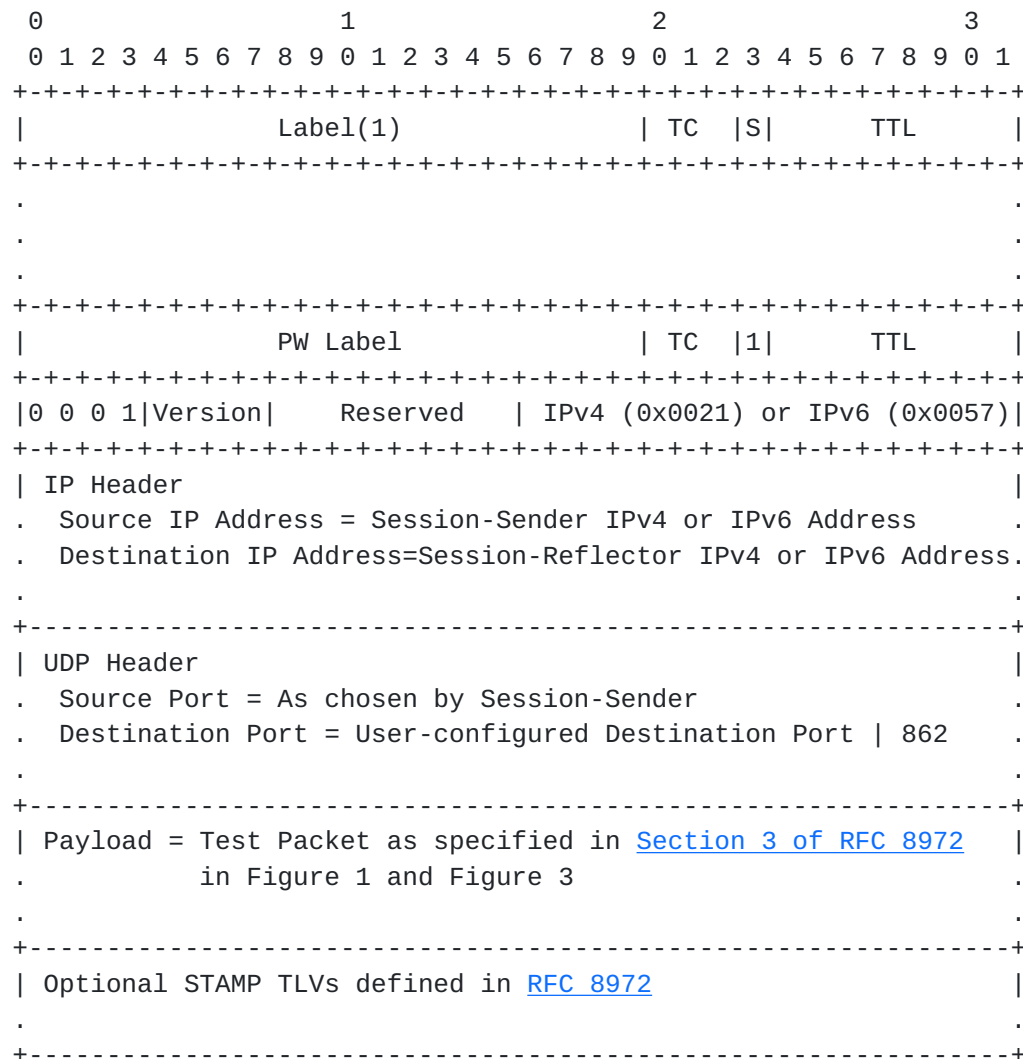


Figure 2: Example Session-Sender Test Packet with IP/UDP Header

The STAMP Session-Sender test packet G-ACh header contains following fields:

Version: The Version field is set to 0, as defined in [RFC4385].

Reserved: Reserved Bits MUST be set to zero upon transmission and ignored upon receipt.

Channel Type: G-ACh channel type for IPv4 header (0x0021) or IPv6 header (0x0057) [[RFC4385](#)].

4.2. Session-Sender Test Packet without IP/UDP Header

The content of an example STAMP Session-Sender test packet encapsulated over a PW associated channel without using an IP/UDP header is shown in Figure 3. The STAMP G-ACh header [RFC5586] with new STAMP Session-Sender G-ACh type (value TBD1) MUST immediately follow the bottom of the MPLS label stack. The payload contains the STAMP Session-Sender test packet defined in [RFC8972].

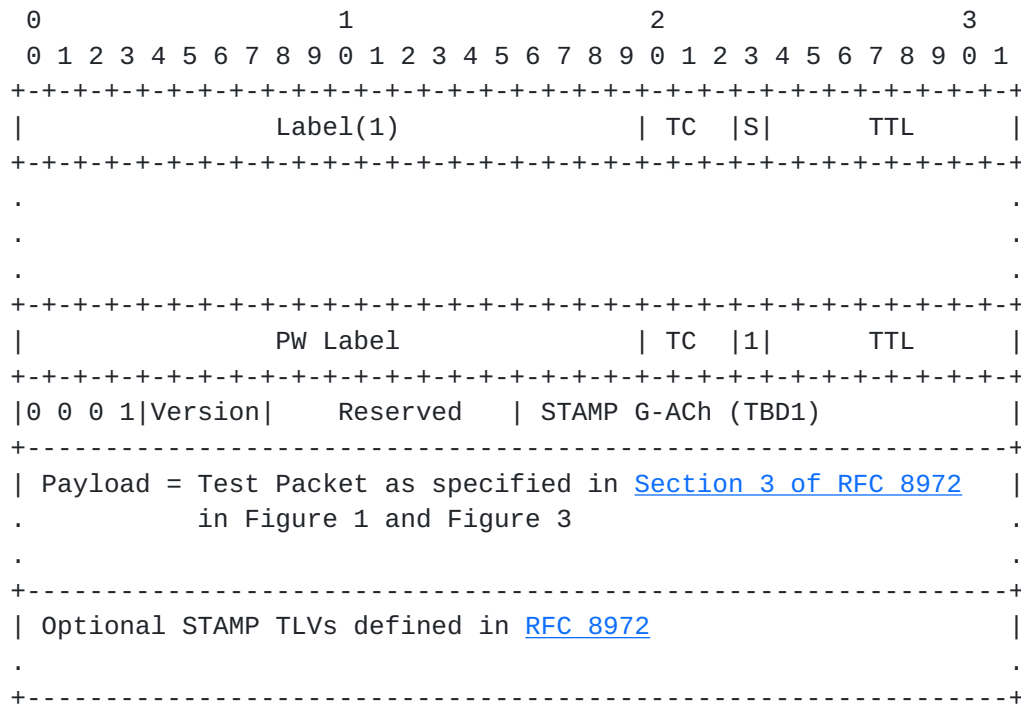


Figure 3: Example Session-Sender Test Packet without IP/UDP Header

The STAMP Session-Sender test packet G-ACh header contains following fields:

Version: The Version field is set to 0, as defined in [RFC4385].

Reserved: Reserved Bits MUST be set to zero upon transmission and ignored upon receipt.

Channel Type: G-ACh channel type for STAMP Session-Sender packet (TBD1).

5. Session-Reflector Test Packet

The STAMP Session-Reflector reply test packet is sent on the same path in the reverse direction of a bidirectional PW. The STAMP test packet can be sent using an MPLS header with or without IP/UDP

header. The Session-Reflector test packet is sent with an IP/UDP header if the Session-Sender test packet is received with an IP/UDP header, otherwise, it is sent without an IP/UDP header.

5.1. Session-Reflector Test Packet with IP/UDP Header

The content of an example STAMP Session-Reflector test packet encapsulated over a PW associated channel using an IP/UDP header is shown in Figure 4. The STAMP G-ACh header [[RFC5586](#)] with G-ACh MUST immediately follow the bottom of the MPLS label stack. The payload contains the STAMP Session-Reflector test packet defined in [[RFC8972](#)].

The STAMP Session-Reflector reply test packet MUST use the IP/UDP information from the received test packet when an IP/UDP header is present in the received test packet.



Figure 4: Example Session-Reflector Test Packet with IP/UDP Header

The STAMP Session-Reflector test packet G-ACh header contains following fields:

Version: The Version field is set to 0, as defined in [[RFC4385](#)].

Reserved: Reserved Bits MUST be set to zero upon transmission and ignored upon receipt.

Channel Type: G-ACh channel type for IPv4 header (0x0021) or IPv6 header (0x0057) [[RFC4385](#)].

5.2. Session-Reflector Test Packet without IP/UDP Header

The content of an example STAMP Session-Reflector test packet encapsulated over a PW associated channel without using an IP/UDP header is shown in Figure 5. The STAMP G-ACh header [RFC5586] with new STAMP Session-Reflector G-ACh type (value TBD2) MUST immediately follow the bottom of the MPLS label stack. The payload contains the STAMP Session-Reflector test packet defined in [RFC8972].

The STAMP Session-Reflector reflects the test packet back to the Session-Sender using the same channel of the reverse direction of the PW on which it was received. The Session-Reflector has enough information to reflect the test packet received by it to the Session-Sender using the PW context.

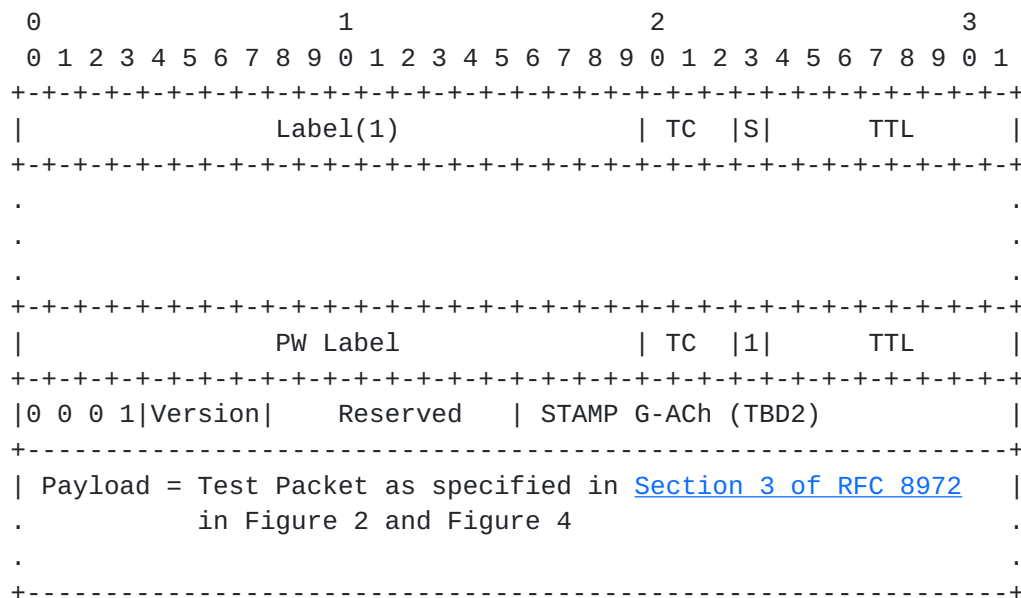


Figure 5: Example Session-Reflector Test Packet without IP/UDP Header

The STAMP Session-Reflector test packet G-ACh header contains following fields:

Version: The Version field is set to 0, as defined in [RFC4385].

Reserved: Reserved Bits MUST be set to zero upon transmission and ignored upon receipt.

Channel Type: G-ACh channel type for STAMP Session-Reflector packet (TBD2).

6. Security Considerations

The usage of STAMP protocol is intended for deployment in limited domains [[RFC8799](#)]. As such, it assumes that a node involved in STAMP protocol operation has previously verified the integrity of the path and the identity of the far-end STAMP Session-Reflector.

If desired, attacks can be mitigated by performing basic validation and sanity checks, at the STAMP Session-Sender, of the counter or timestamp fields in received reply test packets. The minimal state associated with these protocols also limits the extent of disruption that can be caused by a corrupt or invalid packet to a single test cycle.

Use of HMAC-SHA-256 in the authenticated mode protects the data integrity of the test packets. Cryptographic measures may be enhanced by the correct configuration of access-control lists and firewalls.

The security considerations specified in [[RFC8762](#)] and [[RFC8972](#)] also apply to the procedure described in this document. Specifically, the message integrity protection using HMAC, as defined in [[RFC8762](#)] [Section 4.4](#), also apply to the procedure described in this document.

Routers that support G-ACh are subject to the same security considerations as defined in [[RFC4385](#)] and [[RFC5586](#)].

7. IANA Considerations

IANA maintains G-ACh Type Registry (see <https://www.iana.org/assignments/g-ach-parameters/g-ach-parameters.xhtml>). IANA is requested to allocate values for the STAMP G-ACh Types from "MPLS Generalized Associated Channel (G-ACh) Types (including Pseudowire Associated Channel Types)" registry.

Value	Description	Reference
TBD1	STAMP Session-Sender G-ACh Type	This document
TBD2	STAMP Session-Reflector G-ACh Type	This document

Table 1: STAMP G-ACh Type

8. References

8.1. Normative References

- [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>>.
- [RFC4385] Bryant, S., Swallow, G., Martini, L., and D. McPherson, "Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN", [RFC 4385](#), DOI 10.17487/RFC4385, February 2006, <<https://www.rfc-editor.org/info/rfc4385>>.
- [RFC5586] Bocci, M., Ed., Vigoureux, M., Ed., and S. Bryant, Ed., "MPLS Generic Associated Channel", [RFC 5586](#), DOI 10.17487/RFC5586, June 2009, <<https://www.rfc-editor.org/info/rfc5586>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in [RFC 2119](#) Key Words", [BCP 14](#), [RFC 8174](#), DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/info/rfc8174>>.
- [RFC8762] Mirsky, G., Jun, G., Nydell, H., and R. Foote, "Simple Two-Way Active Measurement Protocol", [RFC 8762](#), DOI 10.17487/RFC8762, March 2020, <<https://www.rfc-editor.org/info/rfc8762>>.
- [RFC8972] Mirsky, G., Min, X., Nydell, H., Foote, R., Masputra, A., and E. Ruffini, "Simple Two-Way Active Measurement Protocol Optional Extensions", [RFC 8972](#), DOI 10.17487/RFC8972, January 2021, <<https://www.rfc-editor.org/info/rfc8972>>.

8.2. Informative References

- [RFC5082] Gill, V., Heasley, J., Meyer, D., Savola, P., Ed., and C. Pignataro, "The Generalized TTL Security Mechanism (GTSM)", [RFC 5082](#), DOI 10.17487/RFC5082, October 2007, <<https://www.rfc-editor.org/info/rfc5082>>.
- [RFC6658] Bryant, S., Ed., Martini, L., Swallow, G., and A. Malis, "Packet Pseudowire Encapsulation over an MPLS PSN", [RFC 6658](#), DOI 10.17487/RFC6658, July 2012, <<https://www.rfc-editor.org/info/rfc6658>>.

[RFC8799] Carpenter, B. and B. Liu, "Limited Domains and Internet Protocols", [RFC 8799](#), DOI 10.17487/RFC8799, July 2020, <<https://www.rfc-editor.org/info/rfc8799>>.

Acknowledgments

TBA.

Authors' Addresses

Rakesh Gandhi
Cisco Systems, Inc.
Canada

Email: rgandhi@cisco.com

Patrice Brissette
Cisco Systems, Inc.
Canada

Email: pbrisset@cisco.com

Edward Leyton
Verizon Wireless

Email: edward.leyton@verizonwireless.com

