Internet Engineering Task Force (IETF)
Request for Comments: 7750
Updates: 5357
Category: Standards Track
ISSN: 2070-1721

J. Hedin
G. Mirsky
S. Baillargeon
Ericsson

February 2016

Differentiated Service Code Point and Explicit Congestion Notification Monitoring in the Two-Way Active Measurement Protocol (TWAMP)

Abstract

This document describes an optional extension for Two-Way Active Measurement Protocol (TWAMP) allowing the monitoring of the Differentiated Service Code Point and Explicit Congestion Notification fields with the TWAMP-Test protocol.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7750.

Table of Contents

1. Introduction

The One-Way Active Measurement Protocol (OWAMP) [RFC4656] defines the Type-P Descriptor field and negotiation of its value in the OWAMP-Control protocol. The Two-Way Active Measurement Protocol (TWAMP) [RFC5357] states that only a Differentiated Services Code Point (DSCP) value (see [RFC2474], [RFC3168], and [RFC3260]) can be defined by Type-P Descriptor, and the negotiated value must be used by both the Session-Sender and Session-Reflector. The TWAMP specification also states that the same DSCP value (found in the Session-Sender packet) MUST be used in the test packet reflected by the Session-Reflector. However, the TWAMP-Test protocol does not specify any methods to determine or report when the DSCP value has changed or is different than expected in the forward or reverse direction. Re-marking the DSCP (changing its original value) in IP networks is possible and often accomplished by a Differentiated Services policy configured on a single node along the IP path. In many cases, a change of the DSCP value indicates an unintentional or erroneous behavior. At best, the Session-Sender can detect a change of the DSCP reverse direction, assuming such a change is actually detectable.

This document describes an OPTIONAL feature for TWAMP. It is called DSCP and ECN Monitoring. It allows the Session-Sender to know the actual DSCP value received at the Session-Reflector. Furthermore, this feature tracks the Explicit Congestion Notification (ECN) value (see [RFC2474], [RFC3168], and [RFC3260]) received at the Session-

Reflector. This is helpful to determine if the ECN is actually operating or if an ECN-capable node has detected congestion in the forward direction.

1.1. Conventions Used in This Document

1.1.1. Terminology

DSCP: Differentiated Services Code Point

ECN: Explicit Congestion Notification

IPPM: IP Performance Metrics

TWAMP: Two-Way Active Measurement Protocol

OWAMP: One-Way Active Measurement Protocol

1.1.2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. TWAMP Extensions

TWAMP connection establishment follows the procedure defined in Section 3.1 of [RFC4656] and Section 3.1 of [RFC5357] where the Modes field is used to identify and select specific communication capabilities. At the same time, the Modes field is recognized and used as an extension mechanism [RFC6038]. The new feature requires a new flag to identify the ability of a Session-Reflector to return the values of received DSCP and ECN values back to a Session-Sender, and to support the new Session-Reflector packet format in the TWAMP-Test protocol. See Section 3 for details on the assigned bit position.

2.1. Setting Up Connection to Monitor DSCP and ECN

The Server sets the DSCP and ECN Monitoring flag in the Modes field of the Server Greeting message to indicate its capabilities and willingness to monitor them. If the Control-Client agrees to monitor DSCP and ECN on some or all test sessions invoked with this control connection, it MUST set the DSCP and ECN Monitoring flag in the Modes field in the Setup Response message.

2.2. TWAMP-Test Extension

Monitoring of DSCP and ECN requires support by the Session-Reflector and changes the test packet format in all the original modes (unauthenticated, authenticated, and encrypted). Monitoring of DSCP and ECN does not alter the Session-Sender test packet format, but certain considerations must be taken when and if this mode is accepted in combination with Symmetrical Size mode [RFC6038].

2.2.1. Session-Reflector Packet Format for DSCP and ECN Monitoring

When the Session-Reflector supports DSCP and ECN Monitoring, it constructs the Sender DSCP and ECN (S-DSCP-ECN) field, presented in Figure 1, for each test packet it sends to the Session-Sender according to the following procedure:

- the six (least-significant) bits of the Differentiated Service field MUST be copied from the received Session-Sender test packet into the Sender DSCP (S-DSCP) field;

- the two bits of the ECN field MUST be copied from the received Session-Sender test packet into the Sender ECN (S-ECN) field.

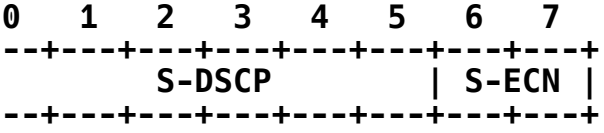


Figure 1: Sender DSCP and ECN Field Format

Formats of the test packet transmitted by the Session-Reflector in unauthenticated, authenticated, and encrypted modes have been defined in Section 4.2.1 of [RFC5357]. For the Session-Reflector that supports DSCP and ECN Monitoring, these formats are displayed in Figures 2 and 3.

For unauthenticated mode:

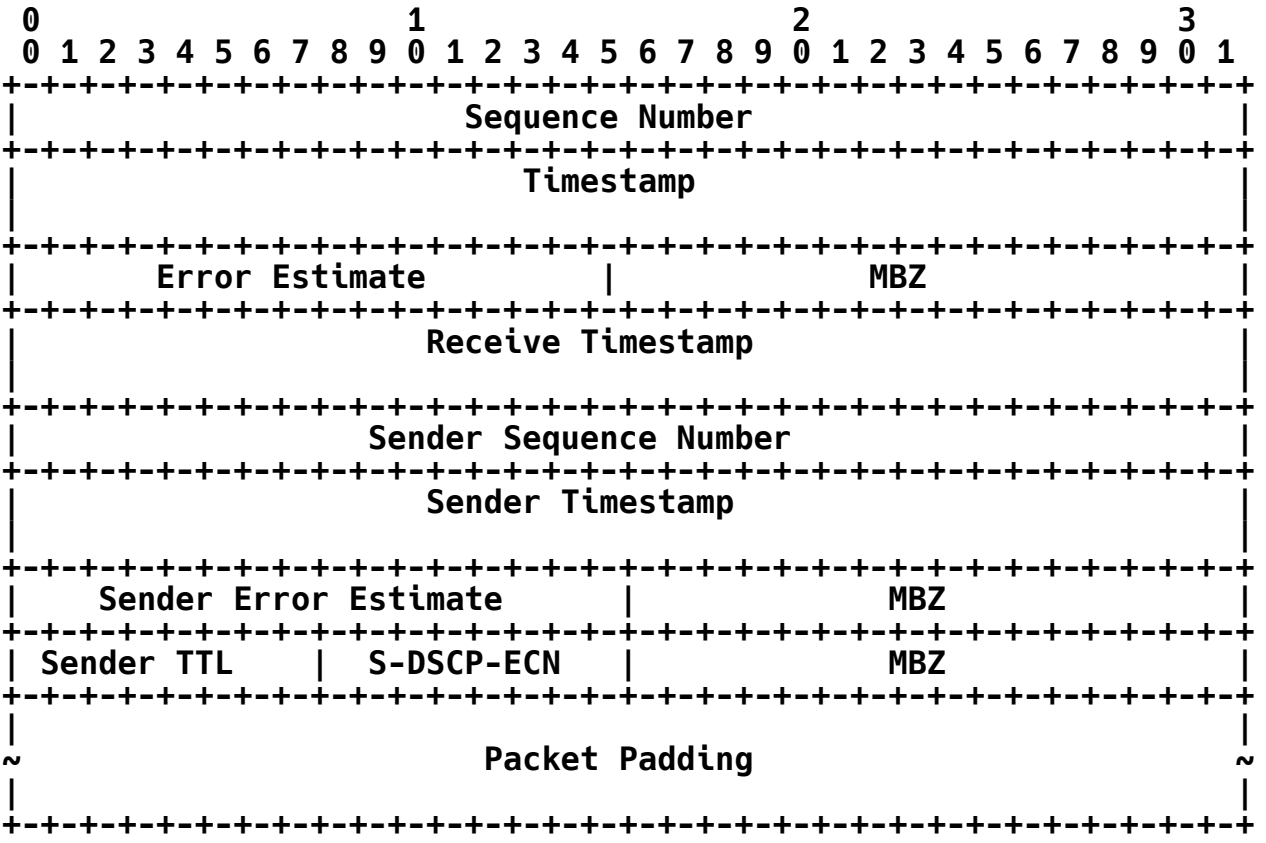


Figure 2: Session-Reflector Test Packet Format with DSCP and ECN Monitoring in Unauthenticated Mode

The DSCP and ECN values (part of the Type-P Descriptor [RFC4656]) can be provisioned through TWAMP-Control or by other means (command-line interface (CLI) or Central Controller). The DSCP and ECN values are often copied into reflected test packets with current TWAMP implementations without TWAMP-Control protocol. With the DSCP and ECN Monitoring extension, the Session-Reflector handles the DSCP as follows:

- the Session-Reflector MUST extract the DSCP and ECN values from the received packet and MUST use them to populate the S-DSCP-ECN field of the corresponding reflected packet;

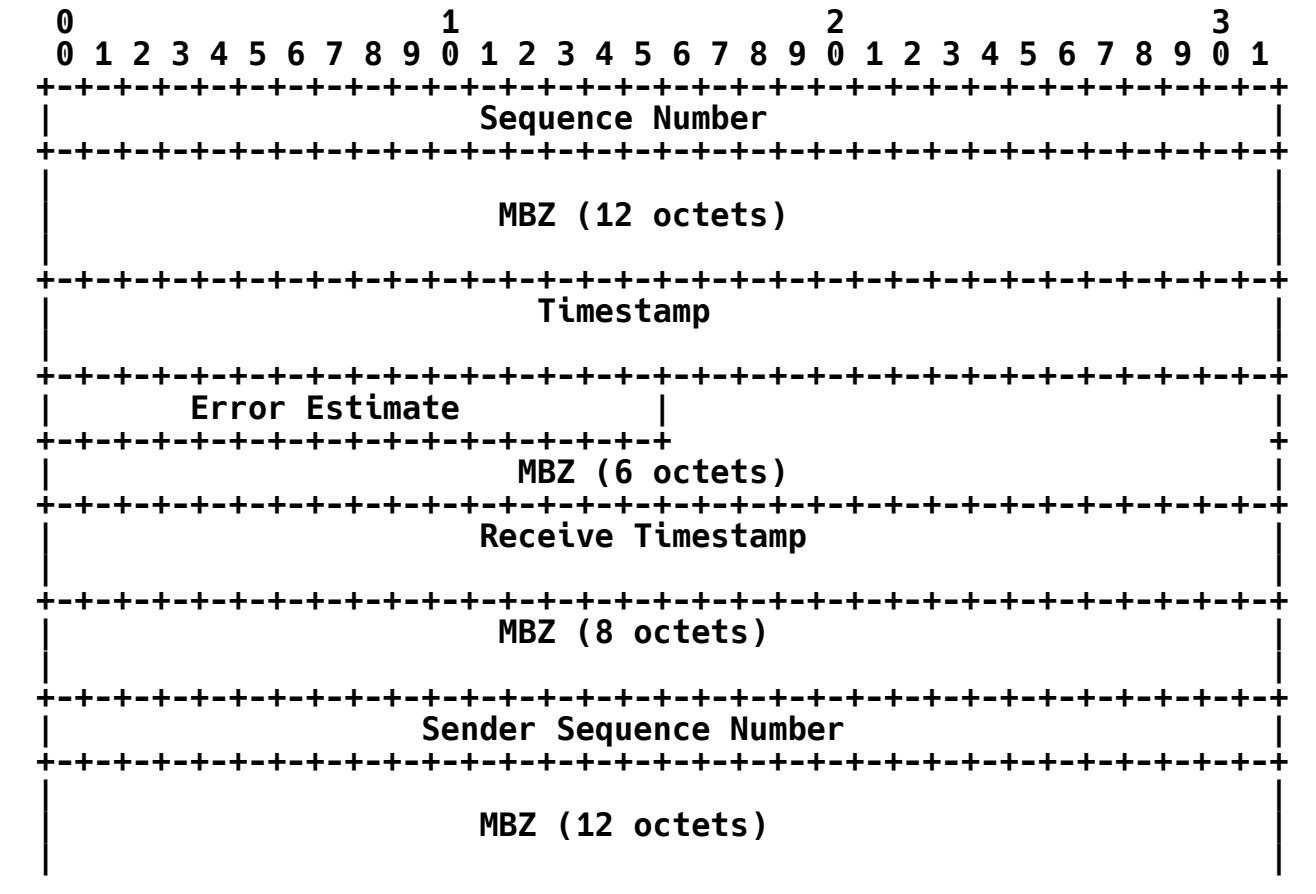
- the Session-Reflector MUST transmit each reflected test packet with the DSCP set to the provisioned value;

- if the provisioned DSCP value is not known (e.g., TWAMP Light), the choice of the DSCP is implementation specific. For instance, the Session-Reflector MAY copy the DSCP value from the received test packet and set it as the DSCP in a reflected packet. Alternatively, the Session-Reflector MAY set the DSCP value to CS0 (zero) [RFC2474];

- if the provisioned ECN value is not known, ECN SHOULD be set to Not-ECT codepoint value [RFC3168]. Otherwise, the provisioned ECN value for the session SHALL be used.

A Session-Reflector in the DSCP and ECN Monitoring mode does not analyze nor act on the ECN value of the received TWAMP test packet; therefore, it ignores congestion indications from the network. It is expected that sending rates are low enough, as TWAMP deployment experience had demonstrated since TWAMP base (RFC 5357) was published in 2008, that ignoring these congestion indications will not significantly contribute to network congestion.

For authenticated and encrypted modes:



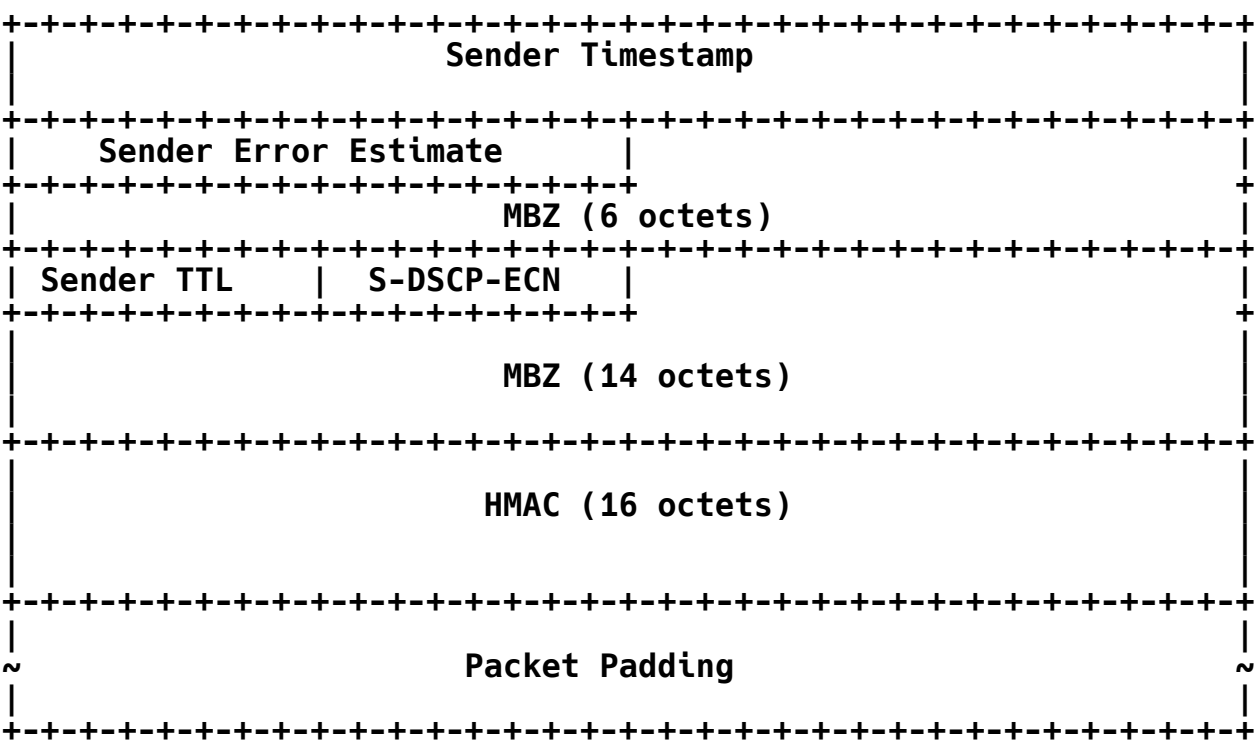


Figure 3: Session-Reflector Test Packet Format with DSCP and ECN Monitoring in Authenticated or Encrypted Modes

2.2.2. DSCP and ECN Monitoring with Extensions from RFC 6038

[RFC6038] defined two extensions to TWAMP -- first, to ensure that the Session-Sender and Session-Reflector exchange TWAMP-Test packets of equal size; second, to specify the number of octets to be reflected by Session-Reflector. If DSCP and ECN Monitoring and Symmetrical Size and/or Reflects Octets modes are being negotiated between Server and Control-Client in Unauthenticated mode, then, because Sender DSCP and Sender ECN increase the size of the unauthenticated Session-Reflector packet by 4 octets, the Padding Length value SHOULD be greater than or equal to 28 octets to allow for the truncation process that TWAMP recommends in Section 4.2.1 of [RFC5357].

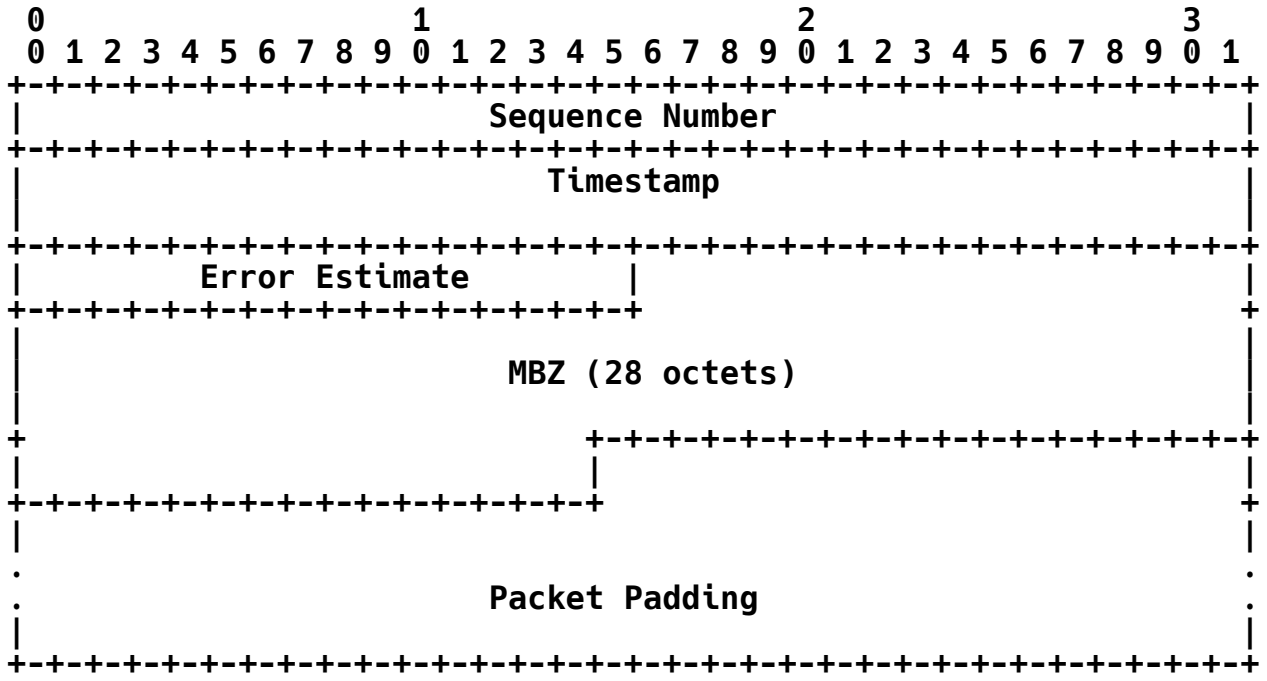


Figure 4: Session-Sender Test Packet Format with DSCP and ECN Monitoring and Symmetrical Test Packet in Unauthenticated Mode

2.2.3. Consideration for TWAMP Light Mode

Appendix I of [RFC5357] does not explicitly state how the value of the Type-P Descriptor is synchronized between the Session-Sender and Session-Reflector and whether different values are considered as error conditions and should be reported. We assume that by some means the Session-Sender and the Session-Reflector of the given TWAMP-Test session have been informed to use the same DSCP value. The same means, i.e., configuration, could be used to inform the

Session-Reflector to support DSCP and ECN Monitoring mode by copying data from received TWAMP test packets. Then Session-Sender may be informed to use the Sender DSCP and ECN field in the reflected TWAMP test packet.

3. IANA Considerations

In the TWAMP-Modes registry defined in [RFC5618], IANA has reserved a new DSCP and ECN Monitoring Capability as follows:

Bit Pos	Description	Semantics Definition	Reference
8	DSCP and ECN Monitoring Capability	Section 2	RFC 7750

Table 1: New Type-P Descriptor Monitoring Capability

4. Security Considerations

Monitoring of DSCP and ECN does not appear to introduce any additional security threat to hosts that communicate with TWAMP as defined in [RFC5357] and existing extensions [RFC6038]. Sections such as 3.2, 4, 4.1.2, 4.2, and 4.2.1 of [RFC5357] discuss unauthenticated, authenticated, and encrypted modes in varying degrees of detail. The security considerations that apply to any active measurement of live networks are relevant here as well. See the Security Considerations sections in [RFC4656] and [RFC5357].

5. References

5.1. 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, <http://www.rfc-editor.org/info/rfc2119>.

[RFC2474] Nichols, K., Blake, S., Baker, F., and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", RFC 2474, DOI 10.17487/RFC2474, December 1998, <http://www.rfc-editor.org/info/rfc2474>.

[RFC3168] Ramakrishnan, K., Floyd, S., and D. Black, "The Addition of Explicit Congestion Notification (ECN) to IP", RFC 3168, DOI 10.17487/RFC3168, September 2001, <http://www.rfc-editor.org/info/rfc3168>.

[RFC4656] Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, "A One-way Active Measurement Protocol (OWAMP)", RFC 4656, DOI 10.17487/RFC4656, September 2006, <http://www.rfc-editor.org/info/rfc4656>.

[RFC5357] Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)", RFC 5357, DOI 10.17487/RFC5357, October 2008, <http://www.rfc-editor.org/info/rfc5357>.

[RFC5618] Morton, A. and K. Hedayat, "Mixed Security Mode for the Two-Way Active Measurement Protocol (TWAMP)", RFC 5618, DOI 10.17487/RFC5618, August 2009, <http://www.rfc-editor.org/info/rfc5618>.

[RFC6038] Morton, A. and L. Ciavattone, "Two-Way Active Measurement Protocol (TWAMP) Reflect Octets and Symmetrical Size Features", RFC 6038, DOI 10.17487/RFC6038, October 2010, <http://www.rfc-editor.org/info/rfc6038>.

5.2. Informative References

[RFC3260] Grossman, D., "New Terminology and Clarifications for Diffserv", RFC 3260, DOI 10.17487/RFC3260, April 2002, <http://www.rfc-editor.org/info/rfc3260>.

Acknowledgements

The authors greatly appreciate thorough review and thoughtful comments by Bill Cerveny, Christofer Flinta, and Samita Chakrabarti.

Authors' Addresses

Jonas Hedin
Ericsson

Email: jonas.hedin@ericsson.com

Greg Mirsky
Ericsson

Email: gregory.mirsky@ericsson.com

Steve Baillargeon
Ericsson

Email: steve.baillargeon@ericsson.com