

IPPM Working Group
Internet-Draft
Intended status: Standards Track
Expires: 29 November 2026

R. Gandhi, Ed.
Cisco Systems, Inc.
P. Schoenmaker
Meta Platforms, Inc.
R. Foote
Nokia
L. Zhang
Huawei Technologies
28 May 2026

Simple Two-Way Active Measurement Protocol (STAMP) Extensions for
Residual Bit Error Rate Measurement
draft-gandhi-ippm-stamp-ber-06

Abstract

The Simple Two-Way Active Measurement Protocol (STAMP), as defined in RFC 8762, along with its optional extensions specified in RFC 8972, can be utilized for active measurement. Networks may experience transmission bit errors due to various factors, including poor fiber quality. Even with efficient CRC and FEC mechanisms, some bit errors may escape detection and correction, referred to as residual bit errors. This document further augments the STAMP extensions specified in RFC 8972 to enable the measurement of the residual bit error rate within the "Extra Padding" TLV of STAMP test packets.

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 29 November 2026.

Copyright Notice

Copyright (c) 2026 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 Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction	3
2. Conventions Used in This Document	4
2.1. Requirements Language	4
2.2. Abbreviations	4
2.3. STAMP Reference Topology	4
3. Overview	5
3.1. Bit Errors in Non-measurement Fields of STAMP	5
4. STAMP Procedure	6
4.1. STAMP Session-Sender	6
4.1.1. Considerations for Bit Pattern	7
4.2. STAMP Session-Reflector	7
4.2.1. STAMP TLV Conformant Check	8
4.3. Considerations for Link Aggregation Group	8
5. STAMP Extensions	9
5.1. Bit Pattern in Padding STAMP TLV	9
5.2. Bit Error Count in Padding STAMP TLV	10
5.3. Maximum Bit Error Burst Size in Padding STAMP TLV	10
6. Operational Considerations	11
6.1. Configuration Data Model Parameters	11
6.2. Operational Data Model Parameters	11
7. Security Considerations	12
8. Implementation Status	12
8.1. Open Source Implementation	12
8.2. Cisco Implementation of IOS-XR	13
9. IANA Considerations	13
10. References	14
10.1. Normative References	14
10.2. Informative References	14
Acknowledgments	15
Authors' Addresses	15

1. Introduction

The Simple Two-Way Active Measurement Protocol (STAMP) is designed to measure various performance metrics in IP networks without relying on a control channel to pre-signal session parameters, as specified in [RFC8762]. STAMP test packets are sent between a Session-Sender and a Session-Reflector to measure delay and packet loss along the path.

[RFC8972] introduces optional extensions for STAMP in the form of Type-Length-Value (TLV) objects, including the capability to transmit "Extra Padding" TLV within STAMP test packets.

Networks may experience transmission bit errors due to various factors, such as poor fiber quality, thereby corrupting packets. Bit errors can be single-bit errors or a burst of bit errors at a time. The bit errors in the received packets can be detected using a Cyclic Redundancy Check (CRC). Packets with CRC checksum failures may be dropped or corrected using Forward Error Correction (FEC). Even with efficient CRC and FEC mechanisms, some bit errors may escape detection and correction, referred to as residual bit errors. These bit errors result in upper-layer (such as UDP or TCP) checksum failures and packet drops. It is beneficial to measure the residual Bit Error Rate (BER) using active measurement packets between two nodes to detect service degradation. For accurate residual BER measurement, transmitting large active measurement packets is preferable, especially on links with low bit error rates. Furthermore, there is a need to transmit test packets at a high rate to measure residual BER on high-capacity links.

The STAMP test packets use a UDP header with a checksum field that can be used for checking the integrity of the header and payload data. The UDP checksum is optional for the IPv4 header. The UDP checksum may be set to 0 to bypass the UDP check for IPv4 and IPv6 headers for the STAMP destination UDP port. However, the checksum field does not provide an accurate measurement of bit errors.

Authenticated mode provides data integrity protection for the STAMP test packets by adding a Hashed Message Authentication Code (HMAC), such as HMAC-SHA-256 [RFC8762]. However, the authenticated mode does not provide an accurate measurement of bit errors. In addition, the HMAC TLV defined in [RFC8972] for authenticating STAMP TLVs does not include checking the "Extra Padding" TLV for data integrity.

This document further augments the STAMP extensions defined in [RFC8972] to enable the measurement of residual bit error rate within the "Extra Padding" TLV of STAMP test packets.

2. Conventions Used in This Document

2.1. 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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2.2. Abbreviations

BER: Bit Error Rate

CRC: Cyclic Redundancy Check

FEC: Forward Error Correction

MTU: Maximum Transmission Unit

STAMP: Simple Two-Way Active Measurement Protocol

TLV: Type-Length-Value

2.3. STAMP Reference Topology

In the STAMP reference topology shown in Figure 1, the STAMP Session-Sender S1 initiates Session-Sender test packets, and the STAMP Session-Reflector R1 transmits reply Session-Reflector test packets.

T1 is a transmit timestamp, and T4 is a receive timestamp added by node S1. T2 is a receive timestamp, and T3 is a transmit timestamp added by node R1.

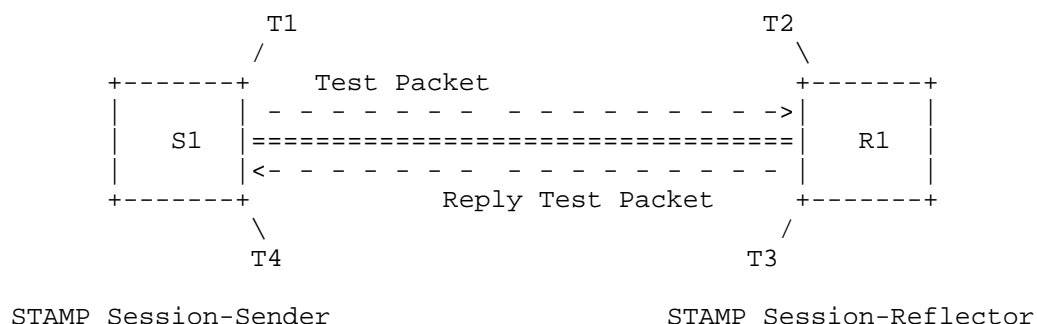


Figure 1: STAMP Reference Topology

3. Overview

The optional extensions for STAMP test packets [RFC8762] are defined in [RFC8972] in the form of TLVs. The Session-Sender transmits optional STAMP TLVs, and the Session-Reflector reflects all received STAMP TLVs from the Session-Sender test packets. [RFC8972] defines an optional TLV extension specifically for transmitting "Extra Padding" (Type=1) TLV in the STAMP test packets. The "Extra Padding" TLV can be filled using either a predefined fixed pattern or a random pattern of bits [RFC8972].

This document defines a procedure to measure residual BER within the "Extra Padding" TLV. The process involves the Session-Sender transmitting the extra padding filled with a predefined bit pattern. The Session-Reflector then checks for bit errors by comparing the received extra padding against the predefined bit pattern. This allows for the detection of a single bit error or a burst of bit errors and the measurement of the residual BER. The Session-Reflector does not discard the STAMP test packet with bit errors but instead reflects it back to the Session-Sender after correcting the bit errors. The Session-Reflector also returns the bit error count to the Session-Sender in the reflected STAMP test packet.

Residual BER is measured in both the forward and reverse directions between the Session-Sender and the Session-Reflector using the procedure and extensions defined in this document. The residual BER is calculated using the number of bit errors detected and the number of bits received, both in the extra padding.

As specified in [RFC8972], the Session-Sender and Session-Reflector test packets are symmetric in size. The Session-Sender and Session-Reflector MUST ensure that the resulting test packets do not exceed the path MTU after adding the STAMP TLVs.

3.1. Bit Errors in Non-measurement Fields of STAMP

Note that the procedure and extensions defined in this document do not use the base STAMP test packets, packet headers, or STAMP TLVs other than the "Extra Padding" TLV for residual BER measurement. It is possible that the bit errors impact those non-measurement fields of the STAMP test packets, causing packet verification failures. Such STAMP test packets are generally reported using a different measurement metric, such as packet loss. The integrity of those fields in the STAMP test packets can be verified using the HMAC mechanisms defined in [RFC8762] and [RFC8972].

Pattern in Padding" TLV, and may optionally carry one "Maximum Bit Error Burst Size in Padding" TLV.

The Session-Sender MUST add an "Extra Padding" TLV [RFC8972] when it adds a "Bit Pattern in Padding" TLV to the Session-Sender test packets. The variable-length data in the "Bit Pattern in Padding" TLV MUST contain the bit pattern employed in the "Extra Padding" TLV. The length of the extra padding MUST be an integer multiple of the length of the Bit Pattern to ease implementation.

The Session-Sender MUST also add an "Extra Padding" TLV [RFC8972] when it adds a "Bit Error Count in Padding" TLV in the Session-Sender test packets. The bit error count in the extra padding MUST be set to 0.

Note that the integrity of the "Bit Pattern in Padding", "Bit Error Count in Padding", and "Maximum Bit Error Burst Size in Padding" TLVs in the STAMP test packets can be protected using the HMAC mechanisms defined in [RFC8972].

If the Session-Sender receives the TLVs defined in this document back with the U flag (Unrecognized) set to 1 in the STAMP TLV Flags, it assumes that the Session-Reflector does not support the residual BER measurement and therefore disables the residual BER measurement but continues with the other STAMP measurements.

4.1.1. Considerations for Bit Pattern

It is possible that the bit pattern in the "Bit Pattern in Padding" TLV itself might contain bit errors. This can result in a measurement error due to a mismatch between the bit pattern and the extra padding. One way to avoid this issue is for the Session-Sender and Session-Reflector to use the local configuration with the default value of "0xFF00" as the bit pattern, which is repeated in the extra padding. In this case, the "Bit Pattern in Padding" TLV is not transmitted in the STAMP test packets.

4.2. STAMP Session-Reflector

When the Session-Reflector receives a STAMP test packet with a "Bit Pattern in Padding" TLV, the Session-Reflector that supports this TLV MUST check the extra padding in the "Extra Padding" TLV against the bit pattern to detect any bits that do not match the bit pattern and count them as bit errors.

When the Session-Reflector receives a STAMP test packet with a "Bit Error Count in Padding" TLV, the Session-Reflector that supports this TLV MUST check the "Extra Padding" TLV against the expected bit

pattern to detect if there are any bits not matching the bit pattern and count them as bit errors. The Session-Reflector updates the bit error count in the received "Bit Error Count in Padding" TLV and reflects the TLV back to the Session-Sender. If no bit errors are detected, the bit error count remains as 0 in the reflected "Bit Error Count in Padding" TLV.

The Session-Reflector corrects the bit errors in the "Extra Padding" TLV by matching the bit pattern and reflects the corrected "Extra Padding" TLV to the Session-Sender for BER measurement in the reverse direction. The corrected "Extra Padding" TLV is used to measure the residual BER in the reverse direction.

If the Session-Reflector does not recognize a TLV defined in this document, it returns the TLV with the U flag (Unrecognized) set to 1 in the STAMP TLV Flags of that TLV as described in [RFC8972].

4.2.1. STAMP TLV Conformant Check

If a Session-Reflector receives a STAMP test packet with a "Bit Pattern in Padding" TLV, a "Bit Error Count in Padding" TLV, or a "Maximum Bit Error Burst Size in Padding" TLV, without an "Extra Padding" TLV or with more than one "Extra Padding" TLV, it MUST set the C flag (Conformant) defined in [I-D.ietf-ippm-asymmetrical-pkts] to 1 in the STAMP TLV Flags of the reflected STAMP test packet for those STAMP TLVs.

If a Session-Reflector receives a STAMP test packet that contains more than one "Bit Pattern in Padding" TLV or more than one "Bit Error Count in Padding" TLV, or more than one "Maximum Bit Error Burst Size in Padding" TLV, it MUST set the C flag (Conformant) defined in [I-D.ietf-ippm-asymmetrical-pkts] to 1 in the STAMP TLV Flags of the reflected STAMP test packet for those STAMP TLVs.

The Session-Reflector MUST set the C flag (Conformant) defined in [I-D.ietf-ippm-asymmetrical-pkts] to 1 in the STAMP TLV Flags of the "Bit Pattern in Padding" TLV if the length of the extra padding is not an integer multiple of the length of the Bit Pattern.

4.3. Considerations for Link Aggregation Group

Networks may experience transmission bit errors differently for different link members of a Link Aggregation Group (LAG). The procedure and extensions defined in this document are equally applicable to measuring residual BER in both directions for each individual member of the LAG.

For delay measurement of LAG member links, a separate STAMP micro-session is created for each member of the LAG. The STAMP extension for the Micro-Session ID TLV, as defined in [RFC9534], is used to identify each member link of the LAG associated with the STAMP micro-session on the Session-Sender and Session-Reflector. The Session-Reflector replies on the same member of the LAG in the reverse direction based on the information in the received Session-Sender test packet and on either the local configuration for the micro-session or the information from the data plane where the test packet was received.

Note that in order to obtain a good approximation of the residual BER measurement, it is RECOMMENDED to transmit the STAMP test packets with the extra padding that matches the link MTU size.

5. STAMP Extensions

5.1. Bit Pattern in Padding STAMP TLV

The "Bit Pattern in Padding" TLV is optional and is carried by the Session-Sender and Session-Reflector test packets. The format of the TLV is shown in Figure 3.

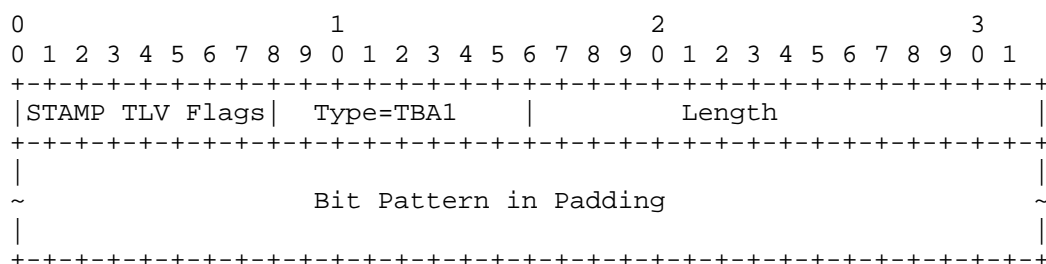


Figure 3: Bit Pattern in Padding STAMP TLV

The TLV fields are defined as follows:

STAMP TLV Flags: The STAMP TLV Flags follow the procedures described in [RFC8972].

Type: Type (value TBA1)

Length: A two-octet field equal to the length of the Data in octets.

Bit Pattern in Padding: The repeated bit pattern used in the extra padding.

5.2. Bit Error Count in Padding STAMP TLV

The "Bit Error Count in Padding" TLV is optional and is carried by the Session-Sender and Session-Reflector test packets. The format of the TLV is shown in Figure 4.

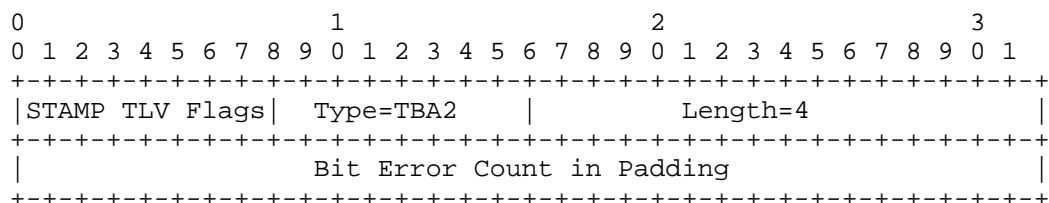


Figure 4: Bit Error Count in Padding STAMP TLV

The TLV fields are defined as follows:

STAMP TLV Flags: The STAMP TLV Flags follow the procedures described in [RFC8972].

Type: Type (value TBA2)

Length: A two-octet field set to 4 for the size of the Data.

Bit Error Count in Padding: The count of bit errors in the extra padding.

5.3. Maximum Bit Error Burst Size in Padding STAMP TLV

The "Maximum Bit Error Burst Size in Padding" TLV is optional and is carried by the Session-Sender and Session-Reflector test packets. The format of the TLV is shown in Figure 5.

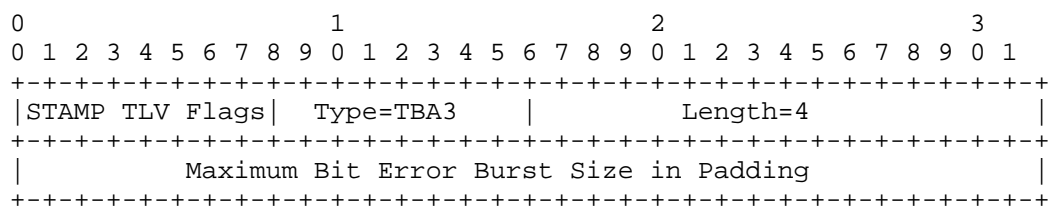


Figure 5: Maximum Bit Error Burst Size in Padding STAMP TLV

The TLV fields are defined as follows:

STAMP TLV Flags: The STAMP TLV Flags follow the procedures described in [RFC8972].

Type: Type (value TBA3)

Length: A two-octet field set to 4 for the size of the Data.

Maximum Bit Error Burst Size in Padding: The maximum size of the bit error burst, i.e., the maximum number of consecutive bit errors in the extra padding.

6. Operational Considerations

The operational considerations specified in [RFC8762] apply to the procedure and extensions defined in this document. Additional operational considerations are specified in the following subsections.

6.1. Configuration Data Model Parameters

The configuration data model for the residual BER measurement using STAMP MUST allow the setting of the following parameters:

- Padding size (number of bytes, which is an integer multiple of the padding bit pattern size in bytes)
- Padding bit pattern (with variable length of bytes)
- Transmit interval for STAMP test packets
- Computation interval as a multiple of transmit interval for reporting the residual BER measurements

6.2. Operational Data Model Parameters

The operational data model for the residual BER measurement using STAMP MUST allow the generation of the following parameters:

Forward direction (near-end) residual BER measurement:

- Total number of STAMP test packets received in the computation interval
- Total number of STAMP test packets received with non-zero Bit Error Count in TLV in the computation interval
- Total number of bits in the extra padding TLV of all received STAMP test packets in the computation interval
- Total Bit Error Count in TLV of all received STAMP test packets in the computation interval

Reverse direction (far-end) residual BER measurement:

- Total number of STAMP test packets received in the computation interval
- Total number of STAMP test packets received with bit errors in the computation interval
- Total number of bits in the extra padding TLV of all received STAMP test packets in the computation interval
- Total number of bit errors in all received STAMP test packets in the computation interval

Thresholds are defined for the forward and reverse directions of the residual BER metrics measured in the computation interval for:

- Number of bit errors per million
- Number of STAMP test packets with bit errors per million

An alarm is generated, and event-driven telemetry is triggered when the computed metric crosses the threshold.

7. Security Considerations

The security considerations specified in [RFC8762] and [RFC8972] apply to the procedure and extensions defined in this document.

8. Implementation Status

Editorial note: Please remove this section prior to publication.

8.1. Open Source Implementation

An open-source implementation of the Simple Two-Way Active Measurement Protocol (RFC 8762) is available in Teaparty.

<https://github.com/cerfcast/teaparty>

An implementation of the solution specified in this document is available at the following location:

[https://github.com/cerfcast/teaparty/
commit/592558a38dbcf9b273acb2a2fe8ab0d8f16d0709](https://github.com/cerfcast/teaparty/commit/592558a38dbcf9b273acb2a2fe8ab0d8f16d0709)

This implementation uses the "Experimental Use" Type 240 for Bit Pattern in Padding TLV and Type 241 for Bit Error Count in Padding TLV.

Additionally, there is also support for residual BER in the Wireshark dissector:

[https://github.com/cerfcaster/teaparty/
commit/608b9e89fce2f25ed88eaa367d0bacc693845da2](https://github.com/cerfcaster/teaparty/commit/608b9e89fce2f25ed88eaa367d0bacc693845da2)

Contact:

William Hawkins

University of Cincinnati

Email: hawkinsw@obs.cr

8.2. Cisco Implementation of IOS-XR

An implementation of the solution defined in this document is shipping in IOS-XR Software Release 26.1.1 running on Cisco's C8000 series of products.

This implementation uses the "Experimental Use" Type 240 for Bit Pattern in Padding TLV and Type 241 for Bit Error Count in Padding TLV.

9. IANA Considerations

IANA has created the "STAMP TLV Types" registry for [RFC8972]. IANA is requested to allocate a value for the "Bit Pattern in Padding" TLV Type, a value for the "Bit Error Count in Padding" TLV Type, and a value for the "Maximum Bit Error Burst Size in Padding" TLV Type from the IETF Review TLV range of the same registry.

Value	Description	Reference
TBA1	Bit Pattern in Padding	This document
TBA2	Bit Error Count in Padding	This document
TBA3	Maximum Bit Error Burst Size in Padding	This document

Table 1: STAMP TLV Types

10. References

10.1. 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>>.
- [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>>.
- [I-D.ietf-ippm-asymmetrical-pkts] Mirsky, G., Ruffini, E., Nydell, H., Foote, R. F., and W. Hawkins, "Performance Measurement with Asymmetrical Traffic Using Simple Two-Way Active Measurement Protocol (STAMP)", Work in Progress, Internet-Draft, draft-ietf-ippm-asymmetrical-pkts-14, 16 March 2026, <<https://datatracker.ietf.org/doc/html/draft-ietf-ippm-asymmetrical-pkts-14>>.

10.2. Informative References

- [RFC9534] Li, Z., Zhou, T., Guo, J., Mirsky, G., and R. Gandhi, "Simple Two-Way Active Measurement Protocol Extensions for Performance Measurement on a Link Aggregation Group", RFC 9534, DOI 10.17487/RFC9534, January 2024, <<https://www.rfc-editor.org/info/rfc9534>>.

Acknowledgments

The authors would like to thank Ianik Semco and Miloslav Kopka for the discussions on the bit error rate measurements. The authors would also like to thank Ruediger Geib, Zhenqiang Li, Carsten Rossenhoevel, Ernesto Ruffini, and Xiao Min for reviewing this document and providing many useful comments and suggestions. The authors would also like to thank William Hawkins for implementing the solution defined in this document and providing many useful suggestions.

Authors' Addresses

Rakesh Gandhi (editor)
Cisco Systems, Inc.
Canada
Email: rgandhi@cisco.com

Peter Schoenmaker
Meta Platforms, Inc.
United Kingdom
Email: psch@meta.com

Richard Foote
Nokia
Email: footer.foote@nokia.com

Li Zhang
Huawei Technologies
China
Email: zhangli344@huawei.com