Workgroup: DetNet Working Group
Internet-Draft: draft-ietf-detnet-mpls-oam-08
Published: 6 September 2022
Intended Status: Standards Track
Expires: 10 March 2023
Authors: G. Mirsky M. Chen B. Varga
Ericsson Huawei Ericsson

Operations, Administration and Maintenance (OAM) for Deterministic Networks (DetNet) with MPLS Data Plane

Abstract

This document defines format and use principals of the Deterministic Network (DetNet) service Associated Channel (ACH) over a DetNet network with the MPLS data plane. The DetNet service ACH can be used to carry test packets of active Operations, Administration, and Maintenance protocols that are used to detect DetNet failures and measure performance metrics.

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 10 March 2023.

Table of Contents

1. Introduction

[RFC8655] introduces and explains Deterministic Networks (DetNet) architecture and how the Packet Replication, Elimination, and Ordering functions (PREOF) can be used to ensure low packet drop ratio in DetNet domain.

Operations, Administration and Maintenance (OAM) protocols are used to detect, localize defects in the network, and monitor network performance. Some OAM functions, e.g., failure detection, work in the network proactively, while others, e.g., defect localization, usually performed on-demand. These tasks achieved by a combination of active and hybrid, as defined in [RFC7799], OAM methods.

Also, this document defines format and use principals of the DetNet service Associated Channel over a DetNet network with the MPLS data plane [RFC8964].

2. Conventions used in this document

2.1. Terminology and Acronyms

The term "DetNet OAM" used in this document interchangeably with longer version "set of OAM protocols, methods and tools for Deterministic Networks".

CW Control Word

DetNet Deterministic Networks

d-ACH DetNet Associated Channel Header

d-CW DetNet Control Word

DNH DetNet Header

GAL Generic Associated Channel Label

G-ACh Generic Associated Channel

OAM: Operations, Administration and Maintenance

PREOF Packet Replication, Elimination, and Ordering Functions

PW Pseudowire

RDI Remote Defect Indication

E2E End-to-end

CFM Connectivity Fault Management

BFD Bidirectional Forwarding Detection

TSN Time-Sensitive Network

F-Label A Detnet "forwarding" label that identifies the LSP used to forward a DetNet flow across an MPLS PSN, e.g., a hop-by-hop label used between label switching routers (LSR).

S-Label A DetNet "service" label that is used between DetNet nodes that implement also the DetNet service sub-layer functions. An S-Label is also used to identify a DetNet flow at DetNet service sub-layer.

Underlay Network or Underlay Layer: The network that provides connectivity between the DetNet nodes. MPLS network providing LSP connectivity between DetNet nodes is an example of the underlay layer.

DetNet Node - a node that is an actor in the DetNet domain. DetNet domain edge node and node that performs PREOF within the domain are examples of DetNet node.

2.2. Keywords

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.

3. Active OAM for DetNet Networks with MPLS Data Plane

OAM protocols and mechanisms act within the data plane of the particular networking layer. And thus it is critical that the data plane encapsulation supports OAM mechanisms in such a way to comply with the OAM requirements listed in [I-D.tpmb-detnet-oam-framework]. One of such examples that require special consideration is requirement #5:

> DetNet OAM packets MUST be in-band, i.e., follow precisely the same path as DetNet data plane traffic both for unidirectional and bi-directional DetNet paths.

The Det Net data plane encapsulation in transport network with MPLS encapsulation specified in [RFC8964]. For the MPLS underlay network, DetNet flows to be encapsulated analogous to pseudowires (PW) over MPLS packet switched network, as described in [RFC3985], [RFC4385]. Generic PW MPLS Control Word (CW), defined in [RFC4385], for DetNet displayed in Figure 1.

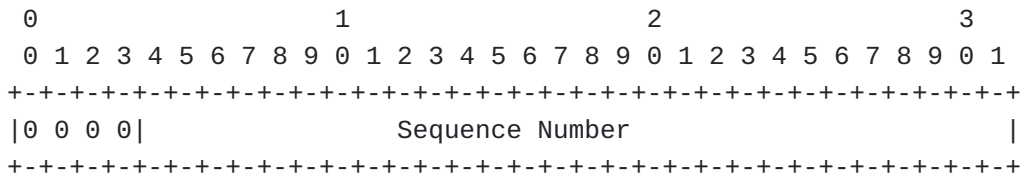

Figure 1: DetNet Control Word Format

PREOF in the DetNet domain composed by a combination of nodes that perform replication and elimination functions. The elimination function always uses the S-Label and packet sequencing information, e.g., the value in the Sequence Number field of DetNet CW (d-CW). The replication sub-function uses the S-Label information only. For data packets Figure 2 presents an example of PREOF in DetNet domain.

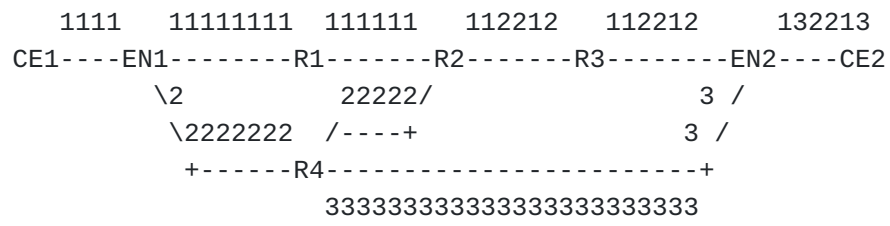

Figure 2: DetNet Data Plane Based on PW

3.1. DetNet Active OAM Encapsulation

DetNet OAM, like PW OAM, uses PW Associated Channel Header defined in [RFC4385]. Figure 3 displays the encapsulation of a DetNet MPLS [RFC8964] active OAM packet.

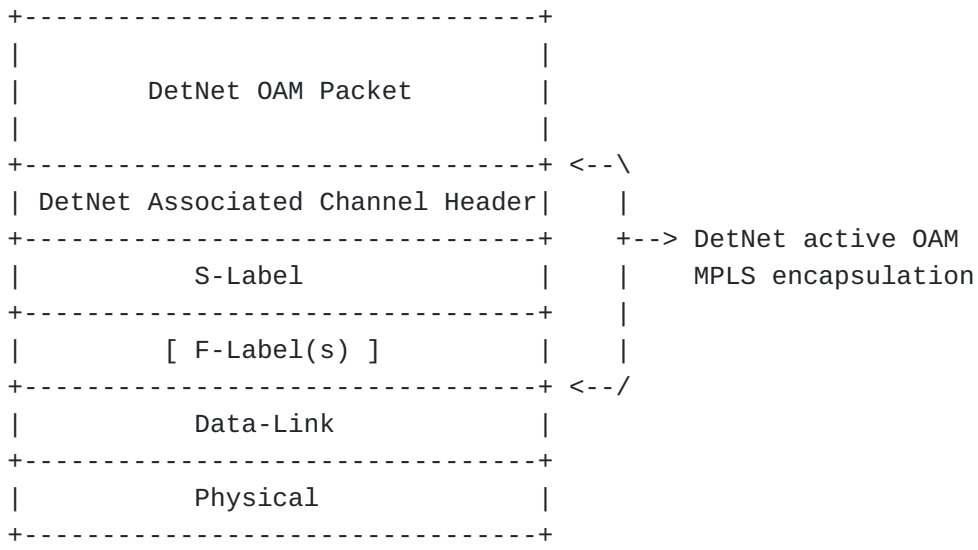

Figure 3: DetNet Active OAM Packet Encapsulation in MPLS Data Plane

Figure 4 displays encapsulation of a test packet of an active DetNet OAM protocol in case of MPLS-over-UDP/IP [RFC9025].

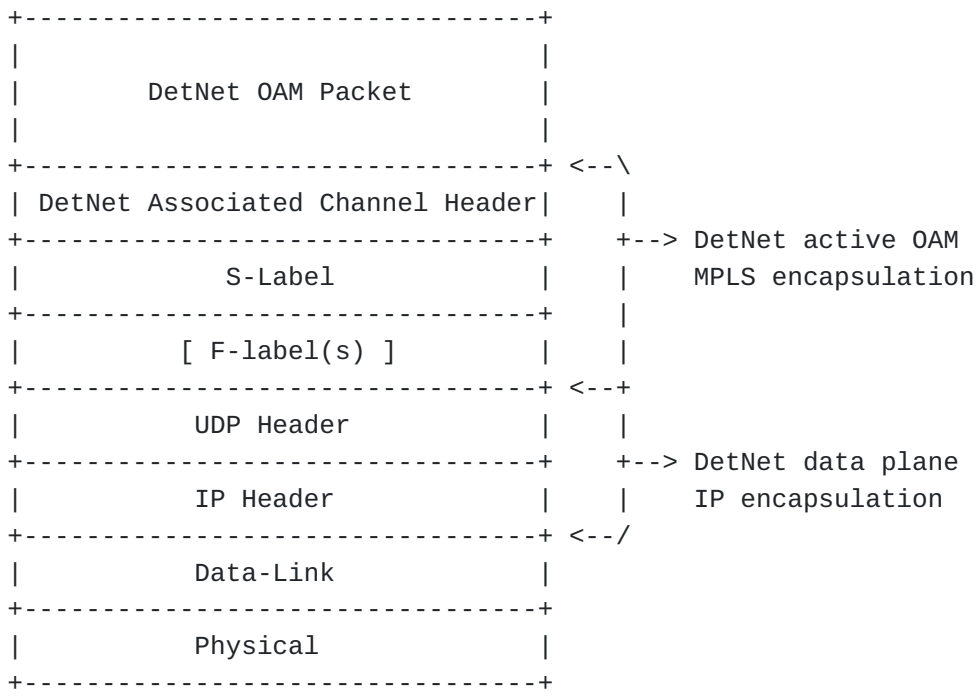

Figure 4: DetNet Active OAM Packet Encapsulation in MPLS-over-UDP/IP

Figure 5 displays the format of the DetNet Associated Channel Header (d-ACH).

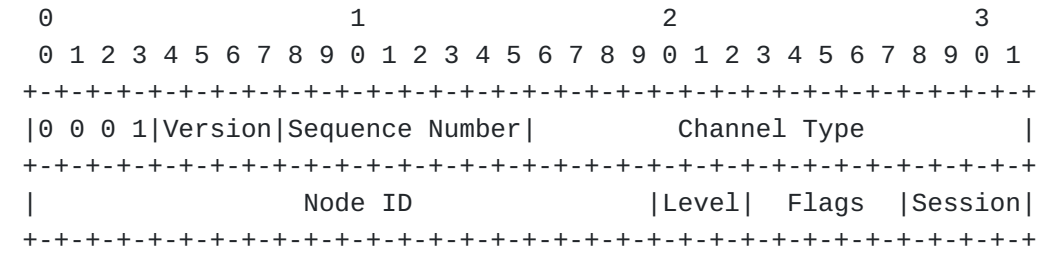

Figure 5: DetNet Associated Channel Header Format

The d-ACH encodes the following fields:

Bits 0..3 MUST be 0b0001. This value of the first nibble allows the packet to be distinguished from an IP packet [RFC4928] and a DetNet data packet [RFC8964].

Version - is a four-bits field, and the value is the version number of the d-ACH. This specification defines version 0x1.

Sequence Number - is an unsigned eight-bit field. The sequence number space is circular with no restriction on the initial value. The originator DetNet node MUST set the value of the

Sequence Number field before the transmission of a packet. The originator node MUST increase the value of the Sequence Number field by 1 for each active OAM packet.

Channel Type - contains the value of DetNet Associated Channel Type. It is one of the values defined in the IANA PW Associated Channel Type registry.

Node ID - is an unsigned 20 bits-long field. The value of the Node ID field identifies the DetNet node that originated the packet. Methods of distributing Node ID are outside the scope of this specification.

Level - is a three-bits field.

Flags - is a five-bits field. Flags field contains five one-bit flags. Section 6.1 creates an IANA registry for new flags to be defined. Flags defined in this specification presented in Figure 6.

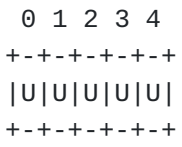

Figure 6: DetNet Associated Channel Header Flags Field Format

U: Unused and for future use. MUST be 0 on transmission and ignored on receipt.

Session ID is a four-bits field.

The DetNet flow, according to [RFC8964], is identified by the S-label that MUST be at the bottom of the stack. Active OAM packet MUST include d-ACH immediately following the S-label.

3.2. DetNet Packet Replication, Elimination, and Ordering Functions Interaction with Active OAM

At the DetNet service sub-layer, special functions MAY be applied to the particular DetNet flow, PREOF, to potentially lower packet loss, improve the probability of on-time packet delivery and ensure in-order packet delivery. PREOF rely on sequencing information in the DetNet service sub-layer. For a DetNet active OAM packet, 28 MSBs of the d-ACH MUST be used as the source of the sequencing information by PREOF.

4. Use of Hybrid OAM in DetNet

Hybrid OAM methods are used in performance monitoring and defined in [RFC7799] as:

> Hybrid Methods are Methods of Measurement that use a combination of Active Methods and Passive Methods.

A hybrid measurement method may produce metrics as close to passive, but it still alters something in a data packet even if that is the value of a designated field in the packet encapsulation. One example of such a hybrid measurement method is the Alternate Marking method described in [RFC8321]. Reserving the field for the Alternate Marking method in the DetNet Header will enhance available to an operator set of DetNet OAM tools.

5. OAM Interworking Models

Interworking of two OAM domains that utilize different networking technology can be realized either by a peering or a tunneling model. In a peering model, OAM domains are within the corresponding network domain. When using the peering model, state changes that are detected by a Fault Management OAM protocol can be mapped from one OAM domain into another or a notification, e.g., an alarm, can be sent to a central controller. In the tunneling model of OAM interworking, usually, only one active OAM protocol is used. Its test packets are tunneled through another domain along with the data flow, thus ensuring the fate sharing among test and data packets.

5.1. OAM of DetNet MPLS Interworking with OAM of TSN

Active DetNet OAM is required to provide the E2E fault management and performance monitoring for a DetNet flow. Interworking of DetNet active OAM with MPLS data plane with the IEEE 802.1 Time-Sensitive Networking (TSN) domain based on [RFC9037].

In the case of the peering model is used in the fault management OAM, then the node that borders both TSN and DetNet MPLS domains MUST support [RFC7023]. [RFC7023] specified the mapping of defect states between Ethernet Attachment Circuits (ACs) and associated Ethernet PWs that are part of an end-to-end (E2E) emulated Ethernet service. Requirements and mechanisms described in [RFC7023] are equally applicable to using the peering model to achieve E2E FM OAM over DetNet MPLS and TSN domains. The Connectivity Fault Management (CFM) protocol [IEEE.CFM] or in [ITU.Y1731] can provide fast detection of a failure in the TSN segment of the DetNet service. In the DetNet MPLS domain BFD (Bidirectional Forwarding Detection), specified in [RFC5880] and [RFC5885], can be used. To provide E2E failure detection, the TSN segment might be presented as a concatenated with the DetNet MPLS and the Section 6.8.17 [RFC5880]

MAY be used to inform the upstream DetNet MPLS node of a failure of the TSN segment. Performance monitoring can be supported by [RFC6374] in the DetNet MPLS and [ITU.Y1731] in the TSN domains, respectively. Performance objectives for each domain should refer to metrics that additive or be defined for each domain separately.

The following considerations are to be realized when using the tunneling model of OAM interworking between DetNet MPLS and TSN domains:

*Active OAM test packet MUST be mapped to the same TSN Stream ID as the monitored DetNet flow.

*Active OAM test packets MUST be treated in the TSN domain based on its S-label and CoS marking (TC field value).

Note that the tunneling model of the OAM interworking requires that the remote peer of the E2E OAM domain supports the active OAM protocol selected on the ingress endpoint. For example, if BFD is used for proactive path continuity monitoring in the DetNet MPLS domain, a TSN endpoint of the DetNet service has also support BFD as defined in [RFC5885].

5.2. OAM of DetNet MPLS Interworking with OAM of DetNet IP

Interworking between active OAM segments in DetNet MPLS and DetNet IP domains can also be realized using either the peering or the tunneling model, as discussed in Section 5.1. Using the same protocol, e.g., BFD, over both segments, simplifies the mapping of errors in the peering model. To provide the performance monitoring over a DetNet IP domain STAMP [RFC8762] and its extensions [RFC8972] can be used.

6. IANA Considerations

6.1. DetNet MPLS OAM Flags Registry

This document describes a new IANA-managed registry to identify DetNet MPLS OAM Flags Bits. The registration procedure is "IETF Review" [RFC8126]. The registry name is "DetNet MPLS OAM Flags". There are five flags in the five-bit Flags field, defined as in Table 1.

Bit	Description	Reference
0-4	Unassigned	This document

Table 1: DetNet MPLS OAM Flags

7. Security Considerations

Additionally, security considerations discussed in DetNet specifications: [RFC8655], [RFC9055], [RFC8964] are applicable to this document. Security concerns and issues related to MPLS OAM tools like LSP Ping [RFC8029], BFD over PW [RFC5885] also apply to this specification.

8. Acknowledgment

Authors extend their appreciation to Pascal Thubert for his insightful comments and productive discussion that helped to improve the document. The authors are enormously grateful to Janos Farcas for his detailed comments and the inspiring discussion that made this document clearer and stronger.

9. References

9.1. 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>.

[RFC7023] Mohan, D., Ed., Bitar, N., Ed., Sajassi, A., Ed., DeLord, S., Niger, P., and R. Qiu, "MPLS and Ethernet Operations, Administration, and Maintenance (OAM) Interworking", RFC 7023, DOI 10.17487/RFC7023, October 2013, <https://www.rfc-editor.org/info/rfc7023>.

[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>.

[RFC8655] Finn, N., Thubert, P., Varga, B., and J. Farkas, "Deterministic Networking Architecture", RFC 8655, DOI 10.17487/RFC8655, October 2019, <https://www.rfc-editor.org/info/rfc8655>.

[RFC8964] Varga, B., Ed., Farkas, J., Berger, L., Malis, A., Bryant, S., and J. Korhonen, "Deterministic Networking (DetNet) Data Plane: MPLS", RFC 8964, DOI 10.17487/RFC8964, January 2021, <https://www.rfc-editor.org/info/rfc8964>.

[RFC9025] Varga, B., Ed., Farkas, J., Berger, L., Malis, A., and S. Bryant, "Deterministic Networking (DetNet) Data Plane: MPLS over UDP/IP", RFC 9025, DOI 10.17487/RFC9025, April 2021, <https://www.rfc-editor.org/info/rfc9025>.

9.2. Informational References

[I-D.tpmb-detnet-oam-framework] Mirsky, G., Theoleyre, F., Papadopoulos, G. Z., and C. J. Bernardos, "Framework of Operations, Administration and Maintenance (OAM) for Deterministic Networking (DetNet)", Work in Progress, Internet-Draft, draft-tpmb-detnet-oam-framework-01, 30 March 2021, <https://datatracker.ietf.org/doc/html/draft-tpmb-detnet-oam-framework-01>.

[IEEE.CFM] IEEE, "Connectivity Fault Management clause of IEEE 802.1Q", IEEE 802.1Q, 2013.

[ITU.Y1731] ITU-T, "OAM functions and mechanisms for Ethernet based Networks", ITU-T Recommendation G.8013/Y.1731, November 2013.

[RFC3985] Bryant, S., Ed. and P. Pate, Ed., "Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture", RFC 3985, DOI 10.17487/RFC3985, March 2005, <https://www.rfc-editor.org/info/rfc3985>.

[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>.

[RFC4928] Swallow, G., Bryant, S., and L. Andersson, "Avoiding Equal Cost Multipath Treatment in MPLS Networks", BCP 128, RFC 4928, DOI 10.17487/RFC4928, June 2007, <https://www.rfc-editor.org/info/rfc4928>.

[RFC5880] Katz, D. and D. Ward, "Bidirectional Forwarding Detection (BFD)", RFC 5880, DOI 10.17487/RFC5880, June 2010, <https://www.rfc-editor.org/info/rfc5880>.

[RFC5885] Nadeau, T., Ed. and C. Pignataro, Ed., "Bidirectional Forwarding Detection (BFD) for the Pseudowire Virtual Circuit Connectivity Verification (VCCV)", RFC 5885, DOI 10.17487/RFC5885, June 2010, <https://www.rfc-editor.org/info/rfc5885>.

[RFC6374] Frost, D. and S. Bryant, "Packet Loss and Delay Measurement for MPLS Networks", RFC 6374, DOI 10.17487/RFC6374, September 2011, <https://www.rfc-editor.org/info/rfc6374>.

[RFC7799] Morton, A., "Active and Passive Metrics and Methods (with Hybrid Types In-Between)", RFC 7799, DOI 10.17487/

RFC7799, May 2016, <https://www.rfc-editor.org/info/rfc7799>.

[RFC8029] Kompella, K., Swallow, G., Pignataro, C., Ed., Kumar, N., Aldrin, S., and M. Chen, "Detecting Multiprotocol Label Switched (MPLS) Data-Plane Failures", RFC 8029, DOI 10.17487/RFC8029, March 2017, <https://www.rfc-editor.org/info/rfc8029>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[RFC8321] Fioccola, G., Ed., Capello, A., Cociglio, M., Castaldelli, L., Chen, M., Zheng, L., Mirsky, G., and T. Mizrahi, "Alternate-Marking Method for Passive and Hybrid Performance Monitoring", RFC 8321, DOI 10.17487/RFC8321, January 2018, <https://www.rfc-editor.org/info/rfc8321>.

[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>.

[RFC9037] Varga, B., Ed., Farkas, J., Malis, A., and S. Bryant, "Deterministic Networking (DetNet) Data Plane: MPLS over IEEE 802.1 Time-Sensitive Networking (TSN)", RFC 9037, DOI 10.17487/RFC9037, June 2021, <https://www.rfc-editor.org/info/rfc9037>.

[RFC9055] Grossman, E., Ed., Mizrahi, T., and A. Hacker, "Deterministic Networking (DetNet) Security Considerations", RFC 9055, DOI 10.17487/RFC9055, June 2021, <https://www.rfc-editor.org/info/rfc9055>.

Authors' Addresses

Greg Mirsky
Ericsson

Email: gregimirsky@gmail.com

Mach(Guoyi) Chen
Huawei

Email: mach.chen@huawei.com

Balazs Varga
Ericsson
Budapest
Magyar Tudosok krt. 11.
1117
Hungary

Email: balazs.a.varga@ericsson.com