

# ETSI GS ENI 034 V4.1.1 (2024-07)



## Experiential Networked Intelligence (ENI); Requirements and Detailed Procedure of Network Policy Conflict Detection

### Document Preview

[ETSI GS ENI 034 V4.1.1 \(2024-07\)](https://standards.iteh.ai/catalog/standards/etsi/060d9534-2e53-4aa9-b5f5-e16a730c7ba8/etsi-gs-eni-034-v4-1-1-2024-07)

<https://standards.iteh.ai/catalog/standards/etsi/060d9534-2e53-4aa9-b5f5-e16a730c7ba8/etsi-gs-eni-034-v4-1-1-2024-07>

#### *Disclaimer*

---

The present document has been produced and approved by the Experiential Networked Intelligence (ENI) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.  
It does not necessarily represent the views of the entire ETSI membership.

---

**Reference**

DGS/ENI-0034v411\_Confli\_Detect

---

**Keywords**

conflict detection, OAM, policy management

---

**ETSI**

650 Route des Lucioles  
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B  
Association à but non lucratif enregistrée à la  
Sous-Préfecture de Grasse (06) N° w061004871

---

**Important notice**

The present document can be downloaded from:

<https://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at [www.etsi.org/deliver](http://www.etsi.org/deliver).

Users of the present document should be aware that the document may be subject to revision or change of status.

Information on the current status of this and other ETSI documents is available at

<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:

<https://portal.etsi.org/People/CommitteeSupportStaff.aspx>

If you find a security vulnerability in the present document, please report it through our

Coordinated Vulnerability Disclosure Program:

<https://www.etsi.org/standards/coordinated-vulnerability-disclosure>

---

**Notice of disclaimer & limitation of liability**

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

---

**Copyright Notification**

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2024.  
All rights reserved.

# Contents

Intellectual Property Rights .....	4
Foreword.....	4
Modal verbs terminology.....	4
Executive summary .....	4
Introduction .....	4
1 Scope .....	5
2 References .....	5
2.1 Normative references .....	5
2.2 Informative references.....	5
3 Definition of terms, symbols and abbreviations.....	5
3.1 Terms.....	5
3.2 Symbols.....	6
3.3 Abbreviations .....	6
4 Overview of Network Policy Conflict Detection .....	6
4.1 Introduction .....	6
4.2 Description of Network Policy Conflict Detection .....	6
4.3 External Requirements for Network Policy Conflict Detection .....	7
4.3.1 Network Policy .....	7
4.3.2 Input Frequency and Assisted System .....	8
4.4 Functional Workflow .....	9
5 Network Policy Conflict Detection Reference Working Pipeline.....	10
5.1 Introduction .....	10
5.2 Input .....	10
5.2.1 User-defined Network Policy as Input.....	10
5.2.2 Network Topo & Configuration as Input .....	11
5.2.3 Forwarding Rule Changes or Self-Changes as Input .....	11
5.3 Forwarding Rule Changes Simulation.....	11
5.4 Network Policy Conflict Detecting and Locating .....	12
5.4.1 Parser Layer Detecting and Locating.....	12
5.4.2 Verifier Layer Detecting and Locating.....	12
5.5 Result Feedback .....	12
5.5.1 Parser Layer Feedback.....	12
5.5.2 Verifier Layer Feedback .....	13
6 Use Cases .....	13
6.1 Network Policy Detection in VxLAN .....	13
6.1.1 Use Case Context.....	13
6.1.2 Description of the use case .....	14
6.1.2.1 Overview .....	14
6.1.2.2 Motivation.....	14
6.1.2.3 Actors and Roles .....	14
6.1.2.4 Initial context configuration .....	14
6.1.2.5 Triggering condition.....	14
6.1.2.6 Operational Flow of Actions .....	14
6.1.2.7 Post-conditions.....	15
7 Areas of Future Study (informative) .....	15
7.1 Open Issues for the present document.....	15
7.2 Issues for Future Study.....	15
History .....	16

---

# Intellectual Property Rights

## Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: "*Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards*", which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<https://ipr.etsi.org/>).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

## Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

**DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

---

# Foreword

This Group Specification (GS) has been produced by ETSI Industry Specification Group (ISG) Experiential Networked Intelligence (ENI).

---

# Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

---

# Executive summary

The present document specifies a high-level functional abstraction of the process of ENI Intent policy Multi-Stage translating in an ENI system in terms of Functional Modules, Internal Reference Points and working pipelines.

---

# Introduction

The present document defines a high-level functional abstraction of Network Policy Conflict Detection for ENI Intent Policies. The organization of the present document is as follows. Clause 1 defines the scope of the present document. Clauses 2 and 3 provide normative and informative references and definition of terms, respectively. Clause 4 provides an informative overview of Network Policy Conflict Detection, including its motivation, benefits, important concepts and an overview of its Functional Modules. Clause 5 defines important design principles of the processing. Clause 6 provides some use cases of Network Policy Conflict Detection. Clause 7 describes areas of future work.

---

# 1 Scope

The present document provides additional information concerning Network Policy local conflict detection for ENI Intent Policies. The present document expands on the work done in ETSI GS ENI 005 [i.2], clause 6.3.9.6.3, to provide additional requirements and procedures to ensure that a new network policy will not conflict with any currently deployed network policies in the same administrative domain. The present document is only intended for Network Policies that are structured as ENI Intent Policies and which meet the requirements defined in clause 4.3.1.

The present document also describes the input(s), output(s), Internal Reference Points, and functionality of every step in the Network Policy local conflict detection process.

If network policies with potential risks are dispatched, they may lead to various errors in the network and cause instability and harm. However, as the scale of the network increases, the difficulty and cost of detecting and correcting network errors also increases. Therefore, Network Policy Conflict Detection is implemented after Policy Validation and Policy Rewriting. This will potentially save time and reduce misconfigurations. Consequently, the stability and availability of the system will be increased.

The present document will encompass research and investigation activities that will address network policy conflict in IP networks at the first stage. Subsequent efforts may extend the work into telecommunication networks.

---

# 2 References

## 2.1 Normative references

Not applicable.

## 2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

- [i.1] ETSI GR ENI 004: "Experiential Networked Intelligence (ENI); Terminology".
- [i.2] ETSI GS ENI 005 (V3.1.1): "Experiential Networked Intelligence (ENI); System Architecture".
- [i.3] ETSI GR ENI 010: "Experiential Networked Intelligence (ENI); Evaluation of categories for AI application to Networks".

---

# 3 Definition of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in ETSI GR ENI 004 [i.1], ETSI GS ENI 005 [i.2] and the following apply:

**black hole:** place in the network where incoming or outgoing traffic is unexcepted discarded, so that the data did not reach its intended recipient

**forwarding loop:** abnormal phenomenon in which a packet reaches the same device twice during the forwarding process

**forwarding model:** edge-labelled directed graph for representing network forwarding behaviour

**hit domain:** set of packets that satisfy the Action rules

**match domain:** set of packets that match the routing table, ACL or NAT

**network invariant:** packet forwarding constraint that needs to be satisfied in any computer network

**network policy:** specific type of policy that affects network behaviour and can be directly understood and executed by network devices within the Assisted System

**self-change:** unpredictable changes due to Network Events such as node faults

**snapshot translation:** kind of data translation in which the raw routing table (also known as flow table), ACL and NAT of each device in the AS are translated into FW, ACL and NAT rules, respectively

**User-Defined Network Policy:** user-defined packet forwarding constraint that needs to be satisfied in a particular computer network to comply with applicable network invariants

**waypoint:** device that the packets need to pass through during the forwarding process in addition to the source and destination

## 3.2 Symbols

Void.

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GR ENI 004 [i.1], ETSI GS ENI 005 [i.2] and ETSI GR ENI 010 [i.3] apply.

---

# 4 Overview of Network Policy Conflict Detection

## 4.1 Introduction

This clause provides an informative introduction to Network Policy Conflict Detection in the ENI System Architecture. Clause 4.2 describes the background and motivation of Network Policy Conflict Detection, and then provides a high-level description of Network Policy Conflict Detection in the ENI System, including which ENI Functional Block it is deployed in and what kind of policy it can and cannot validate. Clause 4.3 describes the external requirements for Network Policy Conflict Detection, including the requirements for the network policy, the maximum input frequency of Network Policy Conflict Detection, and the architecture of the Assisted System. Clause 4.4 describes the functional architecture of Network Policy Conflict Detection in terms of Conflict Detection Functional Modules.

## 4.2 Description of Network Policy Conflict Detection

In an increasingly interconnected world, network traffic is increasingly diverse and demanding, whether it is communication between small everyday devices on LANs or communication between large global data centres on the Internet. This diversity in network traffic has driven the design and widespread adoption of a new open network architecture called Software-Defined Networking (SDN). SDN is built upon programmable network switches, which enable the separation of the network control plane from the data plane. This separation allows the control plane to customize the data plane with User-Defined Policies that users want the network forwarding behaviour to meet.