detnet Working Group
Internet-Draft
Intended status: Standards Track
Expires: 1 September 2026

L. Zhang
H. Huang
T. Zhou
Huawei
W. Gao
CAICT

28 February 2026

Echo Request/Reply for DetNet Capability Discovery
draft-tan-detnet-cap-discovery-04

Abstract

This document describes an extension to the echo request/reply mechanisms used in IP, MPLS or other DetNet data plane environments, which can be used within the DetNet domain, allowing the ping initiator node to discover the enabled DetNet capabilities of each relay node of detnet service-sub layer, which including discovering DetNet relay nodes, collecting DetNet service sub-layer specific information from DetNet relay nodes, as well as discovering the locations of PREOF functions.

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 1 September 2026.

Copyright Notice

Table of Contents

1. Introduction 2
1.1. Requirements Language 3
1.2. Terminology 3
2. DetNet Capability Discovery 4
2.1. DetNet Capability Discovery Operation 4
2.2. DetNet Capability Discovery Header 4
2.3. DetNet Capabilities Discovery Objects 4
2.3.1. DetNet Capability Object 5
2.3.2. DetNet Relay Node Identifier Object 5
2.3.3. DetNet service protection function objects 6
2.3.4. DetNet Service Flow Information Objects 8
2.4. DetNet Data Plane Considerations 12
2.4.1. MPLS Data Plane 12
2.4.2. IP Data Plane 13
3. IANA Considerations 13
4. Security Considerations 13
5. References 13
5.1. Normative References 13
5.2. Informative References 14
Acknowledgements 14
Authors' Addresses 14

1. Introduction

[RFC8655] provides the overall architecture for Deterministic Networking (DetNet), which provides a capability to carry specified unicast or multicast data flows for real-time applications with extremely low data loss rates and bounded latency within a network domain. Currently DetNet operates on IP and MPLS data plane.

DetNet functionality is divided into two sub-layers. The DetNet service sub-layer provides DetNet service protection with functionalities and operation of PREOF, a collective name for Packet Replication, Elimination, and Ordering Functions. The DetNet forwarding sub-layer provides resource allocation for DetNet flows over paths provided by the underlying network.

[I-D.ietf-detnet-oam-framework] details the specific requirements of the Operation, Administration, and Maintenance (OAM) recommended to maintain a deterministic network. OAM for the DetNet MPLS data plane is described in [I-D.ietf-detnet-mpls-oam] and OAM for the DetNet IP data plane is described in [I-D.ietf-detnet-ip-oam].

[I-D.ietf-detnet-oam-framework] described the DetNet service sub-layer oam requirements of discovering DetNet relay nodes , collecting DetNet service sub-layer specific (e.g., configuration/operation/ status) information from DetNet relay nodes, as well as discovering the locations of PREOF functions.

These requirements, could be satisfied using alternative technologies like NETCONF/YANG, IGP flooding or ping/traceroute. [I-D.varga-detnet-service-sub-layer-oam] introduced a ping/traceroute method, "DetNet Ping", and mentions that it could be used for discovering DetNet capabilities of DetNet relay nodes.

This document introduced extensions to DetNet Ping (echo request/ reply) used in IP, MPLS or other DetNet data plane environments, which can be used within the DetNet domain, allowing the ping initiator node to discover the enabled DetNet capabilities of each relay node of detnet service-sub layer.

1.1. 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.

1.2. Terminology

The abbreviations used in this document are:

DetNet: Deterministic Networking

OAM: Operation, Administration, and Maintenance

PRF: Packet Replication Function

PEF: Packet Elimination Function

POF: Packet Ordering Function

PREOF: Packet Replication, Elimination and Ordering Function

2. DetNet Capability Discovery

2.1. DetNet Capability Discovery Operation

Once the DetNet PING initiator node is triggered to discover the enabled DetNet capabilities of each DetNet relay node, the initiator node will send DetNet echo requests that include the DetNet Capabilities Discovery Header.
First, with TTL equal to 1 to reach the closest node, which may be an DetNet relay node or not. Then with TTL equal to 2 to reach the second nearest node, which also may be an DetNet relay node or not. And further, increasing by 1 the TTL every time the initiator node sends a new echo request. As a result, the echo requests sent by the initiator node will reach all nodes one by one along the transport path of DetNet service flow.
Alternatively, if the initiator node knows precisely all the DetNet relay nodes beforehand, once the initiator node is triggered to discover the enabled DetNet capabilities, it can send an echo request to each DetNet relay node directly, without TTL expiration.

2.2. DetNet Capability Discovery Header

For echo DetNet request/reply message used for DetNet capability discovery, DetNet capabilities information are delivered by several kinds of DetNet Capabilities Discovery Objects. This document introduces an abstract header which has the corresponding format depending on the type of DetNet data plane. The format of DetNet Capabilities Discovery Object is shown as below.

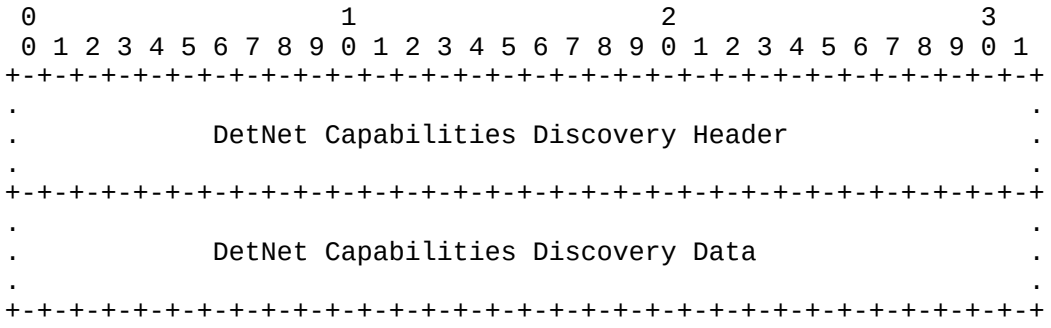

Figure 1: The Format of Mandatory Section of A BFD Control Packet

DetNet Capabilities Discovery Header: abstract header of DetNet Capabilities Discovery Object, with varied length and format depending on the type of DetNet data plane.
DetNet Capabilities Discovery Data: detailed information of DetNet Capabilities Discovery Object, with fixed length and format depending on the type of Detnet capability.

2.3. DetNet Capabilities Discovery Objects

2.3.1. DetNet Capability Object

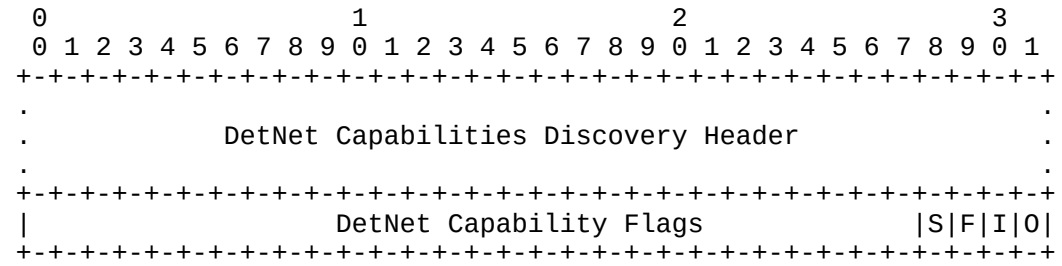

Figure 2: DetNet Capability Object Format

Flags (4 bytes): DetNet Capability Flags
* S: Service sub-layer capability
* F: Forwarding sub-layer capability
* I: Incoming flow configuration
* O: Outgoing flow configuration

2.3.2. DetNet Relay Node Identifier Object

2.3.2.1. DetNet Node Identifier Object (MPLS)

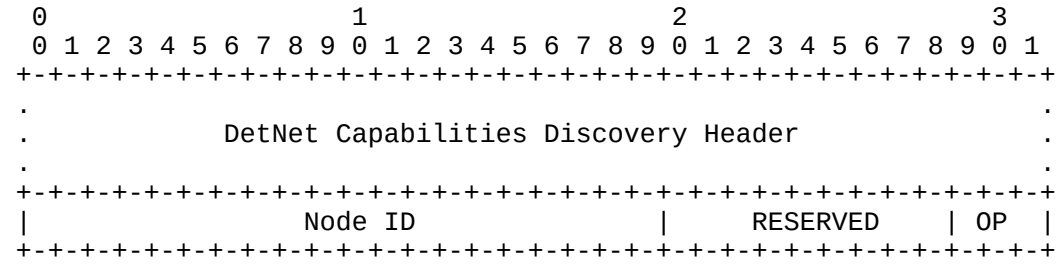

Figure 3: DetNet Node Identifier Object (MPLS) Format

Node ID (20 bits): The value of the Node ID field identifies the DetNet node that originated the packet. It is same as defined in {{I-D.ietf-detnet-mpls-oam}}.
OP (3 bits): Service operation on the node.
0x00: No operation for DetNet service sub-layer
0x01: Initiation for DetNet service sub-layer encapsulation
0x02: Termination for DetNet service sub-layer encapsulation
0x03: Relay(Swap) operation for DetNet service sub-layer

2.3.2.2. DetNet Node Identifier Object (IPv4)

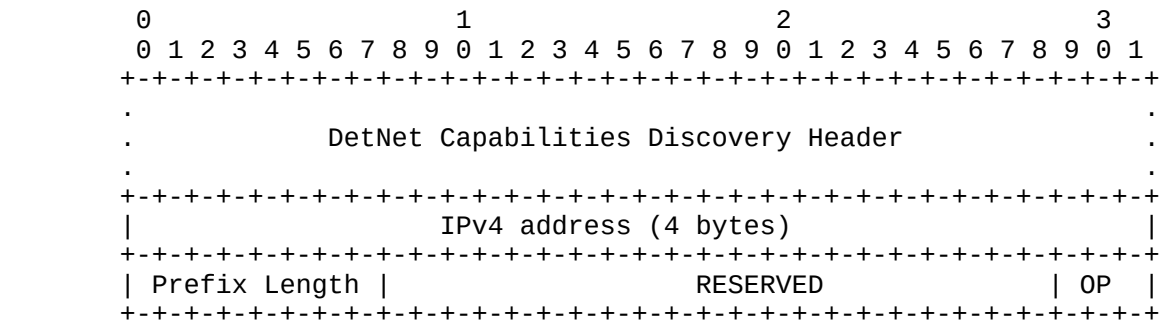

Figure 4: DetNet Node Identifier Object (IPv4) Format

IPv4 address(4 bytes): An IPv4 address. This address is treated as a prefix based on th
e prefix length value.
Prefix length(1 bytes): Length in bits of the IPv4 prefix.
OP (3 bits): Service operation on the node.
0x00: No operation for DetNet service sub-layer
0x01: Initiation for DetNet service sub-layer encapsulation
0x02: Termination for DetNet service sub-layer encapsulation
0x03: Relay(Swap) operation for DetNet service sub-layer

2.3.2.3. DetNet Node Identifier Object (IPv6)

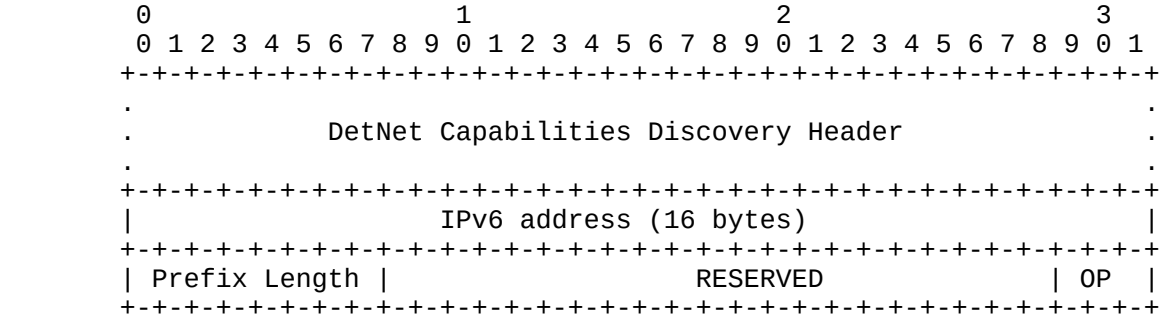

Figure 5: DetNet Node Identifier Object (IPv6) Format

IPv6 address: An IPv6 address. This address is treated as a prefix based on the prefix
length value.
Prefix length: Length in bits of the IPv6 prefix.
OP (3 bits): Service operation on the node.
0x00: No operation for DetNet service sub-layer
0x01: Initiation for DetNet service sub-layer encapsulation
0x02: Termination for DetNet service sub-layer encapsulation
0x03: Relay(Swap) operation for DetNet service sub-layer

2.3.3. DetNet service protection function objects

2.3.3.1. Service Protection Object

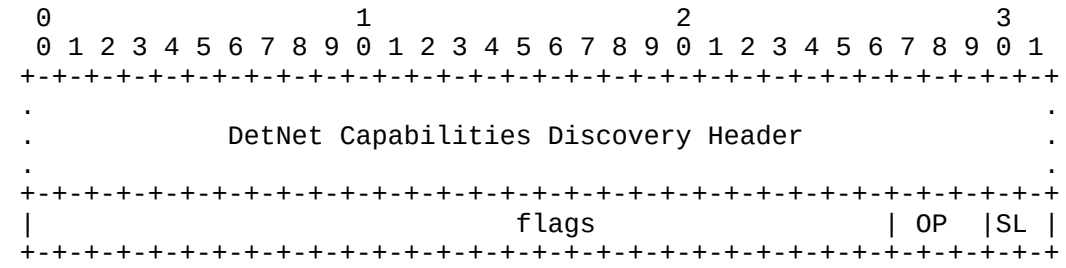

Figure 6: Service Protection Object Format

flags (4 bytes): service protection flags.
* SL (2 bits): Sequence number length.
0b00: no sequence number
0b01: sequence number length of 16 bits
0b10: sequence number length of 28 bits

2.3.3.2. Replication Capability Object

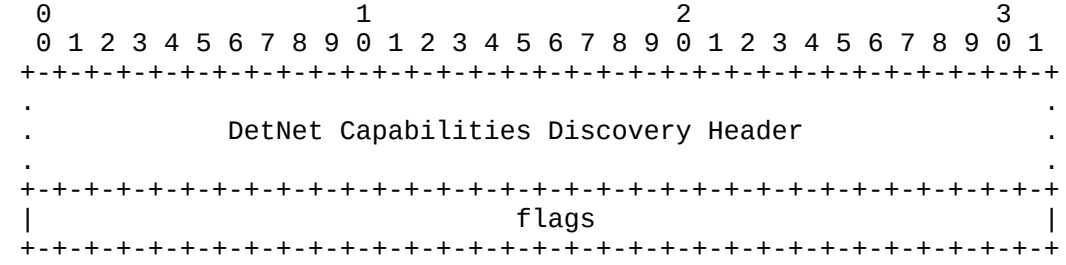

Figure 7: Replication Capability Object Format

Flags (4 bytes): unused.

2.3.3.3. Elimination Capability Object

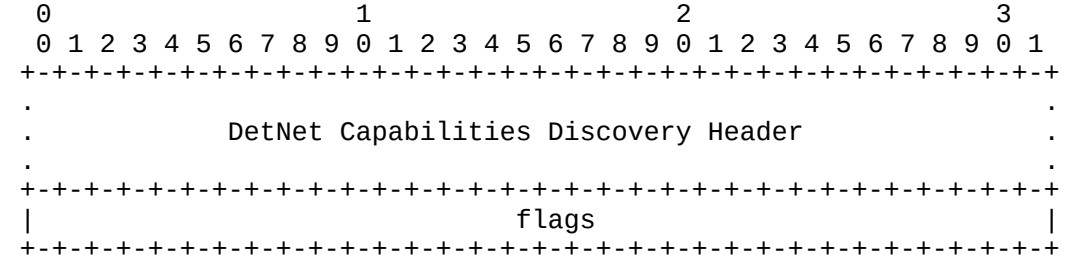

Figure 8: Elimination Capability Object Format

Flags (4 bytes): unused.

2.3.3.4. Ordering Capability Object

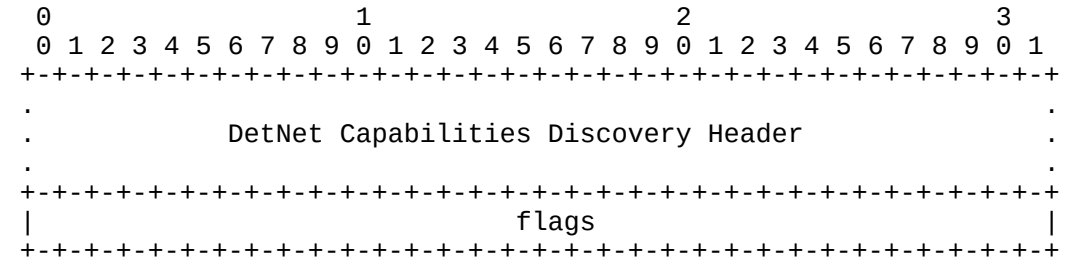

Figure 9: Ordering Capability Object Format

Flags (4 bytes): unused.

2.3.4. DetNet Service Flow Information Objects

2.3.4.1. DetNet Service Flow Identifier Object (MPLS)

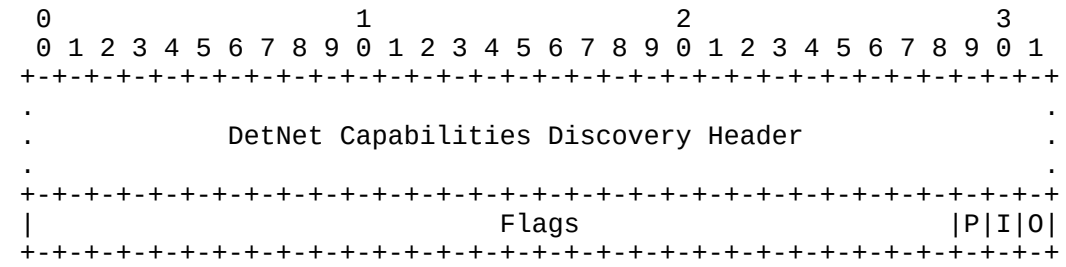

Figure 10: DetNet Service Flow Identifier Object Format

Flags (4 bytes):
* I: Incoming flow
* O: Outgoing flow
* P: platform-label-space

2.3.4.2. Service Label Object

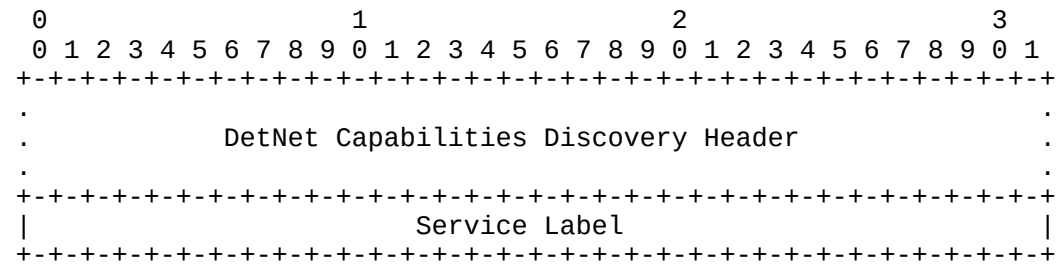

Figure 11: Service Label Object Format

Service Label (4 bytes): S-Label, DetNet Service identifier with MPLS data plane.

2.3.4.3. DetNet Service Flow Identifier Object (IPv4)

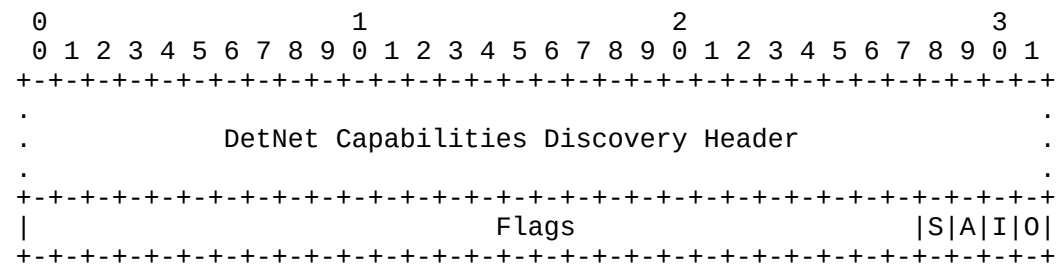

Figure 12: DetNet Service Flow Identifier Object (IPv4) Object Format

Flags (4 bytes):
 * I: Incoming flow
 * O: Outgoing flow
 * A: IPv4 flow identifier, including Source Address, Destination Address, Source Port, Destination Port, Protocol and Dscp
 * S: IPSec-spi

2.3.4.4. IPv4 Flow Identifier Object

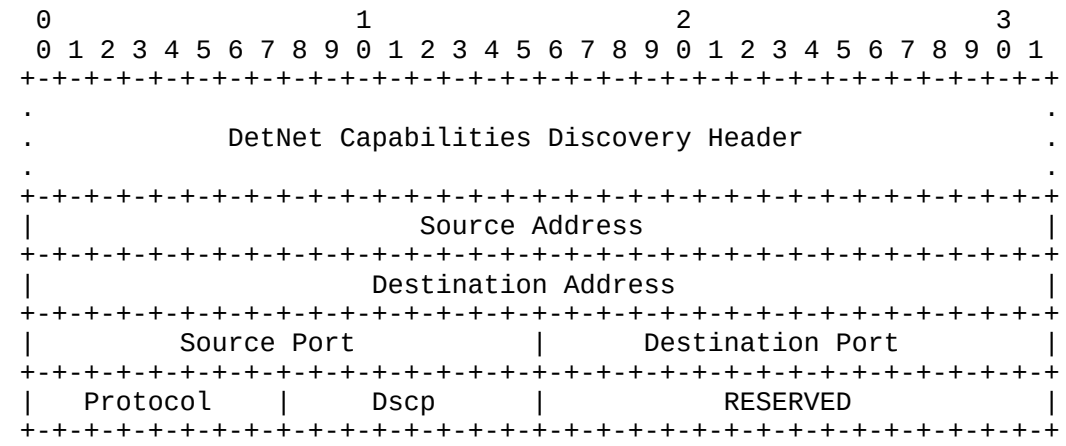

Figure 13: IPv4 Flow Identifier Object Format

Source Address (4 bytes): IPv4 source address of the packet.
Destination Address (4 bytes): IPv4 destination address of the packet.
Source Port (2 bytes): Source port of the packet.
Destination Port (2 bytes): Destination port of the packet.
Protocol (1 byte): Protocol of the packet.
Dscp (1 byte): Differentiated Services Code Point.

2.3.4.5. DetNet Service Flow Identifier Object (IPv6)

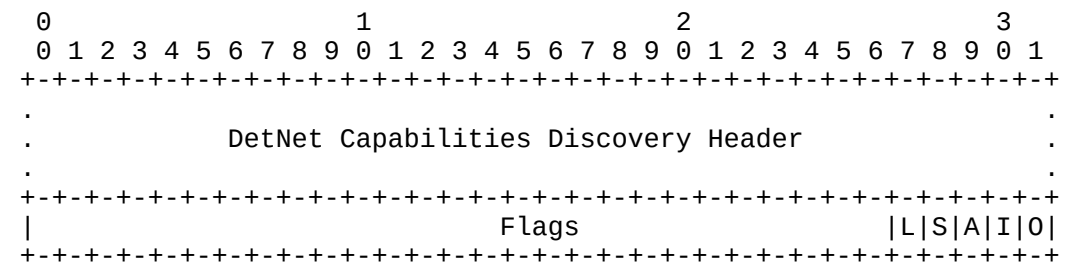

Figure 14: DetNet Service Flow Identifier Object (IPv6) Object Format

Flags (4 bytes):
 * I: Incoming flow
 * O: Outgoing flow
 * A: IPv6 flow identifier, including Source Address, Destination Address, Source Port, D
estination Port, Protocol and Dscp
 * S: IPSec-spi
 * L: IPv6 flow label

2.3.4.6. IPv6 Flow Identifier Object

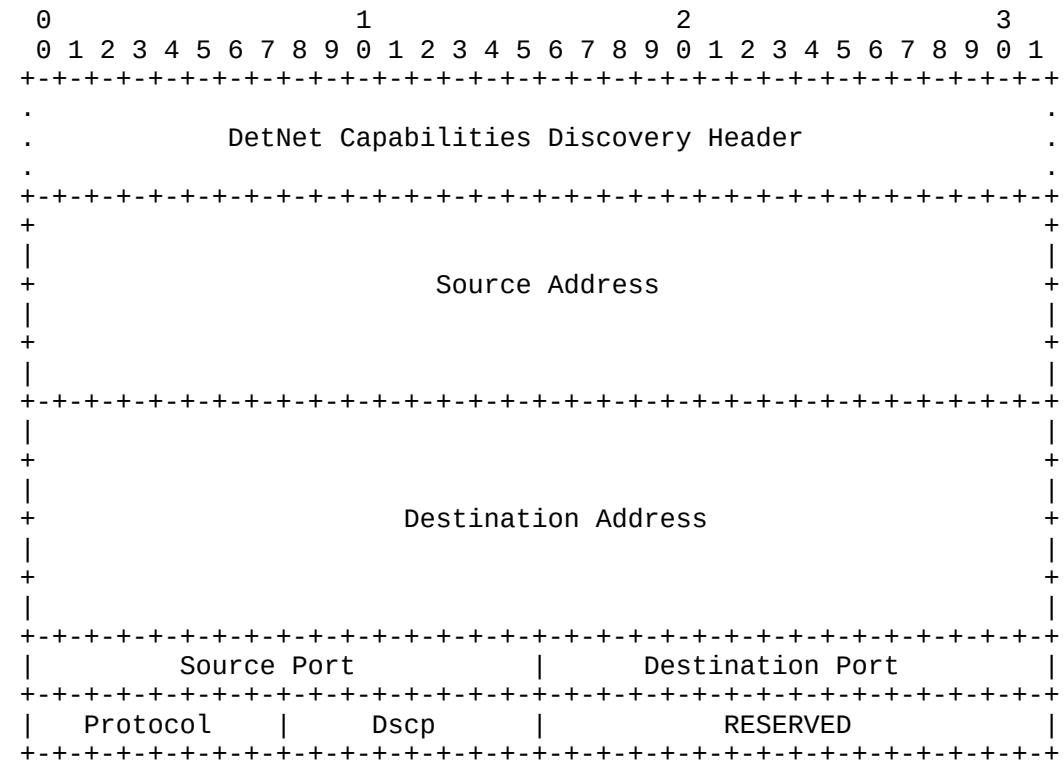

Figure 15: IPv6 Flow Identifier Object Format

Source Address (16 bytes): IPv6 source address of the packet.
Destination Address (16 bytes): IPv6 destination address of the packet.
Source Port (2 bytes): Source port of the packet.
Destination Port (2 bytes): Destination port of the packet.
Protocol (1 byte): Protocol of the packet.
Dscp (1 byte): Differentiated Services Code Point.

2.3.4.7. IPv6 Flow Label Object

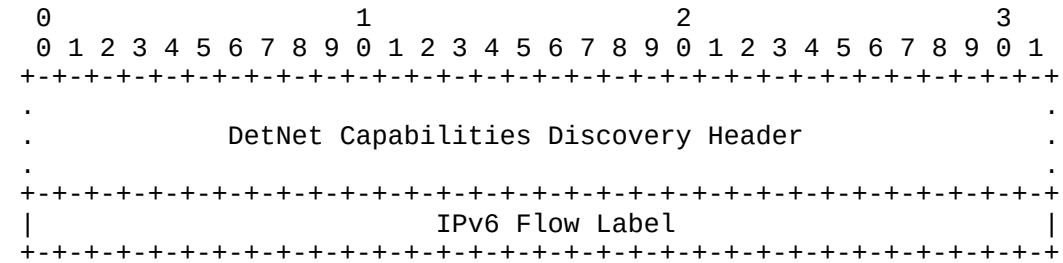

Figure 16: IPv6 Flow Label Object Format

IPv6 Flow Label (4 bytes): The flow label value of the header. IPv6 only.

2.3.4.8. IPSec-SPI Object

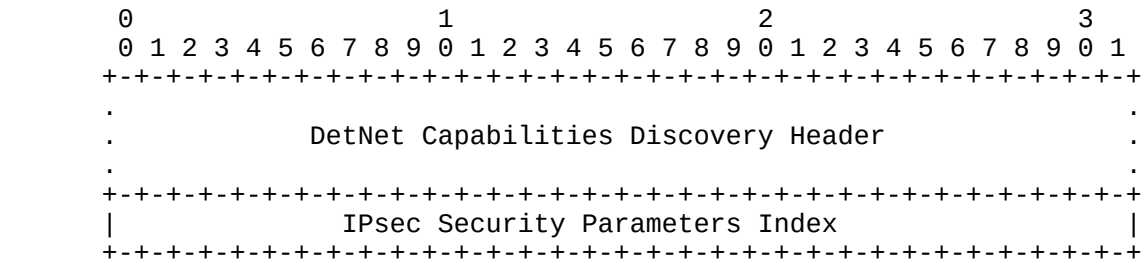

Figure 17: IPSec-SPI Object Format

IPSec-SPI (4 bytes): IPsec Security Parameters Index

2.4. DetNet Data Plane Considerations

2.4.1. MPLS Data Plane

DetNet echo request/reply messages in MPLS data plane, could encapsulate DetNet Capabilities Discovery Objects with typical TLV header format in place of the "DetNet Capabilities Discovery Header", as defined in {#detnet-cap-disc-obj}. The values of tlv types had not been defined yet.

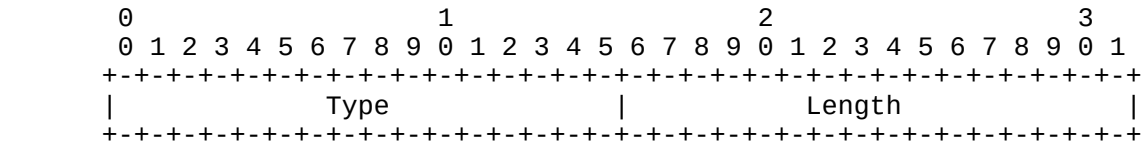

Figure 18: MPLS TLV Header Format

Type (2 bytes): Tlv type
Length (2 bytes): Tlv Length

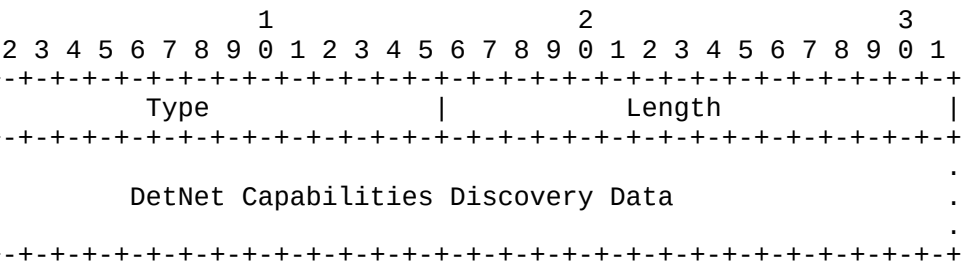

Figure 19: DetNet Capabilities Discovery Object (MPLS) Format

2.4.2. IP Data Plane

TBD.

3. IANA Considerations

NA.

4. Security Considerations

The security considerations described in [RFC8655] apply to the extensions defined in this document as well. This document does not raise new security issues.

5. References

5.1. Normative References

[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/rfc/rfc8655>.

[I-D.ietf-detnet-oam-framework] Mirsky, G., Theoleyre, F., Papadopoulos, G. Z., Bernardos, C. J., Varga, B., and J. Farkas, "Framework of Operations, Administration and Maintenance (OAM) for Deterministic Networking (DetNet)", Work in Progress, Internet-Draft, draft-ietf-detnet-oam-framework-11, 8 January 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-detnet-oam-framework-11>.

[I-D.ietf-detnet-mpls-oam] Mirsky, G., Chen, M., and B. Varga, "Operations, Administration and Maintenance (OAM) for Deterministic Networks (DetNet) with MPLS Data Plane", Work in Progress,

Internet-Draft, draft-ietf-detnet-mpls-oam-15, 12 January 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-detnet-mpls-oam-15>.

[I-D.ietf-detnet-ip-oam]
Mirsky, G., Chen, M., and D. L. Black, "Operations, Administration, and Maintenance (OAM) for Deterministic Networks (DetNet) with IP Data Plane", Work in Progress, Internet-Draft, draft-ietf-detnet-ip-oam-13, 14 February 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-detnet-ip-oam-13>.

[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/rfc/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/rfc/rfc8174>.

5.2. Informative References

[I-D.varga-detnet-service-sub-layer-oam]
Varga, B., Farkas, J., and G. Mirsky, "Deterministic Networking (DetNet): OAM Functions for The Service Sub-Layer", Work in Progress, Internet-Draft, draft-varga-detnet-service-sub-layer-oam-03, 25 July 2022, <https://datatracker.ietf.org/doc/html/draft-varga-detnet-service-sub-layer-oam-03>.

Acknowledgements

Authors' Addresses

Li Zhang
Huawei
China
Email: zhangli344@huawei.com

Hongyi Huang
Huawei
China
Email: hongyi.huang@huawei.com

Tianran Zhou
Huawei
China
Email: zhoutianran@huawei.com

Wei Gao
CAICT
Email: gaowei@caict.ac.cn