

Workgroup: Network Working Group  
Internet-Draft:  
draft-du-programmable-ip-in-iot-network-00  
Published: 23 October 2022  
Intended Status: Informational  
Expires: 26 April 2023  
Authors: Z. Du  
China Mobile

## **Programmable IP Format in IOT Network**

### **Abstract**

This document describes a programmable IP format communication mechanism for the IOT network .

### **Requirements Language**

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119](#) [[RFC2119](#)].

### **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 26 April 2023.

### **Copyright Notice**

Copyright (c) 2022 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](#)
- [2. Proposed Mechanism Description](#)
- [3. IANA Considerations](#)
- [4. Security Considerations](#)
- [5. Acknowledgements](#)
- [6. References](#)
  - [6.1. Normative References](#)
  - [6.2. Informative References](#)
- [Author's Address](#)

## 1. Introduction

There will be more and more IOT devices deployed in the future. IOT networks are deployed widely in the residential scenarios and in the smart city scenarios. However, the IOT devices belonging to different vendors are hard to communicate.

Normally, they need to connect to the servers in the cloud, and then perhaps they can make some cooperation. It is to say that they can not communicate freely in the local network. We suggest that what we need here is a new layer 3 narrow waist for different IOT networks.

IOT devices have many different requirements, so that we need a programmable IP format for a specific IOT network. For example, some IOT networks may need an IP format that has simplified format; meanwhile, some IOT networks may need an IP format that contains more security considerations.

In this document, we introduce a mechanism to signal the selected format for an IOT network. Our final goal is to support a programmable IP format for various IOT networks.

## 2. Proposed Mechanism Description

In the current Internet, we have designed a uniform IP format [[RFC4291](#)]. It can benefit the communication among all the devices in the Internet. However, the IOT networks are quite different from the traditional IP network, and we need a programmable layer 3 for them to enable a better local communication.

As we have not assumed a unified format in the layer 3, we need to determinate the encapsulation format of the layer 3. For example, we can make a bitmap to communicate between the gateway of the IOT network and a new IOT device that needs to communicate with the IOT

network. In other words, they can negotiate the format of the layer 3.

We suggest using some communications in the layer 2 to determine the encapsulation format of the layer 3. The new IOT device may send a L2 frame to the gateway of the IOT network. The gateway may response another L2 frame that contains the information about the format in this IOT network.

By using the information in the frame from the gateway, the new IOT device can connect to the IOT network and communicate with the IOT devices in the IOT network.

The encapsulation information can be an index of some pre-configured format, or it can be a bitmap that describes the encapsulation format in the IOT network. In the later case, the bitmap may indicate whether a specific item is encoded in the format, for example, the SA, the TTL, or the next header. Each bit in the bitmap should be pre-configured and can be understood without ambiguity. Following the bitmap, some offsets should be given, so that we can determine the length of each item that is contained in the format. Hence, we can make a flexible platform for the encapsulation of the layer 3 in the IOT network, while the different format requirements of the IOT networks can be fulfilled.

### **3. IANA Considerations**

TBD.

### **4. Security Considerations**

TBD.

### **5. Acknowledgements**

TBD.

### **6. References**

#### **6.1. 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>>.

#### **6.2. Informative References**

[RFC4291]

Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <<https://www.rfc-editor.org/info/rfc4291>>.

**Author's Address**

Zongpeng Du  
China Mobile  
No.32 XuanWuMen West Street  
Beijing  
100053  
China

Email: [duzongpeng@foxmail.com](mailto:duzongpeng@foxmail.com)