

Internet Area Working Group
Internet-Draft
Intended status: Experimental
Expires: October 16, 2022

Z. Chen
Huawei
S. Jiang
April 14, 2022

Native Minimal Protocols with Flexibility at Edge Networks
draft-jiang-intarea-nmp-edge-01

Abstract

This document introduces a flexible native minimal protocol for fast short packet transmission in edge networks, and can communicate with IPv6 nodes through gateways.

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 October 16, 2022.

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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Internet-Draft

NMP

April 2022

Table of Contents

1.	Introduction	2
2.	Requirements Notation	3
3.	Overview	3
4.	Protocol Design	4
4.1.	Packet Header Format	4
4.1.1.	Data Packet Header Format	5
4.1.2.	Control Packet Format	6
4.2.	Control Messages	6
4.2.1.	Address Request and Assignment Messages	6
4.2.2.	Address Lease Extension Messages	7
4.3.	DNS Delegation Messages	8
4.4.	Functionalities of Gateway	9
4.4.1.	Address Management	9
4.4.2.	Address Translation	10
5.	Renumber Considerations	10
6.	Security Considerations	10
7.	IANA Considerations	10
8.	Acknowledgments	10
9.	Normative References	10
	Authors' Addresses	11

[1.](#) Introduction

TCP/IP protocol suites are adopted widely in different areas. However, there are still numerous edge networks uses non-IP technologies like ZigBee, BLE, CAN-bus, and Modbus for different reasons (e.g., power-constrained devices, low transport rate media). For such networks, application-layer gateways (or protocol translators) are usually deployed to connect them with the Internet, as shown in Figure 1.

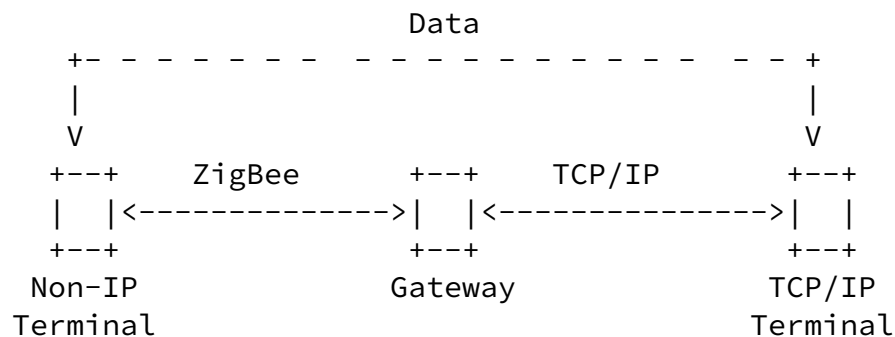


Figure 1: Communication Architecture with Application Gateway

The application-layer translation mechanism MAY bring three main drawbacks: 1. End-to-end security channel like IPsec or TLS is not

supported, a malicious gateway may manipulate data that is transmitted between two terminals. 2. Non-IP terminals are invisible to the TCP/IP network, which makes it hard to conduct QoS or OAM operations, e.g., guaranteeing SLA of a specific non-IP terminal's traffic, or "ping" a non-IP terminal. 3. When a non-IP terminal joins or one leaves the network, corresponding rules SHOULD be configured on the gateway, thus increasing operation costs (i.e., OPEX).

Therefore, it would be beneficial to make those non-IP terminals adopt TCP/IP protocol suites, thus eliminating aforementioned drawbacks. The Internet Protocol Version 6 (IPv6) is expected to achieve the goal, however, it is challenging in some cases due to its long address and header length (40 bytes in total). For instance, it would consume more energy for power constrained terminals like IoT devices, and would amplify flow completion time on low-rate transport media or one with low MTU, thus decreasing user experiences.

To this end, this document proposes Native Minimal Protocol (NMP), which is applied at edge networks by using minimal address length and fields. Simultaneously, NMP eliminates the drawbacks that may be brought by application layer gateways.

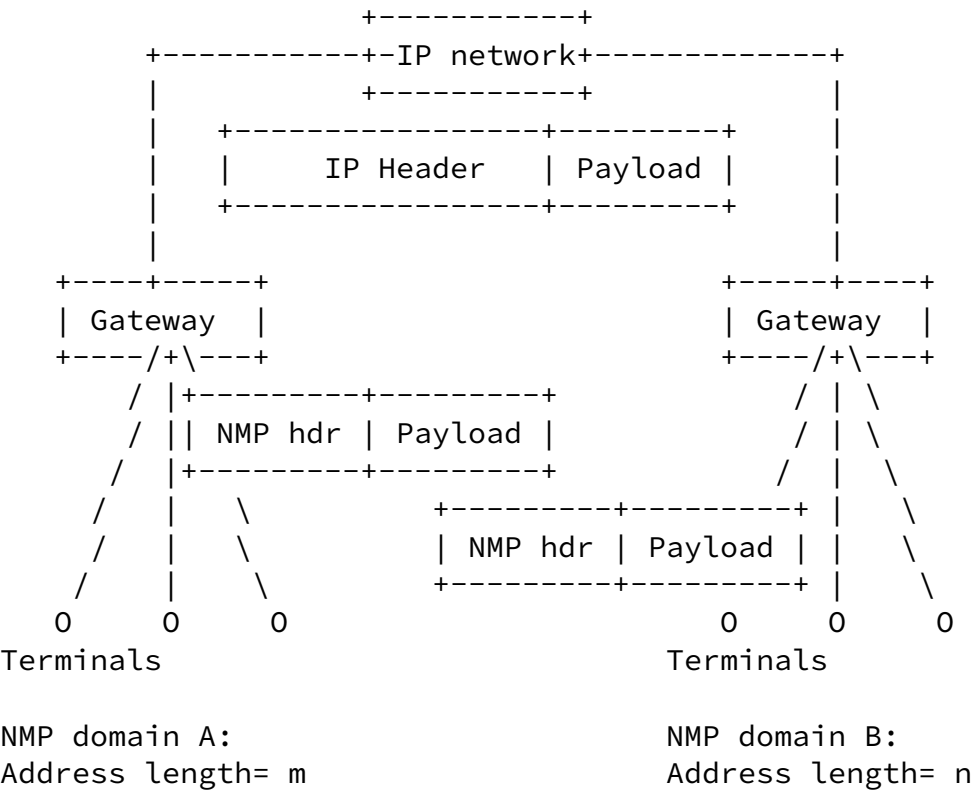
[2.](#) Requirements Notation

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 \[RFC2119\]](#) and [\[RFC8174\]](#) when, and only when, they appear in all capitals, as shown here.

[3.](#) Overview

NMP is an inter-node communication method and network layer protocol for edge network with native addresses. It is designed for extreme minimal IoT devices that communicate with each other and sometimes with normal IP nodes. NMP nodes and NMP gateways use native short

addresses to identify themselves and use these addresses as source and destination addresses for network communication. NMP data packets and signaling packets are encapsulated in a simplified manner. The NMP-IPv6 translation function is deployed on the gateway to implement IP connections on the edge network. See Figure 2.



Only Support Extreme Simplified Control Messages within NMP Domain

Figure 2: Overview of Native Minimal Protocol

4. Protocol Design

[4.1.](#) Packet Header Format

The first bit at the beginning of the packet header indicates whether the packet is encapsulated with extreme concise format or not. If the first bit is 0, packet format is specified as follows Figure 3.

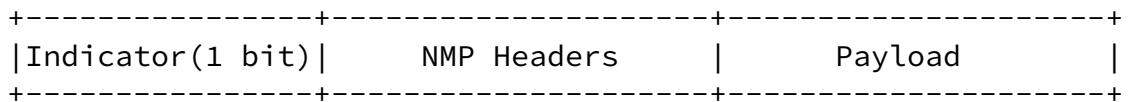


Figure 3: Basic Format of Native Minimal Protocol Packet

- o Indicator one-bit indicator to indicate whether extreme concise format is used. 0 - NMP headers follows; 1 - undefined.
- o NMP Headers Record the fields of packet header in [Section 4.1.1](#) .

- o Payload The payload of the packet. For control plane packets, the control plane messages defined in [Section 4.1.2](#) are carried in this part.

[4.1.1.](#) Data Packet Header Format

For data packet header, NMP uses bitmap with variable length to indicate which in-line headers appear in the packet. The specification is in Figure 4.

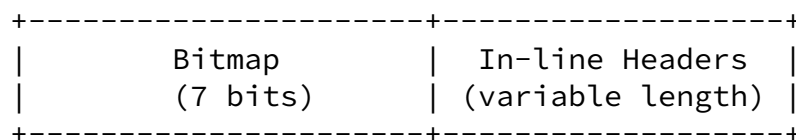


Figure 4: NMP Header Format

- o Bitmap A variable-length bitmap with at least 7 bits is used to indicate whether a NMP field is carried in a packet. The bit of 1 indicates that the packet carries this field and is located in the

following in-line headers field. The value 0 indicates that the packet does not contain this field. The length of bitmap is defined as follows.

bitmap format	number of bits for indicator	scope fo headers
xxx xxx0	6 bits	header 1 ~ 6

- o In-line Headers The headers in NMP packet. Each header corresponds to a position in preceding bitmap.

Bitpos	Header Name	Header Length
1	TTL	8 bit
2	Total Length	16 bit
3	Next Header	8 bit
4	Reserved	N/A
5	Destination	Variable Length
6	Source	Variable Length

7	Next Bitmap Byte	N/A
---	------------------	-----

4.1.2. Control Packet Format

Message Type (8 bits)	Checksum (8 bits)
--------------------------	----------------------

Figure 5: Control Packet Header Format

- o Type This field carries value to indicate the type of this control message.
- o Checksum The checksum is the 8-bit one's complement of the one's complement sum of the entire control message, starting with the message type field, and prepended with a "1" of indicator header fields, as specified in [Section 4.1](#). For computing the checksum, the checksum field is first set to zero.

4.2. Control Messages

4.2.1. Address Request and Assignment Messages

A NMP host broadcasts an Address Request (AR) message to request an address from the gateway of the NMP domain. The gateway sends an Address Assignment (AA) message to the host to configure the host's NMP address. #### Format of Address Request The value of the message Type is 1. The message body is defined as follows.

ID length (8 bits)	Host ID
--------------------	---------

- o ID length Length of this field is 1 octet. This header specifies the length of the Host ID field, in octets.

- o Host ID Indicates the identifier of the host that accesses the NMP network. The identifier can be a MAC address or another globally unique identifier.

[4.2.1.1.](#) Format of Address Assignment

The value of the message Type is 2. The message body is defined as follows.

-----+	-----+	-----+	-----+	-----+
NMP Address Length	NMP	Gateway	ID length	Host ID
8 bits	Address	Address	(8 bits)	
-----+	-----+	-----+	-----+	-----+

- o NMP Address Length Length of this field is 1 octet. This parameter specifies the length of the NMP address used in the local NMP domain.
- o NMP Address Network layer address assigned to the host node. The length is specified by the NMP Address Length field.
- o Gateway Address Network layer address of the gateway. The length is the same as length of NMP Address
- o ID length Length of this field is 1 octet. This header specifies the length of the Host ID field, in octets.
- o Host ID Indicates the identifier of the host that accesses the NMP network. The identifier can be a MAC address or another globally unique identifier.

[4.2.2.](#) Address Lease Extension Messages

To reduce the complexity of the NMP host, the gateway records the lease information of each NMP address. When the lease of a host address expires, the gateway sends a Renewal Challenge message to the host and waits for an response from the host. If a Renewal Response message is received from the host, the lease information is updated

based on the preconfigured strategy. Otherwise, the gateway releases

the NMP address.

[4.2.2.1.](#) Renewal Challenge Message

The value of the message Type is 3. The message body is defined as follows.

-----+-----+-----+-----+
NMP Address Length NMP ID length Host ID
8 bits Address (8 bits)
-----+-----+-----+-----+

- o NMP Address Length Length of this field is 1 octet. This parameter specifies the length of the NMP address used in the local NMP domain.
- o NMP Address Network layer address assigned to the host node. The length is specified by the NMP Address Length field.
- o ID length Length of this field is 1 octet. This header specifies the length of the Host ID field, in octets.
- o Host ID Indicates the identifier of the host that accesses the NMP network. The identifier can be a MAC address or another globally unique identifier.

[4.2.2.2.](#) Renewal Response Message

The value of the message Type is 4. The message body is defined in [Section 4.2.2.1.](#)

[4.3.](#) DNS Delegation Messages

Many IoT products are written into the domain name of the IoT service platform when they are manufactured. The IP address of the server needs to be obtained through the DNS to establish communication.

Within the NMP domain, some modifications are required to traditional DNS messages in [[RFC1035](#)]. The NMP host sends a DNS query packet to the gateway. It Must set next header indicator to 1, the value of in-line next header is 17. Destination port in UDP header is 53. Destination of the packet is set to NMP address of gateway. When the gateway receives the packet, it directly translates the network layer information and sends a regular DNS packet to the DNS server configured on the gateway.

NMP is replaced by IPv6 protocol after the gateway. The source address is changed to 'IPv6 address prefix stored in the gateway + padding bit + NMP address', the destination address is changed to the DNS server address configured on the gateway, and the payload information remains unchanged.

When the DNS response packet sent by the DNS server reaches the gateway, the gateway resolves the response packet and allocates an available NMP address to the destination IPv6 address. The NMP address is used as an in-network mirror of the IPv6 address and replaces the target address in the DNS response packet. Then, the gateway sends the DNS response packet to the NMP host.

The header format of an DNS delegation message is defined as follows. For details about the format of a DNS message body, see [[RFC1035](#)].

```

+-----+-----+-----+-----+-----+-----+
| 0 | 0110110 | Total Length | Nxt Hdr | GW Addr | NMP src |
+-----+-----+-----+-----+-----+-----+
| UDP header(port=53) |
+-----+-----+
|
| DNS message body defined in RFC 1035
|
+-----+-----+

```

[4.4.](#) Functionalities of Gateway

[4.4.1.](#) Address Management

The NMP gateway initializes the NMP address pool based on the network configuration and assigns an address to itself. This address is used as the default gateway by the hosts in the domain.

Intra-domain address management functionaliteis includes: * intra-domain host address allocation The gateway listens to the NMP address request message, allocates the corresponding NMP address based on the message content, generates an address assignment message, and returns the message to the host. The assigned addresses must meet the uniqueness requirements within the NMP domain. * intra-domain host address life cycle management The gateway manages the validity period of NMP addresses. The lease renewal challenge mechanism is used to renew or release host addresses.

Internet-Draft

NMP

April 2022

[4.4.2.](#) Address Translation

The NMP address space can be mapped to specific subspaces of IPv6 address space. When traffic is destined to a destination outside the domain, the gateway translates the host address (source address) in the domain into an IPv6 address. For details about the translation method, see TBD.

For traffic from outside of the domain, determines whether the destination is within the domain. If the destination is within the domain, then the gateway translates the destination address to the corresponding NMP address.

[5.](#) Renumber Considerations

The NMP renumbering problem is not beyond the scope of [[RFC6866](#)] and [[RFC7010](#)], [[RFC5887](#)].

[6.](#) Security Considerations

Checksum is used to defend against malformed packets and null packet attacks caused by network bit errors. ICMPv6 uses a 16-bit checksum. NMP uses an 8-bit checksum to reduce the computing load on the host side and improve the packet encapsulation efficiency. This leads to a higher probability of network errors.

[7.](#) IANA Considerations

If NMP is running on Ethernet, a new Ethtype is required. In addition to Ethernet, other link-layer protocols that need to carry multiple upper-layer protocols need to assign specific identifiers to NMP to instruct devices to process network-layer packets according to this document.

This document requires to define new registry for NMP control message types, six of which are defined in this document.

[8.](#) Acknowledgments

The authors would like to acknowledge the contributions Guangpeng Li and Zhaochen Shi provided during the development of the solution.

9. Normative References

- [RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, [RFC 1035](#), DOI 10.17487/RFC1035, November 1987, <<https://www.rfc-editor.org/info/rfc1035>>.

Jiang & Chen

Expires October 16, 2022

[Page 10]

Internet-Draft

NMP

April 2022

- [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>>.
- [RFC5887] Carpenter, B., Atkinson, R., and H. Flinck, "Renumbering Still Needs Work", [RFC 5887](#), DOI 10.17487/RFC5887, May 2010, <<https://www.rfc-editor.org/info/rfc5887>>.
- [RFC6866] Carpenter, B. and S. Jiang, "Problem Statement for Renumbering IPv6 Hosts with Static Addresses in Enterprise Networks", [RFC 6866](#), DOI 10.17487/RFC6866, February 2013, <<https://www.rfc-editor.org/info/rfc6866>>.
- [RFC7010] Liu, B., Jiang, S., Carpenter, B., Venaas, S., and W. George, "IPv6 Site Renumbering Gap Analysis", [RFC 7010](#), DOI 10.17487/RFC7010, September 2013, <<https://www.rfc-editor.org/info/rfc7010>>.
- [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>>.

Authors' Addresses

Sheng Jiang
Huawei Technologies
Beiqing Road, Haidian District
Beijing 100095
P.R. China

Email: jiangsheng@huawei.com

Zhe Chen
Huawei Technologies
Beiqing Road, Haidian District
Beijing 100095
China

Email: chenzhe17@huawei.com