Network Working Group H. Yu
Internet-Draft China Internet Network Information Center
Intended status: Informational K. Zhang
Expires: 19 August 2026University of Electronic Science and Technology of China
15 February 2026

Carrying Traffic Shaping Mechanism in IPv6 Extension Header
draft-yu-traffic-shaping-01

Abstract

Starting from the traffic shaping mechanism, one of the core technologies of network deterministic assurance, we summarize the characteristics of different traffic scheduling and shaping methods and propose a solution design for IPv6 to carry these traffic scheduling and shaping methods, taking into account deterministic and security factors. At the same time, the network scope of practical applications is becoming larger and larger, and the demand for deterministic network services will no longer be restricted to LANs, but will require deterministic forwarding beyond LAN boundaries, extending the deterministic assurance capability previously provided in LANs to WANs through network layer technologies.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://z-Endeavor.github.io/Internet-Draft/draft-ietf-traffic-shaping.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ietf-traffic-shaping/.

Source for this draft and an issue tracker can be found at https://github.com/z-Endeavor/Internet-Draft.

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/.

Copyright Notice

Table of Contents

1. Introduction

Time Sensitive Network (TSN) is a network that guarantees the quality of service for delay-sensitive flows, achieving low latency, low jitter and zero packet loss. Time-sensitive streams can be divided into periodic time-sensitive streams (PTS), such as cyclic control instructions in the plant, synchronization information, and non-periodic/sporadic time-sensitive streams (STS), such as event alarm information.

For periodic time-sensitive flows, traffic synchronous scheduling shaping mechanisms are generally used, requiring precise nanosecond clock synchronization of network-wide devices. Current mechanisms studied include Time-Triggered Ethernet (TTE), Time-Aware Shaping (TAS), Cyclic Queuing and Forwarding (CQF) and Credit-Based Shaping (CBS).

Scheduling and shaping mechanisms are two quality of service assurance mechanisms in the switch. Scheduling refers to queue scheduling, which is generally implemented at the outgoing port of the switch and consists of three parts: entering the queue, selecting the sending queue according to the scheduling algorithm, and exiting the transmission; shaping refers to traffic shaping, which prevents congestion within the switch or at the next hop by limiting the forwarding rate of the port.

"IPv6 Hop-by-Hop Options Processing Procedures" [HbH-UPDT] further specifies the procedures for how IPv6 Hop-by-Hop options are processed to make their processing even more practical and increase their use in the Internet. In that context, it makes sense to consider Hop-by-Hop Options to transport the information that is relevant to carry traffic shaping mechanism.

Since the asynchronous scheduling and shaping mechanism cannot guarantee that the worst delay of the packet meets a certain threshold, it can only guarantee that the average delay of the packet is comparable to the synchronous method, and the delay jitter is relatively large, and the delay-sensitive stream is prone to packet loss in the case of network congestion, the current asynchronous mechanism is not mature, and in order to better elucidate the nature of the delay-sensitive network, this document of using the synchronous mechanism to transmit periodic time-sensitive stream (PTS) is mainly discussed.

For the traffic shaping mechanism, one of the core technologies of network deterministic assurance, we summarize the characteristics of different traffic scheduling and shaping methods and propose a solution design for IPv6 to carry these traffic scheduling and

shaping methods, taking into account deterministic and security factors. At the same time, the network scope of practical applications is becoming larger and larger, and the demand for deterministic network services will no longer be restricted to LANs, but will require deterministic forwarding beyond LAN boundaries, extending the deterministic assurance capability previously provided in LANs to WANs through network layer technologies.

This document gives a description of the design of the IPv6 carrying traffic shaping mechanism and specifies the technical requirements and security specifications of the IPv6 carrying traffic shaping mechanism. This document applies to deterministic data communication of IPv6 networks that have implemented traffic synchronous scheduling shaping mechanism.

2. Conventions and Definitions

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. Abbreviations in This Document

TSN Time Sensitive Network PTS Periodic Time-sensitive Streams TTE Time-Triggered Ethernet TAS Time-Aware Shaping CQF Cyclic Queuing and Forwarding CBS Credit-Based Shaping

4. Network Communication System

Based on the premise of deterministic requirements, this document only considers the design of synchronization schemes where the network uses synchronization mechanisms to transmit PTS, while requiring accurate nanosecond time synchronization of devices within the entire network communication scenario.

4.1. General Model of Network Transmission

An applicable time-sensitive traffic shaping network communication model is given in Figure 1 and illustrates the network elements in it.

4.2. Network Node Description

It is expected to be deployed in a variety of IPv6 devices and situations. Therefore, It is important to specify IPv6 node requirements will allow traffic shaping mechanisms to work well and interoperate over IPv6 in a large number of situations and deployments.

4.3. Network Communication Process

Figure 2 gives the communication flow of the network system.

* Collect the corresponding network topology information, traffic period, traffic size, end-to-end delay jitter requirement information and corresponding security requirements from various deterministic services, complete the centralized user configuration, and send it down to the network controller through the network user interface (UNI).

* The network controller receives the network deterministic and security requirements and calculates the route scheduling control information for the traffic according to the corresponding algorithm. If the calculation is successful, the gating list is automatically synthesized and sent down through the southbound interface, and then the packet start time is returned to the sender; if the calculation fails, the orchestrator is told that the sender flow is not available for scheduling.

* Centralized collaborative scheduling of switches to achieve traffic scheduling shaping and complete deterministic transmission by planning routes or dividing time slots, etc.

5. Definition of Carrying Traffic Shaping Mechanism

Carrying traffic shaping mechanism in IPv6 extension header is in the form of a field on the extended header that specifies the basic traffic scheduling shaping protocol interface options for resolving the semantics of the scheduling shaping mechanism in the packet, allowing the network determinism to be transmitted through the extended header as well as for the adaptation of the upper layer protocols and network functions for use. This field information can be examined and processed by each node of the packet transmission path.

The requirements for the use of scheduling shaping include the scheduling shaping technical solution options and the control information necessary of specific solution. The definition format consists of four fields, including options, flag bits, fill bit

length, and control information. The definition format is shown in Figure 1. The technical scheme here mainly specifies the synchronous scheduling and shaping mechanism option, and the asynchronous scheduling and shaping mechanism information is not transmitted through this design.

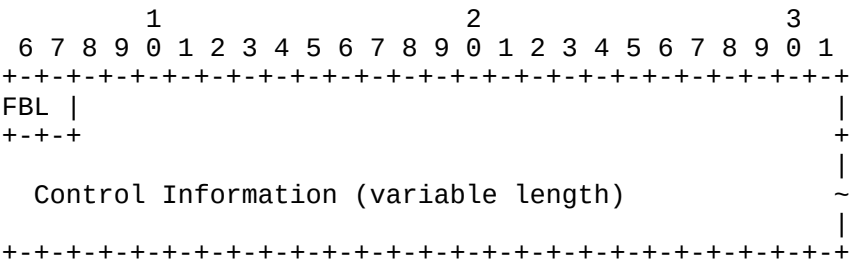

Figure 1: Definition of Carrying Traffic Shaping Mechanism

where

* Options: 4-bits. Indicating the synchronous traffic scheduling shaping technology scheme used.

* F: 1-bit. Used as a flag bit to record whether the protocol content has reached its maximum length.

* FBL: 3-bit. The number of bits used to record the padding at the end of the protocol is 0 to 7 bits to ensure that the total length of the definition content is an integer multiple of 8 bits.

* Control Information: Variable length. Used to carry the network control information necessary for the use of a specific scheduling and shaping mechanism, in a format and content determined by the specific scheduling and shaping mechanism.

The F identifiers is a flag bit. The value of this field specifies:

* 0 - the length of the protocol content has not exceeded the maximum value and the information has been read completely.

* 1 - the length of the protocol content exceeds the maximum value and needs to be read further.

FBL indicates Fill Bit Length which is for compatibility with subsequent adaptations in the IPv6 extension header. The actual length of the control information is obtained by parsing the length of the padding bits to facilitate the reading and processing of the network control device. The padding method is to set all the padding bits at the end to 0.

The Control Information contains standard control frame format of each specific scheduling shaping mechanism, which is used to ensure the integrity of the control information to complete the standard adaptation to various network devices.

6. Specification in Hop-by-Hop Options

6.1. Format in Hop-by-Hop Option

The definition of carrying traffic shaping mechanism shall conform to the relevant specifications in [RFC8200] for extended headers. The content in Section 3 should be placed in a Hop-by-Hop option header in the extended header to carry information that will not be inserted or removed and that can be examined or processed by each node in the packet transmission path until the packet reaches the node identified in the destination address field of the IPv6 header(or in the case of multicast, each of a group of nodes).

The definition populates one or more sub-options of the TLV encoding format into the option field of the hop-by-hop option header, where the TLV encoding format is shown in Figure 2.

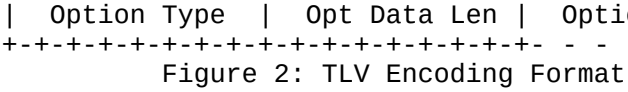

Figure 2: TLV Encoding Format

where

* Option Type: 8-bit identifier of the type of option.

* Opt Data Len: 8-bit unsigned integer. Length of the Option Data field of this option, in octets.

* Option Data: Variable-length field. Option-Type-specific data.

In the definition above, some specific instructions are required:

The Option Type identifiers are internally encoded such that their highest-order 2 bits specify the action that must be taken if the processing IPv6 node does not recognize the Option Type. Actions are selected by the controller in the network, refer to [RFC8200] for specific action definitions.

The third-highest-order bit of the Option Type specifies whether or not the Option Data of that option can change en route to the packet's final destination. The option data is changed during packet forwarding with traffice shaping information so that this bit needs to be set to 1.

The low-order 5 bits of the Option Type should not conflict with the Option Type field already defined by IPv6.

Option Data is used to carry the definition content of Section 3.

In addition, the length of the protocol defined in Section 3 exceeds the maximum length of an option, the F identifiers should be set to 1 and the protocol will continue to be stored in the next option. The protocol content in Section 3 is split into at most two options.

6.2. Hop-by-Hop processing definition

HBH Processing draft should define the HBH processing.

7. Security Considerations

Security issues with IPv6 Hop-by-Hop options are well known and have been documented in several places, including [RFC6398], [RFC6192], and [RFC9098]. Security Considerations in IPv6 are composed of a number of different pieces. These are mainly required to provide the three characteristics of replay protection, integrity and confidentiality.

7.1. Replay Protection

Replay Protection requires ensuring the uniqueness of each IP packet to ensure that the information cannot be reused in the event that it is intercepted and copied.

* It should be ensured that access cannot be regained using the same packets to prevent attackers from intercepting deciphered information and then impersonating illegal access.

* A secret key based on algorithm independent exchange should be set at the host side by the customer and the service provider, and when each packet is transmitted, a checksum is generated based on the secret key and the packet, and the checksum is recalculated and compared at the data receiving side.

* Authentication data should be included in the transmission to protect the fields that cannot be changed during IP packet transmission.

* The cache data should be cleared and guaranteed to be unrecoverable.

7.2. Integrity

Integrity of data is to prevent data from being tampered with during transmission and to ensure that the outgoing and incoming data are identical.

* Two-way authentication mechanism for shared data information components should be provided.

* Encrypted transmission channels should be used to prevent data from being eavesdropped during network transmission.

* Should have the ability to test the integrity of the data and provide the corresponding recovery control measures.

7.3. Confidentiality

Confidentiality is used to prevent attackers from accessing packet headers or content, ensuring that information cannot be read during transmission, even if IP packets are intercepted.

* Encryption policy of terminal data should be established to ensure the confidentiality of sensitive data output and shared at the terminal.

* A cryptographic checksum should be generated for each packet, and the receiver should calculate the checksum before opening the packet; if the packet is tampered with and the checksum does not match, the packet is discarded.

8. IANA Considerations

This document has no IANA actions.

9. References

9.1. Normative References

[HbH-UPDT] Hinden, R. M. and G. Fairhurst, "IPv6 Hop-by-Hop Options Processing Procedures", Work in Progress, Internet-Draft, draft-hinden-6man-hbh-processing-01, 2 June 2021, <https://datatracker.ietf.org/doc/html/draft-hinden-6man-hbh-processing-01>.

[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>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/rfc/rfc8200>.

9.2. Informative References

[RFC5409] Martin, L. and M. Schertler, "Using the Boneh-Franklin and Boneh-Boyen Identity-Based Encryption Algorithms with the Cryptographic Message Syntax (CMS)", RFC 5409, DOI 10.17487/RFC5409, January 2009, <https://www.rfc-editor.org/rfc/rfc5409>.

[RFC6192] Dugal, D., Pignataro, C., and R. Dunn, "Protecting the Router Control Plane", RFC 6192, DOI 10.17487/RFC6192, March 2011, <https://www.rfc-editor.org/rfc/rfc6192>.

[RFC6398] Le Faucheur, F., Ed., "IP Router Alert Considerations and Usage", BCP 168, RFC 6398, DOI 10.17487/RFC6398, October 2011, <https://www.rfc-editor.org/rfc/rfc6398>.

[RFC9098] Gont, F., Hilliard, N., Doering, G., Kumari, W., Huston, G., and W. Liu, "Operational Implications of IPv6 Packets with Extension Headers", RFC 9098, DOI 10.17487/RFC9098, September 2021, <https://www.rfc-editor.org/rfc/rfc9098>.

Acknowledgments

TODO acknowledge.

Authors' Addresses

Haisheng Yu
China Internet Network Information Center
Email: yuhaisheng1@gmail.com

Kaicheng Zhang
University of Electronic Science and Technology of China

Email: 457642057@qq.com