Network Working Group
Internet Draft
Intended status: Experimental
Expires: February 14, 2023

R.R. Chodorek
AGH Univ. of Science and Technology

August 14, 2022

# An IP option for describing the traffic flow
# draft-chodorek-traffic-flow-option-10

Abstract

Information about the behavior of the stream that will be transmitted in the near future will allow for better management of queues in the router and thus improve QoS and reduce the potential for a serious overload. Such information is often available in the transmitter. The proposed IP option allows for the sending of information about forthcoming traffic from the transmitter to the intermediate nodes.

Table of Contents



## 1. Introduction

Information about the behavior of the stream that will be transmitted in the near future will allow for better management of queues in the router and thus improve QoS and reduce the potential for a serious overload. Such information is often available in the transmitter. Information on the amount of data that in the near future will be sent by the application can be derived from measurements taken in the output buffer or as a result of prediction (e.g. the prediction of video traffic [Cho2002]). This information can be used for dynamic bandwidth allocation (e.g. the extension to RSVP protocol, based on dynamic resource reservations [Cho2010] or prediction-based bandwidth renegotiation module [Cho2003]).

The proposed IP Traffic Flow Description (TFD) Hop-by-Hop option allows for the sending of information about forthcoming traffic from the transmitter to the intermediate nodes. The proposed IP option can be used by applications which transmit streaming and elastic traffic. The proposed option will be used mainly for self-limited traffic. Self-limited traffic is generated e.g. by IoT devices that periodically send a limited

amount of data and streaming applications (streaming applications have a limited output bandwidth depending on the properties of transmitted media and used compression and coding).

The proposed option can be used to active queues (e.g. RED) or fair queuing (e.g. WFQ).

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].

## 2. Traffic Flow Description option

The Traffic Flow Description (TFD) header is used by an IP source to carry information describing traffic flow. This option must be examined by every node along a packet's delivery path.

The proposed IPv4 [RFC791] option has the following format:

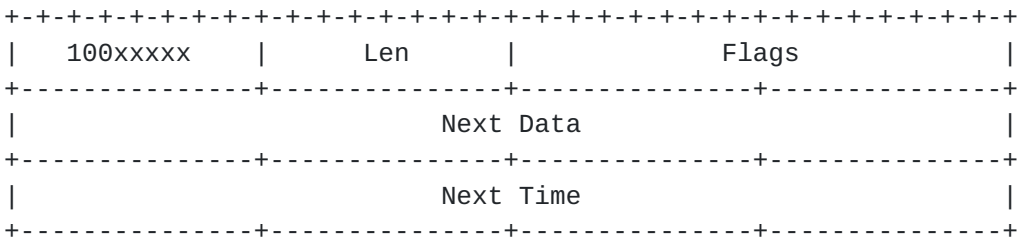



Figure 1 Proposed IP Option for IPv4.

The proposed IPv6 [RFC8200] Hop-by-Hop Options has the following format:

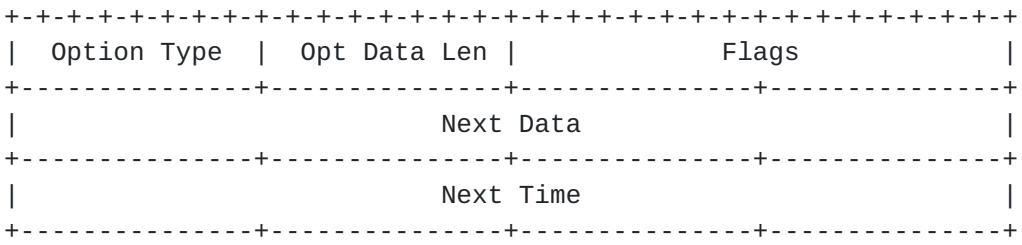



Figure 2 Proposed IP Option for IPv6.

For IPv4 the first byte (the option type) is as follows:

Type:

Copied flag: 1 (all fragments must carry the option)

Option class: 0 (control)

Option number: xxxxx to be allocated by IANA for this option

For IPv6 the Traffic Flow Description header is identified by a Option Type value of 000xxxxx, and is as follows:

Unrecognized option action: 00
(skip option, process the rest of the header)

Option Data does not change en-route: 0
(option data cannot change while the datagram is en route)

Option number: xxxxx to be allocated by IANA for this option

Option Type (8 bit):

Identifies the type of option.

For IPv4:

Len (8 bit):

Variable length of IP option in bytes (including the Type and Len bytes). This field MUST be set to 12.

For IPv6:

Opt Data Len (8 bit):

Length of IP option in bytes. This field MUST be set to 10.

Flags (16 bit):

Determines the format of next field and the properties (types) of the transmitted data, and has the following format:


Res (8 bit):

The Res (Reserved) field MUST be set to zero

N (1 bit):

When the flag N is set to one, this indicates that there is at least one router on the path that is net neutral and not apply traffic differentiation.

D (1 bit):

Size in field Next Data represents:
0 Positive integer value
1 Floating-point value

M (1 bit):

When the flag M is set to one, this indicates that the value of the Next Data field is set in the transmitter to a maximum value for the transmission.

B (1 bit):

When the flag B is set to one, this indicates that the value of the Next Data field is set in the transmitter on the basis of buffer analysis.

F (1 bit):

When the flag F is set to one, this indicates that the value of the Next Data field is set in the transmitter on the basis of prediction (forecasting).

L (1 bit):

When the flag L is set to one, a large amount of data will be transmitted.

S (1 bit): stream traffic indication

0 No stream
1 Stream

E (1 bit): elastic traffic indication

0 No elastic
1 Elastic

Note:

If S == 1, E MUST be set to 0 and if E == 1, S MUST be set to 0.

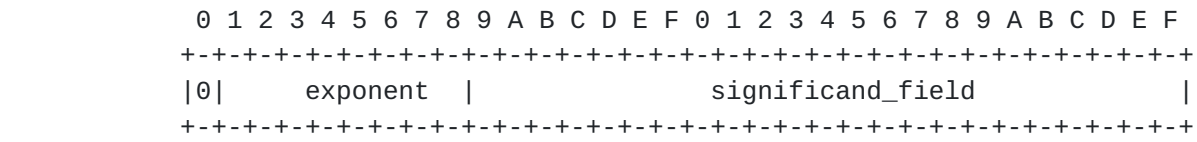
Next Data (32 bit):

size (in bytes) of data sent in the near future.

If Flag D is not set (D == 0), Next Data represents an unsigned integer value:

Next Data = Next Data

If Flag D is set (D == 1), Next Data represents a floating-point value as follows (representation is used in accordance with IEEE 754 single precision [IEEE754]):




Note(1): infinity stream is defined:

as FFFFFFFF hex value if D == 0
as exponent = FF and significand_field = 0 if D == 1

Note(2): sign bit is always zero (positive number).

Next Time (32 bit):

Time (in milliseconds) the counting of data that were included in the field Next Data.

## 3. Procedures

The source node sends a packet with the IP option of the Traffic Flow Description. The type of traffic, which can be elastic or streaming, and its basic parameters are defined by the application that is capable of using the optional Traffic Flow Description. Information on the amounts of data that in the near future will sent by the application can be derived from measurements taken of the output buffer or as a result of prediction.

Intermediate nodes will receive information transmitted by the Traffic Flow Description for each active flow and on the basis of the obtained information modify their decisions regarding traffic management.

If router is net neutral (router not apply traffic differentiation), router must set flag N.

The proposed option can be used by active queues (e.g. RED) or fair queuing (e.g. WFQ) [Cho2015]. The proposed option can use constant time horizon [Cho2015] or a variable time horizon (based on scene detection and analysis of the frames of the sending movie) [Cho2016].

### 3.1. The streaming application

The streaming application, located at the source node, sets the IP packet option of the Traffic Flow Description. Flag S (which indicates streaming) is set to 1. When the stream was characterized by analyzing the application output buffer, flag B is set to 1. The field Next Time is set according to the buffer delay (e.g. 500 ms). The value of the field Next Data is set as a sum of all data currently stored in output buffer.

### 3.2. The elastic application

The elastic application, located at the source node, sets the IP packet option of the Traffic Flow Description. The flag E (which indicates an elastic application) is set to 1. When an elastic application uses the TCP protocol it's a problem to estimate Next Data. We can only calculate maximum throughput according to RTT, congestion and the receiver window. It will be setting the

maximum throughput in the Traffic Flow Description by setting flag M to 1 and Next Data and Next Time according to a calculation (Next Data to calculate throughput and Next Time to RTT). If it is not possible to calculate throughput we set Next Data to infinite value and field Next Time to RTT.

When an elastic application uses a transport protocol (e.g. PGM), which implements rate limiting mechanisms, we set maximum throughput according to protocol settings. The flag E (which indicates an elastic application) is set to 1, flag M is set to 1 and Next Data and Next Time is set according to protocol settings. If it is possible to estimate the throughput of the transport protocol in a given period we use this information and set flag F (instead of M) to 1 and field Next Data and Next Time according to predicted values.

## 4. Security Considerations

Security considerations to be provided.

## 5. IANA Considerations

An option type must be assigned by IANA for the Traffic Flow Description (TFD) option.

## 6. References

### 6.1. Normative References

[RFC791] Postel, J., "Internet Protocol Specification", RFC791, September 1981.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC8200] Deering, S., Hinden, R., "Internet Protocol, Version 6 (IPv6) Specification", RFC8200, July 2017.

[IEEE754] Institute of Electrical and Electronics Engineers, "Standard for Floating-Point Arithmetic", IEEE Standard 754, August 2008.

### 6.2. Informative References

[Cho2016] Chodorek, R., and Chodorek, A., "TFD-capable dynamic QoS assurance using a variable time horizon based on scene changes", Proc. of 2016 International Conference on Signals and Electronic (ICSES'16), 2016, pp. 275-280.

[Cho2015] Chodorek, R., and Chodorek, A., "Providing QoS for high definition video transmission using IP Traffic Flow Description option", Proc. of 8th international conference on Human System Interaction (HIS 2015), 2015, pp. 102-107.

[Cho2010] Chodorek, R., and Chodorek, A., "An Analysis of QoS Provisioning for High Definition Video Distribution in Heterogeneous Network", Proc. of 14th International Symposium on Consumer Electronics (ISCE 2010), 2010, pp. 326-331.

[Cho2003] Chodorek, A., "Prediction-based dynamic QoS assurance for multicast multimedia delivery", High-Speed Networks and Multimedia Communications: 6th IEEE International Conference HSNMC 2003, Estoril, Portugal, July 23-25, 2003, Proceedings. Vol. 6. Springer, 2003, pp. 128-135.

[Cho2002] Chodorek, A., "A fast and efficient model of an MPEG-4 video traffic based on phase space linearised decomposition", Proc. of 14th European Simulation Symposium ESS'2002, 2002, pp. 44-55.

Authors' Addresses

Robert R. Chodorek
AGH Univ. of Science and Technology
Al. Mickiewicza 30
30-059 Krakow
Poland

Email: chodorek@agh.edu.pl